



Note de transition de la norme ISO/CEI 27006:2015 vers la norme ISO/IEC 27006:2015/AMD 1:2020

Indice de
révision : 00

1. Introduction

1.1 Contexte

Un amendement à la norme ISO/IEC 27006:2015 a été préparé par le comité technique ISO/IEC JTC 1/SC 27 Sécurité de l'information, cybersécurité et protection de la vie privée.

La norme amendée ISO/IEC 27006:2015/AMD 1:2020 a été publiée le 27/03/2020.

1.2 Principaux changements

Il n'a pas été identifié de changement significatif de structure ni de mises à jour majeures en termes d'exigences.

Les principales modifications apportées par l'amendement consistent en des précisions ou compléments relatifs :

- à la qualification et aux compétences des auditeurs en particulier en matière d'audit des SMSI (7.2.1.1.d et 7.2.1.1.g) ;
- à la référence, dans les documents de certification, aux standards nationaux ou internationaux tels que jugés nécessaires dans la déclaration d'applicabilité (8.2.1) ;
- aux modalités de réalisation de la revue de l'étape 1 des audits initiaux avant de procéder à l'étape 2 (9.3.1.1) ;
- au nombre de personnes à prendre en compte pour le calcul du temps d'audit (B.2.1) ;
- au calcul du temps d'audit sur site (B.3.6) ;
- à des exigences complémentaires pour le calcul et la répartition du temps d'audit entre les différents sites dans le cas de certificats multisites (B6).

1.3 délais de transition

En juillet 2020, l'IAF a publié une note relative aux dispositions de transition précisant ([https://www.iaf.nu/articles/ISO IEC 27006 2015 AMD 1 2020 Transitional Arrangement /661](https://www.iaf.nu/articles/ISO_IEC_27006_2015_AMD_1_2020_Transitional_Arrangement_661)) :

- que les organismes d'accréditation doivent être prêts à évaluer selon l'ISO/IEC 27006:2015/AMD 1:2020 dans un délai de 8 mois à compter du dernier jour du mois de publication de l'amendement (soit au 30/11/2020) ;
- que les OC doivent avoir achevé leur transition vers la norme ISO/IEC 27006:2015/AMD 1:2020, par le biais d'une évaluation du siège, dans les 24 mois suivant le dernier jour du mois de publication de l'amendement (soit au 31/03/2022).

2. Modalités d'accréditation des organismes candidats

L'instruction des demandes d'accréditation initiale ou d'extension majeure reçues à compter du 1^{er} décembre 2020 et leur évaluation subséquente sont réalisées selon la norme ISO/IEC 27006:2015/AMD 1:2020.



Note de transition de la norme ISO/CEI 27006:2015 vers la norme ISO/IEC 27006:2015/AMD 1:2020

Indice de
révision : 00

3. Evaluation des organismes déjà accrédités selon la norme ISO/IEC 27006:2015

3.1 Modalités de transition

La transition vers la norme ISO/IEC 27006:2015/AMD 1:2020 sera traitée comme une extension majeure de la portée d'accréditation conformément au règlement d'accréditation.

Les demandes de transition seront traitées en 2 temps :

- analyse documentaire des éléments communiqués dans le cadre de la demande de transition ;
- vérification de la mise en œuvre du plan d'actions décidé lors de l'évaluation au siège prévue dans le cycle.

Suite à l'analyse satisfaisante du plan de transition et du rapport d'évaluation de l'organisme (et après correction des éventuels écarts relevés), l'extension de la portée d'accréditation sera prononcée.

Le dossier de demande de transition devra être constitué du plan de transition cité ci-après et devra être adressé par chaque organisme certificateur à la structure permanente du Cofrac avant le **01/03/2021**.

3.2 Plan de transition

Chaque organisme certificateur accrédité selon l'ISO/IEC 27006:2015 devra établir un plan de transition détaillant les dispositions mises en place pour prendre en compte les changements apportés par la norme amendée ISO/IEC 27006 :2015/AMD 1:2020.

Il comprendra a minima :

- l'analyse des impacts de cette nouvelle version sur le fonctionnement de l'organisme ;
- des dispositions relatives aux modifications du processus de certification et aux procédures à mettre à jour le cas échéant ;
- des dispositions relatives aux compétences des équipes d'audit ;
- des dispositions pour la mise à jour éventuelle des documents de certification ;
- des dispositions pour la réalisation de la revue de l'étape 1 des audits initiaux ;
- des dispositions relatives au calcul du temps d'audit et le cas échéant, celles prises pour la modification de contrats de clients ;
- les modalités d'information des auditeurs et du personnel intervenant dans le processus de certification ;
- les modalités d'information des entreprises certifiées ;
- le plan d'actions décidé en conséquence et son état d'avancement.

Ce plan de transition fera l'objet d'une analyse par la structure permanente du COFRAC qui vérifiera l'adéquation des dispositions prévues pour prendre en compte les exigences de la norme ISO/IEC 27006:2015/AMD 1: 2020.

3.3 Evaluation sur site

La mise en œuvre complète des dispositions prévues dans le plan de transition sera vérifiée lors de la prochaine évaluation d'accréditation prévue dans le cycle à partir du 01/04/2021 et au plus tard avant le 31/01/2022.

Nota Bene : à compter du 01/04/2022, toutes les accréditations selon la version ISO/IEC 27006:2015 seront retirées.