OLAS OFFICE LUXEMBOURGEOIS D'ACCREDITATION ET DE SURVEILLANCE	Politique de transition pour les organismes de certification : passage de l'ISO/IEC 27006 : 2015 à l'ISO/IEC 27006-1 :2024	ILNAS

1. Objet

Cette politique établit les exigences de l'OLAS applicables aux organismes de certification de systèmes de management de la sécurité de l'information (OC) pour assurer la transition vers la norme ISO/IEC 27006-1:2024[1]. Elle prend en compte le document IAF MD 29[2].

Elle s'appuie sur les évolutions majeures identifiées dans la nouvelle version, notamment :

- l'alignement sur ISO/IEC 27001:2022 et ISO/IEC 27002:2022 ;
- la mise à jour pour les audits à distance ;
- la suppression des redondances avec ISO/IEC 17021-1 ;
- la révision des annexes relatives aux compétences et au temps d'audit.

2. Champ d'application

Cette politique s'applique aux OC actifs dans le domaine de la certification selon l'ISO/IEC 27001.

3. Exigences générales applicables aux organismes de certification

3.1 Analyse comparative des versions de la norme

L'OC doit réaliser une analyse comparative formelle et documentée entre l'ISO/IEC 27006:2015 et l'ISO/IEC 27006-1:2024 afin d'identifier les modifications à apporter à son propre fonctionnement.

Cette analyse doit couvrir au minimum les nouvelles exigences de l'ISO/IEC 27006-1:2024 :

- compétences (chapitre 7) ;
- planification et programme d'audit ;
- détermination du temps d'audit (Annexe C) ;
- audit à distance ;
- revue de la demande ;
- revue des rapports et décision de certification ;
- exigences documentaires (chapitre 8).

L'OLAS peut demander des preuves, telles que :

- l'analyse comparative ;
- le plan d'action ;
- les preuves de mise en œuvre.

3.2 Mise à jour du système de management de l'OC

L'OC doit mettre à jour :

- son système de management de la qualité ;
- ses critères de compétence ;
- ses formulaires de revue de la demande ;

[1] La norme ISO/IEC 27006-1:2024 remplace la norme ISO/IEC 27006:2015
[2] IAF MD 29 – Transition requirements for ISO/IEC 27006-1 :2024

- ses règles de détermination du temps d'audit.

L'OLAS vérifiera que les documents reflètent les nouvelles exigences, notamment :

- la nouvelle structure des compétences (7.1.1 à 7.1.3) ;
- les règles de référence aux normes dans les certificats (8.2.3) ;
- les exigences actualisées sur les audits à distance.

3.3 Compétence du personnel

L'OC doit démontrer que son personnel répond aux exigences 7.1.2 et 7.1.3 de l'ISO/IEC 27006-1:2024.

L'OLAS vérifiera :

- le plan de formation couvrant ISO/IEC 27006-1:2024, ISO/IEC 27001:2022 et ISO/IEC 27002:2022 ;
- la mise à jour des dossiers de compétence ;
- la démonstration que les auditeurs maîtrisent les nouvelles pratiques d'audit (cf. annexe E).

3.4 Mise à jour des méthodes de détermination du temps d'audit

L'OC doit appliquer les nouvelles règles de l'Annexe C de l'ISO/IEC 27006-1:2024, notamment :

- l'intégration du concept de personnes effectuant certaines activités identiques ;
- l'adaptation aux organisations sans site physique ;
- la prise en compte des audits à distance.

L'OLAS vérifiera :

- les règles internes de calcul ;
- les exemples appliqués ;
- la cohérence des durées d'audit planifiées.

3.5 Intégration des audits à distance

L'OC doit démontrer qu'il a intégré les exigences de l'ISO/IEC 27006-1:2024 relatives :

- aux audits à distance ;
- aux organisations ayant peu ou pas de sites physiques pertinents.

L'OLAS exigera :

- une procédure dédiée,
- des critères de faisabilité,
- des règles de proportionnalité,
- des preuves d'application.

3.6 Mise à jour des documents de certification

Les OC doivent adapter leurs certificats conformément à la section 8.2.3 de l'ISO/IEC 27006-1:2024, notamment :

- règles de référence à d'autres normes ;
- clarification de la portée ;
- alignement sur ISO/IEC 27001:2022.

L'OLAS vérifiera :

- les modèles de certificats ;
- les certificats émis pendant la transition.

3.7 Transition des clients certifiés

L'OC doit établir un plan de transition client incluant :

- la migration vers ISO/IEC 27001:2022 ;
- l'intégration des nouvelles exigences d'audit ;
- la communication aux clients.

L'OLAS vérifiera :

- les communications envoyées ;
- les plans d'audit de transition ;
- les rapports d'audit mis à jour.

4. Exigences applicables à l'OLAS

4.1 Soumission d'un dossier de transition

L'OC doit soumettre à l'OLAS un dossier comprenant :

- l'analyse d'écarts ;
- le plan d'action ;
- les procédures mises à jour ;
- les preuves de formation ;
- les modèles de certificats révisés ;
- les règles de calcul du temps d'audit ;
- les preuves d'audits pilotes (si exigé).

4.2 Audit d'évaluation de transition

L'OLAS se réserve le droit d'effectuer :

- un audit documentaire,
- un audit sur site ou à distance,
- une revue des dossiers d'audit récents,
- une évaluation des compétences des auditeurs.

L'OC doit démontrer une mise en œuvre complète et opérationnelle.

4.3 Délai de transition

L'OLAS fixe :

- une date limite pour l'acceptation des audits selon ISO/IEC 27006:2015,
- une date obligatoire d'application de l'ISO/IEC 27006-1:2024,
- une date limite pour la mise à jour des certificats.

5. Non-conformités et sanctions

En cas de non-respect :

- non-conformités majeures,
- suspension de l'accréditation,
- retrait de l'accréditation en cas de non-résolution.

6. Entrée en vigueur

La présente politique entre en vigueur à la date de sa publication et s'applique à tous les OC accrédités ou candidats à l'accréditation.