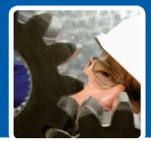
L'accréditation OLAS :
La preuve de la compétence

OFFICE LUXEMBOURGEOIS D'ACCREDITATION ET DE SURVEILLANCE





Projet de norme nationale (ILNAS 107:2019) sur la sécurité de l'information dans le cadre de l'accréditation des laboratoires

JCA du 18 octobre 2019

Léon Treff

Welcome · Bienvenue · Willkommen

ILNAS

PROGRAMME

- Contexte
- Analyse comparative
- Projet de norme nationale
- Groupe de travail
- Structure du document « martyr »
- Informations au laboratoire
- Exemples de mesures de sécurité
- Relevé des mesures
- Exemples de bonnes pratiques d'audit
- Continuation du projet

CONTEXTE

Été 2018: Demande de l'OLAS:

Est-ce que, en considérant les exigences et bonnes pratiques des normes de la famille ISO/IEC 27000 en matière de sécurité de l'information, il est possible de proposer une réponse adéquate à la question « Comment harmoniser l'audit des exigences du chapitre 5.10.3 de la norme ISO 15189:2012 ?

Contexte:

L'accréditation des laboratoires (essais, étalonnages et biologie médicale) ne repose pas uniquement sur leurs compétences à réaliser leurs activités spécifiques, mais aussi de garantir qu'ils maitrisent la **sécurité des informations** qu'ils gèrent. En tant que signataire des accords de reconnaissance mutuelle d'EA et d'ILAC, l'OLAS doit pouvoir démontrer que ces aspects sont examinés par des **auditeurs compétents**.

ILNAS

ANALYSE COMPARATIVE

Analyse comparative des normes d'accréditation:

- **ISO 15189 : 2012** - Laboratoires de biologie médicale - Exigences concernant la qualité et la compétence;
- **ISO/CEI 17025 : 2017** - Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais.

Les exigences concernées:

Les normes concernées prescrivent des exigences spécifiques pour encadrer la SI liée aux activités des laboratoires.

- ISO 15189 - **§ 5.10** – Gestion des informations de laboratoire;
- ISO/CEI 17025 - **§ 7.11** – Maîtrise des données et gestion de l'information.

Constat:

- Malgré des différences de formes, les objectifs à remplir en terme de sécurité des informations sont équivalents pour chaque type de laboratoire.
- Les exigences donnent des indications sur le « **QUOI** » sans pour autant dire le « **COMMENT** ».

ILNAS

PROJET DE NORME NATIONALE

Objectifs:

L'OLAS souhaite rédiger un **guide** décrivant les **bonnes pratiques en matière de sécurité de l'information** applicables aux laboratoires accrédités (ou candidats à une accréditation).

- Donner aux laboratoires concernés la possibilité de **participer** à la rédaction
- Prendre en compte les spécificités des **petites et grandes structures**
- Déterminer quel est le **minimum requis** pour répondre aux exigences des normes ISO 15189:2012 et ISO/IEC 17025:2017
- **S'aligner aux exigences et bonnes pratiques** des normes existantes de la famille ISO/IEC 27000, notamment 27001, 27002 et 27799
- **Harmoniser** l'approche des auditeurs OLAS

Champ d'application:

Le guide s'adressera

- aux responsables de la gestion de la SI et de la gestion des risques auprès des laboratoires concernés;
- aux auditeurs intervenant pour l'organisme d'accréditation.

Format du guide: **Norme nationale**

ILNAS

GROUPE DE TRAVAIL

Historique:

- 07.03.2019: Séance d'information
- 05.06.2019: Réunion de constitution du groupe de travail ILNAS TC 107:
  - Président: Mr. Dominique FERRAND
  - Secrétaire: Mr. Léon TREFF
  - Représentant ILNAS: Mr. Jérôme HOEROLD
  - Membres actifs (ca. 24)
  - Membres observateurs
- 05.06.2019: 1ère réunion de travail
  - Présentation du document « martyr »
- 05.07.2019: 2e réunion de travail
  - Analyse du document « martyr »
- 08.11.2019: Prochaine réunion de travail
  - Suite de l'analyse du document « martyr »

ILNAS

STRUCTURE DU DOCUMENT „MARTYR“

Sommaire

INFORMATIONS AU LABORATOIRE

Actifs informationnels du métier:

- Documents relatifs aux méthodes d'analyse
- Rapports d'analyse
- Contrats avec les clients
- Echantillons fournis par les clients
- Enregistrements techniques
- …

Actifs informationnels de gestion du système de management:

- Dossiers du personnel
- Documents du système de management
- Documents relatifs à la gestion des risques
- Plans de continuité des activités
- Enregistrements du système de management
- …

Actifs de support:

- L'infrastructure informatique
- Les bâtiments, locaux et équipements techniques
- Les logiciels de gestion des accès et de traitement, transfert et stockage des informations
- Les enregistrements de configuration et de mise à jour des équipements
- Le personnel externe
- …

ILNAS

EXEMPLES DE MESURES DE SECURITE (1)

Gestion des accès

Mesure spécifique au laboratoire:

L.5.2.4	Gestion d'accès	Le laboratoire définit et gère les accès au système d'information

Cette mesure fait référence à ces exigences dans les deux normes:

ISO 15189 - §5.10.3	ISO/IEC 17025 - §7.11.3
Le ou les systèmes utilisés pour la collecte, le traitement, l'enregistrement, le compte-rendu, le stockage ou la récupération de données et information doivent être: … c) protégés contre tout accès non autorisé; …	Le ou les systèmes de gestion de l'information du laboratoire doivent : a) être protégés contre tout accès non autorisé; …

Clarification:

Le laboratoire définit les droits d'accès de tous les utilisateurs du système d'information, selon le principe du besoin de connaître (need to know), et en conformité avec la mesure L.5.2.2 sur les rôles et responsabilités. Il attribue les accès selon le principe du moindre privilège (attribuer uniquement les accès réellement requis), gère les changements et effectue une revue régulière des accès.

EXEMPLES DE MESURES DE SECURITE (2)

Bonnes pratiques d'implémentation spécifique au laboratoire:

- Créer une procédure pour gérer la création et suppression des accès
- Créer une procédure pour gérer les accès en cas de changement de service de personnel
- Saisir l'identité exacte des utilisateurs et leur attribuer des accès au système d'information clairs et sans équivoque
- Gérer les droits d'accès
  - Vérifier la conformité des droits d'accès aux exigences à respecter
  - Vérifier que les droits d'accès ne sont pas exploités sans autorisation préalable
- Assurer la gestion adéquate des droits d'accès privilégiés des administrateurs du système d'information ou du personnel intervenant en cas d'incident
- Assurer la gestion adéquate des droits d'accès du personnel métier intervenant pour fournir des soins d'urgences
- Assurer la gestion adéquate des mots de passe et autres informations secrètes d'authentification de tous les utilisateurs du système d'information
- Revoir régulièrement les accès aux actifs de support
- Assurer la revue régulière de l'application des exigences à la gestion des droits d'accès
- Vérifier la gestion adéquate des droits d'accès et la disponibilité et l'accès aux documents nécessaires, dans le cas où la gestion du système d'information a été confiée ou bien au service IT interne ou à l'entité de tutelle du laboratoire ou bien à un prestataire externe
- Négocier des SLA (Service Level Agreement) comprenant ces informations

EXEMPLES DE MESURES DE SECURITE (3)

Sauvegarde des actifs de support

Mesure spécifique au laboratoire:

L.5.2.5	Sauvegarde des actifs de support	Le laboratoire sauvegarde les actifs de support du système d'information afin d'assurer leur intégrité et la continuité des activités.

Cette mesure fait référence à ces exigences dans les deux normes:

ISO 15189 - §5.10.3	ISO/IEC 17025 - §7.11.3
Le ou les systèmes utilisés pour la collecte, le traitement, l'enregistrement, le compte-rendu, le stockage ou la récupération de données et information doivent être: … d) sauvegardés en cas d'accès non autorisés ou de perte; …	Le ou les systèmes de gestion de l'information du laboratoire doivent : ... b) être protégés de la falsification et de la perte; …

Clarification:

Le laboratoire assure la sauvegarde des actifs de support du système d'information, notamment les logiciels d'exploitation, les logiciels d'application, les procédures d'installation, les fichiers de configuration, les bases de données, les journaux et toutes autres informations utiles pour pouvoir les restaurer en cas de perte ou de risque de détérioration d'intégrité en cas d'accès non autorisés.

ILNAS

EXEMPLES DE MESURES DE SECURITE (4)

Bonnes pratiques d'implémentation spécifique au laboratoire:

- Etablir un plan de réalisation des sauvegardes des actifs de support du système d'information du laboratoire, de manière similaire que pour les actifs informationnels (données et enregistrements) du laboratoire
- Tester et documenter régulièrement les procédures de sauvegarde et de restauration
- Assurer la confidentialité des données sensibles sauvegardées, notamment par l'utilisation de moyens de chiffrement
- Vérifier la gestion adéquate des sauvegardes des actifs de support et la disponibilité et l'accès aux documents nécessaires, dans le cas où la gestion du système d'information a été confiée ou bien au service IT interne ou à l'entité de tutelle du laboratoire ou bien à un prestataire externe

RELEVE DES MESURES

Résumé:

Objectif: Sécurité de l'information au laboratoire

Mesures:

1. Disponibilité et intégrité de la documentation relative aux actifs de support
2. Rôles et responsabilités
3. Gestion des changements
4. Gestion d'accès
5. Sauvegarde des actifs de support
6. Conditions environnementales adéquates
7. Stockage des actifs de support
8. Protection des données
9. Transfert de l'information
10. Continuité des activités
11. Conformité des fournisseurs

ILNAS

EXEMPLES DE BONNES PRATIQUES D'AUDIT

Bonnes pratiques d'audit (gestion des accès):

- Vérifier les enregistrements pour la revue régulière des accès
- Comparer les niveaux d'accès et les rôles (du personnel) qui ont accès à ces informations
- Vérifier que les profils des sortants sont immédiatement désactivés
- Vérifier comment on s'assure que tous les accès accordés sont conformes aux politiques relatives au contrôle d'accès et à la séparation des tâches
- Examiner les accès au système/contrôle de comptes pour les utilisateurs de systèmes privilégiés, de bases de données, d'applications et de gestionnaires de réseaux
- Vérifier si les mots de passe d'utilisateurs ou de groupes d'utilisateurs connus (connus de ceux qui quittent ou déménagent en interne) sont modifiés lorsque de tels départs ou déplacements se produisent

Bonnes pratiques d'audit (sauvegarde des actifs de support):

- Examiner la documentation des tests de la bonne exécution des sauvegardes
- Examiner la documentation des tests de restauration des sauvegardes
- Les supports de sauvegarde sont-ils physiquement protégés au moins au même niveau que les informations contenues ?
- Les sauvegardes sont-elles stockées dans des endroits appropriés ?

CONTINUATION DU PROJET

Groupe de travail ILNAS TC 107:

- Prochaine réunion: 08.11.2019
- Quelques réunions supplémentaires encore nécessaires
- Mise à jour et revue du document
- Finalisation de l'avant-projet de norme nationale

Procédure publique

- 30 jours pour introduire observations et objections

Ratification

- Ratification du projet définitif par le comité de direction « Normalisation » au sein de l'ILNAS

OFFICE LUXEMBOURGEOIS D'ACCRÉDITATION ET DE SURVEILLANCE (OLAS)

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux

Tel. : (+352) 24 77 43 -60 · Fax : (+352) 24 79 43 -60

E-mail : olas@ilnas.etat.lu

www.portail-qualite.lu

Thank you · Merci · Danke

ILNAS