Grand-Duché de luxembourg.

ILNAS

Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services

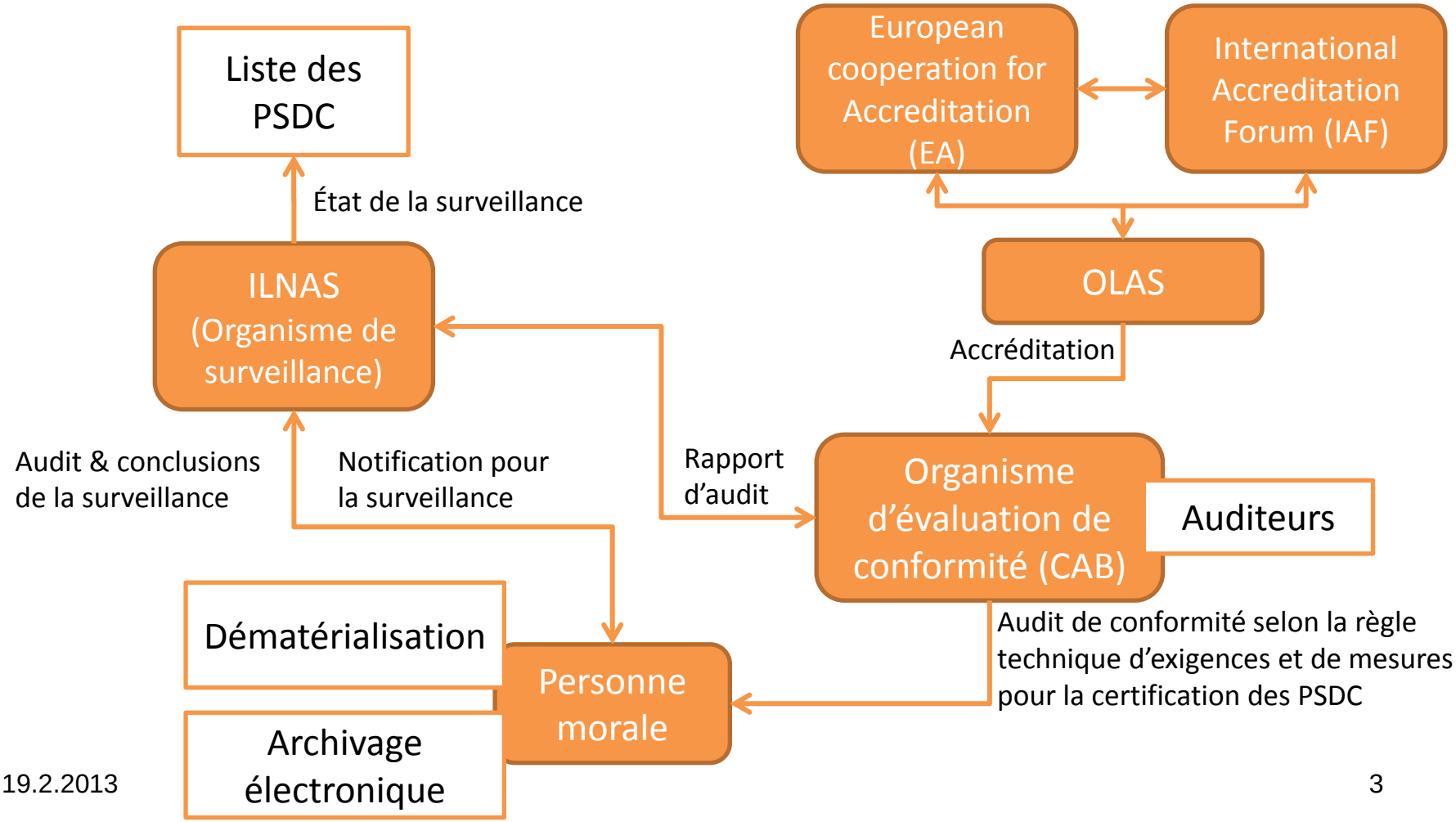
Archivage électronique
-
Règle technique d'exigences et de mesures pour la certification des PSDC

19.2.2013

Sommaire

- Description du modèle de surveillance
- Définitions
- Objectifs de la surveillance des PSDC
- Présentation de la règle technique d'exigences et de mesures pour la certification des PSDC
- Processus d'obtention du statut de « PSDC »
- Lignes directrices d'audit
- Conclusion et perspective

Description du modèle de surveillance



Définitions

- Statut de « PSDC » :
  - **P**restataire de **S**ervices de **D**ématérialisation ou de **C**onservation surveillé par le Département de la confiance numérique de l'ILNAS
    - PSDC -D
    - PSDC -C
    - PSDC -DC

- Dématérialisation :
  - Numérisation de documents analogiques

- Conservation :
  - Archivage numérique dans le temps

Objectifs de la surveillance des PSDC

- Instaurer une relation de confiance entre utilisateurs
  - Vérification externe
  - Améliorer la qualité des produits et services
- Reconnaissance de la valeur juridique des documents dématérialisés
  - Loi relative à l'archivage électronique
- Valoriser l'activité d'archivage électronique
  - Effet « marketing »
  - « Bonne image » du PSDC
- Réduire les coûts
  - Réduire les archives analogiques
  - Réduire les incidents

Règle technique pour la certification des PSDC

- La règle technique présente les exigences et les mesures pour la certification des Prestataires de Services de Dématérialisation ou de Conservation

- La règle technique constitue une référence unique contenant toutes les conditions pour obtenir le statut de « PSDC »

- La règle technique est basée sur des standards internationaux
  - ISO/IEC 27001:2005
  - ISO/IEC 27002:2005
  - ISO 30301:2011
  - …

- La règle technique est publiée sur le site web de l'ILNAS :
  - Version originale en français
  - Traductions en anglais et en allemand

Règle technique pour la certification des PSDC - Contenu

- **Concepts généraux**
  - Description des processus de dématérialisation et de conservation
  - Principes de sécurité

- **Système de Management de la Sécurité de l'Information (SMSI)**
  - Basé sur ISO/IEC 27001:2005
  - Compléments concernant le processus de dématérialisation
  - Compléments concernant le processus de conservation

- **Objectifs et mesures de gestion de la sécurité et de gestion opérationnelle**
  - Basés sur ISO/IEC 27002:2005
  - Compléments concernant le processus de dématérialisation
  - Compléments concernant le processus de conservation

- **Annexes informatives et documentaires**

Systèmes de Management de la Sécurité de l'Information (SMSI)

- Gestion de la sécurité de l'information
- Définir, implémenter, maintenir et améliorer un SMSI
  - afin de gérer les risques liés aux processus de dématérialisation ou de conservation
- Doit respecter l'ensemble des exigences de la sécurité de l'information spécifiées dans :
  - la norme internationale ISO/IEC 27001:2005
  - la clause 6 de la règle technique, complétant les exigences

Objectifs et mesures de gestion de la sécurité et de gestion opérationnelle

- Définition 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 27002:2005

- Cette clause a été définie de manière à refléter la structure de la norme ISO/IEC 27002:2005 (clauses 5 à 15) :

  - Des amendements et des compléments aux objectifs de sécurité et mesures associées afin de couvrir la dématérialisation et la conservation

  - Des objectifs et mesures de gestion de la sécurité de l'information et de gestion opérationnelle additionnels afin de couvrir la dématérialisation et la conservation

Exigences et mesures de la règle technique de certification PSDC

- Politique de sécurité
  - Apporter une orientation / sécurité
  - Soutien de la direction
  - Politique de dématérialisation
  - Politique de conservation

- Organisation de la sécurité de l'information
  - Gérer la sécurité de l'information
  - Contrôler la mise en œuvre de la sécurité de l'information

- Gestion des biens
  - Responsabilités relatives aux biens
  - Classification des informations

- Sécurité liée aux ressources humaines
  - Avant le recrutement
  - Pendant la durée du contrat
  - Fin ou modification de contrat

Exigences et mesures de la règle technique de certification PSDC

- Sécurité physique et environnementale
  - Empêcher tout accès physique non autorisé
  - Sécurité du matériel

- Gestion de l'exploitation et des télécommunications
  - Procédures d'exploitation documentées
  - Séparer les tâches et les domaines de responsabilité
  - Séparer les équipements de développement, de test et d'exploitation
  - Protection contre les codes malveillants
  - Réaliser des copies de sauvegarde
  - Gestion de la sécurité des réseaux
  - Surveillance
  - Assurer la gestion correcte et sécurisée des documents dans le cadre du processus de dématérialisation et de conservation

- Contrôle d'accès
  - Maîtriser l'accès à l'information

Exigences et mesures de la règle technique de certification PSDC

- Acquisition, développement et maintenance des systèmes d'information
  - Veiller à ce que la sécurité fasse partie intégrante des systèmes d'information
  - Bon fonctionnement des applications
  - Mesures cryptographiques

- Gestion des incidents liés à la sécurité de l'information
  - Signalement des événements et des failles
  - Gestion des améliorations et incidents

- Gestion du plan de continuité de l'activité
  - Neutraliser les interruptions

- Conformité
  - Conformité avec les exigences légales
  - Conformité avec les politiques et normes de sécurité
  - Prise en compte de l'audit

Processus d'obtention du statut de « PSDC »

Processus d'obtention du statut de « PSDC »

- Préparation par le PSDC
  - Se conformer à la règle technique publiée par l'ILNAS
    - spécifier la "policy"
    - évaluation des risques
    - spécifier les pratiques de dématérialisation ou de conservation
    - SMSI effectif
    - documenter & implémenter les procédures
    - réaliser des audits internes
    - implémenter des actions correctives
    - réaliser des revues de direction
  - Demander la certification auprès d'un organisme d'évaluation de conformité accrédité

Processus d'obtention du statut de « PSDC »

- Audit de conformité selon la règle technique d'exigences et de mesures pour la certification des PSDC par un organisme d'évaluation de conformité (CAB) accrédité par l'OLAS ou par tout autre organisme d'accréditation reconnu par OLAS dans le cadre des accords de reconnaissance mutuelle européens ou internationaux.

  - Audit technique et documentaire
  - Rapport intermédiaire
  - Actions correctives et évaluation des actions correctives
  - Rapport final d'audit
  - Le CAB ne décide pas du statut de « PSDC »

Processus d'obtention du statut de « PSDC »

- Notification pour la surveillance auprès de l'ILNAS contenant les indications suivantes
  - Rapport final d'audit
  - Validation de la notification par l'ILNAS

Processus d'obtention du statut de « PSDC »

- Validation de la notification par ILNAS sur base de :
  - L'actualité de l'accréditation du CAB et l'étendue de sa portée
  - L'actualité de la certification du demandeur de la notification et l'étendue de sa portée
  - La connaissance par les auditeurs de la règle technique ainsi que de la législation nationale
  - La couverture de l'audit de certification par la règle technique pour la certification des PSDC
  - La rédaction du rapport d'audit dans une des langues administratives conformément à la loi du 24 février 1984 sur le régime des langues ou en anglais
  - Le cas échéant, la levée des écarts majeurs soulevés lors de l'audit

Processus d'obtention du statut de « PSDC »

- Surveillance par ILNAS
  - PSDC doit notifier tout changement à l'ILNAS
  - Réunions semestrielles entre l'ILNAS et le PSDC
  - Suspension volontaire à la demande du PSDC
  - Statut « PSDC » retiré si non-conformité

Processus d'obtention du statut de « PSDC »

- Attribution du statut de « PSDC »
  - ➢ Inscription de l'état de surveillance dans la liste des PSDC
  - ➢ Publication de la liste sur le site web de l'ILNAS

Lignes directrices d'audit de la règle technique d'exigences et de mesures pour la certification des PSDC

- Recommandations pratiques pour tout intervenant impliqué dans un audit
- Sur base de retours d'expériences
- Faciliter la compréhension de l'établissement d'exigences et de mesures spécifiées dans la règle technique pour la certification des PSDC
- Faciliter l'évaluation de leur définition et mise en œuvre
- Assurer que ces exigences et mesures répondent à des objectifs définis
- Publiées sur le site web de l'ILNAS

Conclusion et perspective

- Augmenter la confiance dans l'archivage électronique
- Certification ISO/IEC 27001 ad hoc => réduction de l'audit
- Règle technique de certification des PSDC est publiée sur le site web de l'ILNAS
- Lignes directrices d'audit sont publiées sur le site web de l'ILNAS
- Veille constante nécessaire => documents en évolution continue
- Aboutissement proche de la loi relative à l'archivage électronique
- Des notifications pour la surveillance pourront être introduites dans les prochains mois
- Lien vers les documents pour l'obtention du statut de « PSDC »

Merci pour votre attention!

Alain Wahl
ILNAS – Département de la confiance numérique

Tél.: (+352) 247 743 53
alain.wahl@ilnas.etat.lu