Exigences spécifiques pour l'accréditation des organismes procédant à la certification de systèmes de management dans le domaine des technologies de l'information

CERT CEPE REF 35 - Révision 04

SOMMAIRE

1. OBJET

Le présent document a pour objet de définir les exigences à satisfaire et le processus d'accréditation pour les domaines suivants :

- la certification de systèmes de management dans le domaine des technologies de l'information faisant référence à la norme ISO/IEC 27001 (sécurité de l'information SMSI) et/ou
- la certification des systèmes de management des hébergeurs de données de santé à caractère personnel (HDS dans la suite du document) faisant référence au référentiel de l'Agence du Numérique en Santé (ANS).

2. REFERENCES ET DEFINITIONS

Les textes référencés dans les § 2.1 à 2.3 ci-dessous s'appliquent en complément du présent document.

2.1. Textes normatifs

- NF EN ISO/IEC 17021-1 « Evaluation de la conformité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management – Partie 1 : Exigences »
- NF EN ISO/IEC 27006 « Technologies de l'information - Techniques de sécurité -Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information » (incluant l'amendement NF EN ISO/IEC 27006+A1)
- NF EN ISO/IEC 27001 : 2017 « Technologies de l'information -Techniques de sécurité - Systèmes de management de la sécurité de l'information – Exigences », valide jusqu'au 31/10/2025
- ISO/IEC 27001 : 2013 « Information technology - Security techniques - Information security management systems - Requirements », valide jusqu'au 31/10/2025
- ISO/IEC 27001 : 2022 « Information security, cybersecurity and privacy protection - Information security management systems - Requirements
- NF ISO/IEC 27001 : 2023 « Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences »
- ISO/IEC 27017 :2015 « Technologies de l'information – Techniques de sécurité – Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage », parties applicables :
  - Chapitre 6.1.1
- ISO/IEC 27018 :2019 « Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors », parties applicables :
  - Chapitre 12.4
  - Annexe A § 1, 2.1, 4.1, 5.1, 5.2, 7.1, 9.1, 9.2, 9.3, 10 et 11

2.2. Autres textes de référence pour la certification de systèmes de management des hébergeurs de données de santé à caractère personnel

2.2.1 Publications de l'ANS[1]

- Référentiel d'accréditation HDS
- Référentiel de certification HDS – Exigences et contrôles

2.2.2 Textes règlementaires

- Loi 2016-41 du 26 janvier 2016 (Article 204) de modernisation de notre système de santé
- Ordonnance n°2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel
- Décret n° 2018-137 du 26/02/2018 relatif à l'hébergement des données de santé à caractère personnel
- Arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel

2.2.3. Lignes directrices de l'IAF[2]

- Les lignes directrices de l'IAF relatives à l'audit et la certification d'un organisme multisite, au transfert de certification, à l'utilisation des technologies de l'information et de la communication (TIC,) aux audits de systèmes de management intégrés, ainsi qu'aux données à transmettre annuellement au Cofrac, sont applicables (documents IAF MD1, IAF MD2, IAF MD4, § 1 et 2 de l'IAF MD5 : 2019, IAF MD11 et IAF MD 15 respectivement).

2.2.4. Note de transition

Note de transition de la norme ISO/IEC 27001:2013 et NF EN ISO/IEC 27001 :2017 vers la norme ISO/IEC 27001 : 2022 / NF ISO/IEC 27001 :2023, établie par le COFRAC.

Disponible sous www.cofrac.fr (https://www.cofrac.fr/qui-sommes-nous/toutes-nos-actualites/detail-dactualite/news/detail/News/securite-de-linformation-transition-vers-la-norme-isoiec-270012022/).

2.3. Définitions et acronymes

Les définitions des documents cités au §2.1 s'appliquent.

Les acronymes suivants sont utilisés dans le présent document :

- ANS Agence du Numérique en Santé
- COFRAC COmité FRançais d'ACcréditation
- OC Organisme de certification
- HDS Hébergeurs de Données de Santé

[1] Documents disponibles sur : https://esante.gouv.fr/services/hebergeurs-de-donnees-de-sante/les-referentiels-de-la-procedure-de-certification

[2] Les documents IAF sont disponibles en anglais sur : www.iaf.nu. Certains documents IAF, traduits en français, sont disponibles sur : www.cofrac.fr

3. DOMAINE D'APPLICATION

Ce document s'applique à toutes les demandes d'accréditation et aux organismes accrédités pour la certification de systèmes de management indiqués en objet.

4. MODALITES D'APPLICATION

Ce document est applicable à compter du 01/04/2023.

5. MODIFICATIONS APPORTEES A L'EDITION PRECEDENTE

Les modifications de fond sont marquées par un trait vertical dans la marge gauche.
Les principaux changements concernent :

- au § 2.1, l'ajout des normes ISO/IEC 27001 :2022 et NF ISO/IEC 27001 :2023 et l'ajout de la fin de validité des normes ISO/IEC 27001 :2013 et NF EN ISO/IEC 27001 :2017,
- au §2.2, ajout du §2.2.4 faisant référence à la Note de transition,
- des simplifications dans l'ensemble du document relatives à la référence à la norme NF EN ISO/IEC 27006 :2020 qui inclut l'amendement NF EN ISO/IEC 27006+A1,
- suppression des mentions à l'ISO/IEC 20000-1 et à l'ISO/IEC 20000-6 dans le cadre de l'arrêt de l'accréditation pour la certification de systèmes de management des services des technologies de l'information faisant référence à la norme ISO/IEC 20000-1 (SMSTI).

Dans la suite du document et pour une meilleure lisibilité, lorsque la référence générique « ISO/IEC 27001 » est employée, elle désigne à la fois ISO/IEC 27001 :2022 et NF ISO/IEC 27001 :2023

6. EXIGENCES A SATISFAIRE PAR L'ORGANISME DE CERTIFICATION

Il appartient à tout organisme candidat ou accrédité de se tenir à jour des documents de référence cités au §2 et de prendre en compte la réglementation applicable en vigueur.

Dans la suite du document, seules les exigences spécifiques à ce domaine ont été précisées, étant entendu que les exigences générales des référentiels d'accréditation et des procédures en vigueur s'appliquent. Elles sont rapportées aux chapitres de la norme qu'elles spécifient et dont l'intitulé est alors repris, ainsi que la référence à la clause correspondante de la norme. De ce fait, quand il n'y a pas d'exigence spécifique, le chapitre de la norme n'est pas repris.

6.1. Certification selon ISO/IEC 27001

Référentiels de certification	NF EN ISO/IEC 17021-1 :2015	Exigences complémentaires
ISO/IEC 27001	§ 5.2 Gestion de l'impartialité	NF EN ISO/IEC 27006 :2020
	§ 7.1 Compétence du personnel	
	§7.2 Personnel intervenant dans les activités de certification	
	§7.3 Intervention d'auditeurs et d'experts techniques externes individuels	

	§8.2 Document de certification	
	§ 8.4 Confidentialité	
	§ 9 Exigences relatives aux processus	
	§9.1.2 Revue de la demande	IAF MD 2
	§9.1.4 Détermination du temps d'audit	NF EN ISO/IEC 27006 :2020 + Annexe B
	§ 9.1.5 Echantillonnage multisites	NF EN ISO/IEC 27006 :2020 + Annexe B IAF MD1

6.2. Certification de systèmes de management des HDS

Chapitre de la norme NF EN ISO/IEC 17021-1 : 2015	NF EN ISO/IEC 27006 incluant l'amendement ISO/IEC 27006/A1:2020	Référentiel d'accréditation HDS V1.1	Décret n°2018-137 du 26/02/2018
		§ 2 Domaine d'application	Article 2 Art. R. 1111-8-8 Art. R. 1111-9
§7.1 – Compétences du personnel	§7.1	§ 5.2.2.1	
§7.2 – Personnel intervenant dans les activités de certification	§7.2	§ 5.2.2.2	
§8.2 – Documents de certification	§8.2	§ 5.2.3.2, § 2	
§ 8.4 - Confidentialité	§ 8.4	§ 5.2.3.4	
§ 9.1.1 – Demande de certification	§9.1.1	§ 5.2.4.1 a), § 7	
§ 9.1.3 – Programme d'audit	§ 9.1.3	§5.2.4.1 c)	
§ 9.1.4 – Détermination du temps d'audit	§ 9.1.4 et annexes B et C	§ 5.2.4.1 d) et annexe A	
§ 9.1.5 – Echantillonnage multiple		§ 5.2.4.1 e)	
§ 9.1.6 – Normes de systèmes de management multiples		§ 5.2.4.1 f)	
§9.4.4 – Obtention et vérification des informations			Article 2 Art. R. 1111-11.- I
§ 9.6 – Maintien de la certification		§ 5.2.4.6	
Annexe B – Méthodes possibles d'évaluation		§ 5.2.5	
/	/	§ 5.2.3.5 - Echanges d'informations entre l'OC et l'autorité compétente + Annexes B, C et D	

7. PROCESSUS D'ACCREDITATION

7.1. Généralités

Les conditions de démarrage de la certification des systèmes de management des HDS sont décrites au § 6.1 du Référentiel d'accréditation HDS V1.1.

7.2. Portée d'accréditation demandée

La portée de la demande d'accréditation est établie selon le document CERT CEPE INF 07.
Les organismes de certification demandant une accréditation pour la certification de systèmes de management des HDS doivent posséder une accréditation selon la norme NF EN ISO/IEC 17021-1 pour l'activité de certification selon l'ISO/IEC 27001 ou en faire la demande conjointement.

7.3. Modalités d'évaluation

Toute demande d'accréditation pour la certification de systèmes de management dans le domaine des technologies de l'information (ISO/IEC 27001 et/ou HDS) sera traitée selon la procédure prévue dans le document CERT REF 05 :

- demande d'accréditation initiale si l'OC n'est pas accrédité selon la NF EN ISO/IEC 17021-1 par le Cofrac,
- extension majeure de la portée d'accréditation à un nouveau domaine (objet du présent document) si l'OC est accrédité selon la NF EN ISO/IEC 17021-1 par le Cofrac.

Pour les organismes accrédités selon l'ISO/IEC 17021-1 et l'ISO/IEC 27006 pour la certification selon l'ISO/IEC 27001 par un autre organisme d'accréditation et faisant une demande d'accréditation HDS auprès du Cofrac :

Le Cofrac pourra prendre en compte cette accréditation, sous les conditions suivantes :

- le candidat à l'accréditation doit être l'entité juridique accréditée selon ISO/IEC 17021-1 et l'ISO/IEC 27006 pour la certification selon l'ISO/IEC 27001 par un autre organisme d'accréditation ;
- l'accréditation doit avoir été délivrée par un organisme d'accréditation signataire des accords multilatéraux de reconnaissance internationaux EA ou IAF ;
- l'accréditation doit être valide au moment de la demande ;
- l'organisme candidat doit fournir au Cofrac, avec sa demande d'accréditation, les coordonnées de son contact au sein de l'organisme d'accréditation afin que le Cofrac puisse vérifier la validité de l'accréditation et toute autre donnée nécessaire à l'instruction de la demande, l'organisme acceptant de ce fait que l'organisme d'accréditation puisse transmettre des données confidentielles le concernant. Lors de la préparation des évaluations HDS du cycle d'accréditation, le Cofrac pourra solliciter l'organisme d'accréditation pour le domaine ISO/IEC 27001 afin qu'il transmette le rapport et le résultat de la dernière évaluation sur le domaine ISO/IEC 27001 ;
- l'organisme doit communiquer au Cofrac sans délai toute modification du statut de l'accréditation. Le retrait ou la suspension de l'accréditation pour la certification selon l'ISO/IEC 27001 entrainera

automatiquement le retrait ou la suspension de l'accréditation pour la certification des systèmes de management des HDS ;

- si l'organisme est accrédité par le Cofrac pour d'autres certifications de systèmes de management, il devra déposer une demande d'extension majeure. Sinon, l'organisme déposera une demande d'accréditation initiale. L'évaluation initiale ou d'extension consistera notamment à évaluer la prise en compte des exigences relatives aux spécificités du schéma HDS.
- lors de l'évaluation pour le domaine HDS, si le Cofrac constate des écarts relatifs au domaine de certification selon l'ISO/IEC 27001, le Cofrac informera l'organisme d'accréditation qui a délivré l'accréditation pour ce domaine.

7.4. Observations d'activités de certification

Il doit être effectué au moins une observation d'activité à chaque évaluation. Dans la mesure du possible, chaque observation réalisée dans le cadre du cycle d'accréditation concerne un auditeur différent, un type d'entreprise de produit certifié différent, et le cas échéant, un pays différent, conformément au règlement d'accréditation CERT REF 05.

Si l'OC est candidat à l'accréditation ou accrédité pour la certification selon **les 2** référentiels cités en objet alors :

- Pour toute demande d'accréditation initiale ou d'extension majeure une observation d'activité est réalisée pour chacun des référentiels de certification sur :
  - ISO/IEC 27001
  - Référentiel de Certification HDS
- Pour les évaluations de surveillance :
  - Il est réalisé une observation d'un audit selon le référentiel HDS à chaque évaluation de surveillance
  - Il est réalisé une observation d'un audit ISO/IEC 27001 sur une évaluation de surveillance du cycle d'accréditation
- Pour les évaluations de renouvellement :
  - Il est réalisé une observation d'un audit ISO/IEC 27001 ou d'un audit selon le référentiel HDS

Lors de l'évaluation initiale ou d'extension, l'observation doit couvrir l'intégralité de la mission d'activité de certification prévue, de la réunion d'ouverture à la réunion de clôture. Pour les évaluations de surveillance et de renouvellement il est possible d'observer partiellement des audits. Ceci est déterminé par la structure permanente du Cofrac, en fonction de certains éléments (évaluations précédentes, réclamations, changements au sein de l'organisme de certification, …).

Pour chaque observation d'audit, l'OC communique à l'évaluateur en charge de l'observation le plan de l'audit observé, les rapports d'audit précédents (le cas échéant), la preuve de la compétence de l'équipe d'audit et la justification du calcul du temps d'audit.
Lorsque cela est pertinent par rapport à l'objectif et à la portée de l'observation d'activité, l'évaluateur chargé de la réalisation de l'observation doit obtenir et examiner le rapport de l'audit observé.

Les observations d'activité peuvent à titre exceptionnel concerner une autre activité du processus de certification telle que la revue de la demande, la revue des rapports, la prise de décision ou la tenue d'un comité de certification.

7.5. Attestation d'accréditation

L'attestation d'accréditation délivrée est établie selon le document CERT CEPE INF 07.

7.6. Confidentialité – Echange d'informations

Pour la certification de systèmes de management des HDS, le Cofrac informe sans délai l'ANS de toute décision d'accréditation initiale, d'extension ou de refus d'accréditation et de toute mesure de suspension ou de retrait d'accréditation d'un organisme de certification.

7.7. Dispositions à prendre en cas de suspension, de retrait d'accréditation ou de cessation d'activité de l'organisme de certification

Les dispositions suivantes viennent en complément de celles de la procédure GEN PROC 03.

7.7.1 Dispositions à prendre en cas de suspension d'accréditation

Les actions à mettre en œuvre par l'organisme concernant les certificats en vigueur émis sous accréditation sont établies au cas par cas en fonction de la raison de la suspension et sont indiquées dans le courrier de notification de suspension.

Le processus de suspension de l'accréditation HDS est décrit au § 6.3 du Référentiel d'accréditation HDS V1.1.

7.7.2 Dispositions à prendre en cas de retrait de l'accréditation ou de cessation d'activité d'un organisme de certification pour le domaine HDS

7.7.2.1 Retrait d'accréditation d'un organisme de certification

L'organisme n'est plus autorisé à délivrer de certificats ni à maintenir les certificats existants. Il doit informer les fournisseurs concernés dans les meilleurs délais pour qu'ils puissent s'adresser à un autre organisme de certification accrédité à cet effet, afin de transférer le cas échéant la certification détenue, conformément aux dispositions de l'IAF MD2 et au § 6.4 du Référentiel d'accréditation HDS V1.1.

7.7.2.2 Cessation d'activité d'un organisme de certification

L'organisme de certification doit informer les fournisseurs concernés dans les meilleurs délais pour qu'ils puissent s'adresser à un autre organisme de certification accrédité à cet effet, afin de transférer le cas échéant la certification détenue, dans les conditions énoncées au § 7.7.2.1 et conformément au § 6.5 du Référentiel d'accréditation HDS V1.1.

7.8. Modalités de transition

En cas d'évolution d'un référentiel d'accréditation ou de certification, le Cofrac établit une note de transition précisant les modalités d'évaluation mises en place pour vérifier la prise en compte des exigences de la/les

nouvelle(s) version(s) de référentiel(s) par les organismes de certification accrédités pour le/les domaine(s) concerné(s).
L'organisme de certification ne peut déclarer être accrédité pour la délivrance de certification selon la/les nouvelle(s) version(s) de référentiel(s) qu'après décision favorable du Cofrac.

8. MODALITES FINANCIERES

Les modalités énoncées dans les documents CERT REF 06 et CERT REF 07 s'appliquent, en considérant les domaines d'accréditation définis au §1.