# Lignes directrices d'audit de la règle technique d'exigences et de mesures pour la certification des Prestataires de Services de Dématérialisation ou de Conservation (PSDC)

ILNAS


1, avenue du Swing
L-4367 Belvaux
Tél.: (+352) 247 743 - 50
Fax: (+352) 247 943 - 50
confiance-numerique@ilnas.etat.lu
www.portail-qualite.lu


**Grand-Duché du Luxembourg**

| Caractéristiques du document | | | |
|---|---|---|---|
| **Niveau de classification du document** | Interne | **Statut du document** | Ebauche |
| **Propriétaire du document** | Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et Qualité des Produits et Services. | | |

| Historique du document | | |
|---|---|---|
| **Version #** | **Date de publication** | **Détails des changements effectués** |
| 1.0 | 19.12.2012 | Document initial. |
| 1.1 | 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. |

# 0 Table des matières

# 1 Introduction

Le présent document définit les lignes directrices d'audit relatives à des exigences et à des mesures spécifiées dans la règle technique d'exigences et de mesures pour la certification des Prestataires de Services de Dématérialisation ou de Conservation (PSDC) (ci-après « règle technique pour la certification des PSDC ») publiée par l'Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et Qualité des Produits et Services (ci-après « ILNAS »).

L'expression « lignes directrices d'audit » doit être interprétée comme des **recommandations** pratiques mises à la disposition de tout intervenant impliqué dans un audit.

Dans le contexte du présent document, ces recommandations ont pour vocation de faciliter:

a) la compréhension de l'établissement d'exigences et de mesures spécifiées dans la règle technique pour la certification des PSDC;

b) l'évaluation de leur définition et mise en œuvre; et

c) l'obtention d'une assurance que ces exigences et mesures répondent à des objectifs définis.

Le présent document doit être également considéré comme un recueil de retours d'expérience d'audits d'évaluation de conformité effectués pour le compte d'organismes d'évaluation de conformité d'après la règle technique pour la certification des PSDC auprès d'organisations exécutant des processus de dématérialisation ou de conservation.

En résumé, le présent document adresse des exigences et des mesures pour lesquelles l'ILNAS a décidé de définir des recommandations pratiques d'audit, sur base essentiellement de ces retours d'expérience.

La règle technique pour la certification des PSDC publiée par l'ILNAS se base essentiellement sur les normes internationales suivantes:

a) ISO/IEC 27001:2013 [1] et ISO/IEC 27002:2013 [2] de manière à ce qu'une organisation puisse être en mesure de définir, d'implémenter, de maintenir et d'améliorer:

   1. 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; et

   2. 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.

b) ISO 30301:2011 [3] de manière à ce qu'une organisation puisse être en mesure de définir, d'implémenter, de maintenir et d'améliorer un processus de conservation intégrant les grands principes opérationnels définis dans cette norme internationale.

NOTE : Pour rappel, la norme internationale ISO 30301:2011 adresse la problématique de la conservation et non celle de la dématérialisation.

Afin d'assurer une consistance dans la définition des exigences et des mesures spécifiées dans la règle technique pour la certification des PSDC, les grands principes définis dans la norme internationale ISO 30301:2011 ont également été adaptés autant que possible à la problématique de la dématérialisation afin d'adresser ce domaine selon l'approche de gestion opérationnelle adoptée pour la conservation.

La norme internationale ISO 30301:2011 n'est pas indispensable pour l'application de la règle technique pour la certification des PSDC.

La fréquence d'actualisation du présent document est amenée à être supérieure à celle planifiée pour la règle technique pour la certification des PSDC qui est d'une fois par an ou suite à des changements significatifs:

a) impactant le fonctionnement de l'ILNAS;

b) issus des besoins métiers liés à la dématérialisation ou à la conservation; ou

c) en matière légal ou réglementaire.

# 2 Domaine d'application

Le présent document définit les lignes directrices d'audit relatives à des exigences et à des mesures spécifiées dans la règle technique pour la certification des PSDC publiée par l'ILNAS.

Le présent document **ne définit pas**:

a) l'établissement d'un plan d'audit d'un SMSI;

NOTE : La norme internationale ISO/CEI 27007:2011 [4] définit les lignes directrices d'audit d'un SMSI.

b) l'établissement d'un plan d'audit de mesures de sécurité et de mesures opérationnelles; et

NOTE 1 : Le rapport technique ISO/CEI TR 27008:2011 [5] définit les lignes directrices d'audit de mesures de sécurité.

NOTE 2 : Il est recommandé de suivre les lignes directrices du rapport technique ISO/IEC TR 27008:2011 pour évaluer la conformité des mesures opérationnelles définies dans la règle technique pour la certification des PSDC.

c) les compétences requises d'un auditeur pour pouvoir être en mesure d'effectuer un audit d'évaluation de conformité d'après la règle technique pour la certification des PSDC.

NOTE : Une procédure est publiée par les organismes d'évaluation de conformité à cet effet.

Le présent document s'adresse à tout intervenant, tel qu'une organisation ou un individu, impliqué dans la préparation, la réalisation, la gestion, la clôture ou le suivi d'un audit d'évaluation de conformité interne ou externe d'après la règle technique pour la certification des PSDC.

# 3 Références normatives

Les références suivantes sont indispensables pour l'application du présent document.

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

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

# 4 Termes, définitions, abréviations et structure du document

## *4.1 Termes et définitions*

Pour les besoins du présent document, les termes et définitions spécifiés dans la règle technique pour la certification des PSDC et les suivants s'appliquent:

**audit**

processus méthodique, indépendant et documenté permettant d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits

[ISO 19011:2011]

**clé d'infrastructure**

clé cryptographique utilisée par un actif technique du SDC-DC, SDC-C ou SDC-D dans le cadre de l'exécution de processus ou d'activités sous-jacents aux processus de dématérialisation ou de conservation

Exemples d'utilisation de la clé d'infrastructure: authentification système, cryptage de données ou signature de journaux d'événements

**critères communs**

norme internationale établie pour l'évaluation de produits de sécurité

**module cryptographique sécurisé**

module disposant de fonctions cryptographiques et dont le niveau de sécurité a été évalué de manière indépendante et documentée selon des objectifs définis.

## 4.2 Abréviations

Pour les besoins du présent document, les abréviations spécifiées dans la règle technique pour la certification des PSDC et les suivantes s'appliquent.

**CSSF** Commission de Surveillance du Secteur Financier

**EAL** Evaluation Assurance Level

**PSF** Professionnel du Secteur Financier

## 4.3 Structure du document

La clause 5 définit les lignes directrices d'audit relatives à des exigences et à des mesures spécifiées dans la règle technique pour la certification des PSDC.

Plus concrètement, chaque clause sous-jacente à la clause 5 adresse une problématique d'audit spécifique à un sujet en lien avec les processus de dématérialisation ou de conservation.

L'intitulé de chaque clause sous-jacente reflète le sujet adressé.

Exemple:

5.x *Définition du domaine d'application du SMSI*

Les lignes directrices associées à ce sujet sont présentées dans un tableau comme suit:

| | |
|---|---|
| **Extrait de la règle technique pour la certification des PSDC** | Extrait de la règle technique pour la certification des PSDC contenant les exigences ou les mesures en lien avec le sujet indiqué dans l'intitulé de la clause et pour lesquelles des recommandations pratiques ont été définies.<br><br>Structurellement, cet extrait peut être composé soit:<br><br>a) de l'entièreté d'une clause de la règle technique pour la certification des PSDC;<br><br>b) d'une partie de plusieurs clauses de cette règle;<br><br>c) d'un ensemble d'exigences ou de mesures de cette règle; ou<br><br>d) de l'entièreté ou d'une partie d'une exigence ou d'une mesure de cette règle. |
| **Recommandations pratiques** | Recommandations pratiques spécifiques à l'extrait précédemment mentionné. |

# 5 Lignes directrices d'audit

## *5.1 Ségrégation des rôles et responsabilités*

| | |
|---|---|
| **Extrait de la règle technique pour la certification des PSDC** | **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)**<br><br>La mesure de sécurité 6.1.1 de la norme internationale ISO/IEC 27002:2013 est complétée de la manière suivante:<br><br><u>Exigences de mise en œuvre</u><br><br>La direction doit:<br>[…]<br>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.<br>[…]<br><u>12.8.1.3 Mécanismes de sécurité du système de dématérialisation SDC-D</u><br><br>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.<br><br>L'organisation doit établir les mécanismes de sécurité suivants:<br>[…]<br>a) mécanismes de gestion des privilèges.<br><br>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.<br><br>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.<br><br>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.<br>[…] |

| | |
|---|---|
| | L'organisation doit établir les mécanismes de sécurité suivants:<br>[…]<br>b) mécanismes de gestion des privilèges.<br><br>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.<br><br>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.<br><br>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. |
| **Recommandations pratiques d'audit** | Il est recommandé de s'assurer que le principe de ségrégation des rôles et responsabilités est correctement établi au niveau:<br><br>a) de la sécurité de l'information et de la gestion opérationnelle de l'organisation;<br><br>La définition et mise en œuvre de processus ou d'activités de sécurité de l'information ou organisationnels en lien avec les processus de dématérialisation ou de conservation sont assumées par une même personne.<br><br>Par contre, cette personne doit être différente de celle qui revoit l'effectivité de leur mise en œuvre et qui s'assure qu'elles répondent à des objectifs définis.<br><br>Enfin, il convient que ces travaux de revue d'effectivité et d'assurance soient eux-mêmes inclus dans le domaine d'application d'un audit d'évaluation de conformité, de manière ainsi à revoir l'effectivité de leur mise en œuvre et de s'assurer qu'elles répondent à des objectifs définis.<br><br>b) des utilisateurs du SDC-DC, SDC-C ou SDC-D de l'organisation.<br><br>Selon les bonnes pratiques en la matière, il est conseillé d'attribuer qu'un seul profil de privilèges par utilisateur.<br><br>Dans la pratique et en fonction des ressources disponibles de l'organisation, il est acceptable qu'un utilisateur dispose à la fois du profil de privilèges d'administration et du profil de privilèges d'opérations. Par contre, ce même utilisateur ne peut pas disposer du profil de privilèges de sécurité qui doit être attribué à un autre utilisateur. Les activités assumées ou effectuées par ce dernier doivent être évaluées dans le cadre d'un audit d'évaluation de conformité, de manière ainsi à revoir l'effectivité de leur mise en œuvre et de s'assurer qu'elles répondent à des objectifs définis. |

## *5.2 Situation financière de l'organisation*

| | |
|---|---|
| **Extrait de la règle technique pour la certification des PSDC** | ***Clause 6.3 Leadership***<br><br>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 :<br><br>b) la preuve de l'existence légale de l'organisation et de la stabilité de sa situation financière.<br><br>NOTE : Une organisation de droit privé pourra par exemple fournir les informations suivantes:<br><br>1. extrait du registre de commerce et des sociétés de Luxembourg.<br><br>2. stratégie financière.<br><br>3. bilans et comptes de résultat des 3 dernières années fiscales.<br><br>4. rapport ou avis financier émis par une autorité de surveillance luxembourgeoise.<br><br>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.<br><br>6. rapport d'auditeurs financiers. |
| **Recommandations pratiques d'audit** | Si l'organisation auditée dispose de l'agrément PSF délivré par la CSSF, il est recommandé de s'adresser à cette commission par le biais de l'ILNAS afin de disposer d'informations relatives à la stabilité financière de l'organisation auditée, et ce avant de transmettre une demande similaire auprès de cette organisation, permettant ainsi d'éviter de la solliciter inutilement pour disposer d'informations déjà en possession d'une administration publique.<br><br>Sur base des informations reçues de la CSSF, une demande spécifique peut être adressée au besoin à l'organisation auditée pour disposer d'informations complémentaires et ainsi évaluer de manière adéquate la conformité de cette organisation eu égard à l'exigence de stabilité financière. |

## *5.3 Garantie de continuité d'exécution des processus de dématérialisation ou de conservation*

| | |
|---|---|
| **Extrait de la règle technique pour la certification des PSDC** | ***Clause 6.3 Leadership***<br><br>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:<br>[…]<br>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 :<br><br>1. processus de dématérialisation exécuté par l'organisation pour le compte d'un tiers.<br><br>2. processus de conservation exécuté par l'organisation pour le compte d'un tiers.<br><br>3. sous-processus de restitution, transfert et suppression des archives numériques exécuté par l'organisation pour son propre compte.<br><br>Cette garantie de continuité doit être gérée par l'organisation et couvrir le risque économique de cessation d'activités.<br><br>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. |
| **Recommandations pratiques d'audit** | Il est recommandé de s'assurer que les conditions présentées par l'organisation en matière de garantie de continuité d'exécution des processus de dématérialisation ou de conservation sont:<br><br>a) particulièrement adaptées:<br><br>1. au contexte métier, c'est-à-dire les raisons pour lesquelles ces processus ont été établis, comme par exemple pour répondre à des besoins internes ou dans le cadre de relations contractuelles avec des tiers;<br><br>2. au volume d'activités lié à ces processus; et<br><br>3. aux conséquences financières en cas de défaut d'exécution de ces processus.<br><br>b) revues de manière régulière (au moins une fois par an) et en cas de |

changement significatifs:

1. impactant l'actionnariat de l'organisation ou son fonctionnement;
2. impactant la gestion opérationnelle de son SDC-DC, SDC-C ou SDC-D;
3. modifiant les rôles et responsabilités des sous-traitants impliqués dans ces processus;
4. issu des besoins des clients (intégration d'un nouveau projet client, modification d'un projet client existant) en matière de dématérialisation ou de conservation; et
5. de nature légale ou réglementaire ayant un impact sur ces processus.

Dans le cadre de l'exécution des processus de dématérialisation ou de conservation par l'organisation, une attention particulière doit être prêtée:

a) aux assurances suivantes:

1. assurance responsabilité civile professionnelle couvrant les risques liés à un défaut de prestation de services en relation avec ces processus; et
2. assurance responsabilité civile produit couvrant les risques liés à un défaut de produit de dématérialisation ou de conservation.

NOTE : Une organisation peut être amenée à souscrire à cette assurance en cas de développement d'applications de dématérialisation ou de conservation et de leur intégration dans les processus de dématérialisation ou de conservation exécutés pour son propre compte ou des tiers.

b) aux risques économiques, tel que le risque de cessation d'activités pour des raisons financières, et stratégiques de l'organisation qui sont rarement couverts par une assurance. Ces risques sont en règle générale couverts par un engagement formel d'un actionnaire institutionnel ou privé majoritaire se portant caution ou par un dépôt garanti de capital afin de couvrir les besoins de continuité d'exécution de ces processus.

En complément ou remplacement de l'engagement formel de l'actionnaire ou du dépôt garanti de capital, l'organisation peut recommander ou demander à ses clients de ces processus de souscrire à une assurance de défaillance financière du fournisseur afin d'obtenir directement un capital qui serait par la suite versé à l'organisation pour lui permettre de continuer pendant une période de transition minimum d'exécuter ces processus selon les besoins des clients.

## *5.4 Processus d'identification et d'évaluation des risques*

| | |
|---|---|
| **Extrait de la règle technique pour la certification des PSDC** | ***Clause 6.4 Planification***<br><br>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 :<br><br>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.<br>[…]<br>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. |
| **Recommandations pratiques d'audit** | Il est recommandé de s'assurer que:<br><br>a) le processus d'identification et d'évaluation des risques de l'organisation intègre une gestion effective des risques liés aux processus de dématérialisation ou de conservation sous sa responsabilité et pouvant impacter:<br><br>1. la sécurité de l'information;<br><br>2. la gestion opérationnelle; et<br><br>3. la stabilité financière de l'organisation et capacité de couverture de responsabilités contractuelles, légales et réglementaires.<br><br>b) les résultats de cette gestion sont uniformisés.<br><br>Cela signifie qu'une même méthode d'analyse de risques devrait être appliquée dans la mesure du possible à l'ensemble des risques liés aux processus de dématérialisation ou de conservation de l'organisation de manière à faciliter leur interprétation et appréciation, et à pouvoir disposer d'une vision globale et cohérente de ces risques.<br><br>Si pour des raisons stratégiques, métiers, organisationnels, légales ou réglementaires, plusieurs méthodes d'analyse de risques sont intégrées dans le processus d'identification et d'évaluation des risques de l'organisation, il faut s'assurer que:<br><br>1. l'établissement de chacune de ces méthodes est légitime et pertinente; et<br><br>2. les techniques d'évaluation intégrées dans ces méthodes et les résultats issus de l'exécution de ces méthodes sont comparables. |

## *5.5 DdA*

| | |
|---|---|
| **Extrait de la règle technique pour la certification des PSDC** | ***Clause 6.4 Planification***<br><br>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 :<br>[…]<br><br>d) la DdA soit 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.<br><br>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.** |
| **Recommandations pratiques d'audit** | Il est recommandé de s'assurer:<br><br>a) que l'exclusion de mesures de sécurité dans le DdA est uniquement possible sous condition 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..<br><br>Cela signifie en d'autres termes que l'organisation ne peut pas exclure de sa DdA des objectifs et des mesures au simple motif d'une acception formelle de risques et ce, en raison d'un appétit élevé pour ces risques.<br><br>Exemple :<br><br>La mesure définie à la clause 12.4.2 *Protection des données système d'essai* de la norme internationale ISO/IEC 27002:2013 adresse les conditions d'utilisation de données personnelles ou d'exploitation dans le cadre du développement et de tests d'applications.<br><br>Si l'organisation n'a pas de nécessité à utiliser des données personnelles ou d'exploitation sous sa responsabilité dans le cadre du développement ou de tests d'applications, cette mesure peut être exclue de sa DdA. (pas de risque associé)<br><br>Par contre, si l'organisation a fourni des données personnelles ou d'exploitation à un sous-traitant effectuant du développement ou des tests d'applications pour le compte de l'organisation, cette dernière ne peut pas exclure cette mesure de sa DdA sous réserve que le sous-traitant est responsable du traitement des données reçues de l'organisation. (exigence légale). |

## *5.6 Définition du domaine d'application du SMSI*

| | |
|---|---|
| **Extrait de la règle technique pour la certification des PSDC** | **12.8.1 *Système de dématérialisation SDC-D* et 12.9.1 *Système de conservation SDC-C***<br>**(mesure de sécurité additionnelles à la Norme internationale ISO/IEC 27002:2013)**<br><br>12.8.1.1 et 12.9.1.1 : Mesure<br><br>L'organisation doit pouvoir démontrer que le système de dématérialisation /Conservation SDC-D/CDC-C est composé d'actifs techniques et de mécanismes de sécurité:<br><br>a) répondant aux besoins des clients (internes ou externes à l'organisation) du processus de dématérialisation.<br><br>b) permettant de garantir l'authenticité, la fiabilité et l'exploitation des documents analogiques et numériques gérés par ce système. |
| **Recommandations pratiques d'audit** | Il est recommandé de s'assurer que:<br><br>a) l'inventaire des actifs est suffisamment documenté pour permettre d'identifier l'importance des actifs listés dans le cadre des processus de dématérialisation ou de conservation de l'organisation;<br><br>Plus concrètement, l'inventaire des actifs supportant les processus de dématérialisation ou de conservation de l'organisation devrait inclure les informations suivantes:<br><br>1. l'intitulé de l'actif;<br><br>2. la description de l'actif;<br><br>3. le type de l'actif;<br><br>4. le propriétaire de l'actif;<br><br>5. la propriété effective de l'actif, c'est-à-dire si cet actif est détenu par par exemple par l'organisation ou fourni par un sous-traitant qui en reste propriétaire;<br><br>6. la valeur financière estimée de l'actif;<br><br>7. la localisation de l'actif; et<br><br>8. le niveau de criticité de l'actif en terme de sécurité de l'information et |

| | |
|---|---|
| | opérationnelle.<br><br>b) l'inventaire des actifs listant ceux supportant les processus de dématérialisation ou de conservation est utilisé dans le cadre de l'exécution du processus d'identification et d'évaluation des risques liés à ces processus et pouvant impacter:<br><br>1. la sécurité de l'information;<br><br>2. la gestion opérationnelle; et<br><br>3. la stabilité financière de l'organisation et sa capacité de couverture de responsabilités contractuelles, légales et réglementaires.<br><br>Cet inventaire peut s'avérer également nécessaire dans le cadre d'une gestion financière des actifs détenus par l'organisation ou dans la souscription d'une assurance couvrant la continuité d'exécution des processus de dématérialisation ou de conservation de l'organisation.<br><br>c) les duplicatas d'informations sont limités si plusieurs inventaires d'actifs sont maintenus par l'organisation et que, le cas échéant, le contenu de ces inventaires est aligné. |

## *5.7 Rapports d'activités des utilisateurs du SDC-DC, SDC-C ou SDC-D*

| | |
|---|---|
| **Extrait de la règle technique pour la certification des PSDC** | 12.8.1.4 Preuves de la conformité<br><br>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.<br><br>En particulier, les preuves suivantes doivent être conservées:<br>[…]<br>c) rapports d'activités des utilisateurs du SDC-D.<br>[…]<br><br>12.9.1.4 Preuves de la conformité<br><br>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.<br><br>Les preuves suivantes doivent être conservées :<br>[…]<br>c) rapports d'activités des utilisateurs du SDC-C. |
| **Recommandations pratiques d'audit** | La rédaction de rapports d'activités par des utilisateurs du SDC-DC, SDC-C ou SDC-D et leur signature électronique par ces utilisateurs ne sont pas une obligation si l'organisation peut démontrer l'effectivité des activités exécutées par ces utilisateurs au travers des journaux d'événements du SDC-DC, SDC-C ou SDC-D et sous réserve que:<br><br>a) les activités exécutées par ces utilisateurs soient spécifiées de manière claire et explicite dans les journaux d'événements;<br><br>b) l'intégrité des journaux d'événements puisse être démontrée par l'organisation aussi longtemps que nécessaire, notamment par l'établissement de mécanismes cryptographiques de sécurité tels que ceux définies:<br><br>1. au point d) 5. de la clause 12.8.1.3 Mécanismes de sécurité du système de dématérialisation SDC-D, et ce dans le cadre du processus de dématérialisation; et<br><br>2. au point d) 5. de la clause 12.9.1.3 Mécanismes de sécurité du système de conservation SDC-C, et ce dans le cadre du processus de |

conservation.

c) l'exploitation, la conservation et la protection des journaux d'événements contre toute manipulation et suppression non autorisées puissent être démontrées par l'organisation aussi longtemps que nécessaire;

d) les journaux d'événements soient signés électroniquement par une clé d'infrastructure dont:

1. la génération se base sur un algorithme asymétrique;

2. l'utilisation est limitée à cet effet, c'est-à-dire à la signature de journaux d'événements;

3. la génération, l'utilisation et le stockage sont réalisés par le biais de l'utilisation d'un module cryptographique sécurisé disposant d'un niveau d'assurance EAL 4 + selon les critères communs;

4. le certificat associé est valide au moment de la signature des journaux d'événements et que cette validité puisse être démontrée aussi longtemps que nécessaire;

   NOTE : Ce certificat peut être auto-signé ou émané d'une autorité de certification.

5. le renouvellement est régulier comme par exemple une fois par an; et

   NOTE : Ce renouvellement peut être effectué en ligne ou par d'autres moyens de communications.

6. l'accès est limité à des utilisateurs disposant d'un profil de privilèges de sécurité.

# Bibliographie

Les références suivantes doivent être considérées comme une assistance dans la mise en œuvre du présent document. Pour les références non datées, la dernière édition s'applique (y compris les éventuels amendements).

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

[2] 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] ISO/IEC 30301:2011, *Information et documentation -- Systèmes de gestion des documents d'activité – Exigences*

[4] ISO/IEC 27007:2011, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information*

[5] ISO/IEC TR 27008:2011, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour les auditeurs des contrôles de sécurité de l'information*