JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 865 du 29 septembre 2017

Règlement grand-ducal du 21 septembre 2017 modifiant le règlement grand-ducal modifié du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l'archivage électronique.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Vu la loi du 25 juillet 2015 relative à l'archivage électronique et notamment son article 4, paragraphe 1er ;

Vu les avis de la Chambre de commerce et de la Chambre des métiers ;

Vu l'article 1er, paragraphe 1er, de la loi du 16 juin 2017 sur l'organisation du Conseil d'État et considérant qu'il y a urgence ;

Sur le rapport de Notre Ministre de l'Économie et après délibération du Gouvernement en conseil ;

Arrêtons :

Art. 1er.

L'article 1er du règlement grand-ducal modifié du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l'archivage électronique prend la teneur suivante :

« Art. 1er.

La certification des prestataires de services de dématérialisation ou de conservation prévue à l'article 4, paragraphe 1er de la loi du 25 juillet 2015 relative à l'archivage électronique intervient, aux choix de ces derniers, jusqu'au 19 juin 2018, soit selon les conditions et modalités de l'annexe I, soit selon les conditions et modalités de l'annexe II.

À partir du 20 juin 2018, la certification des prestataires de services de dématérialisation ou de conservation prévue à l'article 4, paragraphe 1er de la loi du 25 juillet 2015 relative à l'archivage électronique intervient obligatoirement selon les conditions et modalités de l'annexe II. »

Art. 2.

Notre Ministre de l'Économie est chargé de l'exécution du présent règlement qui sera publié au Journal officiel du Grand-Duché de Luxembourg.

Le Ministre de l'Économie,
Étienne Schneider

Palais de Luxembourg, le 21 septembre 2017.
Henri

ANNEXE I

Règle technique d'exigences et de mesures pour la certification des Prestataires de Services de Dématérialisation ou de Conservation (PSDC)

Historique du document		
Version #	**Date de publication**	**Détails des changements effectués**
Règle technique PSDC 1.0	05.06.2012	Le référentiel PSDC est validé comme règle technique PSDC. Version initiale de la règle technique.
1.1	12.06.2012	Correction de fautes.
1.2	19.12.2012	Adaptation au nouveau cadre légal national de la règle technique d'exigences et de mesures pour la certification des PSDC.
1.3	04.02.2013	Changement d'adresse.
2.0	16.06.2014	Mise à jour, suite à la mise à jour des normes internationales ISO/IEC 27001:2013 et ISO/IEC 27002:2013.
2.1	11.12.2014	Mise à jour suite à l'avis du Conseil d'État
2.2	04.09.2017	Corrections mineures

0 Table des matières

1 Introduction

La loi relative à l'archivage électronique du 25 juillet 2015 dispose qu'une personne peut, si elle détient une certification selon les exigences et les mesures définies dans la règle technique d'exigences et de mesures pour la certification des Prestataires de Services de Dématérialisation ou de Conservation (PSDC), en regard de l'exécution de ses processus de dématérialisation ou de conservation, procéder à une notification auprès de l'Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et Qualité des Produits et Services (ci-après « ILNAS »), en vue d'obtenir le statut de « PSDC ».

Si les critères de vérification établis par la loi relative à l'archivage électronique et par le système qualité ad hoc de l'ILNAS (Département de la confiance numérique) sont validés, l'ILNAS procèdera à l'inscription de la personne concernée dans la liste des PSDC (précisant les processus relatifs à la certification) établissant ainsi le statut de « PSDC ». Tout événement ou incident significatif détecté et tout changement majeur relatif à la portée de la certification, doit obligatoirement être notifié à l'ILNAS. Tout retrait, suspension ou non renouvellement de la certification entraîne de facto le retrait du statut de « PSDC ».

Ce statut de « PSDC » demeure volontaire, sauf disposition réglementaire ou sectorielle l'imposant.

NOTE 1 : Par le terme « dématérialisation », il faut comprendre la numérisation des documents analogiques (non numériques) et le contrôle des résultats de la numérisation aussi longtemps que nécessaire. Un processus de dématérialisation doit donc être compris comme un processus composé de processus sous-jacents consistant à numériser des documents analogiques et à contrôler les résultats de la numérisation aussi longtemps que nécessaire.

NOTE 2 : Par le terme « conservation », il faut comprendre la création et la préservation d'archives numériques dans le temps. Un processus de conservation doit donc être compris comme un processus composé de processus sous-jacents consistant à créer et à préserver des archives numériques dans le temps.

La certification effective selon la règle technique d'exigences et de mesures pour la certification des PSDC de toute personne permet la demande du statut de Prestataire de Services de Dématérialisation ou de Conservation (ci-après « PSDC ») délivré par le Département de la confiance numérique de l'ILNAS et qui se décline de la manière suivante :

- PSDC-DC : prestataire de services de dématérialisation et de conservation.
- PSDC-D : prestataire de services de dématérialisation.
- PSDC-C : prestataire de services de conservation.

L'ILNAS reconnaît formellement, via ce statut, la personne concernée en tant que « PSDC ».

La personne certifiée doit être en mesure de garantir les résultats de l'exécution des processus de dématérialisation ou de conservation pour lesquels elle a obtenu la certification. Cela signifie que les documents numériques résultants de la numérisation des documents analogiques et les archives numériques seront reconnus comme conformes à la règle technique d'exigences et de mesures pour la certification des Prestataires de Services de Dématérialisation ou de Conservation (PSDC).

Ainsi une copie sera présumée être conforme à l'original lorsqu'elle sera certifiée comme telle par un Prestataire de Services de Dématérialisation ou de Conservation.

La règle technique d'exigences et de mesures des PSDC est applicable à toute organisation publique ou privée, indépendamment de son type, de sa taille, de ses processus ou de ses activités, pour ses besoins internes ou dans le cadre de services proposés à ses clients.

La présente règle technique a été définie à partir de normes internationales publiées et maintenues par l'Organisation Internationale de Normalisation (ci-après « ISO »).

La présente règle technique doit donc être considérée comme un supplément à ces normes en amendant et complétant leur contenu spécifiquement aux processus de dématérialisation et de conservation.

2 Domaine d'application

La présente règle technique définit des exigences et des mesures permettant à une organisation d'établir une gestion de la sécurité de l'information et une gestion opérationnelle spécifiques aux processus de dématérialisation et de conservation.

Du point de vue de la gestion de la sécurité de l'information, la présente règle technique se base sur les Normes internationales ISO/IEC 27001:2013 et ISO/IEC 27002:2013 de manière à ce qu'une organisation puisse être en mesure de définir, d'implémenter, de maintenir et d'améliorer:

a) un Système de Management de la Sécurité de l'Information (ci-après « SMSI ») basé sur la Norme internationale ISO/IEC 27001:2013 et intégrant les processus de dématérialisation ou de conservation.

b) des objectifs et des mesures de la sécurité de l'information basés sur la Norme internationale ISO/IEC 27002:2013 et spécifiques aux processus de dématérialisation ou de conservation.

Du point de vue de la gestion opérationnelle, la présente règle technique intègre les grands principes de la Norme internationale ISO 30301:2011 [1].

La présente règle technique est utilisée pour les audits d'évaluation de conformité d'une organisation exécutant des processus de dématérialisation ou de conservation.

Ces audits doivent être effectués par des organismes d'évaluation de conformité indépendants, tandis que l'ILNAS est la seule autorité nationale luxembourgeoise habilitée à conférer à une organisation un statut de « PSDC-DC », « PSDC-D » ou « PSDC-C ».

NOTE :
Comme indiqué précédemment, les grands principes de la Norme internationale ISO 30301:2011 ont été intégrés dans la présente règle technique. Il est à noter que cette norme adresse essentiellement la problématique de la conservation et non de la dématérialisation.

Afin d'assurer une consistance générale dans la définition des exigences et des mesures de la présente règle technique, ces grands principes ont été également adaptés autant que possible à la problématique de la dématérialisation afin d'adresser ce domaine selon l'approche adoptée pour la conservation.

La Norme internationale ISO 30301:2011 n'est pas indispensable à l'organisation dans l'application de la présente règle technique.

3 Références normatives

Les documents de référence suivants sont indispensables pour l'application de la présente règle technique.

Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 27001:2013, *Technologies de l'information -- Techniques de sécurité -- Systèmes de gestion de la sécurité de l'information -- Exigences*

ISO/IEC 27002:2013, *Technologies de l'information -- Techniques de sécurité -- Code de bonne pratique pour la gestion de la sécurité de l'information*

4 Termes, définitions, abréviations et structure de la règle technique

4.1 Termes et définitions

Pour les besoins de la présente règle technique, les termes et définitions suivants s'appliquent :

4.1.1

actif
tout élément représentant de la valeur pour l'organisation.

NOTE 1 : Il existe plusieurs sortes d'actifs, dont :
a) l'information (4.1.8).
b) les documents (4.1.6).
c) les archives (4.1.3).
d) les actifs techniques, par exemple un scanner, un serveur ou des disques durs.
e) les actifs techniques immatériels, par exemple des unités de stockage virtuelles.
f) le personnel d'une organisation.
g) les actifs incorporels, par exemple la réputation et l'image.

NOTE 2 : Définition adaptée de l'ISO/IEC 30300:2011, définition 3.1.2.

4.1.2
analogique
non numérique.

NOTE : Un support de stockage analogique est un support de stockage non numérique, comme par exemple le papier, le film argentique ou le disque vinyle.

4.1.3
archivage électronique
conservation d'archives numériques sur support électronique en vue de leur utilisation pérenne.

4.1.4
archive
document conservé en l'état en vue d'une utilisation pérenne.

NOTE : Définition adaptée de l'ISO/IEC 30300:2011, définition 3.1.1.

4.1.5
certification pouvant ouvrir au statut de « PSDC »
procédure par laquelle un organisme de certification (accrédité par l'organisme national d'accréditation ou tout autre organisme d'accréditation reconnu en tant que tel par l'OLAS) évalue la conformité d'une personne comme étant conforme pour exercer une activité de dématérialisation ou de conservation, aux exigences de la règle technique d'exigences et de mesures pour la certification des Prestataires de Services de Dématérialisation ou de Conservation.

4.1.6
conservation
la création et la préservation d'archives numériques dans le temps.

NOTE 1 : Un processus de conservation est composé de processus sous-jacents consistant à créer et à préserver des archives numériques dans le temps.

NOTE 2 : Définition adaptée de l'ISO 15489-1:2001, définition 3.14.

4.1.7
dématérialisation
la numérisation des documents analogiques et le contrôle des résultats de la numérisation aussi longtemps que nécessaire.

NOTE : Un processus de dématérialisation est composé de processus sous-jacents consistant à numériser des documents analogiques et à contrôler les résultats de la numérisation aussi longtemps que nécessaire.

4.1.8
document
information ou objet documentaire enregistré qui peut être traité comme une unité.

[ISO 15489-1:2001]

4.1.9
établissement
définition, mise en œuvre ou en exploitation, maintenance et amélioration.

NOTE : L'établissement d'un processus de dématérialisation correspond à sa définition, mise en œuvre, maintenance et amélioration.

4.1.10
indexation
définition de points d'accès pour faciliter la recherche des documents.

NOTE 1 : La génération de métadonnées liées aux documents numériques et aux archives numériques est généralement utilisée pour faciliter leur recherche.

NOTE 2 : Définition adaptée de l'ISO 15489-1:2001, définition 3.11.

4.1.11
information
savoir ou données représentant de la valeur pour l'organisation.

NOTE : Définition adaptée de l'ISO/IEC 27000:2009, définition 2.18.

4.1.12
intégrité
propriété de protection de l'exactitude et de la complétude des actifs.

[ISO 27000:2009]

4.1.13
métadonnées
données décrivant le contexte, le contenu et la structure des documents ainsi que leur gestion dans le temps.

NOTE : Définition adaptée de l'ISO/IEC 30300:2011, définition 3.1.6.

4.1.14
prestataire de services de dématérialisation ou de conservation (PSDC)
statut attribué par l'ILNAS à une organisation exerçant à titre principal ou secondaire, pour ses propres besoins ou dans le cadre de services proposés à ses clients, des processus de dématérialisation ou de conservation formellement reconnus par l'ILNAS comme conformes aux exigences et aux mesures définies dans la présente règle technique.

NOTE :

a) Une organisation ayant obtenu le statut de « PSDC-DC » par l'ILNAS signifie qu'elle exécute des processus de dématérialisation et de conservation conformes aux exigences et aux mesures définies dans la présente règle technique.
b) Une organisation ayant obtenu le statut de « PSDC-D » par l'ILNAS signifie qu'elle exécute uniquement un processus de dématérialisation conforme aux exigences et aux mesures définies dans la présente règle technique.
c) Une organisation ayant obtenu le statut de « PSDC-C » par l'ILNAS signifie qu'elle exécute uniquement un processus de conservation conforme aux exigences et aux mesures définies dans la présente règle technique.

4.1.15
preuve
document démontrant l'effectivité d'une opération.

NOTE 1 : La preuve d'une opération signifie qu'il peut être démontré qu'elle a été créée dans le cadre normal de la conduite de l'activité de l'organisation et qu'elle est intacte et complète. Ne se limite pas au sens légal du terme.

NOTE 2 : Définition adaptée de l'ISO/IEC 30300:2011, définition 3.1.5.

4.1.16
processus
ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie.

[ISO 9000:2005]
4.1.17
système
ensemble d'actifs techniques corrélés ou interactifs.

NOTE 1 :

a) Un système spécifique aux processus de dématérialisation ou de conservation sera dénommé système de dématérialisation ou de conservation (ci-après « SDC »).
b) Un système spécifique aux processus de dématérialisation et de conservation sera dénommé système de dématérialisation et de conservation (ci-après « SDC-DC »).
c) Un système spécifique au processus de dématérialisation sera dénommé système de dématérialisation (ci-après « SDC-D »).
d) Un système spécifique au processus de conservation sera dénommé système de conservation (ci-après « SDC-C »).

NOTE 2 : Définition adaptée de l'ISO 9000:2005

4.1.18
traçabilité
fait de créer, d'enregistrer et de préserver les données relatives aux mouvements et à l'utilisation des documents analogiques et numériques et des archives numériques.

NOTE : Définition adaptée de l'ISO 15489-1:2001, définition 3.19.

4.2 Abréviations

Dans la présente règle technique, les abréviations suivantes s'appliquent :

DdA	Déclaration d'Applicabilité (*terme anglais :* Statement of Applicability (SoA)), Déclaration relative à l'applicabilité des objectifs et mesures de sécurité)
DPI	Dots Per Inch (*terme anglais*)
L2TP	Layer 2 Tunneling Protocol (*terme anglais*)
IPSec	Internet Protocol Security (*terme anglais*)
OID	Object Identifier (*terme anglais*)
PPP	Point to Point Protocol (*terme anglais*)
PSDC	Prestataire de Services de Dématérialisation ou de Conservation
PSDC-DC	Prestataire de Services de Dématérialisation et de Conservation
PSDC-C	Prestataire de Services de Conservation
PSDC-D	Prestataire de Services de Dématérialisation
RT	Règle technique d'exigences et de mesures pour la certification des PSDC
SDC	Système de Dématérialisation ou de Conservation
SDC-DC	Système de Dématérialisation et de Conservation
SDC-C	Système de Conservation
SDC-D	Système de Dématérialisation
SFTP	SSH File Transfer Protocol (*terme anglais*)
SMSI	Système de Management de la Sécurité de l'Information
SSH	Secure SHell (*terme anglais*)
STD	Norme internationale ISO/IEC 27002:2013
TLS	Transport Layer Security (*terme anglais*)
UTC	Temps Universel Coordonné

4.3 Structure de la règle technique

La clause 5 décrit les processus de la dématérialisation et de conservation, ainsi que les principes de sécurité de l'information à appliquer dans le cadre de l'établissement de ces processus.

La clause 6 définit les exigences relatives à l'établissement d'un Système de Management de la Sécurité de l'Information (SMSI) basé sur la Norme internationale ISO/IEC 27001:2013 et spécifiques aux processus de dématérialisation ou de conservation.

La clause 7 définit les objectifs et les mesures requises pour la gestion de la sécurité de l'information et de gestion opérationnelle spécifiques aux processus de dématérialisation ou de conservation.

L'Annexe A indique les clauses de la Norme internationale ISO/IEC 27001:2013 pour lesquelles des exigences complémentaires ont été définies dans la présente règle technique.

L'Annexe B énumère des exemples de risques liés à l'établissement des processus de dématérialisation ou de conservation.

L'Annexe C décrit un tableau montrant les liens entre la Norme internationale ISO/IEC 27002 :2013 et la présente règle technique. Ce tableau énumère également les clauses, les objectifs de sécurité et les mesures de sécurité à considérer par l'organisation dans le cadre de l'appréciation des risques liés à l'établissement des processus de dématérialisation ou de conservation.

L'Annexe D décrit des exemples de niveaux de service liés à l'exécution des processus de dématérialisation ou de conservation.

5 Concepts généraux

5.1 Introduction

La règle technique d'exigences et de mesures des PSDC est applicable à une organisation ou un groupement d'organisations :

a) indépendamment du secteur d'activités de l'organisation.

b) indépendamment de la taille et de la complexité de l'organisation.

c) pour les besoins internes de l'organisation ou dans le cadre de services proposés à des clients.

La présente règle technique s'adresse à toute organisation qui :

a) collecte, numérise, stocke, exploite, restitue, transfert, détruit ou supprime des documents analogiques et numériques ainsi que des archives numériques.

NOTE : La destruction s'applique aux documents analogiques et implique l'utilisation de moyens physiques comme une déchiqueteuse. La suppression s'applique aux documents et archives numériques et implique l'utilisation de moyens applicatifs.

b) reconnaît l'importance de la gestion de ces documents et de ces archives, de l'information contenue dans ces documents et ces archives et de leur nature.

c) est consciente des risques qui impactent ces documents et ces archives, sur les activités et les actifs de l'organisation liés à ces documents et ces archives.

d) souhaite introduire une gestion du risque permettant d'identifier et d'évaluer les risques pouvant avoir un impact sur l'organisation, les documents analogiques et numériques ainsi que les archives numériques gérés par l'organisation.

e) souhaite mettre en œuvre des mesures de sécurité et des mesures opérationnelles adéquates pour protéger les documents analogiques et numériques ainsi que les archives numériques gérés par l'organisation, et réduire ainsi le niveau général du risque à un niveau acceptable.

La présente règle technique doit être utilisée par toute organisation qui souhaite :

a) définir, implémenter, maintenir et améliorer un SMSI, des mesures de sécurité et des mesures opérationnelles afin de gérer correctement les risques liés aux processus de dématérialisation ou de conservation.

b) s'assurer de la conformité de sa gestion de la sécurité de l'information et de sa gestion opérationnelle liées aux processus de dématérialisation ou de conservation.

c) démontrer la conformité de sa gestion de la sécurité de l'information et de sa gestion opérationnelle liées aux processus de dématérialisation ou de conservation en demandant auprès de l'ILNAS l'obtention du statut de « PSDC-DC », « PSDC-D » ou « PSDC-C ».

5.2 Approche processus

La gestion de la dématérialisation et de la conservation doit être organisée selon une approche « processus », permettant ainsi :

a) de définir pour chacun de ces domaines un ensemble de processus.

b) d'y associer un ensemble d'activités corrélées et interactives.

c) de pouvoir améliorer l'ensemble de manière continue tant sur le plan de la sécurité de l'information que du point de vue opérationnel.

5.3 Concepts clés

Les processus de dématérialisation et de conservation peuvent être définis respectivement de la manière suivante :

5.3.1 Processus de dématérialisation

Le processus de dématérialisation est composé de processus sous-jacents tels que présentés dans le diagramme suivant :

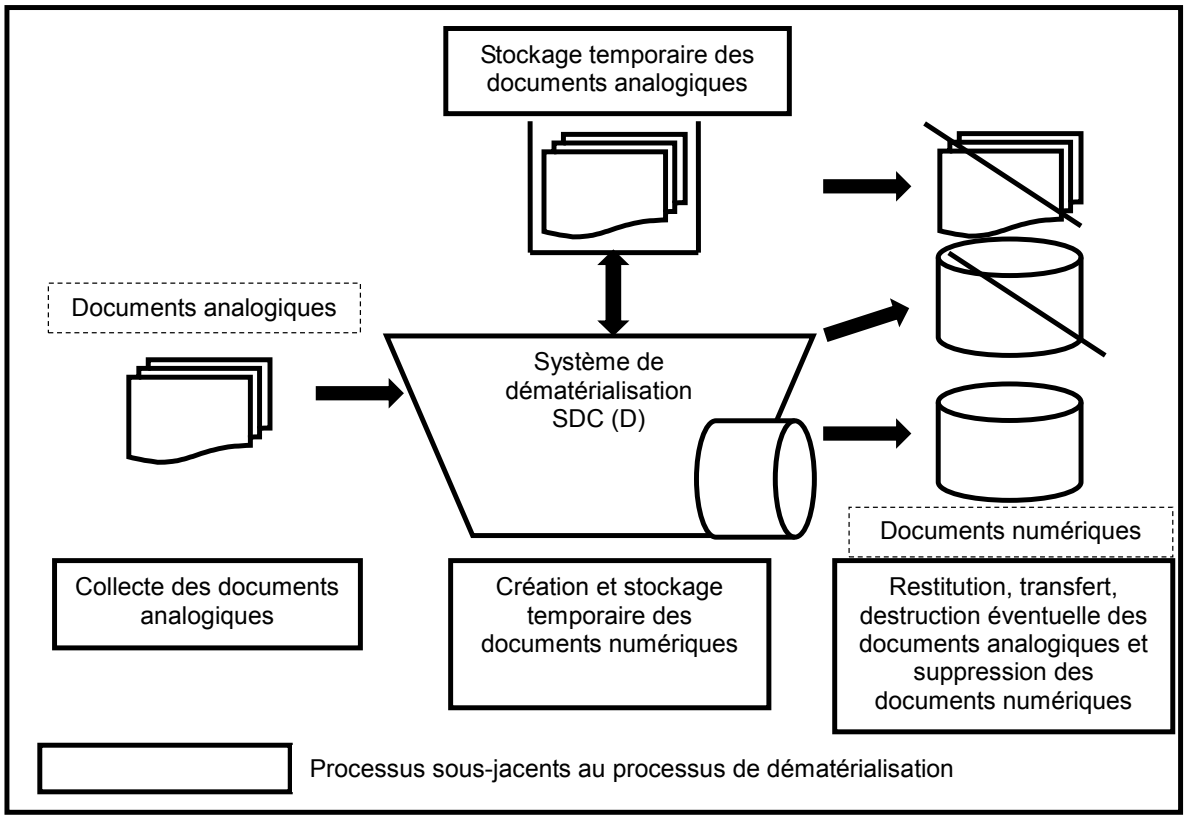

Figure 1 : Processus de dématérialisation et processus sous-jacents

Processus sous-jacents au processus de dématérialisation

a) collecte des documents analogiques.

   Ce processus correspond à la récupération des documents analogiques par l'organisation, ou à la soumission de ces derniers, par le client (interne ou externe à l'organisation) et à leur stockage dans un site sous la responsabilité de l'organisation.

b) création et stockage temporaire des documents numériques.

   Ce processus correspond :

   1. à la préparation des documents analogiques en vue de leur numérisation.

   2. à la conversion de ces documents au format numérique (*opération de numérisation*) et à l'association de métadonnées aux documents numériques.

   3. au stockage temporaire des documents numériques.

   NOTE : Le mot temporaire doit être compris comme une période inférieure à la durée légale de rétention des documents.

c) stockage temporaire des documents analogiques.

   Ce processus correspond au stockage des documents analogiques dans un site géré par l'organisation en attente (dans un premier temps) de leur numérisation et (dans un second temps) en attente de leur restitution au client (interne ou externe à l'organisation) ou de leur destruction éventuelle.

   NOTE : Le mot temporaire doit être compris comme une période inférieure à la durée légale de rétention des documents.

d) restitution, transfert, destruction éventuelle des documents analogiques et suppression des documents numériques.

   Ce processus correspond :

   1. à la restitution des documents analogiques et numériques par l'organisation auprès du bénéficiaire ou à leur récupération par ce dernier.

   2. au transfert des documents analogiques et numériques par l'organisation auprès d'un tiers.

   3. à la destruction éventuelle des documents analogiques par l'organisation.

   4. à la suppression des documents numériques par l'organisation.

Système de dématérialisation SDC-D

Système composé d'un ensemble d'actifs techniques permettant la création des documents numériques à partir des documents analogiques, le stockage temporaire des documents analogiques et numériques, leur restitution, leur transfert, la destruction éventuelle des documents analogiques et la suppression des documents numériques.

5.3.2 Processus de conservation

Le processus de conservation est composé de processus sous-jacents tels que présentés dans le diagramme suivant :

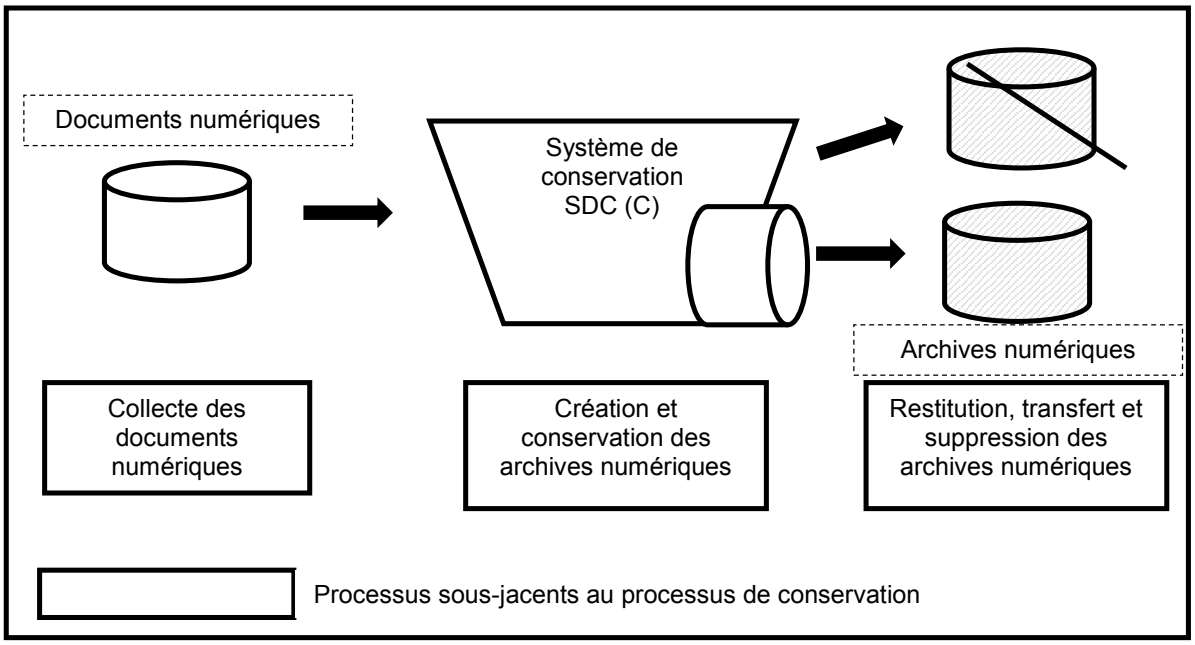

Figure 2 : Processus de conservation et processus sous-jacents

Processus sous-jacents au processus de conservation

a) collecte des documents numériques.

   Ce processus correspond à la récupération des documents numériques par l'organisation ou à leur soumission par le client (interne ou externe à l'organisation) et à leur versement dans le SDC-C pour traitement.

b) création et conservation des archives numériques.

   Ce processus correspond :

   1. à la préparation des documents numériques en vue de leur archivage.

   2. à la conversion de ces documents en archives numériques et à l'association de métadonnées aux archives numériques ainsi créées.

      NOTE 1 : la principale différence entre un document numérique et une archive numérique est que cette dernière contient des informations figées, c'est-à-dire un contenu qui n'est plus modifié à partir du moment où cette archive est créée. Il convient également de créer une archive numérique de telle manière à pouvoir y associer un ensemble de métadonnées destinées en particulier à suivre son évolution dans le temps.

      NOTE 2 : Les Normes internationales ISO 14721:2012 [2], ISO/IEC 15489-1:2001 [3] ISO 23081-1 :2006 et ISO23081-2 :2009 [4] décrivent des lignes directrices en matière de gestion des métadonnées associées à des documents numériques ou des archives numériques.

   3. à la conversion (si nécessaire et à la demande du client) des archives numériques dans un format différent de leur format initial.

4. à la suppression des documents numériques dont le versement dans le SDC-C a été confirmé.

5. à la conservation des archives numériques aussi longtemps que nécessaire.

c) restitution, transfert et suppression des archives numériques.

Ce processus correspond :

1. à la restitution partielle ou totale des archives numériques par l'organisation auprès du client ou à leur récupération partielle ou totale par ce dernier.

   NOTE : Le mot partiel doit être compris comme des informations liées à l'archive numérique et non l'archive numérique en tant que telle.
   La restitution partielle d'une archive numérique peut par exemple correspondre à la transmission par le SDC-C d'informations liées à l'existence de cette archive en réponse à une requête soumise par un client souhaitant disposer d'une confirmation de son archivage effectif.

2. au transfert des archives numériques par l'organisation auprès d'un tiers.

3. à la suppression des archives numériques par l'organisation.

Système de conservation SDC-C

Système composé d'un ensemble d'actifs techniques permettant le stockage temporaire des documents numériques en vue de leur archivage, leur conversion en archives numériques, leur suppression et la conservation des archives numériques aussi longtemps que nécessaire, leur exploitation, leur restitution partielle ou totale, leur transfert et leur suppression.

5.3.3 Principes de sécurité de l'information

L'établissement des processus de dématérialisation ou de conservation au sein d'une organisation nécessite la conformité aux principes suivants de la sécurité de l'information afin de garantir une confidentialité, une intégrité et une disponibilité des documents analogiques et numériques et des archives numériques aussi longtemps que nécessaire :

Authenticité

L'organisation doit pouvoir démontrer que toutes les activités effectuées dans le cadre de l'établissement des processus de dématérialisation ou de conservation sont authentiques, à savoir que l'organisation peut prouver que :

a) le document analogique ou numérique a bien été transmis par la personne qui est supposée l'avoir transmis.

b) le document numérique résultant de la numérisation d'un document analogique ou l'archive numérique a bien été créé par la personne ou le système au moment présumé.

c) le document numérique ou l'archive numérique est bien ce qu'il est supposé être.

Fiabilité

L'organisation doit pouvoir démontrer que :

a) toutes les activités effectuées dans le cadre de l'établissement des processus de dématérialisation ou de conservation sont fiables, c'est-à-dire exécutées conformément aux politiques et aux procédures définies et mises en œuvre par l'organisation en la matière.
b) le document numérique ou l'archive numérique créé et exploité est conforme et non modifié de son état original ou par des modifications non autorisées.

Exploitation

L'exploitation des processus de dématérialisation ou de conservation doit pouvoir permettre de créer un document numérique ou une archive numérique qui soit à tout moment localisable, lisible, intelligible, utilisable avec les informations nécessaires à la compréhension de son origine et disponible aussi longtemps que nécessaire.

L'organisation doit par conséquent définir et mettre en œuvre des politiques et des procédures pour contrôler la collecte, la création, le stockage, la conservation, l'exploitation, la restitution partielle ou totale, le transfert, la destruction éventuelle de documents analogiques et la suppression de documents numériques ou d'archives numériques de manière à s'assurer de leur origine, de leur protection contre les accès, modifications, altérations, destructions et suppressions non autorisées, de leur utilisation et de leur disponibilité aussi longtemps que nécessaire.

6 Système de Management de la Sécurité de l'Information (SMSI)

Pour pouvoir prétendre à l'obtention par l'ILNAS du statut de « PSDC-DC », « PSDC-D » ou « PSDC-C », l'organisation doit se conformer à l'ensemble des exigences de la présente clause 6, relative à l'établissement, l'implémentation, la maintenance et l'amélioration continue d'un SMSI basé sur la Norme internationale ISO/IEC 27001:2013 et spécifiques aux processus de dématérialisation ou de conservation.

6.1 Exigences générales

L'organisation doit établir, définir, implémenter, maintenir et améliorer un SMSI afin de gérer les risques liés aux processus de dématérialisation ou de conservation.

L'établissement de ce SMSI doit respecter l'ensemble des exigences de la sécurité de l'information spécifiées dans :

a) la Norme internationale ISO/IEC 27001:2013, en particulier aux clauses suivantes du standard :
    4. Contexte de l'organisation.
    5. Responsabilité de la Direction.
    6. Planification.
    7. Support
    8. Mise en œuvre
    9. Évaluation des performances
    10. Amélioration.

b) la présente clause 6, complétant les exigences définies dans la Norme internationale ISO/IEC 27001:2013.

NOTE : L'Annexe A de la présente règle technique indique les clauses de la Norme internationale ISO/IEC 27001:2013 pour lesquelles des exigences complémentaires ont été définies dans la présente règle technique.

L'organisation est libre d'intégrer les processus de dématérialisation ou de conservation dans un SMSI existant ou de définir, d'implémenter, de maintenir et d'améliorer un SMSI spécifique à ces processus.

La clause 7 de la présente règle technique fournit des objectifs et des mesures de gestion de la sécurité de l'information et de gestion opérationnelle qui doivent être appliqués dans le traitement de risques liés aux processus de dématérialisation ou de conservation, en supplément des objectifs de sécurité et des mesures associées définis dans la Norme internationale ISO/IEC 27002:2013.

6.2 Contexte de l'organisation

En complément des exigences définies à la clause 4 *« Contexte de l'organisation »* de la Norme internationale ISO/IEC 27001:2013, l'organisation doit s'assurer :

a) de prendre en considération des facteurs internes et externes liés au processus de dématérialisation et de conservation dans la compréhension de l'organisation et de son contexte ;

b) de la bonne compréhension des exigences, des besoins et des attentes des intervenants dans le processus de dématérialisation et de conservation ;

c) que la définition du domaine d'application du SMSI, de ses limites et de la politique de sécurité intègre les processus de dématérialisation et de conservation, ainsi que les actifs supportant ces processus.

6.3 Leadership

En complément des exigences définies à la clause 5.1 *Implication de la direction* de la Norme internationale ISO/IEC 27001:2013, la direction de l'organisation doit fournir :

a) la preuve de l'existence légale de l'organisation et de la stabilité de sa situation financière.

NOTE : Une organisation de droit privé pourra par exemple fournir les informations suivantes :

1. extrait du registre de commerce et des sociétés de Luxembourg.
2. stratégie financière.
3. bilans et comptes de résultat des 3 dernières années fiscales.
4. rapport ou avis financier émis par une autorité de surveillance luxembourgeoise.
5. niveau d'exposition des activités métiers aux facteurs externes à l'organisation, comme par exemple le cours du pétrole ou celui de l'acier.
6. rapport d'auditeurs financiers.

b) la preuve de la compatibilité des processus de dématérialisation ou de conservation avec l'orientation stratégique de l'organisation.

c) la définition des rôles et des responsabilités dans le cadre de l'établissement des processus de Dématérialisation ou de conservation.

d) la preuve de la sensibilisation de l'organisation quant à :

1. l'importance de satisfaire les exigences de la présente règle technique, d'établir les mesures de sécurité de la présente règle technique et de respecter toute la documentation relative aux processus de Dématérialisation ou de conservation.
2. ses responsabilités au titre de la loi luxembourgeoise en matière de dématérialisation et de conservation.

e) l'engagement formel quant à la fourniture de ressources suffisantes pour la gestion de la sécurité de l'information des processus de Dématérialisation ou de conservation, et pour la gestion opérationnelle de ces processus.

f) une gestion adéquate de la sécurité de l'information associée aux processus de dématérialisation ou de conservation.

g) une gestion adéquate opérationnelle des processus de dématérialisation ou de conservation.

h) la garantie de continuité d'exécution (c.-à-d. pendant une période de transition minimum permettant d'assurer un transfert) des processus de Dématérialisation ou de conservation, en particulier pour les cas suivant :

1. processus de dématérialisation exécuté par l'organisation pour le compte d'un tiers.
2. processus de conservation exécuté par l'organisation pour le compte d'un tiers.
3. sous-processus de restitution, transfert et suppression des archives numériques exécuté par l'organisation pour son propre compte.

Cette garantie de continuité doit être gérée par l'organisation et couvrir le risque économique de cessation d'activités.

NOTE : Un moyen pour l'organisation de garantir cette continuité d'exécution pendant une période de transition minimum est par exemple de contracter une assurance spécifique ou d'obtenir un engagement formel d'un actionnaire institutionnel ou privé majoritaire se portant garant.

6.4 Planification

En complément des exigences définies à la clause 6. *« Planification »* de la Norme internationale ISO/IEC 27001:2013, la direction de l'organisation doit s'assurer que :

a) les risques de sécurité de l'information et opérationnels associés à l'établissement des processus de dématérialisation ou de conservation sont intégrés dans son processus d'identification et d'évaluation des risques.

NOTE 1 : L'Annexe B de la présente règle technique énumère des exemples de ces risques.

b) les risques pouvant impacter la stabilité financière de l'organisation et sa capacité de couverture de responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation sont également intégrés dans son processus d'identification et d'évaluation des risques.

c) les objectifs et les mesures suivants sont sélectionnés dans le cadre du processus d'appréciation et de traitement des risques appliqué aux processus de dématérialisation ou de conservation :

1. les objectifs de sécurité et les mesures associées définis dans la Norme internationale ISO/IEC 27002:2013, plus particulièrement aux clauses 5 à 18.
2. les amendements et les compléments aux objectifs de sécurité et aux mesures associées de la Norme internationale ISO/IEC 27002:2013 (plus particulièrement les clauses 5 à 15) et qui sont définis dans la clause 7 de la présente règle technique.
3. les objectifs et les mesures associées de gestion de la sécurité de l'information et de gestion opérationnelle définis dans la clause 7 de la présente règle technique et qui sont additionnels à ceux de la Norme internationale ISO/IEC 27002:2013 (plus particulièrement les clauses 5 à 18).

Des objectifs et des mesures additionnels à ceux définis dans la Norme internationale ISO/IEC 27002:2013 et ceux de la présente clause 7 peuvent être également définis et sélectionnés.

NOTE :

Pour rappel, l'Annexe A de la Norme internationale ISO/IEC 27001:2013 énumère des objectifs de sécurité et les mesures associées qui dérivent directement et exclusivement de la Norme internationale ISO/IEC 27002:2013. Contrairement à ISO/IEC 27002:2013 cette Annexe ne contient pas les préconisations de mise en œuvre et autres informations liées à ces objectifs de sécurité et les mesures associées.

Il convient donc dans le cadre du processus d'appréciation et de traitement des risques liés à l'établissement des processus de dématérialisation ou de conservation de sélectionner les objectifs de sécurité et les mesures associées définis dans la Norme internationale ISO/IEC 27002:2013 ainsi que les objectifs et les mesures associées définis à la clause 7 de la présente règle technique et qui relatent de la gestion de la sécurité de l'information et de la gestion opérationnelle de ces processus.

d) la DdA doit être élaborée en incluant les objectifs et les mesures associées définis dans la Norme internationale ISO/IEC 27002:2013 et dans la clause 7 de la présente règle technique.

Des mesures de sécurité peuvent être exclues pourvu qu'il n'y ait pas de risque associé ou si le niveau de risque est en dessous du seuil d'acceptation, à condition qu'il n'y ait aucune exigence légale, réglementaire ou contractuelle requérant leur mise en œuvre pour réduire le risque à un niveau en dessous du seuil d'acceptation. **Toute exclusion doit être documentée dans la DdA.**

NOTE : L'indication dans la DdA des objectifs et des mesures associés définis à la clause 7 de la présente règle technique peut être effectuée de la manière suivante:

1. 14.1.1 (STD/RT). Cela correspond à la mesure de sécurité 14.1.1 définie dans la Norme ISO/IEC 27002:2013 **et** complétée par le contenu de la clause 7 de la présente règle technique.

2. 5.2.1. (RT) Cela correspond à la mesure 5.2.1 définie à la clause 7 de la présente règle technique et additionnelle aux mesures de sécurité définies dans la Norme ISO/IEC 27002:2013).

6.5 Évaluation de la performance

En complément des exigences définies à la clause 9.3 *« Revue de direction »* de la Norme internationale ISO/IEC 27001:2013, l'organisation doit réexaminer les résultats de l'analyse de risques pouvant impacter la stabilité financière de l'organisation et sa capacité de couverture de responsabilités contractuelles, légales et réglementaires liées aux processus de dématérialisation ou de conservation de manière régulière (au moins une fois par an) et suite à des changements significatifs :

1. impactant le fonctionnement de l'organisation.

2. issus des besoins actuels de l'organisation.

3. de nature légale et réglementaire ayant un impact sur les activités et les processus de l'organisation.

NOTE : Ce réexamen pourra également conduire à l'identification, à l'évaluation et au traitement de nouveaux risques liés à la stabilité financière de l'organisation et à sa capacité de couverture de responsabilités contractuelles, légales et réglementaires liées aux processus de dématérialisation ou de conservation.

Suite à la clause 9.3 « Revue de direction » de la Norme internationale ISO/IEC 27001:2013, la direction de l'organisation peut identifier la nécessité d'apporter des changements au SMSI, ces changements peuvent inclure :

a) la mise à jour de l'analyse des risques de sécurité de l'information et opérationnels liés à la dématérialisation ou à la conservation, ainsi que du plan de traitement de ces risques.

b) la mise à jour de l'analyse des risques liés à la dématérialisation ou à la conservation et pouvant impacter la stabilité financière de l'organisation et sa capacité de couverture de responsabilités contractuelles, légales et réglementaires ainsi que la mise à jour du plan de traitement de ces risques.

c) la modification de la stratégie financière de l'organisation et de sa capacité de couverture de responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation.

6.6 Amélioration

En complément de la ligne directrice définie à la clause 10 « *Amélioration »* de la Norme internationale ISO/IEC 27001:2013, l'organisation doit améliorer de manière permanente l'efficacité de son SMSI via la mise à jour constante de la politique de dématérialisation ou la politique de conservation.

7 Objectifs et mesures

La présente clause 7 définit des objectifs et des mesures de gestion de la sécurité de l'information et de gestion opérationnelle spécifiques aux processus de dématérialisation ou de conservation et sur base de la Norme internationale ISO/IEC 27002:2013.

Plus concrètement, le contenu de la présente clause 7 a été défini de manière à refléter la structure de la Norme ISO/IEC 27002:2013 (clauses 5 à 18).

Le contenu de la présente clause 7 doit être compris comme :

a) des amendements et des compléments aux objectifs de sécurité et mesures associées définis dans la Norme internationale ISO/IEC 27002:2013.

b) des objectifs et mesures de gestion de la sécurité de l'information et de gestion opérationnelle additionnels à ceux définis dans la Norme internationale ISO/IEC 27002:2013.

Des mesures qui ne sont pas alignées avec les mesures préconisées par la Norme ISO27002 :2013 doivent être justifiées dans le DdA. Le même principe reste d'application quand les objectifs de contrôle du standard ISO27002:2013 sont atteints en mettant en œuvre des mesures qui sont différents des mesures décrites dans le standard ISO27002 :2013.

Le contenu de la présente clause 7 **ne fournit pas** d'exigences supplémentaires pour **toutes** les mesures et informations complémentaires du standard ISO27002:2013. Dans le cas où aucune exigence complémentaire n'est formulée dans la présente clause 7, uniquement les exigences du standard ISO27002:2013 s'appliqueront.

NOTE : L'Annexe C décrit un tableau montrant les liens entre la Norme internationale ISO/IEC 27002 :2005 et la présente règle technique. Ce tableau énumère également les clauses, les objectifs de sécurité et les mesures de sécurité à considérer par l'organisation dans le cadre de l'appréciation des risques liés à l'établissement des processus de dématérialisation ou de conservation.

5 *Politiques de sécurité de l'information* (clause existante de la Norme internationale ISO/IEC 27002:2013)

La clause 5 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

5.1 *Orientations de la direction en matière de sécurité de l'information* (objectif de sécurité existant à la Norme internationale ISO/IEC 27002:2013)

5.1.1 *Politiques de sécurité de l'information* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 5.1.1 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

Une organisation établissant des processus de dématérialisation ou de conservation doit intégrer suivant dans sa politique de sécurité de l'information :

a) une brève explication des politiques et principes liés aux processus de dématérialisation ou de conservation exécutés par l'organisation.

5.2 *Politique de dématérialisation* (objectif de sécurité additionnel à la Norme internationale ISO/IEC 27002:2013)

Objectif : La direction doit définir des dispositions générales claires relatives à la gestion de la sécurité de l'information et à la gestion opérationnelle appliquées au processus de dématérialisation exécuté par l'organisation.

5.2.1 *Document de politique de dématérialisation* (mesure de sécurité additionnelle à la Norme internationale ISO/IEC 27002:2013)

Mesure

L'organisation doit définir une politique de dématérialisation conforme aux lois et aux règlements qui lui sont applicables. Ce document doit être approuvé par la direction, communiqué auprès de l'ensemble du personnel concerné (de l'organisation et des tiers), et mis en œuvre.

Exigences mise en œuvre

La politique de dématérialisation doit définir le domaine d'application du processus de dématérialisation, la gestion de la sécurité de l'information et la gestion opérationnelle appliquées à ce processus.

Ce document doit contenir les éléments suivants :

a) présentation de l'organisation, de son historique et de ses activités métiers.

b) définition du domaine d'application du processus de dématérialisation.

NOTE : L'organisation doit définir le type de clients (internes ou externes à l'organisation) potentiels de ce processus. Cela consiste à indiquer si ce processus s'adresse à l'organisation ou à des tiers. Si le processus s'adresse à l'organisation, il est recommandé de spécifier si ce processus supporte l'entièreté de l'organisation, des activités, des processus ou des fonctions spécifiques de l'organisation.

c) une description générale organisationnelle et technique des processus suivants sous-jacents au processus de dématérialisation :

1. collecte des documents analogiques.
2. création et stockage temporaire des documents numériques.
3. stockage temporaire des documents analogiques.
4. restitution, transfert, destruction éventuelle des documents analogiques et suppression des documents numériques.

L'organisation doit également indiquer, pour chacun des processus précédemment cités, si une ou plusieurs des activités associées sont sous-traitées, de manière à pouvoir en assurer une traçabilité et un contrôle spécifique.

d) une description générale technique du système de dématérialisation SDC-D et de son niveau de conformité à des normes et des référentiels reconnus.

Exemples:

1. ISO 32000-1:2008, *Document management -- Portable document format -- Part 1 : PDF 1.7*
   Norme définissant un format de documents numérisés.
2. Dublin Core Metadata
   Référentiel utilisé dans le cadre de l'indexation de documents numérisés.
3. ISO 12653, *Electronic imaging -- Test target for the black-and-white scanning of office documents*
   Norme en deux parties définissant des méthodes d'évaluation technique des scanners.

e) les rôles et les responsabilités spécifiques au processus de dématérialisation et aux processus sous-jacents exécutés par l'organisation et en matière de gestion de la sécurité de l'information et de gestion opérationnelle.

f) les grands principes de sécurité de l'information appliqués au processus de dématérialisation exécuté par l'organisation, notamment en termes d'authenticité, de fiabilité et d'exploitabilité.

g) les références aux lois et aux règlements applicables à l'organisation et spécifiques au processus de dématérialisation.

h) la gestion de la documentation supportant le processus de dématérialisation.

i) des références aux documents, comme par exemple les procédures d'administration, d'opérations et de sécurité, supportant la politique de dématérialisation.

j) les modalités de revue de la politique de dématérialisation.

k) un identifiant unique propre à la politique de dématérialisation et à sa version afin d'en permettre une traçabilité et une utilisation en tant que référence dans la génération d'enregistrements ou de métadonnées liées aux documents numériques résultant de la numérisation des documents analogiques.

NOTE : La gestion de cet identifiant unique doit être documentée. Il est recommandé que cet identifiant unique soit généré à partir d'un identifiant racine propre à l'organisation et attribué par un tiers reconnu.

Exemple :
Object Identifier (OID) repository
http://www.oid-info.com

Informations supplémentaires

Une politique commune aux processus de dématérialisation et de conservation peut être établie par l'organisation sous réserve que les exigences définies spécifiquement pour la politique de dématérialisation et pour la politique de conservation soient adressées dans la politique commune.

5.2.2 *Revue de la politique de dématérialisation* (mesure de sécurité additionnelle à la Norme ISO/IEC 27002:2013)

Mesure

Une revue de la politique de dématérialisation doit régulièrement être effectuée afin de permettre son alignement aux changements impactant l'organisation.

Exigences de mise en œuvre

La direction de l'organisation doit s'assurer de la révision régulière (au moins une fois par an) de la politique de dématérialisation afin de s'assurer de la cohérence de cette politique avec le processus de dématérialisation exécuté par l'organisation et de son amélioration continue.

La direction de l'organisation doit également s'assurer de la révision effective de la politique de dématérialisation et de sa cohérence suite à des changements significatifs :

a) impactant le fonctionnement de l'organisation.

b) issus des besoins actuels de l'organisation.

c) de nature légale et réglementaire ayant un impact sur le processus de dématérialisation.

5.3 *Politique de conservation* (objectif de sécurité additionnel à la Norme internationale ISO/IEC 27002:2013)

Objectif : La direction doit définir des dispositions générales claires relatives à la gestion de la sécurité de l'information et à la gestion opérationnelle appliquées au processus de conservation exécuté par l'organisation.

5.3.1 *Document de politique de conservation* (mesure de sécurité additionnelle à la Norme internationale ISO/IEC 27002:2013)

Mesure

L'organisation doit définir une politique de conservation conforme aux lois et aux règlements qui lui sont applicables. Ce document doit être approuvé par la direction, communiqué auprès de l'ensemble du personnel concerné (de l'organisation et des tiers), et mis en œuvre.

Exigences de mise en œuvre

La politique de conservation doit définir le domaine d'application du processus de conservation, la gestion de la sécurité de l'information et la gestion opérationnelle appliquées à ce processus.

Ce document doit contenir les éléments suivants :

a) présentation de l'organisation, de son historique et de ses activités métiers.

b) définition du domaine d'application du processus de conservation.

NOTE : L'organisation doit définir le type de clients (internes ou externes à l'organisation) potentiels de ce processus. Cela consiste à indiquer si ce processus s'adresse à l'organisation ou à des tiers. Si le processus s'adresse à l'organisation, il est recommandé de spécifier si ce processus supporte l'entièreté de l'organisation, des activités, des processus ou des fonctions spécifiques de l'organisation.

c) une description générale organisationnelle et technique des processus suivants sous-jacents au processus de conservation :

1. collecte des documents numériques.
2. création et conservation des archives numériques.
3. restitution, transfert et suppression des archives numériques.

Pour chacun des processus précédemment cités, l'organisation doit également indiquer si une ou plusieurs des activités associées sont sous-traitées, de manière à pouvoir en assurer une traçabilité et un contrôle spécifique.

d) une description générale technique du système de conservation SDC-C et de son niveau de conformité à des normes et référentiels reconnus.

Exemple :

1. ETSI TS 102 573 v1.1.1 (2007-07), *Electronic Signatures and Infrastructures (ESI) ; Policy requirements for trust service provides signing and/or storing data for digital accounting*

   Norme définissant des exigences en matière d'archivage de documents numériques.

e) les rôles et les responsabilités spécifiques au processus de conservation et aux processus sous-jacents exécutés par l'organisation et en matière de gestion de la sécurité de l'information et de gestion opérationnelle.

f) les grands principes de sécurité de l'information appliqués au processus de conservation exécutés par l'organisation, notamment en termes d'authenticité, de fiabilité et d'exploitabilité.

g) les références aux lois et aux règlements applicables à l'organisation et spécifiques au processus de conservation.

h) la gestion de la documentation supportant le processus de conservation.

i) des références aux documents, comme par exemple les procédures d'administration, d'opérations et de sécurité, supportant la politique de conservation.

j) les modalités de revue de la politique de conservation.

k) un identifiant unique propre à la politique de conservation et à sa version afin d'en permettre une traçabilité et une utilisation en tant que référence dans la génération d'enregistrements ou de métadonnées liées aux archives numériques.

NOTE : La gestion de cet identifiant unique doit être documentée. Il est recommandé que cet identifiant unique soit généré à partir d'un identifiant racine propre à l'organisation et attribué par un tiers reconnu.

Exemple :
Object Identifier (OID) repository
http://www.oid-info.com

Informations supplémentaires

Une politique commune aux processus de dématérialisation et de conservation peut être établie par l'organisation sous réserve que les exigences définies spécifiquement pour la politique de dématérialisation et pour la politique de conservation soient adressées dans la politique commune.

5.3.2 *Revue de la politique de conservation* (mesure de sécurité additionnelle à la Norme ISO/IEC 27002:2013)

Mesure

Il convient qu'une revue de la politique de conservation soit régulièrement effectuée afin de permettre son alignement aux changements qui impactent l'organisation.

Exigences de mise en œuvre

La direction de l'organisation doit s'assurer de la révision régulière (par exemple tous les ans) de la politique de conservation afin de s'assurer de la cohérence de cette politique avec le processus de conservation exécuté par l'organisation et de son amélioration continue.

La direction de l'organisation doit également s'assurer de la révision effective de la politique de conservation et de sa cohérence suite à des changements significatifs :

a) impactant le fonctionnement de l'organisation.

b) issus des besoins actuels de l'organisation.

c) de nature légale et réglementaire ayant un impact sur le processus de conservation.

6 *Organisation de la sécurité de l'information* (clause existante de la Norme internationale ISO/IEC 27002:2013)

La clause 6 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

6.1 *Organisation interne* (objectif de sécurité existant de la Norme internationale ISO/IEC 27002:2013)

L'objectif de sécurité 6.1 de la Norme internationale ISO/IEC 27002:2013 est complété de la manière suivante :

Objectif :

La direction de l'organisation doit également approuver les politiques de dématérialisation ou de conservation, définir et assigner les rôles et les responsabilités liés à la gestion de la sécurité de l'information et à la gestion opérationnelle des processus de dématérialisation ou de conservation, et réexaminer régulièrement la mise en œuvre de ces gestions.

6.1.1 *Fonctions et responsabilités liées à la sécurité de l'information* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 6.1.1 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Mesure

La direction doit soutenir les politiques de dématérialisation ou de conservation par la définition de dispositions générales claires relatives à la gestion de la sécurité de l'information et à la gestion opérationnelle liées aux processus de dématérialisation ou de conservation, et par l'attribution explicite de rôles et de responsabilités associés à ces gestions. La coordination de la sécurité de l'information doit s'assurer que les activités de la sécurité de l'information ainsi que les activités liées à la dématérialisation et à la conservation soient conformes aux politiques de dématérialisation et de conservation.

Exigences de mise en œuvre

La direction doit :

a) s'assurer que les objectifs de la sécurité de l'information spécifiques aux processus de dématérialisation ou de conservation soient :

    1. identifiés et compatibles avec les objectifs de la sécurité de l'information adoptés pour des besoins de l'organisation autres que ceux liés à la dématérialisation ou à la conservation.

    2. intégrés dans des processus adaptés.

b) s'assurer de la définition des politiques de dématérialisation et de conservation, de la définition des procédures associées aux politiques, de leur approbation et de leur révision régulière.

c) contrôler l'efficacité de la mise en œuvre des politiques de dématérialisation ou de conservation et des procédures associées.

d) veiller à ce que la coordination de la sécurité de l'information s'assure également de l'exécution conforme des activités de la sécurité de l'information et des activités opérationnelles de dématérialisation et de conservation aux politiques de dématérialisation et de conservation.

e) d'attribuer les rôles et les responsabilités en matière de sécurité de l'information et d'activités opérationnelles conformément aux politiques de Dématérialisation ou de conservation.

f) revoir la définition et l'attribution des rôles et des responsabilités en matière de sécurité de l'information et d'activités opérationnelles de manière régulière afin de s'assurer leur conformité avec les changements :

    1. impactant le fonctionnement de l'organisation.

    2. issus des besoins actuels de l'organisation.

    3. de nature légale et réglementaire ayant un impact sur l'organisation.

g) s'assurer que les personnes assumant des rôles et des responsabilités dans l'établissement de processus ou d'activités de la sécurité de l'information ou opérationnels liés à la dématérialisation ou la conservation n'assument pas la revue de l'efficacité de l'exécution de ces rôles et responsabilités, et l'évaluation de leur conformité à des objectifs définis.

La direction de l'organisation doit nommer un responsable des processus de Dématérialisation et de conservation, incluant dans le périmètre de ses rôles et de ses responsabilités les éléments suivants :

a) la gestion de la documentation (politiques, procédures) supportant ces processus.

b) leur définition au niveau opérationnel, incluant le système de dématérialisation ou de conservation SDC et les mécanismes de sécurité associés.

c) la supervision de leur mise en œuvre.

d) la définition de leurs critères de performances.

e) leur évaluation selon les critères de performances.

f) l'émission de recommandations en vue d'améliorer leur gestion opérationnelle.

Les personnes assumant une partie ou l'entièreté de ces rôles et ces responsabilités peuvent déléguer des activités associées. Néanmoins, elles demeurent responsables de la bonne exécution de ces activités.

Informations supplémentaires

L'organisation doit définir et attribuer clairement les rôles et les responsabilités en matière de gestion des risques pouvant impacter la stabilité financière de l'organisation et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation.

Cette coordination doit :

a) définir et approuver les méthodes relatives à la gestion des risques pouvant impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation.
b) évaluer l'adéquation des mesures adoptées en vue de mitiger les risques pouvant impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation, et jugés non acceptable par la direction de l'organisation.

   Exemple de mesure visant à couvrir les risques pouvant impacter la capacité de couverture des responsabilités de l'organisation :

   1. souscription à une assurance couvrant la continuité de l'exécution des processus de dématérialisation et de conservation de l'organisation même en cas de cessation d'activités et pendant une période minimum de transition.

c) identifier les changements en termes de risques pouvant impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation de manière régulière (au moins une fois par an) et suite à des changements significatifs :

   1. impactant le fonctionnement de l'organisation.
   2. issus des besoins actuels de l'organisation.
   3. de nature légale et réglementaire ayant un impact sur l'organisation.

d) sensibiliser le personnel (de l'organisation et des tiers) concerné par les processus de dématérialisation ou de conservation exécutés par l'organisation quant aux risques pouvant

impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles et juridiques associées à ces processus.

e) identifier et évaluer les problèmes et les incidents liés à la perte de stabilité financière de l'organisation et à la perte de la capacité de couverture de responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation.

f) émettre des recommandations quant aux actions préventives et correctives à adopter en réponse aux problèmes et aux incidents évalués.

g) établir une coordination de la gestion des risques pouvant impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation en s'appuyant sur les membres de la direction de l'organisation ainsi que sur du personnel spécialisé dans la gestion du risque, des problèmes juridiques, de la dématérialisation ou de la conservation, de la sécurité de l'information, ainsi que dans les domaines de l'assurance et de l'audit.

6.1.3 *Relations avec les autorités* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 6.1.3 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Mesure

L'organisation doit s'assurer que :

a) des procédures ont été définies et mise en œuvre pour notifier les autorités compétentes, en particulier l'ILNAS, en prévision de l'établissement de changements significatifs pouvant impacter la sécurité de l'information et les activités opérationnelles des processus de dématérialisation ou de conservation exécutés par l'organisation.

   Exemples de changements significatifs :

   1. changement de direction de l'organisation.

   2. modification du système de dématérialisation ou de conservation SDC impactant les processus associés.

   3. modification du périmètre d'activités gérées par des fournisseurs impactant les processus de dématérialisation ou de conservation exécutés par l'organisation.

   NOTE : Il est recommandé que l'organisation avertisse les autorités compétentes de la planification de changements significatifs avant leur établissement ou à défaut dans les meilleurs délais suivants l'établissement de ces changements si leur notification ne pouvait pas être effectuée avant leur établissement.

b) les transmissions d'informations avec les autorités compétentes soient :

   1. protégées par des mécanismes cryptographiques conformes aux bonnes pratiques en la matière de manière à s'assurer de l'authenticité des correspondants, de la confidentialité et de l'intégrité des échanges.

      NOTE : Des mécanismes cryptographiques tels que :
      a. des dispositifs sécurisés (carte à puce, clé USB cryptographique) de création de signature contenant un certificat électronique qualifié peuvent être utilisés à des fins d'authentification de l'émetteur et des destinataires.
      b. des protocoles sécurisés de transmissions d'information SFTP, TLS, PPP, L2TP et IPSec, ou des mécanismes de calcul d'empreintes digitales peuvent être utilisés à des fins de confidentialité ou de l'intégrité des échanges.

2. conservées aussi longtemps que nécessaire conformément aux durées légales de rétention.

   Si les durées légales de rétention n'ont pas été définies pour certains types de transmissions d'information ou en fonction de la nature des informations échangées, l'organisation doit appliquer les mesures spécifiées dans la politique de rétention des données.

Informations supplémentaires

L'organisation doit définir également des procédures de notification des autorités compétentes afin de les informer :

a) régulièrement (au moins une fois par an) de la stabilité financière de l'organisation et de sa capacité de couverture des responsabilités contractuelles, légales et réglementaires liées aux processus de dématérialisation ou de conservation.

b) de l'établissement planifié de changements significatifs pouvant impacter la stabilité financière de l'organisation ainsi que sa capacité de couverture des responsabilités contractuelles, légales et réglementaires liées aux processus de dématérialisation ou de conservation.

   NOTE : Si la notification de ces changements ne pouvait pas être effectuée avant leur établissement, il convient que l'organisation avertisse les autorités compétentes dans les meilleurs délais suivants leur établissement.

c) dans les meilleurs délais de la survenance de problèmes ou d'incidents liés à la stabilité financière de l'organisation et à sa capacité de couverture des responsabilités contractuelles, légales et réglementaires liées aux processus de dématérialisation ou de conservation.

7 *La sécurité des ressources humaines* (clause existante de la Norme internationale ISO/IEC 27002:2013)

La clause 7 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

7.2 *Pendant la durée du contrat* (objectif de sécurité existant de la Norme internationale ISO/IEC 27002:2013)

7.2.1 *Responsabilités de la direction* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 7.2.1 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

Il relève de la direction de l'organisation que son personnel et celui des fournisseurs impliqués dans la gestion opérationnelle des processus de dématérialisation ou de conservation exécutés par l'organisation :

a) soient correctement informés de leurs rôles et responsabilités liés aux processus de dématérialisation et de conservation.

b) s'engagent par écrit à respecter les politiques de dématérialisation et de conservation.

7.2.2 *Sensibilisation, apprentissage et formation à la sécurité de l'information* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 7.2.2 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

L'organisation doit dispenser les formations suivantes à son personnel et à celui des fournisseurs impliqués dans la gestion opérationnelle des processus de dématérialisation ou de conservation exécutés par l'organisation :

a) formation sous forme de sensibilisation pour présenter les politiques de Dématérialisation ou de conservation, les attentes et les besoins de l'organisation en la matière, afin de s'assurer d'une compréhension commune de ces éléments.

b) formation continue de manière à rappeler les exigences liées à la dématérialisation ou à la conservation, à présenter les procédures associées à ces exigences et les récentes modifications apportées à l'ensemble de la documentation liée aux domaines concernés.

8. Gestion des actifs

La clause 8 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

8.2 *Classification de l'information* (objectif de sécurité existant de la Norme internationale ISO/IEC 27002:2013)

8.2.1 *Classification des informations* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 8.2.1 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

Des lignes directrices et des niveaux de classification doivent être définis et mis en œuvre par l'organisation spécifiquement pour les documents et les archives numériques des clients gérés par l'organisation dans le cadre des processus de dématérialisation ou de conservation.

L'organisation doit :

a) définir les lignes directrices et les niveaux de classification en intégrant les exigences relatives à l'authenticité, à la fiabilité et à l'exploitation aussi longtemps que nécessaire des éléments suivants :

    1. les documents collectés (analogiques et numériques) des clients.

    2. les documents numériques résultants de la numérisation des documents analogiques des clients.

    3. les archives numériques des clients.

b) s'assurer de la revue de ces lignes directrices et de ces niveaux de classification par le responsable du processus de dématérialisation ou de conservation de manière régulière (au moins une fois par an), suite à une modification significative du système de dématérialisation ou de conservation SDC-DC, SDC-D, ou SDC-C et des processus de dématérialisation ou de conservation.

8.2.2 *Marquage des informations* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 8.2.2 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

L'organisation doit définir et mette en œuvre des procédures de marquage de l'information spécifiques aux lignes directrices et niveaux de classification pour les documents et les archives numériques des clients gérés par l'organisation dans le cadre des processus de dématérialisation et de conservation.

8.3 *Manipulation des supports* (objectif de sécurité existant de la Norme internationale ISO/IEC 27002:2013)

8.3.2 *Mise au rebut des supports* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 8.3.2 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

L'organisation doit envisager les directives suivantes :

a) une destruction des éléments suivants doit être réalisée par des mécanismes sécurisés :

   1. les documents analogiques des clients selon les conditions définies dans les documents contractuels établis entre les clients et l'organisation.

   2. tout support de stockage de l'organisation contenant les informations des clients (incluant les documents et archives numériques) ou de nature confidentielle à l'organisation.

   NOTE : L'incinération et le déchiquetage sont considérés comme des mécanismes sécurisés de destruction pour les éléments précédemment mentionnés.

b) la suppression de toutes les informations des clients contenues dans les supports de stockage de l'organisation devrait être réalisée par des mécanismes sécurisés si ces supports ne peuvent pas être détruits de manière sécurisée.

   NOTE : Une réécriture multiple sur des données ne permettant plus de les retrouver en l'état est considérée comme un mécanisme sécurisé de suppression d'informations.

c) la destruction des documents analogiques et des supports de stockage et la suppression des informations stockées dans ces supports doivent être évalués par un tiers pouvant attester de l'effectivité de leur destruction et de leur suppression ne permettant plus de retrouver les informations d'origine.

d) la destruction des documents analogiques et des supports de stockage et la suppression des informations stockées dans ces supports réalisées par un fournisseur de l'organisation s'accompagnent d'une attestation de ce fournisseur stipulant que :

   1. les supports de stockage remis au tiers par l'organisation en vue de leur destruction sont biens ceux qui ont été détruits.

2. les informations stockées dans les supports de stockage remis par l'organisation en vue de leur suppression ont bien été supprimées.
3. la destruction des documents analogiques et des supports de stockage et la suppression des informations stockées dans ces supports ont été respectivement effectuées par une méthode sécurisée basée sur les bonnes pratiques en la matière.

NOTE : Si nécessaire, les pièces issues d'un déchiquetage doivent être jetées séparément afin de réduire les risques de reconstruction des supports.

9 *Contrôle d'accès* (clause existante de la Norme internationale ISO/IEC 27002:2013)

La clause 9 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

9.1 *Exigences métier en matière de contrôle d'accès* (objectif de sécurité existant de la Norme internationale ISO/IEC 27002:2013)

9.1.1 *Politique de contrôle d'accès* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 9.1.1 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

La politique de contrôle d'accès de l'organisation doit tenir compte de l'exigence de la séparation effective des activités d'administration, d'opérations et de sécurité du système de dématérialisation et de conservation SDC-DC, SDC-D ou SDC-C.

9.2 *Gestion de l'accès utilisateur* (objectif de sécurité existant de la Norme internationale ISO/IEC 27002:2013)

9.2.3 *Gestion des privilèges d'accès* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 9.2.3 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

Les mots de passe des comptes des utilisateurs du système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C et des comptes techniques des actifs techniques du ne doivent en aucune circonstance être stockés dans un support de stockage de l'organisation sous une forme non protégée.

11 *Sécurité physique et environnementale* (clause existante de la Norme internationale ISO/IEC 27002:2013)

11.1 *Zones sécurisées* (objectif de sécurité existant de la Norme internationale ISO/IEC 27002:2013)

11.1.1 *Périmètre de sécurité physique* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 11.1.1 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

L'organisation doit s'assurer que les systèmes de détection d'intrus adaptés soient activés en permanence pour les portes et les fenêtres accessibles dans leur zone de surveillance afin de détecter une ouverture prolongée de ces éléments. Cette mesure est à considérer particulièrement pour le site de l'organisation hébergeant les actifs techniques liés aux processus de dématérialisation ou de conservation ainsi que les documents analogiques collectés des clients.

En cas de désactivation de ces systèmes de détection, notamment pour pouvoir déplacer du matériel, d'autres mécanismes de surveillance doivent être mis en place afin de réduire le risque d'accès non autorisé à ces actifs et aux documents analogiques des clients.

11.1.2 *Contrôles physiques des accès* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 11.1.2 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

L'organisation doit prendre en compte les directives suivantes :

a) tous les visiteurs de l'organisation :

    1. doivent être accompagnés par un membre de l'organisation habilité de manière permanente à circuler dans les zones où les visiteurs sont situés, même si l'accès à ces zones leur a déjà été autorisé.

    2. ne devraient pas accéder aux zones associées au processus de dématérialisation, notamment en cas d'activités de traitement de documents analogiques de clients pour réduire les risques de divulgation non autorisée d'informations. Les mesures nécessaires doivent toujours être prises pour s'assurer que les visiteurs ne puissent pas voir des informations d'autres clients.

b) les tiers autorisés de manière permanente à accéder aux zones sécurisées de l'organisation ne devraient pas pouvoir accéder aux actifs techniques du système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C et aux documents analogiques des clients sans une surveillance effective de leur intervention.

c) les actifs techniques du système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C devraient être protégés contre des accès non autorisés :

    1. en cas d'évacuation des zones hébergeant ces actifs.

    2. s'ils sont situés dans des sites multi-occupants.

11.2 *Matériels* (objectif de sécurité existant de la Norme internationale ISO/IEC 27002:2013)

11.2.1 *Emplacement et protection du matériel* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 11.2.1 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

Les documents analogiques des clients doivent être considérés comme des actifs nécessitant une protection spéciale (au sens de 11.2.1 d) de la Norme ISO/IEC 27002:2013) au niveau des conditions ambiantes et des autres menaces liées.

11.2.5 *Sortie des actifs* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 11.2.5 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

Les documents analogiques des clients doivent être considérés comme étant des actifs et ne doivent pas sortir de l'organisation sans autorisation préalable de ces derniers, excepté pour prévenir la destruction de ces biens en cas de catastrophe.

12 Sécurité liée à *l'exploitation* (clause existante de la Norme internationale ISO/IEC 27002:2013)

***12.4 Journalisation et surveillance* (objectif de sécurité existant de la Norme internationale ISO/IEC 27002:2013)**

12.4.4 *Synchronisation des horloges* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 12.4.4 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

L'organisation doit s'assurer que :

a) les actifs techniques supportant le système de dématérialisation ou de conservation soient synchronisés avec selon le temps universel coordonné (UTC), *via* une source de temps faisant autorité.

b) les événements liés à la synchronisation régulière de l'horloge système des actifs techniques du système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C soient enregistrés et conservés aussi longtemps que nécessaire.

c) un unique format de la date et de l'heure soit adopté pour la génération des événements du système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C pour faciliter la traçabilité des actions effectuées.

d) une synchronisation avec l'horloge maitre soit faite de façon suffisamment régulière pour s'assurer que la variation entre l'horloge maitre et l'horloge des systèmes dans le périmètre de la certification reste en dessous du seuil d'une seconde.

e) toute variation supérieure à la variation tolérée soit détectée dans les plus brefs délais afin que des actions correctrices puissent être adoptées.

12.8 *Dématérialisation* (objectif de sécurité additionnel à la Norme internationale ISO/IEC 27002:2013)

Objectif : assurer la gestion correcte et sécurisée des documents analogiques et numériques dans le cadre du processus de dématérialisation.

L'organisation doit intégrer les principes d'authenticité, de fiabilité et d'exploitation dans la définition, la mise en exploitation et l'utilisation de son système de dématérialisation SDC-D.

12.8.1 *Système de dématérialisation SDC-D* (mesure de sécurité additionnelle à la Norme internationale ISO/IEC 27002:2013)

12.8.1.1 Mesure

L'organisation doit pouvoir démontrer que le système de dématérialisation SDC-D est composé d'actifs techniques et de mécanismes de sécurité :

a) répondant aux besoins des clients (internes ou externes à l'organisation) du processus de dématérialisation.

b) permettant de garantir l'authenticité, la fiabilité et l'exploitation des documents analogiques et numériques gérés par ce système.

NOTE : Un système de dématérialisation SDC-D est un système composé d'un ensemble d'actifs techniques permettant la création de documents numériques à partir de documents analogiques, le stockage temporaire des documents analogiques et numériques, leur restitution, leur transfert, la destruction éventuelle des documents analogiques et la suppression des documents numériques.

Exigences de mise en œuvre

12.8.1.2 Description détaillée du système de dématérialisation SDC-D

L'organisation doit définir et maintenir une description détaillée du système de dématérialisation SDC-D en :

a) identifiant et en documentant les actifs techniques supportant les processus sous-jacents au processus de dématérialisation, à savoir :

   1. la collecte des documents analogiques.
   2. la création et le stockage temporaire des documents numériques.
   3. le stockage temporaire des documents analogiques.
   4. la restitution, le transfert, la destruction éventuelle des documents analogiques et la suppression des documents numériques.

b) identifiant, en évaluant et en documentant de manière régulière les possibilités techniques du SDC-D, comme par exemple les suivantes :

   1. nombres minimum et maximum de couleurs et les niveaux de gris applicables par le(s) scanner(s).
   2. nombres minimum et maximum de dpi, de bits par pixel applicables par le(s) scanner(s).

3. possibilité de dématérialisation recto/verso ou uniquement verso de documents analogiques.

4. possibilité de dématérialiser des documents analogiques de différents formats, comme par exemple A3, A4 et A5.

5. méthodes de correction d'images applicables par le(s) scanner(s), comme le redressement, la suppression de points isolés, et la suppression des marges.

6. méthodes de compression des images applicables par le(s) scanner(s).

7. nombre de documents analogiques ou nombre de pages composant les documents analogiques pouvant être numérisés par le(s) scanner(s) dans un laps de temps donné.

NOTE : L'identification et l'évaluation des possibilités techniques du SDC-D sont indispensables pour assurer sa conformité avec les besoins des clients (internes ou externes à l'organisation).

c) identifiant et en évaluant de manière régulière les capacités techniques du SDC-D et en les documentant.

Le responsable du processus de dématérialisation doit revoir les capacités techniques du SDC-D de manière régulière (au moins une fois par an), et suite à une modification significative du SDC-D et suite à un changement :

1. impactant le fonctionnement de l'organisation ou la gestion opérationnelle du SDC-D.

2. issu des besoins des clients (intégration d'un nouveau projet client, modification d'un projet client existant).

3. de nature légale et réglementaire ayant un impact sur le processus de dématérialisation.

NOTE : La connaissance des capacités techniques du SDC-D est indispensable à l'organisation pour assurer la disponibilité du SDC-D, la définition adéquate des projets de dématérialisation, la planification appropriée des ressources de l'organisation en matière de dématérialisation et la projection des futurs dimensionnements du SDC-D.

12.8.1.3 Mécanismes de sécurité du système de dématérialisation SDC-D

L'organisation doit établir et documenter les mécanismes de sécurité du système de dématérialisation SDC-D permettant d'assurer l'authenticité, la fiabilité et l'exploitation des documents analogiques et numériques gérés par ce système.

L'organisation doit établir les mécanismes de sécurité suivants :

a) mécanismes de gestion des accès au SDC-D.

L'organisation doit protéger les accès aux actifs techniques du SDC-D, aux documents analogiques et numériques gérés par le SDC-D en :

1. s'assurant que les conditions d'accès à ces actifs et ces documents s'appliquent à toute personne physique et à tout actif tentant d'y accéder.

2. établissant une gestion adéquate des comptes des utilisateurs autorisés à accéder au SDC-D et des comptes techniques des actifs techniques du SDC-D, avec une capacité de révocation immédiate de ces comptes.

   Un compte unique doit être attribué à un utilisateur ou à un actif de manière à pouvoir identifier sans ambigüité les activités et les actions système effectuées.

3. établissant des mécanismes d'authentification appropriés et sécurisés pour les comptes des utilisateurs autorisés et les comptes des actifs techniques du SDC-D.

b) mécanismes de gestion des privilèges.

Une gestion des privilèges pour l'ensemble des comptes des utilisateurs du SDC-D et des comptes techniques des actifs techniques du SDC-D doit être établie.

En particulier l'organisation doit s'assurer d'une séparation effective des activités d'administration, d'opérations et de sécurité du SDC-D en établissant des profils de privilèges pour les comptes des utilisateurs autorisés à accéder au SDC-D de manière à réduire les risques de conflits d'intérêts et d'accès non autorisés au SDC-D et aux documents gérés par ce système.

Il convient d'attribuer à un utilisateur du SDC-D un seul des profils de privilèges suivants. Pour des raisons liées au fonctionnement de l'organisation, il est toutefois acceptable qu'un utilisateur du SDC-D dispose à la fois du profil de privilèges d'administration et du profil de privilèges d'opérations.

1. profil de privilèges d'administration

   Il convient qu'un utilisateur disposant de ce profil puisse créer, modifier ou supprimer des comptes du SDC-D, et définir, modifier ou supprimer des paramètres associés à la gestion opérationnelle du SDC-D.

   Il convient que cet utilisateur ne puisse pas accéder aux éléments suivants :

   a. paramètres de sécurité du SDC-D, comme par exemple les conditions d'authentification des utilisateurs et des actifs techniques du SDC-D.

   b. paramètres de surveillance et de journalisation des évènements du SDC-D.

   c. journaux d'événements du SDC-D.

   d. documents numériques gérés par le SDC-D.

2. profil de privilèges d'opérations

   Il convient qu'un utilisateur disposant de ce profil puisse uniquement :

   a. exécuter les activités d'opérations du SDC-D.

   b. accéder aux documents numériques gérés par le SDC-D et les exploiter dans le cadre du processus de dématérialisation.

   c. assigner à un profil de privilèges de lecture les documents numériques auxquels un utilisateur disposant de ce profil aura accès.

3. profil de privilèges de sécurité

   Il convient qu'un utilisateur disposant de ce profil puisse uniquement :

   a. définir, modifier ou supprimer les paramètres de sécurité du SDC-D, comme par exemple les conditions d'authentification des utilisateurs du SDC-D.

   b. définir, modifier ou supprimer les paramètres de surveillance du SDC-D et de génération de journaux d'événements du SDC-D.

   c. accéder aux journaux d'événements du SDC-D en vue de leur exploitation.

4. profils de privilèges de lecture

   Il convient de définir un profil de privilèges de lecture pour le personnel d'un client autorisé à accéder à distance aux documents numériques du client par le biais de l'utilisation de comptes du SDC-D.

   Il convient que ce profil limite l'accès exclusivement à ces documents, qui auront été au préalable assignés à ce profil avec un droit de lecture par un utilisateur du SDC-D disposant d'un profil de privilèges d'opérations.

Il convient de s'assurer que toute modification ou suppression des documents numériques créés qui n'était pas programmée lors de la définition du projet de dématérialisation nécessite l'approbation de deux utilisateurs disposant du profil de privilèges d'opérations.

L'organisation doit pouvoir démontrer que les profils de privilèges établis pour l'ensemble des comptes des utilisateurs du SDC-D et des comptes techniques des actifs techniques du SDC-D **respectent le principe de séparation effective des activités d'administration, d'opérations et de sécurité du SDC-D**.

c) mécanismes de surveillance de manière à identifier, à enregistrer et à centraliser dans des journaux tous les événements en lien avec le SDC-D, en particulier :

1. l'ensemble des activités effectuées par les comptes des utilisateurs du SDC-D, incluant les activités effectués hors de conditions normales d'utilisation du SDC-D, comme par exemple :

   a. les tentatives de connexion d'utilisateurs hors des heures normales de bureau.

   b. les activités effectuées par les utilisateurs dans un laps de temps plus court que la normale, pouvant conduire à suspecter qu'elles sont réalisées par des actifs techniques et non des personnes physiques.

   c. la duplication de sessions utilisateurs.

2. les événements système des actifs du SDC-D.

3. les événements liés aux documents analogiques et numériques traités par le SDC-D.

4. les erreurs et dysfonctionnements des actifs du SDC-D.

5. les événements du SDC-D liés à la génération de journaux d'événements.

Les journaux d'événements générés doivent être exploitables, conservés et protégés contre toute manipulation et suppression non autorisées pour assurer une traçabilité aussi longtemps que nécessaire de tous les événements enregistrés par ces mécanismes de surveillance.

d) mécanismes cryptographiques de sécurité devant assurer :

1. une authentification appropriée et sécurisée protégeant l'accès aux actifs techniques du SDC-D, aux documents analogiques et numériques gérés par le SDC-D.

   Un dispositif sécurisé doit être utilisé, comme par exemple une carte à puce ou une clé USB cryptographique contenant un certificat électronique d'authentification, un token d'authentification ou des techniques de biométrie pour s'assurer de l'authentification sécurisée d'un utilisateur aux actifs techniques du SDC-D et aux documents gérés par le SDC-D.

   Il convient d'utiliser un dispositif de filtrage d'adresses IP associé à un moyen cryptographique, comme par exemple un certificat SSL, pour s'assurer de l'authentification sécurisée d'un actif technique du SDC-D aux autres actifs du SDC-D et documents gérés par le SDC-D.

2. une signature sécurisée des utilisateurs du SDC-D.
   Un certificat qualifié doit être utilisé, pour permettre :

   a. à un utilisateur du SDC-D de signer électroniquement des rapports d'activités d'administration, d'opérations et de sécurité du SDC-D de manière à s'assurer de l'authenticité des activités effectuées.

   b. à une personne de l'organisation de signer électroniquement les transmissions d'informations et de documents numériques à destination des clients (internes ou externes à l'organisation) et des autorités compétentes de manière à s'assurer de l'authenticité des envois.

   Le dispositif sécurisé de création de signature électronique et le certificat électronique qualifié utilisés doivent répondre aux exigences définies par l'Union européenne en la matière.

   Il convient également d'utiliser des formats de signatures électroniques comme par exemple CAdES [5], XAdES [6] et PAdES [7] pour maintenir une pérennité de la signature électronique, des informations et des documents numériques attachés à cette signature.

3. une transmission sécurisée d'informations et de documents numériques.

   Des protocoles sécurisés (SFTP, TLS, PPP, L2TP et IPSec, …) doivent être utilisés, pour sécuriser la transmission d'informations et de documents numériques entre les éléments suivants :

   a. les actifs techniques du SDC-D, même pour ceux appartenant à un même réseau.

   b. les parties concernées par le processus de dématérialisation comme l'organisation, les clients (internes ou externes à l'organisation) et les autorités compétentes.

4. une intégrité des documents numériques générés par le SDC-D pour s'assurer que ces documents issus de la conversion de documents analogiques sont correctement stockés, restitués ou transférés.

   Une empreinte digitale doit être calculée à partir d'un document numérique dès sa création, c'est-à-dire dès que possible au cours de l'opération de conversion du document analogique de manière à pouvoir préserver l'intégrité de ce document numérique à partir de sa création jusqu'à sa restitution, son transfert ou sa suppression.

   Par conséquent cette empreinte digitale doit être :

   a. associée à ce document numérique en tant que métadonnée de contrôle.

   b. utilisée comme un identifiant unique du document numérique lors de son stockage, de sa restitution ou de son transfert pour maintenir son intégrité durant l'exécution du processus de dématérialisation.

5. une intégrité dans le temps des journaux d'événements.

   Il convient en particulier de s'assurer de :

   a. l'établissement d'un schéma de liaison pour lier les évènements enregistrés d'un journal entre eux permettant de détecter toute suppression d'événements survenus par le passé.

   b. l'horodatage régulier, par exemple une fois par jour, des journaux d'événements par une autorité d'horodatage qualifiée.

e) mécanismes de contrôle régulier de l'intégrité du SDC-D pour s'assurer que :

   1. le fonctionnement du SDC-D n'a pas été altéré suite à des :

      a. opérations de maintenance ou des mises à jour.

      b. remplacements d'actifs du SDC-D comme par exemple les scanners ou des composants de ces actifs comme par exemple les supports de stockage.

   2. les fichiers de configurations du SDC-D n'ont pas été modifiés de manière non autorisée.

   3. l'intégrité des documents numériques stockés, des métadonnées associées ainsi que des journaux d'événements est préservée.

f) Mécanismes de vérification de l'adéquation du nombre de documents analogiques en entrée (ou du nombre de pages composant ces documents) avec le nombre de documents (ou de pages) en sortie (numériques et analogiques rejetés).

g) Mécanismes de vérification du contenu des documents numériques résultant de la numérisation de documents analogiques pour s'assurer de la reproduction conforme à l'original.

   L'organisation doit exercer une vérification du contenu des documents numériques par rapport aux documents analogiques si la destruction de ces derniers est programmée à la suite de leur numérisation.

h) mécanismes de destruction sécurisée des documents analogiques (voir 10.7.2) et de suppression de documents numériques, comme par exemple une réécriture multiple sur les informations ne permettant plus de les retrouver en l'état.

12.8.1.4 Preuves de la conformité

Les preuves de la conformité du fonctionnement du SDC-D et des activités effectuées par le personnel concerné par rapport aux politiques et aux procédures liées au processus de dématérialisation exécuté par l'organisation doivent être conservées en utilisant des supports de stockage pérennes pour une conservation appropriée aussi longtemps que nécessaire.

En particulier, les preuves suivantes doivent être conservées :

a) journaux d'événements du SDC-D.

b) les événements liés aux documents analogiques et numériques traités par le SDC-D.

c) rapports d'activités des utilisateurs du SDC-D.

d) rapports de mises à jour du SDC-D, d'incidents ou de changements liés au SDC-D.

e) jetons d'horodatage générés dans le cadre du fonctionnement du SDC-D et des activités des utilisateurs du SDC-D.

f) signatures électroniques des utilisateurs du SDC-D.

NOTE : La validité de la signature électronique d'un utilisateur du SDC-D doit pouvoir être vérifiée aussi longtemps que nécessaire en démontrant qu'au moment de la signature électronique le certificat électronique qualifié de l'utilisateur était valide et issu d'une autorité de certification reconnue.

Plusieurs techniques sont possibles à cette fin comme par exemple les suivantes :

1. utilisation du protocole de vérification en ligne de certificats (OCSP) de l'autorité de certification émettrice du certificat électronique qualifié.

2. horodatage du rapport d'activités signé et récupération de la liste de révocation des certificats (CRL) publiée régulièrement par l'autorité de certification émettrice du certificat électronique qualifié.

12.8.1.5 Conformité par rapport aux lois et aux règlements en vigueur au Luxembourg

a) le système de dématérialisation SDC-D et les mécanismes de sécurité associés doivent être conformes aux lois et aux règlements en vigueur au Luxembourg.

b) le fonctionnement du SDC-D et celui des mécanismes de sécurité du SDC-D doivent être évalués par un tiers pouvant attester de la conformité de son fonctionnement et des activités effectuées par le personnel concerné par rapport à la description détaillée du système de dématérialisation SDC-D et par rapport aux spécifications des mécanismes de sécurité du SDC-D.

Cette évaluation doit permettre de s'assurer que les documents analogiques collectés ont été correctement traités, restitués, transférés ou détruits et que les documents numériques ont été correctement créés, stockés de manière temporaire, restitués, transférés ou supprimés.

L'organisation doit en particulier démontrer que le niveau général de sécurité du SDC-D est conforme aux bonnes pratiques en la matière, notamment en démontrant que les actifs critiques du SDC-D et les mécanismes de sécurité, comme par exemple les mécanismes cryptographiques, ont été évalués et certifiés par des organismes indépendants spécialisés dans ce type de revues ou qu'ils sont conformes à des normes ou des référentiels reconnus et qu'ils sont utilisés conformément aux bonnes pratiques en la matière.

NOTE : La Norme ETSI TS 102 176-1 [8] énumère des algorithmes cryptographiques et recommande une durée de validité de leur utilisation.

Tout changement significatif programmé (modification d'actifs techniques critiques, suppression d'un mécanisme critique de sécurité) du SDC-D doit être justifié et faire l'objet d'une approbation préalable des clients (internes ou externes à l'organisation) du processus de dématérialisation et qui sont impactés par ce changement.

La description détaillée du système de dématérialisation SDC-D et les spécifications des mécanismes de sécurité du SDC-D doivent être revues par le responsable du processus de dématérialisation de manière régulière (au moins une fois par an), et suite à une modification significative du SDC-D et du processus de dématérialisation.

12.8.2 *Utilisation correcte du système de dématérialisation SDC-D* (mesure de sécurité additionnelle à la Norme internationale ISO/IEC 27002:2013)

12.8.2.1 Mesure

Les procédures d'administration, d'opérations et de sécurité du système de dématérialisation SDC-D et d'exploitation du processus de dématérialisation doivent être définies, mises en œuvre et respectées par le personnel concerné (de l'organisation et des fournisseurs).

Ces procédures doivent être considérées dans la définition et la mise en œuvre des projets de dématérialisation.

Exigences de mise en œuvre

12.8.2.2 Règles à suivre pour l'exécution des activités d'administration, d'opérations et de sécurité du système de dématérialisation SDC-D

L'organisation doit définir et documenter les règles à suivre pour l'exécution des activités d'administration, d'opérations et de sécurité du système de dématérialisation SDC-D dans des procédures, dont les suivantes :

a) gestion des accès au SDC-D et des privilèges associés aux comptes du SDC-D.

b) gestion des fonctionnalités d'administration, d'opérations et de sécurité du SDC-D et instructions pour les exécuter.

c) gestion de la configuration du SDC-D.

d) instructions du fonctionnement du SDC-D en mode dégradé, de son redémarrage et de sa récupération.

e) gestion des mécanismes de surveillance du SDC-D.

f) gestion des journaux d'événements du SDC-D et instructions pour leur exploitation.

g) gestion des mécanismes cryptographiques de sécurité du SDC-D, comme les suivants :

1. mécanismes d'authentification et de signature des utilisateurs du SDC-D.

2. protocoles sécurisés de transmission d'informations et de documents numériques.

3. mécanismes d'intégrité des documents numériques et des journaux d'événements.

NOTE : Ces procédures de gestion doivent également adresser le remplacement des mécanismes cryptographiques pour lesquelles des vulnérabilités sont détectées. Leur remplacement ne doit pas altérer le fonctionnement et l'intégrité du SDC-D.

h) gestion des mécanismes de contrôle régulier d'intégrité du SDC-D.

NOTE : L'organisation doit s'assurer que l'intégrité du fonctionnement du SDC-D, des documents analogiques et numériques gérés par le SDC-D soit vérifiée de manière régulière, suite à une modification significative du SDC-D et du processus de dématérialisation.

Pour les cas de perte d'intégrité du fonctionnement du SDC-D ou de documents analogiques ou numériques gérés par le SDC-D, l'organisation doit documenter dans une procédure les instructions précisant à partir de quel moment les procédures de gestion d'incidents doivent être activées, la manière dont les procédures de restauration doivent être utilisées et à quel moment les clients (internes ou externes à l'organisation) concernés et l'ILNAS doivent être avertis de cet incident.

i) gestion des mécanismes de vérification de l'adéquation du nombre de documents analogiques (ou du nombre de pages composant ces documents) numérisés.

j) gestion des mécanismes de vérification du contenu des documents numériques.

k) gestion des mécanismes de destruction des documents analogiques et de suppression de documents numériques gérées par le SDC-D.

l) gestion des supports de stockage du SDC-D, de leur remplacement et de leur mise au rebut.

m) gestion des sauvegardes du SDC-D et des sauvegardes des documents numériques gérés par le SDC-D et de leur restauration respective.

n) gestion de la continuité et de la reprise du SDC-D même en cas de désastre.

o) gestion des changements du SDC-D.

p) gestion des incidents pouvant impacter le SDC-D.

q) maintenance des actifs techniques avec gestion du support des fournisseurs en cas de dysfonctionnement du SDC-D.

r) gestion des métadonnées de description et de contrôle associées aux documents numériques.

Ces procédures doivent être mises en œuvre et respectées par le personnel concerné (de l'organisation et des fournisseurs).

12.8.2.3 Règles à suivre dans le cadre de l'exécution des activités de dématérialisation

Les règles à suivre dans le cadre de l'exécution des activités des processus suivants sous-jacents au processus de dématérialisation doivent être documentées :

a) collecte des documents analogiques.

b) création et stockage temporaire des documents numériques.

c) stockage temporaire des documents analogiques.

d) restitution, transfert, destruction éventuelle des documents analogiques et suppression des documents numériques.

NOTE : Il convient que la destruction des documents analogiques et la suppression des documents numériques gérés par l'organisation pour le compte d'un client (interne ou externe à l'organisation) soit uniquement réalisée à compter de la confirmation par écrit de la réception des documents numériques par le client et que ces documents constituent la reproduction fidèle des documents analogiques originaux.

12.8.2.4 Exemples

Voici des exemples de règles à suivre dans le cadre de l'exécution de certaines activités de processus sous-jacents au processus de dématérialisation :

a) activité « déplacement du personnel de l'organisation vers le lieu de collecte des documents analogiques des clients ».

Il convient en particulier de respecter les règles suivantes :

1. déplacement en équipe composée au minimum de 2 personnes.

2. création d'un bordereau de récupération comprenant les spécifications liées aux documents analogiques à collecter, comme par exemple le nombre de cartons ou de documents, le poids des cartons et la nature des documents analogiques.

3. identification de la personne du client soumettant les documents analogiques pour vérifier qu'elle figure bien sur la liste des personnes habilitées par le client à effectuer cette tâche.

4. contrôle que les documents analogiques à collecter correspondent bien aux spécifications mentionnées sur le bordereau de récupération.

b) activité « collecte effective des documents analogiques ».

Il convient en particulier de respecter les règles suivantes :

1. chargement des documents analogiques dans des containers sécurisés et localisés dans le véhicule de transport.

2. scellement des containers.

3. approbation par la personne du client soumettant les documents analogiques de leur collecte adéquate.

c) activité « conversion des documents analogiques en documents numériques »

Il convient en particulier de respecter les règles suivantes:

1. préparation des documents analogiques à dématérialiser en les regroupant par lot et assignement d'un identifiant unique à chaque document et à chaque lot.

2. utilisation d'un mécanisme d'authentification appropriée et sécurisée par l'utilisateur du SDC-D afin d'accéder aux fonctionnalités du SDC-D pour effectuer la dématérialisation des documents analogiques.

3. numérisation effective des documents analogiques contenus dans un lot avec l'insertion éventuelle de métadonnées de description et de contrôle.

   NOTE : Il convient que la numérisation des documents analogiques contenus dans un lot ne démarre pas avant que le précédent lot de documents analogiques soit traité dans son entièreté, à moins que l'intégrité de la conversion en documents numériques des documents analogiques de ce précédent lot puisse être conservée et soit évaluable par un tiers pouvant attester de cette préservation d'intégrité.

4. assignement d'un identifiant unique comme par exemple, une empreinte digitale à chaque document numérique résultant de la numérisation d'un document analogique.

5. inventaire du nombre et des types d'erreurs survenues pendant le traitement du lot.
   Si une erreur nécessite le retrait de documents analogiques, cette information doit être enregistrée dans le SDC-D comme une anomalie avec l'identifiant de chaque document concerné par cette erreur.

6. vérification de l'adéquation du nombre de documents analogiques en entrée (ou du nombre de pages composant ces documents) avec le nombre de documents (ou de pages) en sortie (numériques et analogiques rejetés) pour le lot.

   Il convient que cette vérification soit effectuée de manière automatique par le SDC-D ou de manière manuelle par l'utilisateur du SDC-D responsable de la numérisation de ce lot.

7. vérification du contenu des documents numériques résultants de la numérisation de documents analogiques pour s'assurer de la reproduction conforme à l'original.

   Il convient que cette vérification soit effectuée de manière automatique par le SDC-D ou de manière manuelle par l'utilisateur du SDC-D responsable de la numérisation de ce lot.

   Il convient de s'assurer de l'application du principe des quatre yeux si cette vérification est exclusivement effectuée manuellement, à savoir que cette vérification doit être effectuée par l'utilisateur du SDC-D responsable de la numérisation du lot, sous la supervision d'une tierce personne habilitée à cette tâche et pouvant attester de la reproduction fidèle du contenu des documents analogiques.

   Il convient de définir les conditions d'échantillonnage de cette vérification en fonction de la nature des documents, des besoins internes à l'organisation ou des clients et si une destruction des documents analogiques est programmée.

8. génération d'une preuve énumérant de manière claire et explicite toutes les règles suivies pendant la dématérialisation des documents analogiques, les activités manuelles effectuées par l'utilisateur du SDC-D responsable du lot, les événements du SDC-D survenus pendant la numérisation des documents analogiques et les erreurs identifiées lors du traitement du lot.

9. validation par écrit de cette preuve par l'utilisateur du SDC-D et du tiers impliqué dans la vérification manuelle du contenu des documents numériques en utilisant un dispositif sécurisé de création de signature et un certificat électronique qualifié répondant aux exigences définies par l'Union européenne en la matière.

10. clôture du lot de documents analogiques à numériser et traitement des anomalies (retrait de documents à numériser) selon les procédures de gestion des incidents du SDC-D.

Tout changement significatif (changement d'instructions d'exploitation des journaux d'événements, modification de la gestion des sauvegardes et de leur restauration) des procédures d'administration, d'opérations et de sécurité du système de dématérialisation SDC-D et des procédures d'exploitation du processus de dématérialisation doit être justifié et faire l'objet d'une approbation préalable des clients (internes ou externes à l'organisation) du processus de dématérialisation et qui sont impactés par ce changement.

12.8.2.5 Exigences par rapport aux règles

Les règles définies dans ces procédures doivent :

a) être mises en œuvre et respectées par le personnel concerné (de l'organisation et des fournisseurs).

b) être conformes aux lois et aux règlements en vigueur au Luxembourg.

c) respecter les bonnes pratiques en la matière définies dans des normes et des référentiels reconnus.

d) soient revues par le responsable du processus de dématérialisation de manière régulière (au moins une fois par an), suite à une modification significative du SDC-D et du processus de dématérialisation.

L'exécution des procédures d'administration, d'opérations et de sécurité du système de dématérialisation SDC-D et des procédures d'exploitation du processus de dématérialisation doit être évaluable par un tiers pouvant attester de la conformité des activités effectuées par le personnel concerné par rapport aux règles définies dans ces procédures pour s'assurer que les documents analogiques ont été correctement collectés, utilisés, stockés, restitués, transférés ou détruits et que les documents numériques ont été correctement créés, stockés, exploités, restitués ou supprimés.

Les preuves de la conformité des activités effectuées par le personnel concerné par rapport aux politiques et aux procédures liées au processus de dématérialisation exécuté par l'organisation doivent être conservées en utilisant des supports de stockage pérennes pour une conservation appropriée aussi longtemps que nécessaire.

12.8.2.6 Preuves

Les preuves suivantes doivent être conservées :

a) bordereaux de récupération ou de livraison de documents analogiques.

b) rapports d'activités des utilisateurs du SDC-D.

c) rapports de mises à jour du SDC-D, d'incidents ou de changements liés au SDC-D.

d) rapports de revue des journaux d'événements du SDC-D.

12.8.2.7 Information contenue dans la preuve

Une preuve liée aux activités effectuées par le personnel concerné doit contenir en particulier les informations suivantes :

a) Auteur(s) des activités effectuées.

b) Date(s) et heure(s) des activités effectuées.

c) Lieu(x) des activités effectuées.

d) Actif(s) utilisé(s) pour la réalisation de ces activités.

e) Descriptif des activités effectuées.

f) Problèmes ou erreurs rencontrés pendant la réalisation de ces activités.

g) Le client (interne ou externe).

12.8.2.8 Gestion des preuves

L'organisation doit définir, et documenter dans une procédure et mettre en œuvre une gestion adéquate des preuves :

a) du fonctionnement du SDC-D (voir 10.11.1).

b) des activités effectuées par le personnel concerné (voir 10.11.1 et 10.11.2).

Autres informations

Si des règles définies dans le cadre d'un projet de dématérialisation sont contraires à celles actuellement mises en œuvre par l'organisation en matière d'administration, d'opérations et de sécurité du système de dématérialisation SDC-D et en matière d'exécution des activités des processus sous-jacents au processus de dématérialisation, il convient d'effectuer une analyse de risques liée à ces règles afin d'identifier et d'évaluer les risques pouvant impacter l'organisation.

Il convient que les options adoptées pour les risques évalués ainsi que le plan de traitement du risque soient définis, documentés et approuvés par les parties prenantes.

Si les risques évalués sont trop élevés et ne peuvent pas être mitigés à un niveau acceptable pour l'organisation, il convient de reconsidérer le projet de dématérialisation.

12.9 *Conservation* (objectif de sécurité additionnel à la Norme internationale ISO/IEC 27002:2013)

Objectif : assurer la gestion correcte et sécurisée des documents numériques et des archives numériques dans le cadre du processus de conservation.

L'organisation doit intégrer les principes d'authenticité, de fiabilité et d'exploitation dans la définition, la mise en exploitation et l'utilisation de son système de conservation SDC-C.

12.9.1 *Système de conservation SDC-C* (mesure de sécurité additionnelle à la Norme internationale ISO/IEC 27002:2013)

12.9.1.1 Mesure

L'organisation doit pouvoir démontrer que le système de conservation SDC-C est composé d'actifs techniques et de mécanismes de sécurité :

a) répondant aux besoins des clients (internes ou externes à l'organisation) du processus de conservation.

b) permettant de garantir l'authenticité, la fiabilité et l'exploitation des documents numériques et des archives numériques gérés par ce système.

NOTE : Un système de conservation SDC-C est un système composé d'un ensemble d'actifs techniques permettant le stockage temporaire des documents numériques en vue de leur archivage, leur conversion en archives numériques, leur suppression et la conservation des archives numériques aussi longtemps que nécessaire, leur exploitation, leur restitution partielle ou totale, leur transfert et leur suppression.

Exigences de mise en œuvre

12.9.1.2 Description détaillée du système de conservation SDC-C

Une description détaillée du système de conservation SDC-C doit être définie et maintenue en :

a) identifiant et en documentant les actifs techniques supportant les processus sous-jacents au processus de conservation, à savoir :

    1. la collecte des documents numériques.
    2. la création et la conservation des archives numériques.
    3. la restitution, le transfert et la suppression des archives numériques.

b) identifiant, en évaluant et en documentant de manière régulière les possibilités techniques du SDC-C, comme par exemple les suivantes :

1. nombre maximum de documents numériques ou poids total maximum de documents numériques pouvant être transmis en une seule fois au SDC-C.
2. débit de transmission des documents numériques vers le SDC-C.
3. délai de réponse du SDC-C.
4. fréquence d'émissions des lots de documents numériques à archiver électroniquement par le SDC-C.
5. poids maximum du document numérique pouvant être transmis au SDC-C en vue de son archivage.
6. protocoles sécurisés de transmission d'informations, de documents numériques et d'archives numériques, comme par exemple SFTP, TLS, PPP, L2TP et IPSec.

NOTE : L'identification et l'évaluation des possibilités techniques du SDC-C sont indispensables pour assurer sa conformité avec les besoins des clients (internes ou externes à l'organisation).

c) identifiant et en évaluant de manière régulière les capacités techniques du SDC-C et en les documentant.

Le responsable du processus de conservation doit revoir les capacités techniques du SDC-C de manière régulière (au moins une fois par an), et suite à une modification significative du SDC-C et suite à un changement :

1. impactant le fonctionnement de l'organisation ou la gestion opérationnelle du SDC-C.
2. issu des besoins des clients (intégration d'un nouveau projet client, modification d'un projet client existant).
3. de nature légale et réglementaire ayant un impact sur le processus de conservation.

NOTE : La connaissance des capacités techniques du SDC-C est indispensable à l'organisation pour assurer la disponibilité du SDC-C, la définition adéquate des projets de conservation, la planification appropriée des ressources de l'organisation en matière de conservation et la projection des futurs dimensionnements du SDC-C.

12.9.1.3 Mécanismes de sécurité du système de conservation SDC-C

L'organisation doit établir et de documenter les mécanismes de sécurité du système de conservation SDC-C permettant d'assurer l'authenticité, la fiabilité et l'exploitation des documents numériques et des archives numériques gérés par ce système.

En particulier les mécanismes de sécurité suivants doivent être établis :

a) mécanismes de gestion des accès au SDC-C.

Les accès aux actifs techniques du SDC-C, aux documents numériques et aux archives numériques gérés par le SDC-C doivent être protégés en :

1. s'assurant que les conditions d'accès à ces actifs, à ces documents et ces archives s'appliquent à toute personne physique et à tout actif tentant d'y accéder.
2. établissant une gestion adéquate des comptes des utilisateurs autorisés à accéder au SDC-C et des comptes techniques des actifs techniques du SDC-C, avec une capacité de révocation immédiate de ces comptes.

   Un compte unique doit être attribué à un utilisateur et à un actif de manière à pouvoir identifier sans ambigüité les activités et les actions système effectuées.

3. établissant des mécanismes d'authentification appropriés et sécurisés pour les comptes des utilisateurs autorisés et les comptes techniques des actifs techniques du SDC-C.

b) mécanismes de gestion des privilèges.

Une gestion des privilèges pour l'ensemble des comptes des utilisateurs du SDC-C et des comptes techniques des actifs techniques du SDC-C doit être établie.

En particulier l'organisation doit s'assurer d'une séparation effective des activités d'administration, d'opérations et de sécurité du SDC-C en établissant des profils de privilèges pour les comptes des utilisateurs autorisés à accéder au SDC-C de manière à réduire les risques de conflits d'intérêts et d'accès non autorisés au SDC-C, aux documents et aux archives gérés par ce système.

Il convient d'attribuer à un utilisateur du SDC-C un seul des profils de privilèges suivants. Pour des raisons liées au fonctionnement de l'organisation, il est toutefois acceptable qu'un utilisateur du SDC-C dispose à la fois du profil de privilèges d'administration et du profil de privilèges d'opérations.

1. profil de privilèges d'administration
   Il convient qu'un utilisateur disposant de ce profil puisse créer, modifier ou supprimer des comptes du SDC-C, et définir, modifier ou supprimer des paramètres associés à la gestion opérationnelle du SDC-C.

   Il convient que cet utilisateur ne puisse pas accéder aux éléments suivants :

   a. paramètres de sécurité du SDC-C, comme par exemple les conditions d'authentification des utilisateurs et des actifs techniques du SDC-C.

   b. paramètres de surveillance et de journalisation des évènements du SDC-C.

   c. journaux d'événements du SDC-C.

   d. documents numériques et archives numériques gérés par le SDC-C.

2. profil de privilèges d'opérations
   Il convient qu'un utilisateur disposant de ce profil puisse uniquement :

   a. exécuter les activités d'opérations du SDC-C.

   b. accéder aux documents numériques et archives numériques gérés par le SDC-C et les traiter dans le cadre du processus de conservation.
      Il convient de s'assurer que toute conversion d'archives numériques dans un format autre que son format initial et que toute modification du calendrier de suppression d'archives numériques conservées nécessitent l'approbation de 2 utilisateurs disposant de ce profil et du client de ces archives.
      Il convient d'interdire toute autre manipulation pouvant modifier ou supprimer les archives numériques conservées.

c. assigner à un profil de privilèges d'écriture et de lecture les éléments suivants auxquels un utilisateur disposant de ce profil aura accès:

i. un répertoire système du SDC-C où des documents numériques peuvent être déposés en vue de leur archivage.

ii. des archives numériques.

3. profil de privilèges de sécurité

Il convient qu'un utilisateur disposant de ce profil puisse uniquement :

a. définir, modifier ou supprimer les paramètres de sécurité du SDC-C, comme par exemple les conditions d'authentification des utilisateurs du SDC-C.

b. définir, modifier ou supprimer les paramètres de surveillance du SDC-C et de génération de journaux d'événements du SDC-C.

c. accéder aux journaux d'événements du SDC-C en vue de leur exploitation.

4. profils de privilèges d'écriture et de lecture

Il convient de définir un profil de privilèges d'écriture et de lecture pour les comptes du personnel d'un client et qui est autorisé à accéder à distance aux éléments suivants du SDC-C :

a. un répertoire système du SDC-C où des documents numériques peuvent être déposés en vue de leur archivage.

b. des archives numériques (lecture seule).

Il convient que ce profil limite l'accès exclusivement à ce répertoire et à ces archives, qui auront été au préalable assignés à ce profil par un utilisateur du SDC-C disposant d'un profil de privilèges d'opérations.

Il convient de s'assurer que toute modification ou suppression des archives numériques créées qui n'était pas programmée lors de la définition du projet de conservation nécessite l'approbation de deux utilisateurs disposant du profil de privilèges d'opérations.

L'organisation doit pouvoir démontrer que les profils de privilèges établis pour l'ensemble des comptes des utilisateurs du SDC-C et des comptes techniques des actifs techniques du SDC-C **respectent le principe de séparation effective des activités d'administration, d'opérations et de sécurité du SDC-C**.

c) mécanismes de surveillance de manière à identifier, à enregistrer et à centraliser dans des journaux tous les événements en lien avec le SDC-C, en particulier :

1. l'ensemble des activités effectuées par les comptes des utilisateurs du SDC-C, incluant les activités effectuées hors de conditions normales d'utilisation du SDC-C, comme par exemple :

a. les tentatives de connexion d'utilisateurs hors des heures normales de bureau.

b. les activités effectuées par les utilisateurs dans un laps de temps plus court que la normale, pouvant conduire à suspecter qu'elles sont réalisées par des actifs techniques et non des personnes physiques.

c. la duplication de sessions utilisateurs.

2. les événements système des actifs du SDC-C.

3. les événements liés aux documents et archives numériques traités par le SDC-C.

4. les erreurs et dysfonctionnements des actifs du SDC-C.

5. les événements du SDC-C liés à la génération de journaux d'événements.

Les journaux d'événements générés doivent être exploitables, conservés et protégés contre toute manipulation et suppression non autorisées pour assurer une traçabilité aussi longtemps que nécessaire de tous les événements enregistrés par ces mécanismes de surveillance.

d) mécanismes cryptographiques de sécurité devant assurer :

1. une authentification appropriée et sécurisée protégeant l'accès aux actifs techniques du SDC-C, aux documents numériques et aux archives numériques gérés par le SDC-C.

Un dispositif sécurisé doit être utilisé, comme par exemple une carte à puce ou une clé USB cryptographique contenant un certificat électronique d'authentification, un token d'authentification ou des techniques de biométrie pour s'assurer de l'authentification sécurisée d'un utilisateur aux actifs techniques du SDC-C, aux documents numériques et aux archives numériques gérés par le SDC-C.

Il convient d'utiliser un dispositif de filtrage d'adresses IP associé à un moyen cryptographique, comme par exemple un certificat SSL, pour s'assurer de l'authentification sécurisée d'un actif technique du SDC-C aux autres actifs du SDC-C, aux documents numériques et aux archives numériques gérés par le SDC-C.

2. une signature sécurisée des utilisateurs du SDC-C.

Un dispositif sécurisé doit être utilisé, pour permettre :

a. à un utilisateur du SDC-C de signer électroniquement des rapports d'activités d'administration, d'opérations et de sécurité du SDC-C de manière à s'assurer de l'authenticité des activités effectuées.

b. à une personne de l'organisation de signer électroniquement les transmissions d'informations, de documents numériques et d'archives numériques à destination des clients (internes ou externes à l'organisation) et des autorités compétentes de manière à s'assurer de l'authenticité des envois.

Le dispositif sécurisé de création de signature électronique et le certificat électronique qualifié utilisés doit répondre aux exigences définies par l'Union européenne en la matière.

Il convient également d'utiliser des formats de signatures électroniques comme par exemple CAdES [5], XAdES [6] et PAdES [7] pour maintenir une pérennité de la signature électronique, des informations, des documents numériques et des archives numériques attachés à cette signature.

3. une transmission sécurisée d'informations et de documents numériques.

   Un protocole sécurisé (SFTP, TLS, PPP, L2TP et IPSec, …), doit être utilisé pour sécuriser la transmission d'informations, de documents numériques et d'archives numériques entre les éléments suivants :

   a. les actifs techniques du SDC-C, même pour ceux appartenant à un même réseau.

   b. les parties concernées par le processus de conservation comme l'organisation, les clients (internes ou externes à l'organisation) et les autorités compétentes.

4. une intégrité des documents numériques collectés par le SDC-C et des archives numériques générées par le SDC-C pour s'assurer que ces documents sont correctement stockés, traités et supprimés et que ces archives sont correctement crées, exploitées, restituées, transférés ou supprimées.

   Il convient que pour chaque document numérique à archiver son empreinte digitale soit calculée par l'émetteur de ce document et transmise de manière sécurisée à l'organisation qui vérifiera l'intégrité du document numérique reçu en calculant et en obtenant une empreinte digitale identique à celle transmise par l'émetteur du document.

   Cette empreinte doit par la suite être :

   a. associée à l'archive numérique créée à partir du document numérique en tant que métadonnée de contrôle.

   b. utilisée comme un identifiant unique de l'archive numérique lors de sa conservation, de son exploitation, de sa restitution ou de son transfert pour maintenir son intégrité durant l'exécution du processus de conservation.

   NOTE : L'utilisation de 2 empreintes digitales calculées à partir de 2 algorithmes de calcul d'empreintes digitales différents pour identifier des archives numériques gérées par le SDC-C peut apporter un niveau d'assurance supplémentaire dans la pérennité de l'intégrité des archives numériques en réduisant les risques liés à l'obsolescence cryptographique.

5. une intégrité dans le temps des journaux d'événements.

   Il convient en particulier de s'assurer de :

   a. l'établissement d'un schéma de liaison pour lier les évènements enregistrés d'un journal entre eux permettant de détecter toute suppression d'événements survenus par le passé.

   b. l'horodatage régulier, par exemple une fois par jour, des journaux d'événements par une autorité d'horodatage qualifiée.

e) mécanisme de détection et de suppression de codes malveillants contenus dans des documents numériques collectés en vue de leur archivage.

Au minimum un antivirus doit être utilisé pour vérifier que tous les documents numériques collectés en vue de leur archivage ne contiennent pas de codes malveillants, comme des virus, des chevaux de Troie et des vers de réseau.

Cet antivirus doit être utilisé dès la réception par le SDC-C des documents numériques et avant le démarrage du processus de création des archives numériques.

NOTE : L'emploi de deux antivirus différents doit apporter un niveau de sécurité supplémentaire pour lutter contre les codes malveillants.

f) mécanismes de contrôle régulier de l'intégrité du SDC-C pour s'assurer que :

1. le fonctionnement du SDC-C n'a pas été altéré suite à des :

a. opérations de maintenance ou des mises à jour.

b. remplacements d'actifs du SDC-C comme par exemple la plateforme d'archivage électronique ou des composants de ces actifs comme par exemple les supports de stockage.

2. les fichiers de configurations du SDC-C n'ont pas été modifiés de manière non autorisée.

3. l'intégrité des éléments suivants est préservée :

a. documents numériques stockés.

b. archives numériques conservées et métadonnées associées.

c. journaux d'événements.

g) mécanismes de suppression sécurisée des documents et archives numériques, comme par exemple une réécriture multiple sur les informations ne permettant plus de les retrouver en l'état.

h) mécanismes de conversion (si nécessaire) des archives numériques dans un format différent de leur format original.

12.9.1.4 Preuves de la conformité

Les preuves de la conformité du fonctionnement du SDC-C et des activités effectuées par le personnel concerné par rapport aux politiques et aux procédures liées au processus de conservation exécuté par l'organisation doivent être conservés en utilisant des supports de stockage pérennes pour une conservation appropriée aussi longtemps que nécessaire.

Les preuves suivantes doivent être conservées :

a) journaux d'événements du SDC-C.

b) les événements liés aux documents et archives numériques traités par le SDC-C.

c) rapports d'activités des utilisateurs du SDC-C.

d) rapports de mises à jour du SDC-C, d'incidents ou de changements liés au SDC-C.

e) jetons d'horodatage générés dans le cadre du fonctionnement du SDC-C et des activités des utilisateurs du SDC-C.

f) signatures électroniques des utilisateurs du SDC-C.

NOTE : L'organisation doit pouvoir démontrer la validité de la signature électronique d'un utilisateur du SDC-C aussi longtemps que nécessaire en démontrant qu'au moment de la signature électronique le certificat électronique qualifié de l'utilisateur était valide et issu d'une autorité de certification reconnue.

Plusieurs techniques sont possibles à cette fin comme par exemple les suivantes :

1. utilisation du protocole de vérification en ligne de certificats (OCSP) de l'autorité de certification émettrice du certificat électronique qualifié.

2. horodatage du rapport d'activités signé et récupération de la liste de révocation des certificats (CRL) publiée régulièrement par l'autorité de certification émettrice du certificat électronique qualifié.

Il convient d'utiliser des supports de stockage pérenne pour une conservation appropriée des archives numériques aussi longtemps que nécessaire.

12.9.1.5 Conformité par rapport aux lois et aux règlements en vigueur au Luxembourg

a) le système de conservation SDC-C et les mécanismes de sécurité associés doivent être conformes aux lois et aux règlements en vigueur au Luxembourg.

b) le fonctionnement du SDC-C et celui des mécanismes de sécurité du SDC-C doivent être évaluables par un tiers pouvant attester de la conformité de leur fonctionnement et des activités effectuées par le personnel concerné par rapport à la description détaillée du système de conservation SDC-C et par rapport aux spécifications des mécanismes de sécurité du SDC-C.

Cette évaluation doit permettre de s'assurer que les documents numériques collectés ont été correctement conservés sous la forme d'archives numériques et par la suite supprimés, et que ces archives ont été correctement exploitées, restituées, transférées ou supprimées.

L'organisation doit en particulier pouvoir démontrer que le niveau général de sécurité du SDC-C est conforme aux bonnes pratiques en la matière, notamment en démontrant que les actifs critiques du SDC-C et les mécanismes de sécurité, comme par exemple les mécanismes cryptographiques, ont été évalués et certifiés par des organismes indépendants spécialisés dans ce type de revues ou qu'ils sont conformes à des normes ou des référentiels reconnus et qu'ils sont utilisés conformément aux bonnes pratiques en la matière.

NOTE : La Norme ETSI TS 102 176-1 [8] énumère des algorithmes cryptographiques et recommande une durée de validité de leur utilisation.

Tout changement significatif programmé (modification d'actifs techniques critiques, suppression d'un mécanisme critique de sécurité) du SDC-C doit être justifié et faire l'objet d'une approbation préalable des clients (internes ou externes à l'organisation) du processus de conservation et qui sont impactés par ce changement.

La description détaillée du système de conservation SDC-C et les spécifications des mécanismes de sécurité du SDC-C doivent être revues par le responsable du processus de conservation de manière régulière (au moins une fois par an) suite à une modification significative du SDC-C et du processus de conservation.

12.9.2 *Utilisation correcte du* système *de conservation SDC-C* (mesure de sécurité additionnelle à la Norme internationale ISO/IEC 27002:2013)

12.9.2.1 Mesure

Les procédures d'administration, d'opérations et de sécurité du système de conservation SDC-C et d'exploitation du processus de conservation doivent être définies, mises en œuvre et respectées par le personnel concerné (de l'organisation et des fournisseurs).

Ces procédures doivent être considérées dans la définition et la mise en œuvre des projets de conservation.

Exigences de mise en œuvre

12.9.2.2 Règles à suivre pour l'exécution des activités d'administration, d'opérations et de sécurité du système de conservation SDC-C

Les règles à suivre pour l'exécution des activités d'administration, d'opérations et de sécurité du système de conservation SDC-C, doivent être définies et de documentées dans des procédures, dont les suivantes :

a) gestion des accès au SDC-C et des privilèges associés aux comptes du SDC-C.

b) gestion des fonctionnalités d'administration, d'opérations et de sécurité du SDC-C et instructions pour les exécuter.

c) gestion de la configuration du SDC-C.

d) instructions du fonctionnement du SDC-C en mode dégradé, de son redémarrage et de sa récupération.

e) gestion des mécanismes de surveillance du SDC-C.

f) gestion des journaux d'événements du SDC-C et instructions pour leur exploitation.

g) gestion des mécanismes cryptographiques de sécurité du SDC-C, comme les suivants :

    1. mécanismes d'authentification et de signature des utilisateurs du SDC-C.

    2. protocoles sécurisés de transmission d'informations, de documents numériques et d'archives numériques.

    3. mécanismes d'intégrité des documents numériques, des archives numériques et des journaux d'événements.

NOTE : Il convient que ces procédures de gestion adressent également le remplacement des mécanismes cryptographiques pour lesquelles des vulnérabilités sont détectées. Leur remplacement ne doit pas altérer le fonctionnement ni l'intégrité du SDC-C.

h) gestion des mécanismes de détection et de suppression de codes malveillants.

NOTE : En cas de collecte par le SDC-C de documents numériques contenant des codes malveillants, l'organisation doit :

1. avertir l'émetteur de ces documents dans les plus brefs délais afin qu'il mette en place des actions correctives appropriées.
2. supprimer le code malveillant en utilisant des outils de détection et de suppression des codes malveillants (antivirus). S'il s'avère impossible de supprimer le code malveillant, le document doit être supprimé.

i) gestion des mécanismes de contrôle régulier d'intégrité du SDC-C.

L'organisation doit s'assurer que l'intégrité du fonctionnement du SDC-C, des documents numériques et des archives numériques gérés par le SDC-C soit vérifiée de manière régulière, suite à une modification significative du SDC-C et du processus de conservation.

Pour les cas de perte d'intégrité du fonctionnement du SDC-C, de documents numériques et d'archives numériques gérés par le SDC-C, l'organisation doit documenter dans une procédure les instructions précisant à partir de quel moment les procédures de gestion d'incidents doivent être activées, la manière dont les procédures de restauration doivent être utilisées et à quel moment les clients (internes ou externes à l'organisation) concernés et l'ILNAS doivent être avertis de cet incident.

j) gestion des mécanismes de suppression des documents numériques et des archives numériques gérées par le SDC-C.

k) gestion des supports de stockage du SDC-C, de leur remplacement et de leur mise au rebut.

l) gestion des sauvegardes du SDC-C, des sauvegardes des documents numériques et des archives numériques gérés par le SDC-C et de leur restauration respective.

m) gestion de la continuité et de la reprise du SDC-C même en cas de désastre.

n) gestion des changements du SDC-C.

o) gestion des incidents pouvant impacter le SDC-C.

p) maintenance des actifs techniques avec gestion du support des fournisseurs en cas de dysfonctionnement du SDC-C.

q) gestion des métadonnées de description et de contrôle associées aux archives numériques.

Ces procédures doivent être mises en œuvre et respectées par le personnel concerné (de l'organisation et des fournisseurs).

12.9.2.3 Règles à suivre dans le cadre de l'exécution des activités de conservation

L'organisation doit définir et documenter dans des procédures les règles à suivre dans le cadre de l'exécution des activités des processus suivants sous-jacents au processus de conservation :

a) la collecte des documents numériques.

b) la création et la conservation des archives numériques.

NOTE : La conversion d'une archive numérique dans un format différent de son format initial ne doit s'appliquer que sur demande écrite du client (interne à l'organisation et externe) concerné par cette archive. Cette conversion est optionnelle et n'est pas obligatoirement proposée par l'organisation. Une identification et une évaluation des risques en matière de perte d'authenticité, de fiabilité et d'exploitation de l'archive numérique concernée doit été réalisée. Les risques évalués doivent être acceptés par le client concerné.

c) la restitution, le transfert et la suppression des archives numériques.

La suppression d'un document numérique collecté par l'organisation dans le cadre du processus de conservation doit uniquement être réalisée à compter de sa conservation effective en tant qu'archive numérique par le SDC-C.

L'organisation doit notifier le client d'une suppression programmée d'une archive numérique du client si un calendrier de suppression spécifique à cette archive a été rédigé lors de la définition du projet de conservation.

En cas d'absence de calendrier de suppression pour une archive numérique, l'organisation doit demander au préalable au client l'autorisation de la supprimer.

12.9.2.4 Exemples

Voici des exemples de règles à suivre pour certaines activités des processus sous-jacents :

a) Activité « collecte des documents numériques ».

Exemples de règles à suivre pour cette activité :

1. vérification du nombre de documents numériques collectés en vue de leur archivage électronique et de leur intégrité par rapport aux informations transmises par le client.
2. surveillance de la remontée d'alertes du SDC-C pour s'assurer que les documents numériques collectés ne contiennent pas de codes malveillants.
3. inventaire du nombre et des types d'erreurs survenues pendant la collecte des documents numériques.
   Si une erreur nécessite le retrait de documents numériques, cette information doit être enregistrée dans le SDC-C comme une anomalie avec l'identifiant de chaque document concerné par cette erreur.
4. génération par le SDC-C d'une preuve attestant de la collecte effective des documents numériques en les énumérant avec leur identifiant associé, en mentionnant la date et l'heure de leur collecte par le SDC-C et en signalant les erreurs survenues pendant leur collecte.
5. validation par écrit de cette preuve par un utilisateur du SDC-C en utilisant un dispositif sécurisé de création de signature et un certificat électronique qualifié répondant aux exigences définies par l'Union européenne en la matière.
6. horodatage de la preuve signée par une autorité d'horodatage qualifiée.
7. transmission de la preuve signée et horodatée au client par l'utilisation d'un protocole sécurisé de transmission d'information.

Tout changement significatif (changement d'instructions d'exploitation des journaux d'événements, modification de la gestion des sauvegardes et de leur restauration) des procédures d'administration, d'opérations et de sécurité du système de conservation SDC-C et des procédures d'exploitation du processus de conservation doit être justifié et faire l'objet d'une approbation préalable des clients (internes ou externes à l'organisation) du processus de conservation et qui sont impactés par ce changement.

12.9.2.5 Exigences par rapport aux règles

Les règles définies dans ces procédures doivent :

a) être mises en œuvre et respectées par le personnel concerné (de l'organisation et des fournisseurs).

b) être conformes aux lois et aux règlements en vigueur au Luxembourg.

c) respecter les bonnes pratiques en la matière définies dans des normes et des référentiels reconnus.

d) être revues par le responsable du processus de conservation de manière régulière (au moins une fois par an), suite à une modification significative du SDC-C et du processus de conservation.

L'exécution des procédures d'administration, d'opérations et de sécurité du système de conservation SDC-C et des procédures d'exploitation du processus de conservation doit être évaluable par un tiers pouvant attester de la conformité des activités effectuées par le personnel concerné par rapport aux règles définies dans ces procédures pour s'assurer que les documents numériques ont été correctement collectés, utilisés et détruits, et que les archives numériques ont été correctement créées, exploitées, restituées, transférées ou supprimées.

Il convient de conserver les preuves de la conformité des activités effectuées par le personnel concerné par rapport aux politiques et aux procédures liées au processus de conservation exécuté par l'organisation en utilisant des supports de stockage pérenne pour une conservation appropriée aussi longtemps que nécessaire.

12.9.2.6 Preuves

En particulier les preuves suivantes doivent être conservées :

a) rapports de conversion d'un lot de documents numériques en archives numériques.

b) rapports d'activités des utilisateurs du SDC-C.

c) rapports de mises à jour du SDC-C, d'incidents ou de changements liés au SDC-C.

d) rapports de revue des journaux d'événements du SDC-C.

12.9.2.7 Information contenue dans la preuve

Une preuve liée aux activités effectuées par le personnel concerné doit contenir en particulier les informations suivantes :

a) Auteur(s) des activités effectuées.

b) Date(s) et heure(s) des activités effectuées.

c) Lieu(x) des activités effectuées.

d) Actif(s) utilisé(s) pour la réalisation de ces activités.

e) Descriptif des activités effectuées.

f) Problèmes ou erreurs rencontrés pendant la réalisation de ces activités.

g) Le client (interne ou externe).

12.9.2.8 Gestion des preuves

L'organisation doit définir, documenter dans une procédure et mette en œuvre une gestion adéquate des preuves :

a) du fonctionnement du SDC-C (voir 10.12.1).

b) des activités effectuées par le personnel concerné (voir 10.12.1 et 10.12.2).

Autres informations

Si des règles définies dans le cadre d'un projet de conservation sont contraires à celles actuellement mises en œuvre par l'organisation en matière d'administration, d'opérations et de sécurité du système de conservation SDC-C et en matière d'exécution des activités des processus sous-jacents au processus de conservation, il convient d'effectuer une analyse de risques afin d'identifier et d'évaluer les risques liés à ces règles et pouvant impacter l'organisation.

Il convient que les options adoptées pour les risques évalués ainsi que le plan de traitement du risque soient définis, documentés et approuvés par les parties prenantes.

Si les risques évalués sont trop élevés et ne peuvent pas être mitigés à un niveau acceptable pour l'organisation, il convient de reconsidérer le projet de conservation.

14 *Acquisition, développement et maintenance des systèmes d'information* (clause existante de la Norme internationale ISO/IEC 27002:2013)

14.1 *Exigences de sécurité applicables aux systèmes d'information* (objectif de sécurité existant de la Norme internationale ISO/IEC 27002:2013)

14.1.1 *Analyse et spécification des exigences de sécurité de l'information* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 14.1.1 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

L'organisation doit s'assurer et pouvoir démontrer que les applications critiques et les systèmes d'information supportant le système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C sont réalisés en respectant des méthodes de développement sécurisé reconnues.

15. Relations avec les fournisseurs (clause existante de la Norme internationale ISO/IEC 27002:2013)

La clause 15 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

15.1 *Sécurité de l'information dans les relations avec les fournisseurs* (objectif de sécurité existant de la Norme internationale ISO/IEC 27002:2013)

15.1.2 *La sécurité dans les accords conclus avec les fournisseurs* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 15.1.2 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

L'organisation doit inclure les conditions suivantes dans le document contractuel établi avec le fournisseur supportant les processus de dématérialisation ou de conservation exécutés par l'organisation :

a) des dispositions quant à la propriété des produits et des services, comme par exemple des documents et des applications, fournis par le fournisseur dans le cadre de son support aux processus de dématérialisation ou de conservation exécutés par l'organisation.

   NOTE : Il est recommandé d'instaurer le principe de dépôts des codes source chez un tiers pour toute application fournie par le fournisseur à l'organisation.

b) des dispositions quant à la continuité de la délivrance des produits et des services fournis par le fournisseur dans le cadre de son support aux processus de dématérialisation ou de conservation exécutés par l'organisation, même en cas de désastre.

c) le respect de la politique de dématérialisation ou de la politique de conservation de l'organisation.

d) des mesures garantissant :

   1. une notification dans les plus brefs délais des changements sécuritaires appliqués aux actifs du fournisseur et de ses fournisseurs pouvant impacter les processus de dématérialisation ou de conservation exécutés par l'organisation.
   2. que les informations de l'organisation accédées par le fournisseur et ses fournisseurs seront utilisées exclusivement pour les finalités pour lesquelles elles ont été rendues accessibles au fournisseur et à ses fournisseurs.
   3. que les changements de fournisseurs du fournisseur impliqués dans le support des processus de dématérialisation ou de conservation exécutés par l'organisation seront sujets à approbation préalable de l'organisation.

e) l'engagement du fournisseur à coopérer avec l'organisation dans le cadre d'investigations effectuées par l'organisation pour la résolution d'un incident pouvant impacter les services ou produits fournis à l'organisation par le fournisseur et dont l'origine présumée ou avérée est autre que le fournisseur ou ses fournisseurs.

f) le droit d'auditer les fournisseurs du fournisseur de manière équivalente à ce dernier et dans le périmètre de leur implication au niveau des processus de dématérialisation ou de conservation exécutés par l'organisation.

g) la conformité du fournisseur et de ses fournisseurs aux lois et aux règlements en vigueur au Luxembourg.

h) les points de contacts de chaque partie concernée par le document contractuel, d'un point de vue contractuel, opérationnel et de la sécurité de l'information.

15.1.4 *La sécurité dans les accords avec les clients* (mesure de sécurité additionnelle à la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 15.1.4 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Mesure

L'organisation doit définir les conditions d'exécution des processus de dématérialisation ou de conservation, ainsi que les besoins de sécurité de l'information associés à ces processus avec le client (interne ou externe à l'organisation).

L'organisation doit documenter ces conditions d'exécution et ces besoins de sécurité dans un document contractuel approuvé par le client et l'organisation.

Exigences de mise en œuvre

L'organisation doit identifier, déterminer et documenter dans un document contractuel les éléments suivants avec le client dans le cadre de l'établissement d'un projet de dématérialisation ou de conservation :

a) le besoin en informations du client liées aux processus de dématérialisation ou de conservation.

NOTE : Les informations suivantes sont par exemple susceptibles d'être transmises par l'organisation au client, sous réserve au préalable de son acceptation par écrit d'un engagement de confidentialité :

1. document attestant le statut de « PSDC » de l'organisation selon les exigences de sécurité et les mesures de sécurité définis dans la présente règle technique.
2. politiques et procédures de l'organisation supportant les processus de dématérialisation ou de conservation.
3. profil (résumé de l'expérience professionnelle et des qualifications) du personnel (de l'organisation et des fournisseurs) impliqué dans les processus de dématérialisation ou de conservation.
4. description des fournisseurs supportant les processus de dématérialisation ou de conservation, comme par exemple l'autorité de certification délivrant les certificats électroniques qualifiés et l'autorité d'horodatage qualifiée délivrant les jetons d'horodatage qualifiés.

b) la description détaillée du projet de dématérialisation ou de conservation, en prenant en compte les aspects techniques, opérationnels, de sécurité de l'information, légaux et réglementaires.

Cette description doit se baser et faire référence aux politiques et aux procédures supportant les processus de dématérialisation ou de conservation préalablement établies par l'organisation.

La description détaillée du projet de dématérialisation ou de conservation doit inclure les éléments suivants :

1. domaine d'application du projet (documents du client à dématérialiser ou à collecter) :

   a. Les documents du client concernés par le projet de dématérialisation ou de conservation doivent être identifiés, leur nature, comme par exemple fiscale, légale ou commerciale, et les processus actuels du client à l'origine de la création de ces documents.

      NOTE : Si ces processus impactent également d'autres documents, ces derniers doivent être listés de manière à valider qu'ils ne font pas partie du domaine d'application du projet.

b. L'organisation doit identifier et évaluer les risques associés à la perte d'authenticité, de fiabilité et d'exploitation des documents concernés par le projet.

Chaque risque identifié devrait être évalué selon une méthode d'appréciation du risque définie et commune au client et à l'organisation, de manière à en faciliter la compréhension.

Les options adoptées pour les risques évalués ainsi que le plan de traitement du risque doivent être définis, documentés et acceptés par le client et l'organisation.

NOTE : Il convient d'utiliser l'analyse de risques effectué dans le cadre du SMSI et lié à l'établissement des processus de dématérialisation ou de conservation afin d'identifier et d'évaluer les risques spécifiques aux documents concernés par le projet.

2. éléments opérationnels et techniques nécessaires à la collecte des documents à dématérialiser ou à conserver :

a. format, grammage (dans le cadre la dématérialisation) et structure des documents à collecter.

b. type de collecte (manuelle, automatique) des documents.

c. moment de collecte des documents, volumétrie et fréquence de collecte.

d. exigences et niveaux de classification, incluant la définition de la durée de rétention, des documents collectés (analogiques et numériques), des documents numériques résultants de la numérisation des documents analogiques ou des archives numériques.

NOTE 1 : Il est recommandé que le client définisse avec l'organisation les niveaux de classification des documents concernés par le projet, leur durée de rétention respective et les droits d'accès associés.

Ces droits doivent être mis en œuvre par l'organisation aussi longtemps que des documents concernés par le projet sont sous sa responsabilité.

Si le client émet des exigences particulières en matière de classification de documents ou d'archives numériques ou de règles d'accès, il appartient à l'organisation d'identifier et d'évaluer les risques inhérents à cette demande.

Les options adoptées pour les risques évalués ainsi que le plan de traitement du risque doivent être définis, documentés et acceptés par le client et l'organisation.

NOTE 2 : Le client doit être sensibilisé quant au fait qu'il est responsable des exigences de classification définies et appliquées à ses documents (documents collectées, documents numériques ou archives numériques).

e. calendriers et méthodes de restitution, de transfert, de destruction et de suppression des documents collectés (analogiques et numériques), des documents numériques résultants de la numérisation des documents analogiques ou des archives numériques.

NOTE : Les événements déclencheurs, comme le début effectif de la durée légale de rétention des documents ou des archives numériques, doivent être considérés dans la définition des calendriers de destruction et de suppression de ces documents ou de ces archives.

3. Au minimum, un niveau de classification de « confidentiel » doit être assigné par défaut par l'organisation pour tout type de document confié par un client et pour lequel le client n'a pas défini spécifiquement de niveau de classification et les mesures associées. L'organisation doit aussi s'assurer que le client est informé de mesures associées au niveau de classification « confidentiel », au minimum en les incluant au contrat.

4. éléments nécessaires à la création des documents numériques résultants de la numérisation des documents analogiques ou des archives numériques :

    a. les métadonnées de description, comme l'identification des clients, la nature des documents concernés par le projet.

       Les métadonnées doivent inclure les sources à partir desquelles elles ont été capturées.

    b. les métadonnées de contrôle associées à l'exécution de la dématérialisation ou de la conservation et générées par les actifs techniques (scanners, plateforme d'archivage) du système de dématérialisation ou de conservation SDC.

    c. format et structure des documents numériques résultants de la numérisation des documents analogiques ou des archives numériques à créer.

    d. délai de création des documents numériques résultants de la numérisation des documents analogiques ou des archives numériques à partir du moment où les originaux ont été collectés, comme par exemple, dans les 24 heures suivant leur collecte.

    e. conditions de stockage temporaire des documents numériques résultants de la numérisation des documents analogiques et de leur disponibilité dans le temps, même en cas d'indisponibilité du système de dématérialisation SDC-D.

    f. conditions de conservation aussi longtemps que nécessaire des archives numériques et de leur disponibilité dans le temps, même en cas d'indisponibilité du système de conservation SDC-C.

    g. conditions de conversion (si nécessaire) des archives numériques dans un format différent que le format initial.

5. éléments nécessaires à la restitution, au transfert, à la destruction et à la suppression des documents collectés (analogiques et numériques), des documents numériques résultants de la numérisation des documents analogiques ou des archives numériques :

    a. mécanismes d'autorisation relatifs aux processus de restitution, de transfert, de destruction et de suppression.

    b. conditions de restitution, de transfert, de destruction et de suppression des documents collectés (analogiques et numériques), des documents numériques résultants de la numérisation des documents analogiques ou des archives numériques.

       Exemples de conditions :

        1. utilisation d'un transporteur ou d'un conditionnement spécifique dans le cadre de la restitution des documents analogiques.

        2. utilisation d'une déchiqueteuse pour la destruction des documents analogiques.

        3. utilisation de méthodes sécurisées et reconnues pour la suppression des archives numériques.

Ces conditions doivent être mises en application et supervisées de manière appropriée.

c. Les informations relatives à la traçabilité de la dématérialisation ou de la conservation des documents et archives numériques concernés par le projet et qui devraient être conservées par l'organisation aussi longtemps que nécessaire.

c) La base de référence des mesures de sécurité et les mesures additionnelles mises en exploitation au niveau du système de dématérialisation ou de conservation SDC permettant d'assurer l'authenticité, la fiabilité et l'exploitation des documents collectés (analogiques et numériques), des documents numériques et des archives numériques du client pendant l'exécution des processus de dématérialisation ou de conservation.

A partir des spécifications des mécanismes de sécurité, l'organisation doit définir les mesures organisationnelles et techniques de la sécurité de l'information à mettre en œuvre dans le cadre du projet de dématérialisation ou de conservation pour protéger les éléments suivants tout au long de l'exécution des processus de dématérialisation ou de conservation :

1. les documents collectés (analogiques et numériques).

2. les documents numériques résultants de la numérisation des documents analogiques.

3. les archives numériques.

d) les niveaux de service liés à l'exécution du système de dématérialisation ou de conservation SDC.

NOTE : L'Annexe D décrit des exemples de niveaux de service liés à l'exécution des processus de dématérialisation ou de conservation.

e) la gestion des changements organisationnels et techniques pouvant impacter les processus de dématérialisation ou de conservation, ainsi que le système de dématérialisation ou de conservation SDC.

f) la gestion des incidents (majeurs) impactant les processus de dématérialisation ou de conservation, ainsi que le système de dématérialisation ou de conservation SDC.

g) Le processus et les modalités à appliquer pour l'évaluation des services ainsi que l'acceptation des services par le client.

h) le plan des tests pour s'assurer du respect de la définition du projet de dématérialisation ou de conservation pendant sa mise en œuvre.

i) les rôles et responsabilités du client et de l'organisation dans le cadre de la mise en œuvre du projet et les conséquences en cas de non-respect de ces rôles et de ces responsabilités.

Il convient que le client s'engage en particulier à :

1. respecter les dispositions définies dans le document contractuel établi avec l'organisation et relatif à son projet de dématérialisation ou de conservation défini avec l'organisation.

2. soumettre à l'organisation des documents analogiques à dématérialiser ou numériques à conserver qui n'entravent pas les lois et réglementations applicables au Luxembourg et conformément aux dispositions définies dans le document contractuel encadrant le projet, comme par exemple le format et la structure des archives numériques à créer.

Si tel était le cas, il convient que le client s'engage à en informer l'organisation dans les plus brefs délais et à assumer les conséquences de la soumission de documents dans un format, une structure ou d'une nature différente de celle définie dans le document contractuel.

3. informer l'organisation dans un délai raisonnable de tout changement des exigences et du niveau de classification associés aux documents collectés (analogiques et numériques), des documents numériques résultants de la numérisation des documents analogiques ou des archives numériques.

4. prendre des précautions adéquates lors de :

    a. l'accès aux documents numériques résultants de la numérisation des documents analogiques ou aux archives numériques.

    b. l'accès et l'utilisation du système de dématérialisation ou de conservation SDC.

5. fournir et maintenir une liste de personnes autorisées à :

    a. soumettre et à récupérer des documents analogiques.

    b. accéder aux documents numériques résultants de la numérisation des documents analogiques ou aux archives numériques.

    c. utiliser le système de dématérialisation ou de conservation SDC.

    d. demander la destruction et la suppression des documents collectés (analogiques et numériques), des documents numériques résultants de la numérisation des documents analogiques ou des archives numériques.

L'organisation doit en particulier s'engager à :

1. respecter les dispositions définies dans le document contractuel établi avec le client et relatif au projet de dématérialisation ou de conservation du client.

2. informer le client de tout changement et incident significatif pouvant impacter :

    a. les documents du client, en particulier :

        i. les documents collectés (analogiques et numériques).

        ii. les documents numériques résultants de la numérisation des documents analogiques.

        iii. les archives numériques.

    b. les processus de dématérialisation ou de conservation utilisés par le client ou pour son compte.

    c. le système de dématérialisation ou de conservation SDC utilisé par le client ou pour son compte.

Tout changement significatif doit être justifié, documenté et accepté par le client.

Si la notification d'un changement significatif ne pouvait pas être effectuée avant son établissement, l'organisation doit en informer le client dans les meilleurs délais, analyser et évaluer les risques éventuels dus à ce changement pouvant impacter le client.

Les risques jugés inacceptables doivent être traités par des actions correctives approuvées par le client.

3. informer dans les plus brefs délais le client en cas de survenance d'incidents pouvant impacter :

    a. les documents du client.

    b. les processus de dématérialisation ou de conservation utilisés par le client ou pour son compte.

    c. le système de dématérialisation ou de conservation SDC utilisé par le client ou pour son compte.

    L'organisation doit effectuer les investigations nécessaires en vue de remédier aux incidents identifiés.

4. informer dans les plus brefs délais le client en cas de tentatives d'accès aux documents du client gérés par l'organisation avec les identifiants de connexion du client et hors des conditions normales de leur utilisation, comme par exemple hors des heures normales de bureau.

5. sensibiliser le client quant aux mesures de sécurité à mettre en œuvre pour un accès sécurisé aux documents numériques résultants de la numérisation des documents analogiques ou aux archives numériques.

    Exemples de mesures de sécurité :

    a. sécurisation (protection des mots de passe, antivirus) des stations de travail et autres périphériques utilisés pour l'accès aux documents.

    b. ne pas divulguer des identifiants de connexion à des personnes n'ayant pas l'autorisation du client de les connaître.

6. documenter toutes les décisions relatives aux restitutions, aux transferts, aux destructions et aux suppressions des documents ou des archives numériques liés au client.

    Il convient en particulier que l'organisation :

    a. notifie au préalable le client et dans un délai raisonnable de la destruction ou de la suppression programmée(s) des documents, conformément au calendrier de destruction ou de suppression associé et défini dans le cadre du projet de dématérialisation ou de conservation de ces documents.

    b. obtienne l'approbation par écrit du client avant d'entamer la destruction ou la suppression de ses documents ou de ses archives numériques si aucun calendrier de destruction ou de suppression n'a été défini spécifiquement pour ces documents ou ces archives.

j) points de contacts du client et de l'organisation, d'un point de vue contractuel, opérationnel et de la sécurité de l'information.

18 Conformité

La clause 18 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

18.1 Conformité aux obligations légales et réglementaires

18.2.1 *Revue indépendante de la sécurité de l'information* (mesure de sécurité existante de la Norme internationale ISO/IEC 27002:2013)

La mesure de sécurité 18.2.1 de la Norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante :

Exigences de mise en œuvre

L'approche et l'implémentation de la gestion de la sécurité de l'information (c.à.d. objectifs de contrôle, mesures, politiques, processus et procédures pour la gestion de la sécurité de l'information) doivent être revues de manière indépendante à intervalle régulier et suite à des changements significatifs. La revue doit inclure les activités de dématérialisation et de conservation.

Informations supplémentaires

Des revues indépendantes doivent être réalisées en matière de gestion des risques pouvant impacter la stabilité financière de l'organisation, de manière à s'assurer de l'adéquation et de l'efficacité de l'approche de l'organisation en matière de gestion de ces risques.

De telles revues doivent être réalisées par des personnes indépendantes du domaine concerné, par exemple des personnes de la fonction d'audit interne ou un organisme indépendant spécialisé dans ce type de revues, et disposant des compétences et de l'expérience nécessaires.

Les résultats de ces revues indépendantes doivent être conservés en forme de documentation/preuves et les information appropriées transmises aux personnes impliquées dans la coordination de la gestion des risques liés à la perte de stabilité financière et à la perte de la capacité de couverture des responsabilités contractuelles et juridiques liés aux processus de dématérialisation ou de conservation, et à la direction.

Les non-conformités doivent être traitées par des actions correctives adoptées par la direction.

Annexe A

(Informative)

Le tableau suivant indique les clauses de la Norme internationale ISO/IEC 27001:2013 pour lesquelles des exigences complémentaires ont été définies dans la présente règle technique :

Clauses de la Norme internationale ISO/IEC 27001:2013	**Clauses de la règle technique d'exigences de sécurité et de mesures de sécurité des PSDC**
4 Contexte de l'organisation	6.2 Contexte de l'organisation
4.1 Compréhension de l'organisation et de son contexte	
4.2 Compréhension des besoins et des attentes des parties intéressées	
4.3 Détermination du domaine d'application du système de management de la sécurité de l'infirmation	
4.4 Système de management de la sécurité de l'information	
5. Leadership	6.3 Leadership
5.1 Leadership et engagement	
5.2 Politique	
5.3 Rôles, responsabilités et autorités au sein de l'organisation	
6 Planification	6.4 Planning
6.1 Actions liées aux risques et opportunités	
6.2 Objectifs de sécurité de l'information et plans pour les atteindre	
7 Support	
7.1 Ressources	
7.2 Compétence	
7.3 Sensibilisation	
7.4 Communication	
7.5. Informations documentées	
8. Fonctionnement	
8.1 Planification et contrôle opérationnels	
8.2. Appréciation des risques de sécurité de l'information	
8.3 Traitement des risques de sécurité de l'information	
9 Évaluation des performances	6.5 Évaluation des performances
9.1 Surveillance, mesures, analyse et évaluation	6.8 Amélioration continue
9.2 Audit interne	
9.3 Revue de la direction	

10 Amélioration	
10.1 Non-conformité et actions correctives	
10.2 Amélioration continue	

Annexe B

(Informative)

Le contenu suivant énumère des exemples de risques liés à l'établissement (définition, mise en œuvre, maintenance et amélioration) des processus de dématérialisation ou de conservation.

Risques communs liés à l'établissement des processus de dématérialisation et de conservation

a) les mécanismes d'authentification du système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C sont indisponibles.

b) les identifiants des comptes des utilisateurs du système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C et des comptes techniques des actifs techniques du SDC sont altérés ou indisponibles.

c) les mots de passe des comptes des utilisateurs du système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C et des comptes techniques des actifs techniques du SDC ont été divulgués.

d) le système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C n'est plus accessible.

e) les profils de privilèges des comptes des utilisateurs du système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C ont été modifiés de manière non autorisée.

f) les journaux d'événements du système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C sont altérés.

g) les journaux d'événements du système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C ont été partiellement supprimés.

Risques liés à l'établissement du processus de dématérialisation

a) la qualité de la numérisation n'est plus suffisante.

b) le contenu de documents numériques résultants de la numérisation de documents analogiques ne reflète plus le contenu original.

c) les documents numériques résultants de la numérisation des documents analogiques ont été altérés ou supprimés de manière non autorisée.

d) les documents analogiques ont été divulgués par inadvertance.

e) les documents analogiques ont été perdus avant leur numérisation.

f) la destruction des documents analogiques d'un client n'est pas réalisée selon les conditions définies dans le document contractuel établi entre le client et l'organisation.

Risques liés à l'établissement du processus de conservation

a) la création d'archives numériques n'est pas possible en raison d'un dysfonctionnement du système de conservation SDC-C.

b) la restitution d'archives numériques n'est pas possible en raison d'un dysfonctionnement du système de conservation SDC-C.

c) les métadonnées de description et de contrôles associées à des archives numériques sont altérées.

d) les mécanismes de sauvegardes du système de conservation SDC-C sont en dysfonctionnement.

e) des archives numériques sont perdues en raison du remplacement de support de stockage du système de conservation SDC-C.

f) des archives numériques ne sont plus exploitables (intelligibles).

g) des archives numériques sont supprimées par inadvertance.

h) des archives numériques ne sont pas supprimées conformément à leur calendrier de suppression.

Annexe C

(Informative)

Le tableau suivant :

a) montre les liens entre la Norme internationale ISO/IEC 27002:2013 et la règle technique d'exigences et de mesures des PSDC, plus particulièrement les modifications apportées (amendements, compléments, nouveaux objectifs de sécurité et nouvelles mesures de sécurité) à la Norme internationale ISO/IEC 27002:2013 en termes de gestion de la sécurité de l'information et de gestion opérationnelle spécifiques aux processus de dématérialisation et /ou de conservation exécutés par l'organisation.

   Ces modifications sont définies à la clause 7 de la présente règle technique.

b) énumère les clauses, les objectifs de sécurité et les mesures de sécurité à considérer par l'organisation dans le cadre de l'appréciation des risques liés à l'établissement des processus de dématérialisation ou de conservation.

   Les clauses, les objectifs de sécurité et les mesures de sécurité énumérés proviennent de la Norme internationale ISO/IEC 27002:2013, augmenté par le contenu de la clause 7 de la présente règle technique.

Explications du tableau

- # : numéro de la clause, de l'objectif ou de la mesure tel que défini dans la Norme internationale ISO/IEC 27002:2013 et à la clause 7 de la présente règle technique.
  - x.x : numéro d'une clause, d'un objectif de sécurité ou d'une mesure de sécurité défini dans la Norme internationale ISO/IEC 27002:2013.
  - x.x : numéro d'un objectif ou d'une mesure de gestion de la sécurité de l'information ou de gestion opérationnelle défini à la clause 7 de la présente règle technique.

- Type : clause (C), objectif de sécurité (O) ou mesure de sécurité / exigences de mise en œuvre (M).

- Intitulé : titre de la clause, de l'objectif de sécurité ou de la mesure de sécurité tel que défini dans la Norme internationale ISO/IEC 27002:2013.

- D : processus de dématérialisation exécuté par l'organisation.

- C : processus de conservation exécuté par l'organisation.

Liens entre la Norme internationale ISO/IEC 27002:2013 et la règle technique d'exigences et de mesures des PSDC				Domaines concernés par les objectifs de sécurité et les mesures de sécurité	
Clauses, objectifs de sécurité et mesures de sécurité de la Norme internationale ISO/IEC 27002:2013			Résumé des modifications apportées à la Norme internationale ISO/IEC 27002:2013 et définies dans la présente règle technique		
#	Type	Intitulé		D	C
5	C	Politiques de sécurité de l'information		X	X
5.1	O	Orientations de la direction en matière de sécurité de l'information		X	X
5.1.1	M	Politiques de sécurité de l'information	Complément à la mesure de sécurité	X	X
5.1.2	M	Revue des politiques de sécurité de l'information		X	X
5.2	O		Politique de dématérialisation (nouvel objectif)	X	
5.2.1	M		Document de politique de dématérialisation (nouvelle mesure)	X	
5.2.2	M		Revue de la politique de dématérialisation (nouvelle mesure)	X	
5.3	O		Politique de conservation (nouvel objectif)		X
5.3.1	M		Document de politique de conservation (nouvelle mesure)		X
5.3.2	M		Revue de la politique de conservation (nouvelle mesure)		X
6	C	Organisation de la sécurité de l'information		X	X
6.1	O	Organisation interne	Complément à l'objectif de sécurité	X	X
6.1.1	M	Fonctions et responsabilités liées à la sécurité de l'information	Complément à la mesure de sécurité	X	X
6.1.2	M	Séparation des tâches		X	X
6.1.3	M	Relations avec les autorités	Complément à la mesure de sécurité	X	X
6.1.4	M	Relations avec des groupes de travail spécialisés		X	X
6.1.5	M	La sécurité de l'information dans la gestion de projet		X	X
6.2	O	Appareils mobiles et télétravail		X	X
6.2.1	M	Politique en matière d'appareils mobiles		X	X

Liens entre la Norme internationale ISO/IEC 27002:2013 et la règle technique d'exigences et de mesures des PSDC				Domaines concernés par les objectifs de sécurité et les mesures de sécurité	
Clauses, objectifs de sécurité et mesures de sécurité de la Norme internationale ISO/IEC 27002:2013			Résumé des modifications apportées à la Norme internationale ISO/IEC 27002:2013 et définies dans la présente règle technique		
#	Type	Intitulé		D	C
6.2.2	M	Télétravail		X	X
7.	C	La sécurité des ressources humaines		X	X
7.1	O	Avant l'embauche		X	X
7.1.1	M	Sélection des candidats		X	X
7.1.2	M	Termes et conditions d'embauche		X	X
7.2	O	Pendant la durée du contrat		X	X
7.2.1	M	Responsabilités de la direction	Complément à la mesure de sécurité	X	X
7.2.2	M	Sensibilisation, apprentissage et formation à la sécurité de l'information	Complément à la mesure de sécurité	X	X
7.2.3	M	Processus disciplinaire		X	X
7.3	O	Rupture, terme ou modification du contrat de travail		X	X
7.3.1	M	Achèvement ou modification des responsabilités associées au contrat de travail		X	X
8	C	Gestion des actifs		X	X
8.1	O	Responsabilités relatives aux actifs		X	X
8.1.1	M	Inventaire des actifs	Complément à la mesure de sécurité	X	X
8.1.2	C	Propriété des actifs		X	X
8.1.3	O	Utilisation correcte des actifs		X	X
8.1.4	M	Restitution de actifs		X	X
8.2	O	Classification de l'information		X	X
8.2.1	M	Classification des informations	Complément à la mesure de sécurité	X	X
8.2.2	M	Marquage des informations	Complément à la mesure de sécurité	X	X
8.2.3	M	Manipulation des actifs		X	X
8.3	O	Manipulation des supports		X	X
8.3.1	M	Gestion des supports amovibles		X	X
8.3.2	M	Mise au rebut des supports	Complément à la mesure de sécurité	X	X
8.3.3	M	Transfert physique des supports		X	X
9	C	Contrôle d'accès		X	X

Liens entre la Norme internationale ISO/IEC 27002:2013 et la règle technique d'exigences et de mesures des PSDC				Domaines concernés par les objectifs de sécurité et les mesures de sécurité	
Clauses, objectifs de sécurité et mesures de sécurité de la Norme internationale ISO/IEC 27002:2013			Résumé des modifications apportées à la Norme internationale ISO/IEC 27002:2013 et définies dans la présente règle technique		
#	Type	Intitulé		D	C
9.1	O	Exigences métier en matière de contrôle d'accès		X	X
9.1.1	M	Politique de contrôle d'accès	Complément à la mesure de sécurité	X	X
9.1.2	M	Accès aux réseaux et aux services en réseau		X	X
9.2	O	Gestion de l'accès utilisateur		X	X
9.2.1	M	Enregistrement et désinscription des utilisateurs		X	X
9.2.2	M	Maîtrise de la gestion des accès utilisateur		X	X
9.2.3	M	Gestion des privilèges d'accès		X	X
9.2.4	M	Gestion des informations secrètes d'authentification des utilisateurs	Complément à la mesure de sécurité	X	X
9.2.5	M	Revue des droits d'accès utilisateur		X	X
9.2.6	M	Suppression ou adaptation des droits d'accès		X	X
9.3	O	Responsabilités des utilisateurs		X	X
9.3.1	M	Utilisation d'informations secrètes d'authentification		X	X
9.4	O	Contrôle de l'accès au système et aux applications		X	X
9.4.1	M	Restriction d'accès à l'information		X	X
9.4.2	M	Sécuriser les procédures de connexion		X	X
9.4.3	M	Système de gestion des mots de passe		X	X
9.4.4	M	Utilisation de programmes utilitaires à privilèges		X	X
9.4.5	M	Contrôle d'accès au code source des programmes		X	X
10	C	Cryptographie		X	X
10.1	O	Mesures cryptographiques		X	X
10.1.1	M	Politique d'utilisation des mesures cryptographiques		X	X
10.1.2	M	Gestion des clés		X	X
11	C	Sécurité physique et environnementale		X	X
11.1	O	Zones sécurisées		X	X

Liens entre la Norme internationale ISO/IEC 27002:2013 et la règle technique d'exigences et de mesures des PSDC				Domaines concernés par les objectifs de sécurité et les mesures de sécurité	
Clauses, objectifs de sécurité et mesures de sécurité de la Norme internationale ISO/IEC 27002:2013			Résumé des modifications apportées à la Norme internationale ISO/IEC 27002:2013 et définies dans la présente règle technique		
#	Type	Intitulé		D	C
11.1.1	M	Périmètre de sécurité physique	Complément à la mesure de sécurité	X	X
11.1.2	M	Contrôles physiques des accès	Complément à la mesure de sécurité	X	X
11.1.3	M	Sécurisation des bureaux, des salles et des équipements		X	X
11.1.4	M	Protection contre les menaces extérieures et environnementales		X	X
11.1.5	M	Travail dans les zones sécurisées		X	X
11.1.6	M	Zones de livraison et de chargement		X	X
11.2	O	Matériels		X	X
11.2.1	M	Emplacement et protection du matériel	Complément à la mesure de sécurité	X	X
11.2.2	M	Services généraux		X	X
11.2.3	M	Sécurité du câblage		X	X
11.2.4	M	Maintenance du matériel		X	X
11.2.5	M	Sortie des actifs	Complément à la mesure de sécurité	X	X
11.2.6	M	Sécurité du matériel et des actifs hors des locaux		X	X
11.2.7	M	Mise au rebut ou recyclage sécurisé(e) du matériel		X	X
11.2.8	M	Matériel utilisateur laissé sans surveillance		X	X
11.2.9	M	Politique du bureau propre et de l'écran vide		X	X
12	C	Sécurité liée à l'exploitation		X	X
12.1	O	Procédures et responsabilités liées à l'exploitation		X	X
12.1.1	M	Procédures d'exploitation documentées		X	X
12.1.2	M	Gestion des changements		X	X
12.1.3	M	Dimensionnement		X	X
12.1.4	M	Séparation des environnements de développement, de test et d'exploitation		X	X
12.2	O	Protection contre les logiciels malveillants		X	X
12.2.1	M	Mesures contre les logiciels malveillants		X	X
12.3	O	Sauvegarde		X	X

Liens entre la Norme internationale ISO/IEC 27002:2013 et la règle technique d'exigences et de mesures des PSDC				Domaines concernés par les objectifs de sécurité et les mesures de sécurité	
Clauses, objectifs de sécurité et mesures de sécurité de la Norme internationale ISO/IEC 27002:2013			Résumé des modifications apportées à la Norme internationale ISO/IEC 27002:2013 et définies dans la présente règle technique		
#	Type	Intitulé		D	C
12.3.1	M	Sauvegarde des informations		X	X
12.4	O	Journalisation et surveillance		X	X
12.4.1	M	Journalisation des événements		X	X
12.4.2	M	Protection de l'information journalisée		X	X
12.4.3	M	Journaux administrateur et opérateur		X	X
12.4.4	M	Synchronisation des horloges	Complément à la mesure de sécurité	X	X
12.5	O	Maîtrise des logiciels en exploitation		X	X
12.5.1	M	Installation de logiciels sur des systèmes en exploitation		X	X
12.6	O	Gestion des vulnérabilités techniques		X	X
12.6.1	M	Gestion des vulnérabilités techniques		X	X
12.6.2	M	Restrictions liées à l'installation de logiciels		X	X
12.7	O	Considérations sur l'audit du système d'information		X	X
12.7.1	M	Mesures relatives à l'audit des systèmes d'information		X	X
12.8	O		Dématérialisation (nouvel objectif)	X	
12.8.1	M		Système de dématérialisation SDC-D (nouvelle mesure)	X	
12.8.2	M		Utilisation correcte du système de dématérialisation SDC-D (nouvelle mesure)	X	
12.9	O		Conservation (Nouvel objectif)		X
12.9.1	M		Système de conservation SDC-C (Nouvelle mesure)		X
12.9.2	M		Utilisation correcte du système de conservation SDC-C (nouvelle mesure)		X
13	M	Sécurité des communications		X	X
13.1		Management de la sécurité des réseaux		X	X
13.1.1		Contrôle des réseaux		X	X

Liens entre la Norme internationale ISO/IEC 27002:2013 et la règle technique d'exigences et de mesures des PSDC				Domaines concernés par les objectifs de sécurité et les mesures de sécurité	
Clauses, objectifs de sécurité et mesures de sécurité de la Norme internationale ISO/IEC 27002:2013			Résumé des modifications apportées à la Norme internationale ISO/IEC 27002:2013 et définies dans la présente règle technique		
#	Type	Intitulé		D	C
13.1.2	M	Sécurité des services de réseau		X	X
13.1.3	M	Cloisonnement des réseaux		X	X
13.2	O	Transfert de l'information		X	X
13.2.1	M	Politiques et procédures de transfert de l'information		X	X
13.2.2	M	Accords en matière de transfert d'information		X	X
13.2.3	M	Messagerie électronique		X	X
13.2.4	M	Engagements de confidentialité ou de non-divulgation		X	X
14	C	Acquisition, développement et maintenance des systèmes d'information		X	X
14.1	O	Exigences de sécurité applicables aux systèmes d'information		X	X
14.1.1	M	Analyse et spécification des exigences de sécurité de l'information	Complément à la mesure de sécurité	X	X
14.1.2	M	Sécurisation des services d'application sur les réseaux publics		X	X
14.1.3	M	Protection des transactions liées aux services d'application		X	X
14.2	O	Sécurité des processus de développement et d'assistance technique		X	X
14.2.1	M	Politique de développement sécurisé		X	X
14.2.2	M	Procédures de contrôle des changements apportés au système		X	X
14.2.3	M	Revue technique des applications après changement apporté à la plateforme d'exploitation		X	X
14.2.4	M	Restrictions relatives aux changements apportés aux progiciels		X	X
14.2.5	M	Principes d'ingénierie de la sécurité des systèmes		X	X
14.2.6	M	Environnement de développement sécurisé		X	X
14.2.7	M	Développement externalisé		X	X
14.2.8	M	Phase de test de la sécurité du système		X	X
14.2.9	M	Test de conformité du système		X	X

Liens entre la Norme internationale ISO/IEC 27002:2013 et la règle technique d'exigences et de mesures des PSDC				Domaines concernés par les objectifs de sécurité et les mesures de sécurité	
Clauses, objectifs de sécurité et mesures de sécurité de la Norme internationale ISO/IEC 27002:2013			Résumé des modifications apportées à la Norme internationale ISO/IEC 27002:2013 et définies dans la présente règle technique		
#	Type	Intitulé		D	C
14.3	O	Données de test		X	X
14.3.1	M	Protection des données de test		X	X
15	C	Relations avec les fournisseurs		X	X
15.1	O	Sécurité de l'information dans les relations avec les fournisseurs		X	X
15.1.1	M	Politique de sécurité de l'information dans les relations avec les fournisseurs		X	X
15.1.2	M	La sécurité dans les accords conclus avec les fournisseurs	Complément à la mesure de sécurité	X	X
15.1.3	M	Chaine d'approvisionnement informatique		X	X
15.1.4	M		La sécurité dans les accords avec les clients (nouvelle mesure)	X	X
15.2	O	Gestion de la prestation du service		X	X
15.2.1	M	Surveillance et revue des services des fournisseurs		X	X
15.2.2	M	Gestion des changements apportés dans les services des fournisseurs		X	X
16	C	Gestion des incidents liés à la sécurité de l'information		X	X
16.1	O	Gestion des incidents liés à la sécurité de l'information et améliorations		X	X
16.1.1	M	Responsabilités et procédures		X	X
16.1.2	M	Signalement des événements liés à la sécurité de l'information		X	X
16.1.3	M	Signalement des failles liées à la sécurité de l'information		X	X
16.1.4	M	Appréciation des événements liés à la sécurité de l'information et prise de décision		X	X
16.1.5	M	Réponse aux incidents liés à la sécurité de l'information		X	X
16.1.6	M	Tirer des enseignements des incidents liés à la sécurité de l'information		X	X
16.1.7	M	Recueil de preuves		X	X
17	C	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité		X	X
17.1	O	Continuité de la sécurité de l'information		X	X

Liens entre la Norme internationale ISO/IEC 27002:2013 et la règle technique d'exigences et de mesures des PSDC				Domaines concernés par les objectifs de sécurité et les mesures de sécurité	
Clauses, objectifs de sécurité et mesures de sécurité de la Norme internationale ISO/IEC 27002:2013			Résumé des modifications apportées à la Norme internationale ISO/IEC 27002:2013 et définies dans la présente règle technique		
#	Type	Intitulé		D	C
17.1.1	M	Organisation de la continuité de la sécurité de l'information		X	X
17.1.2	M	Mise en oeuvre de la continuité de la sécurité de l'information		X	X
17.1.3	M	Vérifier, revoir et évaluer la continuité de la sécurité de l'information		X	X
17.2	O	Redondances		X	X
17.2.1	M	Disponibilité des moyens de traitement de l'information		X	X
18	C	Conformité		X	X
18.1	O	Conformité aux obligations légales et réglementaires		X	X
18.1.1	M	Identification de la législation et des exigences contractuelles applicables		X	X
18.1.2	M	Droits de propriété intellectuelle		X	X
18.1.3	M	Protection des enregistrements		X	X
18.1.4	M	Protection de la vie privée et protection des données à caractère personnel		X	X
18.1.5	M	Réglementation relative aux mesures cryptographiques		X	X
18.2	O	Revue de la sécurité de l'information		X	X
18.2.1	M	Revue indépendante de la sécurité de l'information	Complément à la mesure de sécurité	X	X
18.2.2	M	Conformité avec les politiques et les normes de sécurité		X	X
18.2.3	M	Examen de la conformité technique		X	X

Annexe D

(Informative)

Le contenu suivant décrit des **exemples** de niveaux de service liés à l'exécution des processus de dématérialisation ou de conservation.

Plage d'accessibilité du système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C

Il convient que la plage d'accessibilité du SDC soit composée des éléments suivants :

a) Nombre de jours d'accessibilité du SDC sur une semaine, comme par exemple 5 jours sur 7.

b) Heures d'ouverture quotidienne du SDC, comme par exemple de 8h00 à 20h00.

Exemples de plages d'accessibilité du SDC
7j/7, 24h/24
7j/7, 8 h 00 – 20 h 00
5j/7, 8 h 00 – 20 h 00
5 j/7, 8 h 00 –12 h 00 et 14 h 00 –18 h 00

Taux de disponibilité du système de dématérialisation ou de conservation SDC-DC, SDC-D ou SDC-C

Il convient de définir le taux de disponibilité du SDC pendant sa plage d'accessibilité.

Exemples de taux de disponibilité du SDC
99,990 %
99,000 %
90,000 %

Volumétrie des documents analogiques pouvant être transmis au SDC-D

Il convient de définir la volumétrie des documents analogiques pouvant être récupérés par l'organisation pour le compte du client ou soumis par ce dernier au SDC-D.

Cette volumétrie peut être estimée par exemple en fonction du nombre de documents analogiques ou de pages composant les documents analogiques à dématérialiser et pour une période donnée, comme par exemple par mois.

Exemples de volumes de documents analogiques pouvant être transmis au SDC-D	
De 10.000 à 50.000 documents analogiques par mois	Jusqu'à 100.000 pages de documents analogiques par mois
De 1.000 à 9 999 documents analogiques par mois	De 10.000 à 50.000 pages de documents analogiques par mois
De 100 à 999 documents analogiques par mois	De 1.000 à 9 999 pages de documents analogiques par mois

Taux de vérification du contenu des documents numériques créés par le SDC-D

Il convient de définir le taux de vérification de la qualité du contenu des documents numériques résultants de la numérisation de documents analogiques pour s'assurer de la reproduction conforme à l'original.

Il convient que ce taux soit défini par principe d'échantillonnage en fonction de la nature et du niveau de classification des documents analogiques originaux.

Exemples de taux de vérification du contenu des documents numériques créés par le SDC-D
100 % documents numériques sont vérifiés (d'un point de vue du contenu) avec les documents analogiques originaux.
50 % documents numériques sont vérifiés (d'un point de vue du contenu) avec les documents analogiques originaux.
10 % documents numériques sont vérifiés (d'un point de vue du contenu) avec les documents analogiques originaux.
5 % documents numériques sont vérifiés (d'un point de vue du contenu) avec les documents analogiques originaux.

Débit de transmission des documents numériques vers le SDC-C

Il convient de définir la capacité du SDC-C à absorber des flux en entrée issus de la récupération par l'organisation des documents numériques du client ou de la soumission par ce dernier de ces documents.

Exemples de débits de transmission des documents numériques vers le SDC-C
10 Go/h
1 Go/h
100 Mo/h
10 Mo/h

Délai de réponse du SDC-C

Il convient de définir le délai de réponse du SDC-C suite à une requête transmise par un utilisateur du SDC-C à des fins de restitution partielle ou totale d'archives numériques.

Exemples de délais de réponse de SDC-C
Moins de 30 secondes
Entre 30 secondes et 2 minutes
Entre 2 et 5 minutes

Temps de mise à disposition par le SDC-C des informations restituées à l'utilisateur

Il convient de définir un temps de mise à disposition « en ligne » des informations restituées à l'utilisateur, c'est-à-dire que ces informations sont accessibles de manière quasi immédiate sans que le délai de réponse standard du SDC-C soit à invoquer dans le cadre de la restitution de ces informations.

Exemples de temps de mise à disposition par le SDC-C des informations restituées à l'utilisateur
Jusqu'à 5 jours à compter de la réponse du SDC-C suite à la requête de l'utilisateur du SDC-C
Jusqu'à 3 jours à compter de la réponse du SDC-C suite à la requête de l'utilisateur du SDC-C
Jusqu'à 8 heures à compter de la réponse du SDC-C suite à la requête de l'utilisateur du SDC-C
Le temps de la session utilisateur.

Volumétrie des documents numériques pouvant être transmis au SDC-C

Il convient de définir la volumétrie des documents numériques pouvant être récupérés par l'organisation pour le compte du client ou soumis par ce dernier au SDC-C.

Cette volumétrie peut être estimée par exemple en fonction d'un volume global pour une période donnée, comme par exemple par mois, ou par le nombre de documents numériques à archiver électroniquement pouvant être transmis pour une période donnée.

Exemples de volumes de documents numériques pouvant être transmis au SDC-C	
De 10,01 Go à 100 Go par mois	Jusqu'à 1 million de documents numériques par mois
De 1,01 à 10 Go par mois	Jusqu'à 100 000 documents numériques par mois
De 0 à 1 Go par mois	Jusqu'à 1 000 documents numériques par mois

Bibliographie

Les normes suivantes doivent être considérées comme une assistance dans la mise en œuvre de la présente règle technique. Pour les références non datées, la dernière édition de la norme s'applique (y compris les éventuels amendements).

[1] ISO 30301:2011, Information et documentation – *Systèmes de gestion des documents d'activité – Exigences ;*

[2] ISO 14721:2003, *Systèmes de transfert des informations et données spatiales – Système ouvert d'archivage d'information – Modèle de référence ;*

[3] ISO/IEC 15489:2001, *Information et documentation – « Records management » ;*

[4] ISO 23081, *Information et documentation – Processus de gestion des enregistrements – Métadonnées pour les enregistrements ;*

[5] ETSI TS 101 733, *Electronic Signatures and Infrastructures (ESI) ; CMS Advanced Electronic Signatures (CAdES) ;*

[6] ETSI TS 101 903, *XML Advanced Electronic Signatures (XAdES) ;*

[7] ETSI TS 102 778, *Electronic Signatures and Infrastructures (ESI) ; PDF Advanced Electronic Signature Profiles ;*

[8] ETSI TS 102 176-1, *Electronic Signatures and Infrastructures (ESI) ; Algorithms and Parameters for Secure Electronic Signatures; Part 1 : Hash functions and asymmetric algorithms ;*

[9] ISO 9000:2005, Systèmes de management de la qualité – *Principes essentiels et vocabulaire ;*

[10] ISO 30300:2011, Information et documentation – Systèmes de gestion des documents d'activité – *Principes essentiels et vocabulaire* ;

[11] ISO/IEC 27000:2014, Information technology – Security techniques – Information security management systems – *Overview and vocabulary*.

ANNEXE II

Règle technique pour un système de management et mesures de sécurité pour les Prestataires de Services de Dématérialisation ou de Conservation (Version 3.1)

Table des matières

0 Introduction

0.1 Contexte

La présente règle technique (ci-après « la Règle technique ») définit des exigences et des mesures permettant à une organisation d'établir une gestion de la sécurité de l'information et une gestion opérationnelle spécifiques aux processus de dématérialisation ou de conservation.

Du point de vue de la gestion de la sécurité de l'information, la Règle technique se base sur les Normes internationales ISO/IEC 27001:2013 et ISO/IEC 27002:2013 de manière à ce qu'une organisation puisse être en mesure de définir, d'implémenter, de maintenir et d'améliorer :

a) un Système de Management de la Sécurité de l'Information (ci-après « SMSI ») basé sur la Norme internationale ISO/IEC 27001:2013 et intégrant les processus de dématérialisation ou de conservation,
b) des objectifs et des mesures de la sécurité de l'information basés sur la Norme internationale ISO/IEC 27002:2013 et spécifiques aux processus de dématérialisation ou de conservation.

La Règle technique a été rédigée selon des exigences de la norme ISO/IEC 27009:2016.

La Règle technique est aussi utilisée pour les audits d'évaluation de la conformité d'une organisation exécutant des processus de dématérialisation ou de conservation.

Ces audits d'évaluation ne doivent pas uniquement porter sur les exigences et les mesures de sécurité, mais aussi sur les préconisations de mise en œuvre. Toute déviation par rapport à ces préconisations, qui n'est pas dûment argumentée, documentée ou évidente, peut donner lieu à une non-conformité mineure. Toute déviation par rapport aux mesures, sauf si l'exclusion de la mesure est dûment justifiée par le processus de traitement des risques ainsi que toute déviation par rapport aux exigences, doit donner lieu à une non-conformité mineure ou majeure telle que définie dans ISO/IEC 17021-1:2015.

L'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ci-après ILNAS) est la seule autorité nationale luxembourgeoise habilitée à conférer à une organisation un statut de prestataire de services de dématérialisation ou de conservation (ci-après statut de PSDC), si cette organisation a été certifiée conforme à la Règle technique par un organisme de certification accrédité pour cette activité selon les exigences de la Norme internationale ISO/IEC 17021-1:2015, « Évaluation de la conformité - Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management » ainsi que les exigences complémentaires de la Norme ISO/IEC 27006:2015 « Requirements for bodies providing audit and certification of information security management systems ». Ces normes définissent les exigences pour réaliser des certifications à reconnaissance internationale de systèmes de management selon la norme ISO/IEC 27001:2013 et la Règle technique.

La Règle technique ne se substitue pas aux règlements, lois, ou normes applicables aux organisations exécutant des processus de dématérialisation ou de conservation. En particulier, le règlement (UE) n°910/2014 du Parlement Européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (aussi appelé règlement « eIDAS ») doit être considéré comme une fondation pour l'établissement des propriétés de sécurité qui y sont exposées, notamment en matière de confidentialité, d'intégrité, de disponibilité, d'authenticité, de fiabilité et d'exploitabilité.

0.2 Structure du document

Ce document est structuré de la façon suivante :

- Le chapitre 1 précise le domaine d'application de la Règle technique.
- Le chapitre 2 cite des références normatives, c'est-à-dire les normes à respecter par les organisations mettant en application la Règle technique.
- Le chapitre 3 définit les termes utilisés dans ce texte.
- Le chapitre 4 cite des exigences spécifiques pour le système de management des prestataires de service de dématérialisation ou de conservation. Ce chapitre est à lire comme un complément à la norme ISO/IEC 27001:2013 « Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences », d'où la numérotation non linéaire des exigences : un complément à une section existante de la norme initiale garde le même numéro, les sections non modifiées ne sont pas incluses dans le présent document, et les nouvelles sections prennent des numéros qui ne sont pas utilisés dans la norme ISO/IEC 27001:2013.
- Le chapitre 5 définit des guidances spécifiques, en particulier des objectifs, des mesures de sécurité, des préconisations de mise en œuvre et des informations complémentaires. Ce chapitre est à lire comme un complément à la norme ISO/IEC 27002:2013 « Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information », d'où la numérotation non linéaire des exigences.
- L'Annexe A résume les objectifs spécifiques et les mesures de sécurité spécifiques énoncés au Chapitre 5 tout en les rendant leur examen obligatoire dans le traitement des risques.

Les transitions requises par ISO/IEC 27009:2016 sont indiquées en *italique*.

1 Domaine d'application

La loi du 25 juillet 2015 relative à l'archivage électronique dispose qu'une personne peut, si elle détient une certification selon les exigences et les mesures définies dans la Règle technique d'exigences et de mesures pour la certification des Prestataires de Services de Dématérialisation ou de Conservation (ci-après PSDC), en regard de l'exécution de ses processus de dématérialisation ou de conservation, procéder à une notification auprès de l'ILNAS, en vue d'obtenir le statut de PSDC.

Si les critères de vérification établis par la loi relative à l'archivage électronique et par le système de qualité ad hoc du Département de la confiance numérique de l'ILNAS sont validés, l'ILNAS procèdera à l'inscription de la personne concernée dans la liste des PSDC, précisant les processus relatifs à la certification, établissant ainsi le statut de PSDC. Tout événement ou incident significatif détecté et tout changement majeur relatif à la portée de la certification, doit obligatoirement être notifié à l'ILNAS. Tout retrait, suspension ou non-renouvellement de la certification entraîne de facto le retrait du statut de PSDC.

Le statut de PSDC demeure volontaire, sauf disposition réglementaire ou sectorielle l'imposant.

La certification effective selon la Règle technique d'exigences et de mesures pour la certification des PSDC de toute personne permet la demande du statut de prestataire de services de dématérialisation ou de conservation délivré par le Département de la confiance numérique de l'ILNAS. L'ILNAS reconnaît formellement, via ce statut, la personne concernée en tant que PSDC.

La personne certifiée doit être en mesure de garantir les résultats de l'exécution des processus de dématérialisation ou de conservation pour lesquels elle a obtenu la certification. La certification garantit que les documents numériques résultants de la numérisation des documents analogiques et les archives numériques seront reconnus comme conformes aux exigences spécifiques liées à l'activité de dématérialisation respectivement de conservation, telles qu'établies dans ce document.

Ainsi une copie sera présumée être conforme à l'original si elle est produite par le processus ad hoc d'un PSDC. De même, une archive numérique est considérée comme équivalente aux originaux numériques, si elle est conservée par le processus ad hoc d'un PSDC.

Indépendamment de son type, de sa taille, de ses processus ou de ses activités, pour ses besoins internes ou dans le cadre de services proposés à ses clients, la Règle technique d'exigences et de mesures des PSDC est applicable à toute organisation publique ou privée.

La Règle technique a été définie à partir de Normes internationales publiées et maintenues par l'Organisation Internationale de Normalisation (ci-après « ISO »).

La Règle technique doit donc être considérée comme un supplément aux normes ISO/IEC 27001:2013 et ISO/IEC 27002:2013 en amendant et complétant leur contenu spécifiquement aux processus de dématérialisation ou de conservation.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application de la Règle technique.

Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 27000:2016, Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Vue d'ensemble et vocabulaire

ISO/IEC 27001:2013, Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences

ISO/IEC 27002:2013, Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information

3 Termes et définitions

Pour les besoins de la Règle technique, les abréviations suivantes s'appliquent :

DdA	Déclaration d'Applicabilité (terme anglais : Statement of Applicability (SoA), déclaration relative à l'applicabilité des objectifs et mesures de sécurité)
eIDAS	Règlement (UE) No 910/2014 du parlement Européen de du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE
L2TP	Layer 2 Tunneling Protocol (terme anglais)
IPSec	Internet Protocol Security (terme anglais)
PPP	Point to Point Protocol (terme anglais)
PSDC	Prestataire de Services de Dématérialisation ou de Conservation
SDC	Système de Dématérialisation ou de Conservation
SFTP	SSH File Transfer Protocol (terme anglais)
SMSI	Système de Management de la Sécurité de l'Information
SSH	Secure SHell (terme anglais)
TLS	Transport Layer Security (terme anglais)
UTC	Temps Univers

Pour les besoins de la Règle technique, les termes et définitions fournis dans la norme ISO/IEC 27000:2016 ainsi que les définitions supplémentaires suivantes s'appliquent.

3.1 actif

tout élément représentant de la valeur pour l'organisation

Note 1 : Il existe plusieurs sortes d'actifs, dont :

a) l'information,
b) les documents,
c) les archives,
d) les actifs techniques, par exemple un scanneur, un serveur ou des disques durs,
e) les actifs techniques immatériels, par exemple des unités de stockage virtuelles,
f) le personnel d'une organisation,
g) les actifs incorporels, par exemple la réputation et l'image,
h) les processus et services.

Note 2 : Définition adaptée de la norme ISO/IEC 30300:2011, définition 3.1.2.

3.2 analogique

non numérique

Note : Un support de stockage analogique est un support de stockage non numérique, par exemple le papier, le film argentique ou le disque vinyle.

3.3 archive

document conservé en l'état en vue d'une utilisation pérenne

Note : Définition adaptée de la norme ISO/IEC 30300:2011, définition 3.1.1.

3.4 archive numérique

archive sous forme de document numérique

3.5 authenticité

propriété selon laquelle une entité est ce qu'elle revendique être

[ISO/IEC 27000:2016]

3.6 confidentialité

propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés

[ISO/IEC 27000:2016]

3.7 conservation (électronique)

l'activité qui consiste à conserver un original numérique ou une copie à valeur probante dans des conditions qui assurent des garanties fiables quant au maintien de l'intégrité du document conservé

[loi du 25 juillet 2015, art. 2 b]

Note : Dans la suite du document, le terme « conservation » est synonyme de « conservation électronique », sauf précision contraire.

3.8 dématérialisation

l'activité qui consiste à créer une copie à valeur probante d'un original existant sous forme analogique dans des conditions qui assurent des garanties fiables quant à la conformité de la copie ainsi créée à l'original

[loi du 25 juillet 2015, art. 2 d]

3.9 disponibilité

propriété d'être accessible et utilisable à la demande par une entité autorisée

[ISO/IEC 27000:2016]

3.10 document

information ou objet documentaire enregistré qui peut être traité comme une unité

[ISO 15489 -1:2001]

3.11 fiabilité

propriété relative à un comportement et des résultats prévus et cohérents

[ISO/IEC 27000:2016]

3.12 gestion

définition, mise en œuvre ou en exploitation, opération, contrôle, révision, maintenance et amélioration

Note : De même, gérer est synonyme de « définir, mettre en œuvre ou en exploitation, opérer, contrôler, réviser, maintenir et améliorer ».

3.13 indexation

définition de points d'accès pour faciliter la recherche des documents

Note 1 : La génération de métadonnées liées aux documents numériques et aux archives numériques est généralement utilisée pour faciliter leur recherche.

Note 2 : Définition adaptée de la norme ISO 15489 -1:2001, définition 3.11.

3.14 intégrité

propriété d'exactitude et de complétude

[ISO/IEC 27000:2016]

3.15 métadonnées

données décrivant le contexte, le contenu ou la structure des documents ainsi que leur gestion dans le temps

Note : Définition adaptée de la norme ISO/IEC 30300:2011, définition 3.1.6.

3.16 non-répudiation

capacité à prouver l'occurrence d'un événement ou d'une action donnée(e) et des entités qui en sont à l'origine

[ISO/IEC 27000:2016]

3.17 organisme

personne ou groupe de personnes qui exerce ses propres fonctions associées aux responsabilités, pouvoirs et relations nécessaires pour atteindre ses objectifs

Note 1 : Le concept d'organisme inclut, sans s'y limiter, les travailleurs indépendants, compagnies, sociétés, firmes, entreprises, autorités, partenariats, œuvres de bienfaisance ou institutions, ou toute partie ou combinaison de ceux-ci, constituée en société de capitaux ou ayant un autre statut, de droit privé ou public.

[ISO/IEC 27000:2016]

Note 2 : Le terme organisme désigne le prestataire qui est ou qui veut être prestataire de service de dématérialisation ou de conservation.

3.18 prestataire de services de dématérialisation ou de conservation (PSDC)

toute personne qui exerce à titre principal ou accessoire, pour ses propres besoins ou pour compte d'autrui, des activités de dématérialisation ou de conservation électronique et qui est, dans les conditions et selon les modalités de la [loi 25 juillet 2015], certifiée à cette fin et inscrite sur la liste visée à l'article 4

(3) [de cette loi]

[loi du 25 juillet 2015, art. 2h]

Note : Les prestataires ne sont concernés que par les processus qu'ils gèrent. Dans tout ce document, le « ou » peut être inclusif ou exclusif selon le contexte opérationnel du prestataire.

3.19 preuve

document démontrant l'effectivité d'une opération

Note 1 : La preuve d'une opération signifie qu'il peut être démontré qu'elle a été créée dans le cadre normal de la conduite de l'activité de l'organisation et qu'elle est intacte et complète. Ne se limite pas au sens légal du terme.

Note 2 : Définition adaptée de la norme ISO/IEC 30300:2011, définition 3.1.5.

3.20 processus

ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie

[ISO 9000:2015]

3.21 sécurité de l'information

protection de la confidentialité, de l'intégrité et de la disponibilité de l'information

Note : En outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité peuvent également être concernées.

[ISO/IEC 27000:2016]

Note pour les PSDC : les propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation, la fiabilité et l'exploitabilité sont incluses dans la notion de sécurité.

3.22 système

ensemble d'actifs techniques corrélés ou interactifs

3.23 système de conservation

système composé d'un ensemble d'actifs techniques permettant le stockage temporaire des documents numériques en vue de leur conservation électronique, leur conversion en archives numériques, leur suppression et la conservation des archives numériques aussi longtemps que nécessaire, leur exploitation, leur restitution partielle ou totale, leur transfert et leur suppression

3.24 système de dématérialisation

système composé d'un ensemble d'actifs techniques permettant la création des documents numériques à partir des documents analogiques, le stockage temporaire des documents analogiques et numériques, leur restitution, leur transfert, la destruction éventuelle des documents analogiques et la suppression des documents numériques

3.25 système de dématérialisation ou de conservation (SDC)

système de dématérialisation, système de conservation, ou un système combinant les deux

4 Exigences spécifiques pour PSDC et complémentaires à la norme ISO/IEC 27001:2013

4.1 Structure de ce standard

Ce standard est un standard lié à la norme ISO/IEC 27001:2013. Il est spécifique aux PSDC au sens de la loi du 25 juillet 2015 relative à l'archivage électronique.

Les objectifs de sécurité et les mesures de sécurité spécifiques sont indiqués dans l'Annexe A.

4.2 Exigences spécifiques aux systèmes de management des PSDC

Toutes les exigences des chapitres 4 à 10 de la norme ISO/IEC 27001:2013 qui ne figurent pas ci-dessous restent applicables sans modification.

4 Contexte de l'organisation

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

4.0 Système de Management des processus de dématérialisation ou de conservation

L'organisation doit gérer un système de management des processus de dématérialisation ou de conservation, intégré au SMSI ou répondant aux mêmes exigences, pour assurer le déroulement adéquat des processus de dématérialisation ou de conservation, la stabilité financière de l'organisation et sa capacité de couverture de responsabilités contractuelles, légales et réglementaires liés aux processus de dématérialisation ou de conservation.

Ce système de management des processus et le SMSI, ou le système de management intégrant ces deux aspects doit s'appliquer aux processus et activités liés à la prestation de services du PSDC et à tous les actifs supportant ces processus.

L'exigence 4.3 de la norme ISO/IEC 27002:2013 est complétée de la façon suivante :

4.3 Détermination du domaine d'applicabilité

Pour établir le domaine d'application du système de management des processus de dématérialisation ou de conservation, l'organisation doit en déterminer les limites et l'applicabilité.

Elle doit définir la nature des processus (dématérialisation ou conservation), le type des documents concernés et le type des clients (internes ou externes à l'organisation, secteurs concernés) qui peuvent bénéficier des services du PSDC.

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

4.5 L'authenticité, la fiabilité, et l'exploitabilité

En complément des propriétés de sécurité de base qui sont

a. la confidentialité,

b. l'intégrité, et

c. la disponibilité,

le système de management doit gérer les propriétés de sécurité complémentaires suivantes :

d. l'authenticité (souvent considéré comme un volet particulier de l'intégrité) :

   L'organisation doit pouvoir démontrer que toutes les activités effectuées dans le cadre de la gestion des processus de dématérialisation ou de conservation sont authentiques, à savoir :

   i. Les documents analogiques ou numériques ont bien été transmis par la personne qui est supposée les avoir transmis.
   ii. Le document numérique résultant de la numérisation d'un document analogique ou l'archive numérique a bien été créé par la personne ou le système au moment présumé.
   iii. Le document numérique ou l'archive numérique est bien ce qu'il est supposé être.

e. la fiabilité :

   L'organisation doit pouvoir démontrer que toutes les activités effectuées dans le cadre de la gestion des processus de dématérialisation ou de conservation sont fiables, à savoir :

   i. Toutes les activités effectuées dans le cadre de l'établissement des processus de dématérialisation ou de conservation sont exécutées conformément aux politiques et aux procédures définies et mises en œuvre par l'organisation en la matière.
   ii. Le document numérique ou l'archive numérique créé et exploité est conforme à son état original et non modifié par des modifications non autorisées.

f. l'exploitabilité :

   L'organisation doit pouvoir démontrer que l'exploitation des processus de dématérialisation ou de conservation crée un document numérique ou une archive numérique qui soit à tout moment localisable, lisible, intelligible, utilisable avec les informations nécessaires à la compréhension de son origine et disponible aussi longtemps que nécessaire.

Note : C'est en ajoutant ces propriétés dans l'envergure du SMSI qu'on généralise le système de management de la norme ISO/IEC 27001:2013 limité à la sécurité de l'information, à un système de management de toutes les propriétés requises aux activités de dématérialisation ou de conservation.

5 Leadership

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

5.4 Rôles, responsabilités et autorités sur les processus de dématérialisation ou de conservation

La direction doit s'assurer que les responsabilités et autorités des rôles concernés par les processus de dématérialisation ou de conservation sont attribuées et communiquées au sein de l'organisation.

La direction doit désigner qui a la responsabilité et l'autorité de :

a. s'assurer que le système de management des processus de dématérialisation ou de conservation est conforme aux exigences du présent document ;

b. définir les critères de performances ;

c. rendre compte à la direction des performances du système de management des processus de dématérialisation ou de conservation ;

d. gérer la documentation (politiques, procédures) supportant ces processus ;

e. définir le système, son fonctionnement et sa sécurité au niveau opérationnel ;

f. superviser la mise en œuvre de la politique ;

g. émettre des recommandations en vue d'améliorer la gestion opérationnelle ;

h. définir et approuver les méthodes relatives à la gestion des risques pouvant impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles, légales et réglementaires ;

i. gérer les risques pouvant impacter la stabilité financière de l'organisation et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation ;

j. évaluer l'adéquation des mesures adoptées en vue de mitiger les risques pouvant impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation, et jugées non acceptables par la direction de l'organisation ;

k. évaluer l'opportunité d'une couverture d'assurance pour garantir la continuité de l'exécution des processus de dématérialisation ou de conservation de l'organisation même en cas de cessation d'activité et pendant une période minimum de transition ;

l. identifier les changements en termes de risques pouvant impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation ;

m. sensibiliser le personnel (de l'organisation et des tiers) concerné quant aux risques ;

n. identifier et évaluer les problèmes et les incidents ;

o. émettre des recommandations quant aux actions préventives et correctives à adopter en réponse aux problèmes et aux incidents évalués.

La direction doit attribuer chaque rôle et responsabilité à une personne ou à une entité dont les membres et le mode de fonctionnement sont documentés, et réviser régulièrement cette attribution.

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

5.5 Leadership et engagement de PSDC

La direction doit faire preuve de leadership et affirmer son engagement en faveur du système de management en :

a. s'assurant qu'une politique et des objectifs sont établis en matière de processus de dématérialisation ou de conservation et qu'ils sont compatibles avec l'orientation stratégique de l'organisation dûment documentée et avec la politique de sécurité de l'information ;

   Note : Une politique dédiée aux processus de dématérialisation et une politique dédiée au processus de conservation peuvent être établies par l'organisation. Si un des processus n'est pas dans le domaine d'applicabilité, cette politique et toutes les exigences y relatives ne sont évidemment pas requises.

b. s'assurant que les exigences de cette politique sont intégrées aux processus ;

c. s'assurant que les ressources nécessaires pour le système de management des processus de dématérialisation ou de conservation sont disponibles (en particulier pour fournir les éléments probants quant à l'intégrité et la fiabilité) ;

d. communiquant sur l'importance de disposer d'un management des processus de dématérialisation ou de conservation efficace et de se conformer à ses exigences ;

e. s'assurant que le système de management des processus de dématérialisation ou de conservation produit le ou les résultats escomptés ;

f. orientant et soutenant les personnes pour qu'elles contribuent à l'efficacité du processus de dématérialisation ou de conservation ;

g. promouvant l'amélioration continue ;

h. aidant les autres managers concernés à faire également preuve de leadership dès lors que cela s'applique à leurs domaines de responsabilités ;

i. fournissant la preuve de l'existence légale de l'organisation ;

j. fournissant la preuve d'une situation financière suffisante et d'une situation stable pour répondre aux attentes des parties intéressées à l'activité de PSDC ;

Note : L'organisation peut mener une étude sur le coût d'un transfert d'activités ou d'une restitution à tous les clients des documents y inclus toutes les informations requises pour maintenir la valeur probante d'un document dématérialisé et d'une archive numérique. L'étude pourra montrer que ce coût est inférieur aux provisions, aux réserves, ou au capital disponible de l'organisation, et que ces paramètres sont stables. L'organisation peut mettre en place un processus de monitoring de ces paramètres qui assure une gestion d'incident en cas de dégradation de la stabilité financière.

Note : Une organisation de droit privé pourra par exemple fournir les informations suivantes :

- une étude sur le coût d'un transfert d'activités et la justification de pouvoir le réaliser à tout moment, compte tenu de son capital, de ses réserves, ou de ses provisions,
- les bilans et comptes de résultat des 3 dernières années fiscales, pour autant que l'ancienneté de l'organisation le permette,
- rapport ou avis financier émis par une autorité de surveillance luxembourgeoise,
- niveau d'exposition des activités métiers aux facteurs externes à l'organisation,
- rapport d'auditeurs financiers.

k. fournissant la garantie de continuité d'exécution (c'est-à-dire, pendant une période de transition minimum permettant d'assurer un transfert) des processus de dématérialisation ou de conservation, en particulier pour les cas suivants :

1. processus de dématérialisation exécuté par l'organisation pour le compte d'un tiers,
2. processus de conservation électronique exécuté par l'organisation pour le compte d'un tiers,
3. sous-processus de restitution, transfert et suppression des archives numériques exécuté par l'organisation pour son propre compte.

Cette garantie de continuité doit être gérée par l'organisation et couvrir le risque économique de cessation d'activités.

Note : Un moyen pour l'organisation de garantir cette continuité d'exécution pendant une période de transition minimum est par exemple de contracter une assurance spécifique ou d'obtenir un engagement formel d'un actionnaire institutionnel ou privé majoritaire se portant garant.

6 Planification

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

6.1.4 Risques liés à l'activité PSDC

L'organisation doit

a. intégrer les risques de sécurité de l'information et opérationnels associés à la gestion des processus de dématérialisation ou de conservation dans son processus d'identification (6.1.2 c) d'analyse (6.1.2.d) et d'évaluation des risques (6.1.2.e), y intégrer également les risques pouvant impacter la stabilité financière de l'organisation et sa capacité de couverture de responsabilités contractuelles, légales et réglementaires liées à ces processus ;

b. appliquer son processus de traitement des risques de sécurité aux risques déterminés au point précédent ;

c. comparer les objectifs et les mesures déterminés en 6.1.3 b) avec celles de l'Annexe A du présent document et vérifier qu'aucune mesure nécessaire n'a été omise ;

d. compléter la déclaration d'applicabilité déterminée en 6.1.3 d) avec les mesures de l'Annexe A de la Règle technique et la justification de leur insertion ou de leur exclusion, ainsi que, le cas échéant, l'indication de leur mise en œuvre ;

e. porter à connaissance des clients et à l'ILNAS la déclaration d'applicabilité, notamment si elle contient des exclusions.

Une exclusion doit être rejetée si elle crée une non-conformité avec une exigence légale, réglementaire ou contractuelle.

7 Support

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

7.4 Sensibilisation à la politique de dématérialisation ou de conservation

Les personnes effectuant un travail sous le contrôle de l'organisation doivent :

1. être sensibilisées à la politique de dématérialisation ou de conservation et respecter toute la documentation relative à cette politique ;
2. avoir conscience de leur contribution à l'efficacité du système de management, y compris aux effets positifs d'une amélioration des performances ;
3. avoir conscience des implications de toute non-conformité aux exigences requises par le système de management ;
4. connaitre leurs responsabilités en vertu de la loi luxembourgeoise en matière de dématérialisation ou de conservation et concernant les processus de dématérialisation ou de conservation.

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

7.5.4 La non-répudiation des informations documentées

L'organisation doit mettre en place un environnement documentaire permettant de démontrer envers un tiers le respect des propriétés de sécurité indiquées au chapitre 4.5 du présent document et l'intégrité de la documentation.

8 Fonctionnement

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

8.4 Acceptation des risques

L'organisation doit faire accepter par la direction l'appréciation des risques, le plan de traitement des risques incluant une indication des ressources requises, le niveau du risque actuel et celui après traitement.

L'organisation doit conserver la preuve de cette acceptation et la documentation de la délibération par la direction.

9 Évaluation des performances

L'exigence 9.1 de la norme ISO/IEC 27001:2013 est complétée de la façon suivante.

9.1 Surveillance, mesures, analyse et évaluation

De la même façon que pour le système de management de la sécurité de l'information, l'organisation doit évaluer les performances de son SDC, ainsi que l'efficacité du système de management des processus de dématérialisation et de conservation.

L'exigence 9.2 de la norme ISO/IEC 27001:2013 est complétée de la façon suivante.

9.2 Audit interne

De la même façon que pour le système de management de la sécurité de l'information, l'organisation doit réaliser des audits internes à des intervalles planifiés afin de recueillir des informations permettant de déterminer si le système de management des processus de dématérialisation et de conservation

a. est conforme :
   1. aux exigences propres de l'organisation concernant son système de management de processus de dématérialisation ou de conservation
   2. à cette règle technique ;

b. est efficacement mis en œuvre et tenu à jour.

L'organisation doit donc inclure ces audits dans le ou les programmes d'audit, définir les critères d'audit et le périmètre de chaque audit, sélectionner des auditeurs et réaliser des audits qui assurent l'objectivité et l'impartialité du processus d'audit, s'assurer qu'il est rendu compte des résultats des audits à la direction concernée, et conserver des informations documentées comme preuves de la mise en œuvre du ou des programme(s) d'audit et des résultats d'audit.

L'exigence 9.3 de la norme ISO/IEC 27001:2013 est complétée de la façon suivante.

9.3 Revue de direction

De la même façon que pour le système de management de la sécurité de l'information, la direction doit procéder à la revue du système de management des processus de dématérialisation ou de conservation mis en place par l'organisation, afin de s'assurer qu'il est toujours approprié, adapté et efficace.

La revue de direction doit prendre en compte :

g. les résultats de l'analyse de risques pouvant impacter la stabilité financière de l'organisation et sa capacité de couverture de responsabilités contractuelles, légales et réglementaires liées aux processus de dématérialisation ou de conservation de manière régulière.

La revue de direction doit avoir lieu au moins une fois par an et suite à des changements significatifs :

1. impactant le fonctionnement de l'organisation,
2. issus des besoins actuels de l'organisation,
3. de nature légale et réglementaire ayant un impact sur les activités et les processus de l'organisation.

10 Amélioration

L'exigence 10.2 de la norme ISO/IEC 27001:2013 est complétée de la façon suivante.

10.2 Amélioration continue

L'organisation doit continuellement améliorer la pertinence, l'adéquation et l'efficacité du système de management des processus de dématérialisation ou de conservation.

5 Code de bonnes pratiques spécifiques aux PSDC en relation avec ISO/IEC 27002:2013

Toutes les catégories de mesures, objectifs de sécurité, mesures, préconisations de mise en œuvre, et informations supplémentaires de la norme ISO/IEC 27002:2013 qui ne figurent pas ci-dessous restent applicables sans modification.

L'Annexe A résume les objectifs spécifiques et les mesures de sécurité spécifiques énoncés dans ce chapitre tout en les rendant leur examen obligatoire dans le traitement des risques.

5 Politiques de sécurité de l'information

Une catégorie de mesures additionnelles à la norme ISO/IEC 27002:2013 est :

5.2 Orientations de la direction en matière de politique de dématérialisation ou de conservation

Objectif : Apporter à la gestion des processus de dématérialisation ou de conservation une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.

5.2.1 Politiques de dématérialisation ou de conservation

Mesure

Il convient de définir une « politique de dématérialisation ou de conservation », de la faire approuver par la direction, de la mettre en application, de la diffuser et de la communiquer aux salariés et aux tiers concernés.

Préconisations de mise en œuvre

Il convient que la politique de dématérialisation ou de conservation définisse le domaine d'application des processus de dématérialisation ou de conservation, la gestion de la sécurité de l'information et la gestion opérationnelle appliqués à ce processus.

Il convient que ce document contienne les éléments suivants :

a. une présentation de l'organisation, de son historique et de ses activités métiers ;
b. le lien avec la stratégie ou la motivation d'implémenter cette activité ;
c. une définition du domaine d'application des processus de dématérialisation ou de conservation ;
d. une description générale organisationnelle et technique des processus suivants sous-jacents
    1. au processus de dématérialisation :
        i. collecte des documents analogiques,
        ii. création et stockage temporaire des documents numériques,
        iii. stockage temporaire des documents analogiques,
        iv. restitution, transfert, destruction éventuelle des documents analogiques et suppression des documents numériques,
        v. le nom des fournisseurs dès qu'une activité du processus est sous-traitée ;
    2. au processus de conservation :
        i. collecte des documents numériques,
        ii. création et conservation des archives numériques,
        iii. restitution, transfert, suppression des archives numériques,
        iv. le nom des fournisseurs dès qu'une activité du processus est sous-traitée ;

e. une description générale technique du SDC et de son niveau de conformité à des normes et des référentiels reconnus ;

f. les rôles et les responsabilités spécifiques au processus de dématérialisation ou de conservation et aux processus sous-jacents exécutés par l'organisation et en matière de gestion de la sécurité de l'information et de gestion opérationnelle ;

g. les grands principes de sécurité de l'information appliqués au processus de dématérialisation ou de conservation exécuté par l'organisation, notamment en matière d'authenticité, de fiabilité et d'exploitabilité ;

h. les références aux lois et aux règlements applicables à l'organisation et spécifiques au processus de dématérialisation ou de conservation ;

i. la gestion de la documentation supportant le processus de dématérialisation ou de conservation ;

j. des références aux documents, comme les procédures d'administration, d'opérations et de sécurité, supportant la politique de dématérialisation ou de conservation ;

k. les modalités de revue de la politique de dématérialisation ou de conservation.

5.2.2 Revue de la politique de dématérialisation ou de conservation

Mesure

Pour garantir la constance de la pertinence, de l'adéquation et de l'efficacité de la politique de dématérialisation ou de conservation, il convient de revoir ces politiques et les processus y relatifs à intervalles programmés et en cas de changements majeurs.

Préconisations de mise en œuvre

Les mêmes préconisations que pour la politique de sécurité de l'information s'appliquent à cette politique.

La catégorie « 6 Organisation de la sécurité de l'information » est complétée de la façon suivante.

6 Organisation de la sécurité de l'information et des processus de dématérialisation ou de conservation

6.1 Organisation interne

Objectif : Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information et des processus de dématérialisation ou de conservation au sein de l'organisation.

6.1.1 Fonctions et responsabilités liées à la sécurité de l'information et aux processus de dématérialisation ou de conservation

Mesure

Il convient de définir et d'attribuer toutes les responsabilités en matière de sécurité de l'information, en particulier celles liées à l'exécution des processus de dématérialisation ou de conservation et celles qui consistent à s'assurer de la conformité des processus et de la gestion opérationnelle aux politiques et aux documents applicables.

Préconisations de mise en œuvre

Il convient d'attribuer les responsabilités conformément à la politique de sécurité de l'information (voir 5.1.1 de l'ISO/IEC 27002:2013) et à la politique de dématérialisation ou de conservation (voir 5.2.1 du présent document).

Il convient de déterminer les responsabilités relatives à la protection des actifs et la mise en œuvre de processus de sécurité spécifiques et des processus de dématérialisation ou de conservation.

Il convient de déterminer les responsabilités liées aux activités de gestion des risques en matière de sécurité de l'information et d'exploitation des processus de dématérialisation ou de conservation et en particulier, celles liées à l'acceptation des risques résiduels. Si nécessaire, il convient de compléter ces responsabilités de directives détaillées, appropriées à certains sites et moyens de traitement de l'information.

Il convient de préciser les domaines de responsabilité de chacun et notamment de prendre les mesures suivantes :

a. il convient d'identifier et de déterminer les actifs et les processus de sécurité ainsi que les processus de dématérialisation ou de conservation ;
b. il convient d'affecter une personne ou une entité responsable à chaque actif ou processus et de documenter ses responsabilités dans le détail (voir 8.1.2) ;
c. il convient de définir et de documenter les différents niveaux d'autorisation ;
d. pour être à même d'assurer les responsabilités, il convient que les personnes désignées soient compétentes dans ce domaine et qu'elles bénéficient de facilités pour se tenir au courant des évolutions ;
e. Il convient d'identifier et de documenter les activités de coordination et de supervision liées aux relations avec les fournisseurs.

Il convient de désigner pour chaque processus de dématérialisation ou de conservation une personne pour chacune des responsabilités suivantes :

a. la gestion de la documentation (politiques, procédures) supportant ces processus,
b. leur définition au niveau opérationnel, incluant le SDC et les mécanismes de sécurité associés,
c. la supervision de leur mise en œuvre,
d. la définition de leurs critères de performances,
e. leur évaluation selon les critères de performances,
f. l'émission de recommandations en vue d'améliorer leur gestion opérationnelle.

Informations supplémentaires

Les personnes auxquelles ont été attribuées des responsabilités peuvent déléguer des tâches. Néanmoins, elles demeurent responsables et il convient qu'elles s'assurent de la bonne exécution de toute tâche déléguée.

6.1.2 Séparation des tâches

Préconisations de mise en œuvre

Il convient de s'assurer que les personnes assumant des rôles et des responsabilités dans la gestion de processus ou d'activités de la sécurité de l'information ou opérationnels liés à la dématérialisation ou la conservation, n'assument pas également la revue de l'efficacité de l'exécution de ces rôles et responsabilités ainsi que l'évaluation de leur conformité à des objectifs définis.

Il convient d'assurer une séparation effective des activités d'administration, d'opérations et de sécurité non seulement dans la description des rôles, mais aussi dans l'attribution des privilèges pour les comptes des utilisateurs autorisés à accéder au SDC, de manière à réduire les risques de conflits d'intérêts et d'accès non autorisés.

Pour respecter le principe de non-répudiation, il convient de pouvoir démontrer que les privilèges d'accès établis pour l'ensemble des utilisateurs du SDC, y compris les accès à travers des comptes techniques, respectent le principe de séparation effective des activités d'administration, d'opérations et de sécurité du système de conservation.

6.1.5 La sécurité de l'information dans la gestion de projet

Préconisations de mise en œuvre

Il convient de rédiger et d'approuver les procédures de gestion du SDC dans la définition et la mise en œuvre des projets de dématérialisation ou de conservation.

Une catégorie de mesures additionnelles à la norme ISO/IEC 27002:2013 est :

6.3 Organisation interne spécifique aux processus de dématérialisation et de conservation

Objectif : Établir un cadre de gestion pour assurer le respect des exigences légales spécifiques des processus de dématérialisation ou de conservation au sein de l'organisation.

6.3.1 Vérification des documents numériques après dématérialisation

Mesure

Il convient d'exercer une vérification du contenu des documents numériques par rapport aux documents analogiques correspondants.

Préconisations de mise en œuvre

En ce qui concerne le processus de dématérialisation, il convient d'implémenter des

a. mécanismes de vérification de l'adéquation du nombre de documents analogiques en entrée (ou du nombre de pages composant ces documents) avec le nombre de documents (ou de pages) en sortie (numériques et analogiques rejetés), et des
b. mécanismes de vérification du contenu des documents numériques résultant de la numérisation de documents analogiques pour s'assurer de la reproduction conforme à l'original.

6.3.2 Principes du double contrôle pour la modification ou la suppression d'archives numériques

Mesure

Il convient de s'assurer que toute modification ou suppression des archives numériques créées, qui n'étaient pas programmées lors de la définition du projet de conservation, nécessitent l'approbation de deux utilisateurs autorisés à exécuter ces opérations.

6.3.3 Gestion des preuves

Mesure

Il convient d'établir une procédure et de mettre en œuvre une gestion adéquate des preuves du fonctionnement du SDC et des activités effectuées par le personnel concerné.

Préconisations de mise en œuvre

Il convient de s'assurer que l'intégrité du fonctionnement du SDC, des documents numériques et des archives numériques gérées par le SDC est vérifiée de manière régulière et suite à une modification significative du SDC et du processus de conservation.

6.3.4 Relations avec l'autorité nationale

Mesure

Il convient de mettre en application des procédures pour notifier aux autorités compétentes, en particulier l'ILNAS, les prévisions de changements significatifs pouvant impacter la sécurité de l'information et les activités opérationnelles ainsi que, dans les meilleurs délais et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence potentiellement importante sur le service de dématérialisation ou de conservation.

Préconisations de mise en œuvre

Il convient notamment de considérer comme changements significatifs :

a. un changement de direction de l'organisation,
b. une modification du SDC impactant les processus associés,
c. une modification du périmètre d'activités gérées par des fournisseurs impactant les processus de dématérialisation ou de conservation exécutés par l'organisation.

Une catégorie de mesures additionnelles à la norme ISO/IEC 27002:2013 est :

6.4 Organisation des processus de dématérialisation et de conservation impliquant les clients

Objectif : Clarifier les responsabilités entre le PSDC et ses clients et assurer la transparence en matière de sécurité et d'exploitation des processus de dématérialisation ou de conservation envers les clients.

6.4.1 La sécurité dans les accords avec le client

Mesure

Il convient d'établir les conditions d'exécution des processus de dématérialisation ou de conservation, ainsi que les besoins de sécurité de l'information associés à ces processus avec le client dans un document contractuel approuvé par le client et le PSDC.

Préconisations de mise en œuvre

Si le client est interne à l'organisation ou appartient à la même entité juridique, le document contractuel peut être remplacé par un document interne établi et validé selon les pratiques de gestion documentaire de l'organisation.

Il convient d'établir avec le client les éléments suivants dans le cadre de la gestion d'un projet de dématérialisation ou de conservation :

a. le besoin en informations du client liées aux processus de dématérialisation ou de conservation ;
b. la description détaillée du projet de dématérialisation ou de conservation, en prenant en compte les aspects techniques, opérationnels, sécuritaires, légaux et réglementaires ;
c. la base de référence des mesures de sécurité et les mesures additionnelles mises en exploitation pour assurer l'authenticité, la fiabilité et l'exploitation des documents collectés (analogiques et numériques),

des documents numériques et des archives numériques du client pendant l'exécution des processus de dématérialisation ou de conservation ;

d. les niveaux de service liés à l'exécution du SDC ;
e. la gestion des changements organisationnels et techniques pouvant impacter les processus de dématérialisation ou de conservation, ainsi que le SDC ;
f. la gestion des incidents (majeurs) impactant les processus de dématérialisation ou de conservation, ainsi que le SDC ;
g. le processus et les modalités à appliquer pour l'évaluation des services ainsi que l'acceptation des services par le client ;
h. les rôles et responsabilités du client et de l'organisation dans le cadre de la mise en œuvre du projet et les conséquences en cas de non-respect de ces rôles et de ces responsabilités ;
i. les points de contacts du client et de l'organisation, d'un point de vue contractuel, opérationnel et de la sécurité de l'information ;
j. l'implication du client dans l'appréciation et le traitement des risques.

La base de référence des mesures de sécurité et les mesures additionnelles mises en exploitation peuvent être documentées dans la déclaration d'applicabilité (voir ISO/IEC 27001) ou dans un document appelé « exigences d'assurance de sécurité » selon les Critères Communs (voir ISO 15408).

Il convient que le client s'engage en particulier à fournir et maintenir une liste de personnes autorisées à :

a. soumettre et à récupérer des documents analogiques ;
b. accéder aux documents numériques résultants de la numérisation des documents analogiques ou aux archives numériques ;
c. utiliser le SDC ;
d. demander la destruction et la suppression des documents collectés (analogiques et numériques), des documents numériques résultants de la numérisation des documents analogiques ou des archives numériques.

Informations supplémentaires

Un changement d'un document contractuel nécessite l'accord des parties contractantes.

C'est à ce niveau que des mesures de sécurité particulières exigées par le client et complémentaires à celles que le PSDC établit de sa propre initiative peuvent être spécifiées.

6.4.2 Obligation d'information préalable du client

Mesure

Préalablement à toute relation contractuelle avec un détenteur, il convient de mettre à disposition, sur un support durable et dans des termes aisément compréhensibles, les informations relatives aux conditions de prestation de service, en particulier toutes les informations légalement requises pour assurer un service transparent.

Préconisations de mise en œuvre

Il convient que le PSDC inclue dans les informations données à ses clients avant d'établir un contrat :

a. la procédure suivie pour la dématérialisation ou pour la conservation,
b. la procédure suivie afin de restituer les copies à valeur probante sous une forme lisible en garantissant la fidélité à l'original,
c. les modalités et conditions d'une éventuelle sous-traitance y compris le lieu de stockage des données,
d. les obligations légales que le PSDC doit observer,

e. les conditions contractuelles de réalisation des prestations, y compris les limites éventuelles de responsabilité du PSDC,
f. les normes et procédures mises en œuvre ainsi que les caractéristiques techniques essentielles des installations utilisées pour la réalisation des prestations,
g. les modalités d'information du client en cas de changement.

Il convient de convenir avec les clients (internes ou externes à l'organisation) qui sont impactés le déroulement détaillé et les règles à suivre dans le cadre de l'exécution et des processus de dématérialisation et de conservation.

Il convient d'inclure ce déroulement détaillé et ces règles dans les procédures d'exploitation des processus de dématérialisation et de conservation, et de les faire approuver par les clients concernés.

Il convient d'impliquer le client dans les changements des procédures qu'il a approuvées.

Il convient d'inclure dans ces procédures le déroulement détaillé :

a. de la collecte des documents analogiques (pour le processus de dématérialisation seulement),
b. de la collecte des documents numériques (pour la conservation),
c. du stockage temporaire des documents numériques,
d. de la création et la conservation des archives numériques (pour la conservation),
e. de la restitution, le transfert et la suppression des archives numériques (pour la conservation).

Il convient de notifier le client d'une suppression programmée d'une archive numérique du client si un calendrier de suppression spécifique à cette archive a été rédigé lors de la définition du projet de conservation.

En cas d'absence de calendrier de suppression pour une archive numérique, il convient de demander au préalable au client l'autorisation de la supprimer.

6.4.3 Classification des actifs du client

Mesure

Il convient que le client définisse avec le PSDC pour tous ses documents analogiques ou numériques et toutes ses archives numériques le niveau de classification, la durée de rétention, ainsi que les éventuelles autres exigences de sécurité comme les droits d'accès particuliers.

Préconisations de mise en œuvre

Il convient que le client assume le rôle du propriétaire pour les informations qui lui appartiennent et qui sont gérées par l'organisation.

Il convient de sensibiliser le client au fait qu'il est responsable des exigences de classification définies et appliquées à ses documents (documents collectés, documents numériques ou archives numériques).

6.4.4 Obligation d'information du client en cas de changements ou d'incidents

Mesure

Il convient d'informer, avant la mise en application ou dans les plus brefs délais, les clients internes ou externes concernés de tout changement des informations préalables et des informations liées aux obligations contractuelles, ainsi que de tout incident pouvant mettre en danger les informations du client, tout en donnant les justifications nécessaires.

Préconisations de mise en œuvre

Il convient d'informer dans les plus brefs délais le client

a. en cas de survenance d'incidents pouvant impacter :
    1. les documents du client,
    2. les processus de dématérialisation ou de conservation utilisés par le client ou pour son compte,
    3. le SDC utilisé par le client ou pour son compte ;
b. en cas de tentatives d'accès aux documents du client gérés par l'organisation avec les identifiants de connexion du client et hors des conditions normales de leur utilisation, par exemple hors des heures normales de bureau.

Il convient de considérer comme changements significatifs les changements signalés à l'autorité nationale (voir 6.3.4).

Il convient d'appliquer une conversion d'une archive numérique dans un format différent de son format initial que sur confirmation écrite du client (interne à l'organisation et externe) concerné par cette archive.

Il convient d'informer le client sur l'effet du changement sur l'appréciation des risques.

Il convient de garder une preuve que cette information a eu lieu, et si le temps avant la mise en application est court, de demander l'approbation du client.

7 La sécurité des ressources humaines

7.2 Pendant la durée du contrat

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

7.2.4 Engagement envers les politiques

Mesure

Il convient que le personnel interne et celui des fournisseurs, s'ils sont impliqués dans la gestion opérationnelle de la sécurité ou des processus de dématérialisation ou de conservation, comprennent et s'engagent par écrit à respecter la politique de sécurité et la politique de dématérialisation ou de conservation.

Préconisations de mise en œuvre

Il convient que le personnel interne et celui des fournisseurs impliqués dans la gestion opérationnelle de la sécurité ou des processus de dématérialisation ou de conservation

1. soient correctement informés de leurs rôles et responsabilités liés aux processus de dématérialisation ou de conservation ;
2. s'engagent par écrit à respecter les politiques de dématérialisation ou de conservation et la politique de sécurité de l'information ;
3. assistent à une formation initiale sous forme de sensibilisation pour présenter les politiques, les attentes et les besoins de l'organisation en la matière, afin de s'assurer d'une compréhension commune de ces éléments ;
4. assistent à une formation continue de manière à rappeler les exigences liées à la dématérialisation ou à la conservation et à présenter les procédures associées à ces exigences et les récentes modifications apportées à l'ensemble de la documentation liée aux domaines concernés.

8. Gestion des actifs

8.1 Responsabilités relatives aux actifs

Des préconisations de mise en œuvre additionnelles sont :

8.1.1 Inventaire des actifs

Préconisations de mise en œuvre

Il convient d'identifier :

a. les processus de dématérialisation ou de conservation,
b. les composants des systèmes de dématérialisation ou de conservation,
c. les clients,
d. les documents collectés (analogiques et numériques) des clients,
e. les documents numériques résultants de la numérisation des documents analogiques des clients,
f. les archives numériques des clients.

8.1.2 Propriété des actifs

Préconisations de mise en œuvre

Il convient que le propriétaire de chaque actif processus de dématérialisation ou de conservation

d. approuve l'évaluation des aspects opérationnels du SDC au moins une fois par an et suite à une modification significative ;
e. revoie la description détaillée du SDC et les spécifications des mécanismes de sécurité du système de conservation de manière régulière (au moins une fois par an) et suite à une modification significative du SDC.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

8.1.4. Cloisonnement d'informations secrètes ou d'informations à caractère personnel

Mesure

Il convient de cloisonner d'éventuelles informations secrètes ou informations à caractère personnel de façon suffisante pour notamment pouvoir donner suite à la demande du propriétaire de les détruire sans mettre en danger d'autres informations archivées ou les preuves de la bonne gestion pour d'autres informations dématérialisées ou conservées.

Préconisations de mise en œuvre

En vue de respecter le règlement européen sur la protection des données à caractère personnel, en particulier le droit à l'oubli, il convient que le client ou le PSDC s'abstienne de mettre dans les métadonnées des informations à caractère personnel, si ces métadonnées font partie du système de traçabilité des opérations.

8.2 Classification de l'information

Des préconisations de mise en œuvre additionnelles sont :

8.2.1 Classification des informations

Préconisations de mise en œuvre

Il convient de définir des niveaux de classification et de les attribuer aux actifs inventoriés en intégrant les exigences relatives à l'authenticité, à la fiabilité et à l'exploitation aussi longtemps que nécessaire.

Il convient d'assurer une revue de ces lignes directrices en cas de changement des spécificités du SDC et en cas de changement des attentes des clients.

Informations supplémentaires

Un critère « fiabilité » peut être défini en complément d'autres critères. Il peut contenir plusieurs niveaux de précision d'une dématérialisation (couleur versus noir et blanc, encodage de la couleur, résolution) et attribuer un tel niveau spécifiquement aux documents collectés des clients et aux archives numériques des clients.

Le critère d'intégrité peut être utilisé pour inclure les exigences liées à l'authenticité.

Le critère de disponibilité peut être utilisé pour inclure les exigences liées à l'exploitabilité.

8.3 Manipulation des supports

Des préconisations de mise en œuvre additionnelles sont :

8.3.2 Mise au rebut des supports

Préconisations de mise en œuvre

Il convient d'envisager :

a. la destruction des éléments suivants, par des mécanismes sécurisés :
    1. les documents analogiques des clients selon les conditions définies dans les documents contractuels établis entre les clients et l'organisation,
    2. tout support de stockage de l'organisation contenant les informations des clients (incluant les documents et archives numériques) ou de nature confidentielle à l'organisation,
    3. la suppression de toutes les informations des clients, contenues dans les supports de stockage de l'organisation par des mécanismes sécurisés si ces supports ne peuvent pas être détruits de manière sécurisée ;
b. l'évaluation par un tiers pouvant attester l'effectivité de la destruction et de la suppression ;
c. en cas de recours à un fournisseur, la production d'une attestation de ce fournisseur stipulant que :
    1. les supports de stockage remis au tiers par l'organisation en vue de leur destruction sont bien ceux qui ont été détruits,
    2. les informations stockées dans les supports de stockage remis par l'organisation en vue de leur suppression ont bien été supprimées,
    3. la destruction des documents analogiques et des supports de stockage et la suppression des informations stockées dans ces supports ont été respectivement effectuées par une méthode sécurisée basée sur les bonnes pratiques en la matière.

9 Contrôle d'accès

9.1 Exigences métier en matière de contrôle d'accès

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

9.1.3 Ségrégation effective liée aux droits d'accès

Mesure

Il convient d'impliquer trois personnes différentes dans la gestion d'un droit d'accès : une pour l'autorisation de l'accès, une pour la vérification du respect des exigences de sécurité, et finalement une pour l'attribution de l'accès sur les systèmes.

Préconisations de mise en œuvre

Il convient qu'un administrateur de droits d'accès sur un SDC n'attribue ce droit que si le droit a été formellement autorisé selon la politique des droits d'accès pour une autre personne et que le respect des exigences de sécurité avec ce droit a été validé par une personne différente.

10 Cryptographie

10.1 Mesures cryptographiques

Des préconisations de mise en œuvre additionnelles sont :

10.1.1 Politique d'utilisation des mesures cryptographiques

Préconisations de mise en œuvre

Lors de l'élaboration d'une politique cryptographique, il convient de prendre en compte le point suivant :

h. l'application des services de confiance qualifiés conformes au règlement eIDAS pour assurer la sécurité des documents dématérialisés et archives numériques.

Informations supplémentaires

La norme ETSI TS 102 176-1 énumère des algorithmes cryptographiques et recommande une durée de validité de leur utilisation.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

10.1.3 Authentification à deux facteurs

Mesure

Pour les personnes qui interagissent avec les actifs techniques du système de conservation ou qui accèdent aux documents numériques et aux archives numériques, il convient d'assurer une authentification appropriée et sécurisée basée sur des mécanismes cryptographiques et, si l'accès est possible à partir de locaux ne requérant pas d'authentification à deux facteurs à l'entrée, une authentification à deux facteurs.

Préconisations de mise en œuvre

Il convient d'utiliser un dispositif sécurisé, par exemple une carte à puce ou une clé USB cryptographique contenant un certificat électronique d'authentification, un dispositif physique d'authentification ou des

techniques de biométrie pour s'assurer de l'authentification sécurisée d'un utilisateur aux actifs techniques du système de conservation, aux documents numériques et aux archives numériques gérés par le système de conservation.

Il convient d'utiliser un dispositif de filtrage d'adresses IP associé à un moyen cryptographique, par exemple un certificat SSL, pour s'assurer de l'authentification sécurisée d'un actif technique du système de conservation aux autres actifs du système de conservation, aux documents numériques et aux archives numériques gérés par le système de conservation.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

10.1.4 Protection de l'intégrité des documents numériques ou des archives numériques

Mesure

Il convient de protéger l'intégrité des documents numériques collectés par le système de conservation et des archives numériques générées par le système de conservation avec des algorithmes et techniques cryptographiques appropriés.

Préconisations de mise en œuvre

Il convient de protéger l'intégrité des documents numériques collectés par le système de conservation et des archives numériques générées par le système de conservation pour s'assurer que ces documents sont correctement stockés, traités et supprimés et que ces archives sont correctement créées, exploitées, restituées, transférées ou supprimées.

Il convient que pour chaque document numérique à archiver, son empreinte digitale soit calculée par l'émetteur de ce document et transmise de manière sécurisée à l'organisation qui vérifiera l'intégrité du document numérique reçu en calculant et en obtenant une empreinte digitale identique à celle transmise par l'émetteur du document.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

10.1.5 Protection de l'intégrité des documents internes

Mesure

Il convient de protéger l'intégrité des documents internes au SDC et aux processus y liés, en particulier les journaux d'événements du SDC, avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.

Préconisations de mise en œuvre

Il convient de protéger l'intégrité des documents internes dans le temps, en particulier des journaux d'événements ou des opérations de vérification.

Il convient en particulier de s'assurer de :

a. l'établissement d'un schéma de liaison pour lier les événements enregistrés d'un journal entre eux permettant de détecter toute suppression d'événements survenus par le passé,
b. l'horodatage régulier, par exemple une fois par jour, des journaux d'événements par une autorité d'horodatage qualifiée.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

10.1.6 Signature électronique des documents internes

Mesure

Il convient que les utilisateurs du SDC utilisent une signature qualifiée ou un mécanisme apportant une garantie équivalente pour valider les documents internes nécessaires à prouver le bon fonctionnement du SDC et des processus y liés.

Préconisations de mise en œuvre

Il convient d'utiliser un dispositif sécurisé pour permettre :

a. à un utilisateur du système de conservation de signer électroniquement des rapports d'activités d'administration, d'opérations et de sécurité du système de conservation de manière à s'assurer de l'authenticité des activités effectuées,
b. à une personne de l'organisation de signer électroniquement les transmissions d'informations, de documents numériques et d'archives numériques à destination des clients (internes ou externes à l'organisation) et des autorités compétentes de manière à s'assurer de l'authenticité des envois.

Le dispositif de création de signature électronique qualifié et le certificat électronique qualifié utilisé doivent répondre aux exigences définies par l'Union européenne en la matière.

Il convient également d'utiliser des formats de signatures électroniques comme CAdES [5], XAdES [6] et PAdES [7] pour maintenir une pérennité de la signature électronique, des informations, des documents numériques et des archives numériques attachés à cette signature.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

10.1.7 Protection des transmissions de documents

Mesure

Il convient de protéger la transmission d'informations et de documents numériques avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.

Préconisations de mise en œuvre

Il convient d'utiliser un protocole sécurisé (SFTP, TLS, PPP, L2TP et IPSec…) pour sécuriser la transmission d'informations, de documents numériques et d'archives numériques entre les éléments suivants :

a. les actifs techniques du système de conservation, même pour ceux appartenant à un même réseau ;
b. les parties concernées par le processus de conservation comme l'organisation, les clients (internes ou externes à l'organisation) et les autorités compétentes.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

10.1.8 Conservation des signatures électroniques

Mesure

Si l'intégrité d'un document numérique à archiver repose sur une signature électronique, il convient de conserver le document avec la preuve que la signature a été vérifiée au plus tard au moment de l'archivage.

Préconisations de mise en œuvre

Il convient de démontrer l'intégrité du document en démontrant :

a. qu'au moment de l'archivage, la signature électronique était correcte, le certificat électronique qualifié y apposé était valide et issu d'une autorité de certification reconnue ;
b. que le système d'archivage conserve l'intégrité des documents archivés aussi longtemps que nécessaire.

Informations supplémentaires

Plusieurs techniques sont possibles à cette fin comme :

a. l'utilisation du protocole de vérification en ligne de certificats (OCSP) de l'autorité de certification émettrice du certificat électronique qualifié,
b. l'horodatage du rapport d'activités signé et récupération de la liste de révocation des certificats (CRL) publiée régulièrement par l'autorité de certification émettrice du certificat électronique qualifié.

11 Sécurité physique et environnementale

11.1 Zones sécurisées

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

11.1.7 Accompagnement des visiteurs

Mesure

Il convient qu'un membre de l'organisation habilité accompagne de manière permanente tous les visiteurs de l'organisation, même si l'accès à ces zones leur a déjà été autorisé.

Préconisations de mise en œuvre

Il convient d'assurer que les visiteurs n'accèdent pas aux zones associées au processus de dématérialisation, notamment en cas d'activités de traitement de documents analogiques de clients pour réduire les risques de divulgation non autorisée d'informations.

Il convient de prendre les mesures nécessaires pour s'assurer que les visiteurs ne puissent pas voir des informations des clients.

Il convient d'assurer une surveillance effective des tiers autorisés de manière permanente à accéder aux zones sécurisées de l'organisation dès qu'ils accèdent aux actifs techniques du SDC et aux documents des clients.

Il convient de protéger les actifs techniques du SDC contre des accès non autorisés :

a. en cas d'évacuation des zones hébergeant ces actifs,
b. au cas où ils sont situés dans des sites multioccupants.

11.2 Matériels

Des préconisations de mise en œuvre additionnelles sont :

11.2.1 Emplacement et protection du matériel

Préconisations de mise en œuvre

Il convient de considérer les documents analogiques des clients comme des actifs nécessitant une protection spéciale (au sens de 11.2.1.d de la norme ISO/IEC 27002:2013) au niveau des conditions ambiantes et des autres menaces liées.

11.2.5 Sortie des actifs

Préconisations de mise en œuvre

Il convient de ne pas sortir de l'organisation sans autorisation préalable du client des documents analogiques du processus de dématérialisation, excepté pour prévenir la destruction de ces actifs en cas de catastrophe.

12 Sécurité liée à l'exploitation

12.1 Procédures et responsabilités liées à l'exploitation

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

12.1.5 Procédures d'exploitation du SDC

Mesure

Il convient de définir, mettre en œuvre, et faire suivre par le personnel concerné (de l'organisation et des fournisseurs) des procédures d'administration, d'opérations du SDC, d'exploitation du processus de dématérialisation ou de conservation, et de contrôle de la sécurité du SDC et des processus incluant toutes les règles à suivre nécessaires pour assurer les propriétés de confidentialité, d'intégrité, de disponibilité, d'authenticité, de fiabilité et d'exploitabilité.

Préconisations de mise en œuvre

Il convient d'inclure dans les procédures de gestion du SDC les activités suivantes :

a. la gestion des accès au SDC et des privilèges associés aux comptes du SDC ;
b. la gestion des fonctionnalités d'administration, d'opérations et de sécurité du SDC et des instructions pour les exécuter ;
c. la gestion de la configuration du SDC ;
d. l'instruction du fonctionnement du SDC en mode dégradé, de son redémarrage et de sa récupération ;
e. la gestion des mécanismes de surveillance du SDC ;
f. la gestion des journaux d'événements du SDC et des instructions pour leur exploitation ;
g. la gestion des mécanismes cryptographiques de sécurité du SDC, comme les suivants :
    1. les mécanismes d'authentification et de signature des utilisateurs du SDC,
    2. les protocoles sécurisés de transmission d'informations, de documents numériques et d'archives numériques,
    3. les mécanismes d'intégrité des documents numériques, des archives numériques et des journaux d'événements, ainsi que

4. le remplacement de ces mécanismes en cas de découverte de vulnérabilités sans altérer l'exploitabilité et l'intégrité des archives ;

h. si c'est convenu dans l'accord avec les clients, la gestion des mécanismes de détection et de suppression de codes malveillants ;

i. gestion des mécanismes de contrôle régulier d'intégrité du SDC ;

j. gestion des mécanismes de suppression des documents numériques et des archives numériques gérées par le SDC ;

k. gestion des supports de stockage du SDC, de leur remplacement et de leur mise au rebut ;

l. gestion des sauvegardes du SDC, des sauvegardes des documents numériques et des archives numériques gérées par le SDC et de leur restauration respective ;

m. gestion de la continuité et de la reprise du SDC même en cas de désastre ;

n. gestion des changements du SDC ;

o. gestion des incidents pouvant impacter le SDC ;

p. maintenance des actifs techniques avec gestion du support des fournisseurs en cas de dysfonctionnement du SDC ;

q. gestion des métadonnées de description et de contrôle associées aux archives numériques ;

et en plus pour les processus de dématérialisation :

r. la gestion des mécanismes de vérification de l'adéquation du nombre de documents analogiques (ou du nombre de pages composant ces documents) numérisés ;

s. la gestion des mécanismes de vérification du contenu des documents numériques.

Des préconisations de mise en œuvre additionnelles sont :

12.4 Journalisation et surveillance

12.4.1 Journalisation des événements

Préconisations de mise en œuvre

Il convient d'identifier et d'enregistrer dans des journaux tous les événements en lien avec le SDC, en particulier :

a. les événements système des actifs du SDC,

b. les erreurs et dysfonctionnements des actifs du SDC,

c. les erreurs et dysfonctionnements liés à la génération de journaux d'événements,

d. les événements liés aux documents analogiques, aux documents numériques et aux archives numériques traitées par le SDC.

12.4.3 Journaux administrateur et opérateur

Préconisations de mise en œuvre

Il convient d'identifier et d'enregistrer dans des journaux toutes les activités effectuées par les comptes des utilisateurs du SDC, incluant les activités effectuées hors de conditions normales d'utilisation du SDC en lien avec le SDC, en particulier :

a. les tentatives de connexion d'utilisateurs hors des heures normales de bureau,

b. les activités effectuées par les utilisateurs dans un laps de temps plus court que la normale, pouvant conduire à suspecter qu'elles sont réalisées par des actifs techniques et non des personnes physiques,

c. la duplication de sessions utilisateurs.

12.4.4 Synchronisation des horloges

Préconisations de mise en œuvre

Il convient d'assurer que :

a. les actifs techniques supportant le SDC soient synchronisés avec le temps universel coordonné (UTC), *via* une source de temps faisant autorité,
b. les événements liés à la synchronisation régulière de l'horloge système des actifs techniques du SDC soient enregistrés et conservés aussi longtemps que nécessaire,
c. un unique format de la date et de l'heure soit adopté pour la génération des événements du SDC pour faciliter la traçabilité des actions effectuées,
d. une synchronisation avec l'horloge maîtresse soit faite de façon suffisamment régulière pour s'assurer que la variation entre l'horloge maître et l'horloge des systèmes dans le périmètre reste en dessous du seuil d'une seconde,
e. toute variation supérieure à la variation tolérée soit détectée dans les plus brefs délais afin que des actions correctrices puissent être adoptées,
f. des éléments de vérification de l'exactitude de l'horloge, comme des jetons d'horodatage sont générés dans le cadre du fonctionnement du SDC.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

12.4.5 Exploitabilité des journaux d'événements

Mesure

Il convient de conserver les journaux d'événements générés sous une forme exploitable et protégée contre toute manipulation et suppression non autorisées pour assurer une traçabilité aussi longtemps que nécessaire de tous les événements enregistrés par ces mécanismes.

Préconisations de mise en œuvre

Il convient de centraliser l'information journalisée en lien avec le SDC.

Il convient d'utiliser des supports de stockage pérennes pour une conservation appropriée aussi longtemps que nécessaire des journaux d'événements.

Une catégorie de mesures additionnelle à la norme ISO/IEC 27002:2013 est :

12.8 Gestion correcte et sécurisée du SDC

Objectif : assurer la gestion correcte et sécurisée des documents analogiques à dématérialiser, des documents numériques et des archives numériques dans le cadre du processus de dématérialisation ou de conservation.

12.8.1 Adéquation du SDC

Mesure

Il convient de démontrer que le SDC est composé d'actifs techniques et de mécanismes de sécurité répondant aux besoins des clients et permettant de garantir l'authenticité, la fiabilité et l'exploitation des documents analogiques à dématérialiser, des documents numériques et des archives numériques gérées par ce système.

12.8.2 Description détaillée du SDC

Mesure

Il convient de définir et de maintenir une description détaillée et compréhensible du SDC comprenant les actifs techniques, les aspects fonctionnels et opérationnels ainsi que les flux et les dépendances entre les différentes composantes.

Préconisations de mise en œuvre

Il convient de définir et de maintenir une description détaillée et compréhensible du SDC :

a. en identifiant et en documentant les actifs techniques supportant les processus sous-jacents au processus de dématérialisation ou de conservation, à savoir :
   1. la collecte des documents analogiques ou numériques,
   2. le stockage temporaire de ces documents,
   3. la création de documents numériques ou des archives numériques,
   4. la restitution, le transfert, la destruction éventuelle des documents analogiques, et la suppression des archives numériques ;

b. en identifiant, en évaluant et en documentant de manière régulière les aspects fonctionnels et opérationnels du SDC, comme les suivants :
   1. pour le système de dématérialisation, pour chaque scanneur,
      i. les nombres minimum et maximum de couleurs et les niveaux de gris,
      ii. les nombres minimum et maximum de dpi, de bits par pixel,
      iii. la possibilité de dématérialisation recto/verso ou uniquement verso,
      iv. les différents formats à l'entré, comme A3, A4 et A5,
      v. les méthodes de correction d'images, comme le redressement, la suppression de points isolés, et la suppression des marges,
      vi. les méthodes de compression des images,
      vii. le nombre de documents analogiques ou nombre de pages composant les documents analogiques pouvant être numérisés dans un laps de temps donné ;
   2. pour le système de conservation,
      i. le nombre maximum ou la taille maximum de documents numériques pouvant être transmis en un lot,
      ii. le débit de transmission des documents numériques ou de restitution d'archives numériques,
      iii. les délais de réponse,
      iv. la fréquence d'émission des lots ou de restitutions d'archives numériques,
      v. les protocoles sécurisés de transmission d'informations, de documents numériques et d'archives numériques supportées, comme SFTP, TLS, PPP, L2TP et IPSec.

c. en documentant sur des schémas l'architecture du réseau, les flux de données entre les actifs, les dépendances entre les actifs.

12.8.3 Mécanismes de sécurité du SDC

Mesure

Il convient de gérer et de documenter les mécanismes de sécurité du SDC permettant d'assurer l'authenticité, la fiabilité et l'exploitation des documents analogiques, des documents numériques et des archives numériques gérés par ce système.

Préconisations de mise en œuvre

Il convient en particulier de gérer les mécanismes de sécurité suivants :

a. Mécanismes de gestion des accès au SDC.

   Il convient de protéger les accès aux actifs techniques du SDC, aux documents analogiques, aux documents numériques et aux archives numériques gérés par le SDC en :

   1. s'assurant que les conditions d'accès à ces actifs s'appliquent à toute personne physique et à tout actif tentant d'y accéder,
   2. assurant une gestion adéquate des comptes des utilisateurs autorisés à accéder au SDC et des comptes techniques des actifs techniques du SDC, avec une capacité de révocation immédiate de ces comptes,
   3. en identifiant sans ambigüité les activités et les actions système effectuées et en pouvant les attribuer de façon incontestable à un auteur, par exemple en attribuant des comptes personnels à chaque utilisateur,
   4. gérant des mécanismes d'authentification appropriés et sécurisés pour les comptes des utilisateurs autorisés et les comptes techniques des actifs techniques du SDC.).

b. Mécanismes de gestion des privilèges.

   Il convient d'assurer une gestion des privilèges pour l'ensemble des comptes des utilisateurs du SDC et des comptes techniques des actifs techniques du SDC (voir 6.1.2 et 6.1.6).

c. Mécanismes de surveillance (voir 12.4.3).

d. Mécanismes cryptographiques de sécurité (voir 10.1).

e. Mécanismes de détection et de suppression de codes malveillants contenus dans des documents numériques collectés en vue de leur conservation électronique, si c'est demandé par le client.

   Il convient d'utiliser au minimum un antivirus pour vérifier que tous les documents numériques collectés en vue de leur conservation électronique ne contiennent pas de codes malveillants, comme des virus, des chevaux de Troie et des vers de réseau.

   Il convient de l'utiliser dès la réception par le SDC des documents numériques et avant le démarrage du processus de création des archives numériques.

f. Mécanismes de suppression sécurisée des documents et archives numériques, comme une réécriture multiple sur les informations ne permettant plus de les retrouver en l'état.

g. Mécanismes de conversion (si nécessaire) des archives numériques dans un format différent de leur format original.

12.8.4 Supervision des aspects opérationnels du SDC

Mesure

Il convient d'évaluer de manière régulière les aspects opérationnels du SDC comme l'espace disponible et les taux d'échecs de composants redondants.

Préconisations de mise en œuvre

Il convient

a. de définir une liste avec les aspects opérationnels du SDC à contrôler ;

b. de l'inclure dans la liste des éléments nécessaires de surveiller selon les exigences de l'évaluation des performances du système de management (voir ISO/IEC 27001 2013, chapitre 9.1) ;

c. d'établir des indicateurs de disponibilité des caractéristiques opérationnelles, comme les durées de vie des disques.

12.8.5 Contrôle régulier de l'intégrité du SDC

Mesure

Il convient d'implémenter des mécanismes de contrôle régulier de l'intégrité du SDC et des informations nécessaires pour assurer la traçabilité.

Préconisations de mise en œuvre

En ce qui concerne le SDC, il convient de s'assurer que :

a. le fonctionnement du SDC n'a pas été altéré suite à des :
   1. opérations de maintenance ou des mises à jour,
   2. remplacements d'actifs du SDC comme les scanneurs, la plateforme de conservation électronique ou des composants de ces actifs comme les supports de stockage ;
b. les fichiers de configurations du SDC n'ont pas été modifiés de manière non autorisée ;
c. l'intégrité est préservée en ce qui concerne les
   1. documents numériques stockés,
   2. métadonnées associées,
   3. archives numériques,
   4. journaux d'événements.

13 Sécurité des communications

Les objectifs, mesures, préconisations de mise en œuvre et informations supplémentaires de la norme ISO/IEC 27001:2013 s'appliquent sans modification.

14 Acquisition, développement et maintenance des systèmes d'information

14.1 Exigences de sécurité applicables aux systèmes d'information

Des préconisations de mise en œuvre additionnelles sont :

14.1.1 Analyse et spécification des exigences de sécurité de l'information

Préconisations de mise en œuvre

Il convient de s'assurer et de pouvoir démontrer que les applications critiques et les systèmes d'information supportant le SDC sont réalisés en respectant des méthodes de développement sécurisé reconnues.

Il convient d'évaluer et le cas échéant d'instaurer le principe de dépôts des codes source chez un tiers pour toute application du SDC fournie par un fournisseur et nécessaire à assurer l'intégrité et la disponibilité des informations.

15. Relations avec les fournisseurs

15.1 Sécurité de l'information dans les relations avec les fournisseurs

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

15.1.4 Conditions contractuelles pour les fournisseurs intervenant dans le processus de dématérialisation et de conservation.

Mesure

Il convient d'inclure dans les contrats établis avec chaque fournisseur intervenant dans le processus de dématérialisation et de conservation les conditions assurant le respect de la politique de sécurité et de la politique de dématérialisation et de conservation.

Préconisations de mise en œuvre

Pour tous les fournisseurs supportant les processus de dématérialisation ou de conservation exécutés par l'organisation, il convient d'étudier les conditions suivantes, puis d'inclure les conditions nécessaires pour maitriser les risques liés à l'activité du fournisseur, dans le document contractuel établi avec ce fournisseur :

a. des dispositions quant à la propriété des produits et des services, comme des documents et des applications, fournis par le fournisseur dans le cadre de son support aux processus de dématérialisation ou de conservation exécutés par l'organisation ;
b. des dispositions quant à la continuité de la délivrance des produits et des services fournis par le fournisseur dans le cadre de son support aux processus de dématérialisation ou de conservation exécutés par l'organisation, même en cas de désastre ;
c. le respect de la politique de dématérialisation ou de la politique de conservation de l'organisation ;
d. des mesures garantissant :
    1. une notification dans les plus brefs délais des changements sécuritaires appliqués aux actifs du fournisseur et de ses fournisseurs pouvant impacter les processus de dématérialisation ou de conservation exécutés par l'organisation,
    2. que les informations de l'organisation seront utilisées exclusivement pour les finalités pour lesquelles elles ont été rendues accessibles au fournisseur et à ses fournisseurs,
    3. que les changements de fournisseurs du fournisseur impliqués dans le support des processus de dématérialisation ou de conservation exécutés par l'organisation seront sujets à approbation préalable de l'organisation ;
e. l'engagement du fournisseur à coopérer avec l'organisation dans le cadre d'investigations effectuées par l'organisation pour la résolution d'un incident pouvant impacter les services ou produits fournis à l'organisation par le fournisseur et dont l'origine présumée ou avérée est autre que le fournisseur ou ses fournisseurs ;
f. le droit d'auditer les fournisseurs du fournisseur de manière équivalente à ce dernier et dans le périmètre de leur implication au niveau des processus de dématérialisation ou de conservation exécutés par l'organisation ;
g. la conformité du fournisseur et de ses fournisseurs aux lois et aux règlements en vigueur au Luxembourg ;
h. les points de contact de chaque partie concernée par le document contractuel, d'un point de vue contractuel, opérationnel et de la sécurité de l'information.

16 Gestion des incidents liés à la sécurité de l'information

16.1 Gestion des incidents liés à la sécurité de l'information et améliorations

Des préconisations de mise en œuvre additionnelles sont :

16.1.1 Responsabilités et procédures

Préconisations de mise en œuvre

Il convient de documenter dans une procédure les instructions précisant à partir de quel moment la gestion d'incidents est activée, la restauration est entamée et les autorités ou les clients concernés (internes ou externes à l'organisation) sont avertis de cet incident.

Informations supplémentaires

Voir mesure 6.1.6.

17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

Une catégorie de mesures additionnelle à la norme ISO/IEC 27002:2013 est :

17.3 Continuité de l'activité et du SDC

Objectif : assurer la gestion correcte de la continuité du SDC et des processus de dématérialisation ou de conservation.

17.3.1 Organisation de la continuité

Mesure

Il convient de déterminer les exigences pour la continuité des processus de dématérialisation ou de conservation en cas de situation défavorable, comme lors d'une crise ou d'un sinistre.

Préconisations de mise en œuvre

Il convient de définir pour les actifs dans le périmètre la durée maximale d'interruption admissible (DMIA) (anglais : Return Time on Objective – RTO) et la perte de données maximale admissible (PDMA) (anglais : Recovery Point Objective – RPO) en tenant compte des exigences des clients et de l'obligation de restitution des documents.

Informations supplémentaires

La Norme internationale ISO/IEC 22301:2014 relative à la « Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences » spécifie les exigences pour planifier, établir, mettre en place et en œuvre, opérer, contrôler, réviser, maintenir et améliorer de manière continue un système de management documenté afin de se protéger des incidents perturbateurs, réduire leur probabilité de survenance, s'y préparer, y répondre et de s'en rétablir lorsqu'ils surviennent. Elle permet à toute organisation, y compris à un PSDC, de concevoir un système de management de la continuité des activités qui soit adapté à ses besoins et qui satisfasse aux exigences des parties intéressées.

17.3.2 Mise en œuvre de la continuité

Mesure

Il convient d'établir, de documenter, de mettre en œuvre et de maintenir les processus, procédures et mesures pour assurer le niveau requis de continuité pendant une situation défavorable.

Préconisations de mise en œuvre

Il convient de définir un processus de reprise d'activé qui inclut les processus de dématérialisation ou de conservation et qui tient compte des exigences des clients, de l'obligation de restitution des documents, et des scénarios de risques qui peuvent interrompre le bon fonctionnement d'une activité.

Il convient de gérer des plans de continuité pour les processus de dématérialisation ou de conservation permettant d'adresser les situations défavorables selon les conditions définies.

Il convient de gérer un plan de reprise de l'activité du SDC permettant d'adresser les situations défavorables selon les conditions définies.

17.3.3 Vérifier, revoir et évaluer la continuité

Mesure

Il convient de vérifier la mise en œuvre des mesures liées à la continuité du SDC à intervalles réguliers pour s'assurer qu'elles sont toujours valides et en vigueur pendant une situation défavorable.

Préconisations de mise en œuvre

Il convient de tester les éléments clés des plans de continuité et des plans de reprises.

18 Conformité

18.1 Conformité aux obligations légales et réglementaires

Des préconisations de mise en œuvre additionnelles sont :

18.1.3 Protection des enregistrements

Préconisations de mise en œuvre

Il convient de conserver les preuves de la conformité des activités effectuées par le personnel concerné par rapport aux politiques et aux procédures liées au processus de dématérialisation ou de conservation exécuté par l'organisation en utilisant des supports de stockage appropriés pour une conservation aussi longtemps que nécessaire.

En particulier il convient de conserver les preuves suivantes :

a. les rapports d'activités des utilisateurs du SDC,
b. les rapports de mises à jour ou de changement du SDC,
c. les rapports d'événements et d'incidents lié aux processus de dématérialisation ou de conservation,
d. les rapports de revue des journaux d'événements du SDC ;
e. en cas de processus de dématérialisation :
    1. les bordereaux de récupération ou de livraison de documents analogiques ;
f. en cas de processus d'archivage :
    1. les rapports de conversion de documents numériques en archives numériques,
    2. les rapports de conversion d'archives numériques en cas de changements de format.

Il convient qu'une preuve liée aux activités effectuées par le personnel concerné contienne en particulier les informations suivantes :

a. les auteurs des activités effectuées,
b. les dates et heures des activités effectuées,
c. les lieux des activités effectuées,
d. les actifs utilisés pour la réalisation de ces activités,
e. les actifs visés par ces activités
f. le descriptif des activités effectuées,
g. les problèmes ou erreurs rencontrés pendant la réalisation de ces activités,
h. les clients (interne ou externe) concernés.

18.2 Revue de la sécurité de l'information

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

18.2.4 Revue indépendante de la conformité du système et des processus de dématérialisation ou de conservation

Mesure

Il convient de réaliser un audit interne de conformité du SDC afin d'attester de la conformité de son fonctionnement et des activités effectuées par le personnel concerné par rapport à la description détaillée du SDC, par rapport aux spécifications des mécanismes de sécurité, par rapport à la politique de dématérialisation et de conservation, par rapport aux procédures et aux règles définies dans ces procédures et par rapport aux lois et aux règlements en vigueur.

Préconisations de mise en œuvre

Il convient que cette évaluation s'assure :

a. par échantillonnage que les documents analogiques collectés ont été correctement transformés en documents numériques et par la suite détruits ou restitués, et que les documents numériques ont été correctement maintenus, restitués ou entrés dans un processus d'archivage ;
b. par échantillonnage que les documents numériques collectés ont été correctement conservés sous la forme d'archives numériques et par la suite supprimés, et que ces archives ont été correctement créées, maintenues, restituées, transférées ou supprimées ;
c. que les actifs critiques du SDC et les mécanismes de sécurité, comme les mécanismes cryptographiques, ont été évalués et certifiés par des organismes indépendants spécialisés dans ce type de revues ou qu'ils sont conformes à des normes ou des référentiels reconnus et qu'ils sont utilisés conformément aux bonnes pratiques en la matière ;
d. par échantillonnage que les procédures d'administration, d'opérations et de sécurité et des procédures d'exploitation du processus et les règles définies dans ces procédures sont respectées.

Informations supplémentaires

La norme ISO/IEC 27007 intitulé « Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information » fournit des préconisations sur la réalisation des audits de SMSI, ainsi que des lignes directrices sur les compétences des auditeurs, en complément des lignes directrices figurant dans l'ISO 19011, qui sont applicables aux systèmes de management en général.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

18.2.5 Revue indépendante de la sécurité du SDC

Mesure

Il convient de réaliser un audit technique du SDC et des mécanismes de sécurité afin d'attester de la sécurité adéquate du SDC et du fonctionnement correct de ses mécanismes de sécurité indiqué dans la description détaillée du SDC.

Préconisations de mise en œuvre

Il convient que cet audit technique inclut des tests, en particulier des tests d'intrusion et des tests d'escalade de privilèges et une conclusion par une personne expérimentée en test d'intrusion.

Informations supplémentaires

Le rapport technique ISO/IEC TR 27008 intitulé « Lignes directrices pour les auditeurs des contrôles de sécurité de l'information » fournit des préconisations pour la revue de la mise en œuvre et de l'exploitation des mesures de sécurité, y compris le contrôle de la conformité technique des mesures de sécurité. Il explique des techniques pouvant être utilisées pour un tel audit technique. L'audit est en général composé d'un audit de la configuration des systèmes et de l'activité du système pour vérifier le fonctionnement correct de chaque mécanisme de sécurité, d'un test d'intrusion externe, et d'un test d'escalade de privilège.

Annexe A (normative) : Objectifs et mesures de référence spécifiques aux PSDC

Les objectifs et les mesures énumérés dans le Tableau A.1 découlent directement de ceux qui sont répertoriés dans le chapitre 5, avec lesquels ils sont en adéquation, et doivent être utilisés dans le contexte du paragraphe 6.1.4 de la clause 4.2 du présent document. La déclaration d'applicabilité doit justifier, en utilisant la méthode retenue pour l'appréciation et de traitement des risques, l'exclusion de toutes mesures.

Tableau A.1 - Objectifs et mesures

A.5 Politiques de sécurité de l'information		
A.5.2 Orientations de la direction en matière de politique de dématérialisation ou de conservation		
Objectif : Apporter à la gestion des processus de dématérialisation ou de conservation une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.		
A.5.2.1	Politiques de dématérialisation ou de conservation	*Mesure* Une politique de dématérialisation ou de conservation doit être définie, approuvée par la direction, mise en application, diffusée et communiquée aux salariés et aux tiers concernés.
A.5.2.2	Revue de la politique de dématérialisation ou de conservation	*Mesure* Pour garantir la constance de la pertinence, de l'adéquation et de l'efficacité des politiques de dématérialisation ou de conservation, ces politiques doivent être revues à intervalles programmés et en cas de changements majeurs.
A.6 Organisation de la sécurité de l'information et des processus de dématérialisation ou de conservation		
A.6.1 Organisation interne		
Objectif : Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information et des processus de dématérialisation ou de conservation au sein de l'organisation.		
A.6.1.1	Fonctions et responsabilités liées à la sécurité de l'information et aux processus de dématérialisation ou de conservation	*Mesure* Toutes les responsabilités en matière de sécurité de l'information et des processus de dématérialisation ou de conservation, en particulier celles liées à l'exécution des processus de dématérialisation ou de conservation et celles qui consistent à s'assurer de la conformité des processus et de la gestion opérationnelle aux politiques et aux documents applicables, doivent être établies et d'attribuées.
A.6.3 Organisation interne spécifique aux processus de dématérialisation et de conservation		
Objectif : Établir un cadre de gestion pour assurer le respect des exigences légales spécifiques des processus de dématérialisation ou de conservation au sein de l'organisation.		
A.6.3.1	Vérification des documents numériques avant destruction des documents analogiques correspondants	*Mesure* Une vérification du contenu des documents numériques par rapport aux documents analogiques doit être exercée si la destruction de ces derniers est programmée à la suite de leur numérisation.
A.6.3.2	Principes du double contrôle pour la modification ou la suppression d'archives numériques	*Mesure* L'organisation doit s'assurer que toute modification ou suppression des archives numériques créées qui n'était pas programmée lors de la définition du projet de conservation nécessite l'approbation de deux utilisateurs autorisés à exécuter ces opérations.

A.6.3.3	Gestion des preuves	*Mesure* Une gestion adéquate des preuves du fonctionnement du SDC et des activités effectuées par le personnel concerné doit être établie dans une procédure et mise en œuvre.
A.6.3.4	Relations avec l'autorité nationale	*Mesure* Des procédures doivent être mises en application pour notifier aux autorités compétentes, en particulier l'ILNAS, les prévisions de changements significatifs pouvant impacter la sécurité de l'information et les activités opérationnelles ainsi que, dans les meilleurs délais et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de dématérialisation ou de conservation.
A.6.4 Organisation des processus de dématérialisation et de conservation impliquant les clients		
Objectif : Clarifier les responsabilités entre le PSDC et ses clients et assurer la transparence en matière de sécurité et d'exploitation des processus de dématérialisation ou de conservation envers les clients.		
A.6.4.1	La sécurité dans les accords avec les clients	*Mesure* Le PSDC doit définir les conditions d'exécution des processus de dématérialisation ou de conservation, ainsi que les besoins de sécurité de l'information associés à ces processus avec le client dans un document contractuel approuvé par le client et le PSDC.
A.6.4.2	Obligation d'information préalable du client	*Mesure* Préalablement à toute relation contractuelle avec un détenteur, le PSDC doit mettre à disposition, sur un support durable et dans des termes aisément compréhensibles, les informations relatives aux conditions de prestation de service, en particulier toutes les informations légalement requises pour assurer un service transparent.
A.6.4.3	Classification des actifs du client	*Mesure* Le client doit définir avec le PSDC pour tous ses documents analogiques ou numériques et toutes ses archives numériques le niveau de classification, la durée de rétention, ainsi que les éventuelles autres exigences de sécurité comme les droits d'accès particuliers.
A.6.4.4	Obligation d'information du client en cas de changements ou d'incidents	*Mesure* Le PSDC doit informer, avant la mise en application ou dans les plus brefs délais, les clients internes ou externes concernés de tout changement des informations préalables et des informations liées aux obligations contractuelles, ainsi que de tout incident pouvant mettre en danger les informations du client, tout en donnant les justifications nécessaires.

A.7	**La sécurité des ressources humaines**	
A.7.2	**Pendant la durée du contrat**	
A.7.2.4	Engagement envers les politiques	*Mesure* Le personnel interne et celui des fournisseurs, s'il est impliqué dans la gestion opérationnelle de la sécurité ou des processus de dématérialisation ou de conservation, doivent comprendre et s'engager par écrit à respecter la politique de sécurité et la politique de dématérialisation ou de conservation.
A.8	**Gestion des actifs**	
A.8.1	**Responsabilités relatives aux actifs**	
A.8.1.4	Cloisonnement d'informations secrètes ou d'informations à caractère personnel	*Mesure* D'éventuelles informations secrètes ou informations à caractère personnel doivent être cloisonnées de façon suffisante pour pouvoir donner suite à la demande du propriétaire de les détruire sans mettre en danger d'autres informations archivées ou les preuves de la bonne gestion pour d'autres informations dématérialisées ou conservées.
A.9	**Contrôle d'accès**	
A.9.1	**Exigences métier en matière de contrôle d'accès**	
A.9.1.3	Ségrégation effective liée aux droits d'accès	*Mesure* Trois personnes différentes doivent être impliquées dans la gestion d'un droit d'accès : une pour l'autorisation de l'accès, une pour la vérification du respect des exigences de sécurité, et finalement une pour l'attribution de l'accès sur les systèmes.
A.10	**Cryptographie**	
A.10.1	**Mesures cryptographiques**	
A.10.1.3	Mesures d'authentification à deux facteurs	*Mesure* Pour les personnes qui interagissent avec les actifs techniques du système de conservation ou qui accèdent aux documents numériques et aux archives numériques, le PSDC doit assurer une authentification appropriée et sécurisée basée sur des mécanismes cryptographiques et, si l'accès est possible à partir de locaux ne requérant pas d'authentification à deux facteurs à l'entrée, une authentification à deux facteurs.
A.10.1.4	Protection de l'intégrité des documents numériques ou des archives numériques	*Mesure* L'intégrité des documents numériques collectés par le système de conservation et des archives numériques générées par le système de conservation doit être protégée avec des algorithmes et techniques cryptographiques appropriés.
A.10.1.5	Protection de l'intégrité des documents internes	*Mesure* L'intégrité des documents internes au SDC et aux processus y liés, en particulier les journaux d'événements du SDC, doit être protégée avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.

A.10.1.6	Signature électronique des documents internes	*Mesure* Les utilisateurs du SDC doivent utiliser une signature qualifiée ou un mécanisme apportant une garantie équivalente pour valider les documents internes nécessaires à prouver le bon fonctionnement du SDC et des processus y liés.
A.10.1.7	Protection des transmissions de documents	*Mesure* La transmission d'informations et de documents numériques doit être protégée avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.
A.10.1.8	Conservation des signatures électroniques	*Mesure* Si l'intégrité d'un document numérique à archiver repose sur une signature électronique, le document doit être conservé avec la preuve que la signature a été vérifiée au plus tard au moment de l'archivage.
A.11 Sécurité physique et environnementale		
A.11.1 Zones sécurisées		
A.11.1.7	Accompagnement des visiteurs	*Mesure* Un membre du PSDC habilité doit accompagner de manière permanente tous les visiteurs du PSDC, même si l'accès à ces zones leur a déjà été autorisé.
A.12 Sécurité liée à l'exploitation		
A.12.1 Procédures et responsabilités liées à l'exploitation		
A.12.1.5	Procédures d'exploitation du SDC	*Mesure* Des procédures d'administration, d'opérations du SDC, d'exploitation du processus de dématérialisation ou de conservation, et de contrôle de la sécurité du SDC et des processus incluant toutes les règles à suivre nécessaires pour assurer les propriétés de confidentialité, d'intégrité, de disponibilité, d'authenticité, de fiabilité et l'exploitabilité doivent être définies, mises en œuvre, et suivies par le personnel concerné (du PSDC et des fournisseurs).
A.12.4.5	Exploitabilité des journaux d'événements	*Mesure* Les journaux d'événements générés doivent être conservés sous une forme exploitable et protégée contre toute manipulation et suppression non autorisées pour assurer une traçabilité aussi longtemps que nécessaire de tous les événements enregistrés par ces mécanismes.
A.12.8 Gestion correcte et sécurisée du SDC		
Objectif : assurer la gestion correcte et sécurisée des documents analogiques à dématérialiser, des documents numériques et des archives numériques dans le cadre du processus de dématérialisation ou de conservation.		
A.12.8.1	Adéquation du SDC	*Mesure* Le PSDC doit démontrer que le SDC est composé d'actifs techniques et de mécanismes de sécurité répondant aux besoins des clients et permettant de garantir l'authenticité, la fiabilité et l'exploitation des documents analogiques à dématérialiser, des documents numériques et des archives numériques gérées par ce système.

A.12.8.2	Description détaillée du SDC	*Mesure* Une description détaillée et compréhensible du SDC comprenant les actifs techniques, les aspects fonctionnels et opérationnels ainsi que les flux et les dépendances entre les différentes composantes doit être définie et maintenue.
A.12.8.3	Mécanismes de sécurité du SDC	*Mesure* Le PSDC doit gérer et documenter les mécanismes de sécurité du SDC permettant d'assurer l'authenticité, la fiabilité et l'exploitation des documents analogiques, des documents numériques et des archives numériques gérés par ce système.
A.12.8.4	Supervision des aspects opérationnels du SDC	*Mesure* Les aspects opérationnels du SDC comme l'espace disponible et les taux d'échecs de composants redondants doivent être évalués de manière régulière.
A.12.8.5	Contrôle régulier de l'intégrité du SDC	*Mesure* Des mécanismes de contrôle régulier de l'intégrité du SDC et des informations nécessaires pour assurer la traçabilité doivent être implémentés.
A.15 Relations avec les fournisseurs		
A.15.1 Sécurité de l'information dans les relations avec les fournisseurs		
A.15.1.4	Conditions contractuelles pour les fournisseurs intervenant dans le processus de dématérialisation et de conservation	*Mesure* Le PSDC doit inclure dans les contrats établis avec chaque fournisseur intervenant dans le processus de dématérialisation et de conservation les conditions assurant le respect de la politique de sécurité et de la politique de dématérialisation et de conservation
A.17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité		
A.17.3 Continuité de l'activité et du SDC		
Objectif : assurer la gestion correcte de la continuité du SDC et des processus de dématérialisation ou de conservation.		
A.17.3.1	Organisation de la continuité	*Mesure* Les exigences pour la continuité des processus de dématérialisation ou de conservation en cas de situation défavorable, comme lors d'une crise ou d'un sinistre doivent être déterminées.
A.17.3.2	Mise en œuvre de la continuité	*Mesure* Les processus, procédures et mesures pour assurer le niveau requis de continuité pendant une situation défavorable doivent être établis, documentés, mis en œuvre et maintenus.
A.17.3.3	Vérifier, revoir et évaluer la continuité	*Mesure* La mise en œuvre des mesures liées à la continuité du SDC doit être vérifiée à intervalles réguliers pour s'assurer qu'elles sont toujours valides et en vigueur pendant une situation défavorable.

A.18 Conformité		
A.18.2 Revue de la sécurité de l'information		
A.18.2.4	Revue indépendante de la conformité du système et des processus de dématérialisation ou de conservation	*Mesure* Un audit interne de conformité du SDC doit être réalisé afin d'attester de la conformité de son fonctionnement et des activités effectuées par le personnel concerné par rapport à la description détaillée du SDC, par rapport aux spécifications des mécanismes de sécurité, par rapport à la politique de dématérialisation et de conservation, par rapport aux procédures et aux règles définies dans ces procédures et par rapport aux lois et aux règlements en vigueur.
A.18.2.5	Revue indépendante de la sécurité du SDC	*Mesure* Un audit technique du SDC et des mécanismes de sécurité doit être réalisé afin d'attester de la sécurité adéquate du SDC et du fonctionnement correct de ses mécanismes de sécurité indiqué dans la description détaillée du SDC.