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 01

SOMMAIRE

1. OBJET

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

- la certification de systèmes de management dans le domaine des technologies de l'information faisant référence à la norme ISO/CEI 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'ASIP Santé, et/ou
- la certification de systèmes de management des services des technologies de l'information faisant référence à la norme ISO/IEC 20000-1 (ITSMS).

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. Publications de l'ISO

- NF EN ISO/CEI 17021-1 :2015 « Evaluation de la conformité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management – Partie 1 : Exigences »
- ISO/CEI 27006 :2015 « 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 »
- NF ISO/CEI 27001 « Technologies de l'information -Techniques de sécurité - Systèmes de management de la sécurité de l'information – Exigences »
- NF ISO/CEI 20000-1 « Technologies de l'information – Gestion des services - Partie 1 : Exigences du système de management des services »
- ISO/CEI 20000-6 « Technologies de l'information - Gestion des services - Partie 6: Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la gestion des services »
- ISO/CEI 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 de nuages », parties applicables :
  - Chapitre 6.1.1
- ISO/CEI 27018 :2014 « 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'ASIP Santé

- 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'hébe rgement 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

- Les lignes directrices de l'IAF relatives au transfert de certification, aux multi sites, aux audits de systèmes de management intégrés, ainsi qu'aux données à transmettre annuellement au Cofrac sont applicables (documents IAF MD2, IAF MD3, IAF MD4, IAF MD11 et IAF MD 15 respectivement).

2.3. Définitions et acronymes

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

Les acronymes suivants sont utilisés dans le présent document :

- ASIP Santé Agence française de la santé numérique
- COFRAC COmité FRançais d'ACcréditation
- OC Organisme Certificateur
- HDS Hébergeurs de Données de Santé

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 15/08/2018.

5. MODIFICATIONS APPORTEES A L'EDITION PRECEDENTE

Pour la certification HDS : ajout au § 7.3 des modalités et conditions de prise en compte par le Cofrac des accréditations ISO 17021-1 et ISO 27006 délivrés par d'autres organismes d'accréditation.
Ajout de précisions pour les observations d'activités au § 7.4.

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/CEI 27001

Référentiels de certification	NF EN ISO/CEI 17021-1	Exigences complémentaires
ISO/CEI 27001	§ 5.2 Gestion de l'impartialité	ISO /CEI 27006
	§ 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	ISO /CEI 27006 + Annexe B
	§ 9.1.5 Echantillonnage multi-sites	L'échantillonnage est réalisé en appliquant le document IAF MD1. L'ISO/IEC 27006 est ensuite appliquée à chaque site échantillonné.

6.2. Certification selon ISO/CEI 20000-1

Référentiels de certification	NF EN ISO/CEI 17021-1	Exigences complémentaires
ISO/CEI 20000-1	§5.2 Gestion de l'impartialité	ISO 20000-6
	§7.1.2 Détermination des critères de compétences	
	§7.2 Personnel intervenant dans les activités de certification	
	§8.2 Document de certification	

	§ 8.4 Confidentialité	
	§ 9.1.2 Revue de la demande	
	§ 9.1.4 Détermination du temps d'audit	
	§ 9.1.5 Echantillonnage multipiste	
	§ 9.1.6 Normes de systèmes de management multiples	
	§ 9.2.1 Détermination des objectifs, du périmètre et des critères d'audit	
	§ 9.2.3 Plan d'audit	
	§ 9.3 Certification initiale	
	§ 9.4.8 Rapport d'audit	

6.3. Certification de systèmes de management des HDS

Chapitre de la norme NF EN ISO/CEI 17021-1	ISO/CEI 27006	Référentiel d'accréditation HDS	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.

7.2. Portée d'accréditation demandée

La portée de la demande d'accréditation est établie selon le document CERT CEPE INF 07.

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/CEI 27001et/ou ISO 20000-1 et/ou HDS) sera traitée selon la procédure prévue dans le document CERT REF 05,

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

Pour toute autre demande de la part d'OC déjà accrédités par le Cofrac pour l'un des domaines, les extensions sont traitées selon le tableau ci-dessous.

Accréditation déjà octroyée / Accréditation demandée	ISO/CEI 27001	ISO/CEI 20000-1
ISO/CEI 27001		Extension majeure
ISO/CEI 20000-1	Extension mineure	
HDS	Extension majeure	Extension majeure

Pour chaque évaluation, l'équipe d'évaluation comprend un évaluateur technique compétent dans le domaine des technologies de l'information.

Pour les organismes accrédités selon ISO 17021-1 et l'ISO/CEI 27006 pour la certification selon l'ISO 27001 par un autre organisme d'accréditation :

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 17021-1 et l'ISO/CEI 27006 pour la certification selon l'ISO 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.

- L'organisme doit communiquer au Cofrac sans délai toute modification du statut de l'accréditation. La suspension de l'accréditation pour la certification ISO 27001 entrainera automatiquement 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 à la certification selon l'ISO 20000-1 et aux spécificités du schéma HDS.

7.4. Observations d'activités de certification

Si l'OC est accrédité pour la certification selon **un** des référentiels cités en objets, les observations d'activités sont réalisées conformément aux dispositions prévues dans le règlement d'accréditation CERT REF 05.

Si l'OC est accrédité ou demande une accréditation pour la certification selon **2 ou les 3** référentiels cités en objets alors :

- Pour toute demande d'accréditation initiale ou d'extension majeure il doit être effectué une observation d'activité sur chacun des référentiels de certification sur l'ensemble de l'audit :
  - ISO 27001
  - Référentiel de Certification HDS
  - ISO 20000-1
- 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 27001 sur une évaluation de surveillance du cycle d'accréditation
  - Il est réalisé une observation d'un audit ISO 20000-1 sur une évaluation de surveillance du cycle d'accréditation
- Pour les évaluations de renouvellement :
  - Il est réalisé une observation d'un audit ISO 27001 ou d'un audit selon le référentiel HDS
  - Il est réalisé une observation d'un audit ISO 20000-1

Lors de l'évaluation initiale ou de l'évaluation 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 réévaluation 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, 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.

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

Le Cofrac informe l'autorité compétente sans délai de toute décision d'octroi, d'extension, de refus, de suspension ou de retrait d'accréditation d'un OC pour la certification de systèmes de management des HDS.

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

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 est décrit au § 6.3 du Référentiel de certification HDS - Accréditation.

7.7.2 Dispositions à prendre en cas de retrait de l'accréditation ou de cessation d'activité d'un organisme certificateur.

7.7.2.1 Retrait d'accréditation d'un organisme certificateur

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 de certification HDS - Accréditation.

7.7.2.2 Cessation d'activité d'un organisme certificateur

L'organisme certificateur 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 de certification HDS – Accréditation.

8. MODALITES FINANCIERES

Les modalités énoncées dans les documents CERT REF 06 et CERT REF 07 s'appliquent, en considérant les activités de certification objet du présent document comme un domaine d'accréditation.