

Programme de certification SMSI/HDS



Version du document	Date de modification	Objet de la modification	Éditeur	Approbateur	Date d'approbation
V1.0	22/06/2024	Création	Guillaume CARAT	Mathieu BAUDAIS	30/08/2024
V1.1	02/09/2024	Modifications mineures	Mathieu BAUDAIS	Guillaume CARAT	02/09/2024
V1.2	31/10/2024	Modifications mineures	Guillaume CARAT	Mathieu BAUDAIS	31/10/2024
V1.3	30/12/2024	Modifications comités	Guillaume CARAT	Mathieu BAUDAIS	30/12/2024
V1.4	13/01/2025	Ajout Impartialité dans comité de stratégie	Guillaume CARAT	Mathieu BAUDAIS	14/01/2025
V1.5	18/01/2025	Prise en compte HDS	Guillaume CARAT	Mathieu BAUDAIS	18/01/2025
V1.6	25/06/2025	Modifications majeures	Guillaume CARAT	Mathieu BAUDAIS	23/07/2025
V1.7	07/08/2025	Corrections de fautes d'orthographe, Précisions sur les délais liés aux audits complémentaires	Guillaume CARAT	Ronan LUCAS	07/08/2025
V1.8	25/08/2025	Reformulation du processus de décision de certification	Guillaume CARAT	Ronan LUCAS	25/08/2025

Table des matières

1. Objet	4
2. Références et définitions	4
2.1. Références	4
2.2. Termes et définitions	4
3. Principes de certification	5
3.1. Impartialité	5
3.2. Compétence	6
3.3. Responsabilité	6
3.4. Confidentialité	6
3.5. Transparence	6
3.6. Traitement des plaintes et des appels	7
3.7. Approche fondée sur les risques	7
4. Modalités juridiques et contractuelles	7
4.1. Modalités juridiques	7
4.2. Modalités contractuelles	7
5. Informations	7
5.1. Modifications émanant de CYBEVAL	7
5.2. Modifications émanant d'un Client certifié	8
6. Processus de certification	8
6.1. Demande de certification	8
6.1.1. Demande de certification d'un Client titulaire d'un document de certification ISO/IEC 27001 et/ou HDS 8	8
6.1.2. Demande de certification d'un Client non certifié	9
6.2. Revue de la demande de certification	10
6.3. Programme d'audit de certification	11
6.4. Contrat de certification	12
6.5. Cas de l'audit à blanc ou pré-audit	12
6.6. Audit de certification initial	13
6.6.1. Audit Etape 1	13
6.6.2. Audit Étape 2	14
6.6.3. Traitement des non-conformités, le cas échéant	14
6.7. Rapport d'audit	14
6.8. Décision de certification	15

6.8.1.	Revue de certification	15
6.8.2.	Décision de certification	16
6.8.3.	Document de certification	16
6.9.	Activités de certification post octroi de la certification.....	16
6.9.1.	Activités de surveillance de la certification	16
6.9.2.	Activités de renouvellement de la certification.....	17
6.9.3.	Audits particuliers.....	18
6.9.3.1.	Extension du périmètre	18
6.9.3.2.	Audits avec un préavis très court	18
6.9.4.	Cas de l’audit à distance.....	18
6.9.5.	Suspension, retrait ou réduction du périmètre de la certification	18
7.	Modalités d’échange d’informations entre CYBEVAL et l’autorité compétence, dans le cas d’une certification HDS	19
7.1.	Rapport de suspension HDS	19
7.2.	Rapport de retrait HDS	19
7.3.	Répertoire Clients HDS	20
7.4.	Rapport annuel HDS	20
8.	Appels.....	20
9.	Plaintes.....	21
10.	Enregistrements relatifs au Client.....	21
ANNEXE I : Échanges d’informations entre CYBEVAL et l’autorité compétente.....		23

1. Objet

Ce document définit le Programme de Certification SMSI/HDS conduit par CYBEVAL, conformément aux normes citées en référence. Le programme décrit les modalités de certification des systèmes de management de la sécurité de l'information (SMSI – ISO/IEC 27001) et des Hébergeurs de Données de Santé (HDS).

La certification des systèmes de management de la sécurité de l'information (SMSI – ISO/IEC 27001) et des Hébergeurs de Données de Santé (HDS) porte seulement sur l'évaluation de la conformité du système de management entrant dans le champ d'application de la norme ISO/IEC 17021-1, et non sur la certification de produits, services ou processus/procédés.

2. Références et définitions

2.1. Références

- Norme NF EN ISO/IEC 17021-1:2015
- Référentiel d'accréditation HDS v2.0
- Norme ISO/IEC 27006-1:2024 Sécurité de l'information, cybersécurité et protection de la vie privée
- Exigences pour les organismes procédant à l'audit de management de la sécurité de l'information – Partie 1 : Généralités
- Exigences spécifiques pour l'accréditation des organismes procédant à la certification de systèmes de management dans le domaine des technologies de l'information COFRAC, CERT CEPE REF 35, version en vigueur
- Exigences spécifiques pour les programmes de certification COFRAC, CERT-REF-09, version en vigueur
- Norme ISO / IEC 19011 :2018 « lignes directrices pour l'audit des systèmes de management »
- Norme NF EN ISO/IEC 27001:2022 Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences
- Référentiel de certification HDS exigences v2.0
- Document d'exigences IAF pour le transfert d'une certification sous accréditation de systèmes de management, IAF MD2, version en vigueur

4

2.2. Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO9000, ISO/IEC 17000, ainsi que les suivants, et HDS s'appliquent.

- Audit de certification : audit réalisé par un organisme d'audit indépendant du Client et des parties qui comptent sur la certification, aux fins de certifier le système de management d'un Client
 1. Les activités d'audit incluent normalement :
 - La conduite de la réunion d'ouverture
 - La réalisation d'une revue documentaire pendant la conduite de l'audit
 - La communication pendant l'audit
 - L'attribution des rôles et des responsabilités de guides et d'observateurs
 - La collecte et la vérification des informations
 - La génération des constats d'audit
 - La préparation des conclusions d'audit
 - La conduite de la réunion de clôture
- Auditeur : personne qui réalise un audit
- Client : organisme dont le système de management est audité à des fins de certification
- Client certifié : organisme dont le système de management a été certifié
- Compétence : aptitude à mettre en pratique des connaissances et un savoir-faire pour obtenir les résultats escomptés
- Conseil en matière de système de management : contribution à l'établissement, à la mise en œuvre ou à l'entretien d'un système de management
- Expert technique : personne apportant à l'équipe d'audit des connaissances ou une expertise spécifique

- Guide : personne nommée par le Client pour assister l'équipe d'audit
- Impartialité : existence d'objectivité (précision : L'objectivité implique soit l'absence de conflits d'intérêts, soit de trouver une solution à ces conflits de manière à ne pas porter préjudice aux activités ultérieures de CYBEVAL)
- Observateur : personne qui accompagne l'équipe d'audit, mais qui n'audite pas
- Non-conformité : non-satisfaction d'une exigence
 1. Non-conformité majeure : non-conformité qui affecte la capacité du système de management à atteindre les résultats escomptés (précision. Les non-conformités pourraient être classées comme majeures dans les circonstances suivantes: s'il existe un doute significatif quant à la mise en place d'une maîtrise efficace des processus ou que des produits ou services rempliront les exigences spécifiées, ou s'il y a plusieurs non-conformités mineures associées à la même exigence ou à un problème pouvant ainsi montrer une défaillance systémique et ainsi constituer une non-conformité majeure)
 2. Non-conformité mineure : non-conformité qui n'affecte pas la capacité du système de management à atteindre les résultats escomptés
- Secteur technique : secteur caractérisé par des éléments communs des processus se rapportant à un type spécifique de système de management et à ses résultats escomptés
- Plaintes : expression d'une insatisfaction, autre qu'un appel, émise par toute personne et relative aux opérations de CYBEVAL, quand une réponse est attendue (Exemple : délai d'action jugé trop important, informations jugées erronées sur le site internet de CYBEVAL, qualité d'investigation ou comportement d'un auditeur ou d'un tiers jugés insatisfaisants)
- Appels : demande exprimée par un Client visant à reconsidérer toute décision défavorable prise par CYBEVAL relative au statut de la certification, ou liée à la classification des constats d'audits

En complément, pour la certification HDS, il convient de consulter le référentiel de certification HDS dans sa version en vigueur.

3. Principes de certification

Les principes de certification sont issus des normes d'audit citées en référence, et ont pour objectif de donner confiance à toutes les parties prenantes que le système de management certifié satisfait aux exigences spécifiées.

L'application des 7 principes ci-après permet ainsi de donner de la valeur à la certification, de la confiance dans le fait que le système de management a été évalué par une tierce partie de manière indépendante, impartiale et avec compétence.

Les parties prenantes sont notamment les Clients de CYBEVAL, au premier chef, mais également leurs propres Clients, les pouvoirs publics, les organismes non gouvernementaux, ainsi que le grand public.

3.1. Impartialité

L'impartialité de CYBEVAL est un pilier fondamental de la confiance dans le processus de certification.

Aucune société de conseil ne dispose de parts sociales dans le capital de CYBEVAL.

Les modalités de contrôle et d'exercice de cette impartialité par CYBEVAL sont documentés dans le document de politique générale relatif à la gestion de l'impartialité (CYB-POL-PUB-Politique-Impartialité.docx).

L'impartialité étant un élément essentiel de l'audit de tierce partie, les auditeurs internes et externes de CYBEVAL doivent connaître cette politique qui est communicable sur demande au Client candidat à la certification.

3.2. Compétence

La compétence du personnel de CYBEVAL intervenant dans les activités de certification, comme les auditeurs, est le deuxième pilier de confiance vis-à-vis des Clients et de l'ensemble des parties prenantes. Une politique spécifique de validation et de maintien des compétences, imposées par les normes en vigueur (Cf. Références) est mise en place à cet effet (CYB-POL-INT-Gestion-Compétences).

Les curriculum vitae des membres de l'équipe d'audit sont fournis systématiquement aux Clients candidats à la certification.

3.3. Responsabilité

CYBEVAL est tenu de réaliser une évaluation suffisante des preuves tangibles sur lesquelles fonder la décision de certification ou de non-certification.

Il est rappelé que l'audit étant fondé sur un échantillonnage du système de management de l'organisme Client, il ne garantit pas une conformité de 100% aux exigences, et que des éléments peuvent ne pas être constatés par les auditeurs de CYBEVAL à ce titre.

Il est également rappelé que, dès lors que la décision de certification a été prise, c'est de la responsabilité du Client certifié de maintenir la conformité de son système de management aux exigences de certification, et non de celle de CYBEVAL.

3.4. Confidentialité

La confidentialité est au cœur des principes fondateurs de CYBEVAL.

CYBEVAL ne divulgue aucune information confidentielle relative à ses Clients ou à leurs données. Tous les éléments collectés lors des audits sont stockés de manière sécurisée dans des répertoires chiffrés, conformément à la politique de confidentialité (CYB-POL-PUB-Politique-Confidentialité.docx).

Dans le cas d'une certification HDS, avant toute intervention de la part de l'équipe d'audit, CYBEVAL doit s'assurer avec le Client candidat à la certification que les informations qui seront communiquées durant l'audit ne contiennent aucune donnée de santé à caractère personnel, ni aucune donnée confidentielle ou sensible. Le cas échéant, CYBEVAL et le Client candidat doivent définir les modalités d'accès au système devant être audité (engagement de confidentialité, etc...).

Dans le cas d'une incapacité à auditer le système d'information sans accéder à des données de santé à caractère personnel ou d'autres données confidentielles ou sensibles, CYBEVAL doit en informer le Client candidat, un accord de confidentialité doit être établi et un professionnel de santé intervenant sous la responsabilité du Client doit être informé.

Les données de santé à caractère personnel et toutes autres données confidentielles ou sensibles auxquelles CYBEVAL aurait accès dans le cadre de l'audit ne peuvent être divulguées ou réutilisées par CYBEVAL, ni par le Client candidat à la certification.

3.5. Transparence

L'obligation de transparence se traduit par le fait d'assurer l'accessibilité des informations appropriées et à jour par CYBEVAL de ses processus d'audit et de certification ainsi que sur le statut de la certification de tout organisme, sur demande.

Pour ce faire, le site Internet de CYBEVAL permet d'interroger CYBEVAL via le formulaire de contact (www.cybeval.fr).

3.6. Traitement des plaintes et des appels

CYBEVAL dispose d'un mécanisme de réception et de traitement des plaintes et des appels.

Dans le cadre d'une activité de certification, un appel ou une plainte peut être déposé(e) en envoyant un mail à l'adresse reclamation@cybeval.fr pour les plaintes, et recours@cybeval.fr pour les appels. Il/Elle sera traité(e) via la procédure interne de traitement des plaintes & appels.

3.7. Approche fondée sur les risques

CYBEVAL mesure et tient compte de différents risques afin de garantir un mécanisme de certification réalisé avec compétence, cohérence et impartialité :

1. Objectifs de l'audit (durant la phase préparatoire à l'audit)
2. Échantillonnage utilisé dans le processus d'audit (phase préparatoire)
3. Impartialité réelle et perçue (phase préparatoire et tout au long de l'audit)
4. Questions juridiques, réglementaires, responsabilités (ateliers spécifiques de l'audit)
5. Organisme Client audité et son environnement opérationnel (atelier spécifique de l'audit)
6. Impact de l'audit sur le Client et ses activités (phase préparatoire)
7. Santé et sécurité des équipes d'audit (phase préparatoire et tout au long de l'audit)
8. Perception des parties intéressées (avant, pendant et après l'audit)
9. Déclarations trompeuses du Client certifié (phase préparatoire et tout au long de l'audit)
10. Utilisation des marques (atelier spécifique de l'audit).
11. Disponibilité des interlocuteurs (avant, pendant et après l'audit)

Dans le cas d'un manquement grave du Client pendant le processus de certification, CYBEVAL se réserve le droit d'interrompre le processus, en documentant la raison de cette décision, et en s'appuyant sur un ou plusieurs des 11 risques identifiés.

4. Modalités juridiques et contractuelles

4.1. Modalités juridiques

CYBEVAL est une entité juridique à part entière pouvant être tenue juridiquement responsable de toutes ses activités de certification.

Un extrait KBIS et une attestation d'assurance qui couvre l'international peuvent être fournis au Client candidat à la certification sur demande.

4.2. Modalités contractuelles

Un contrat spécifique juridiquement exécutoire est signé entre CYBEVAL et chaque Client candidat à la certification, préalablement au déclenchement du processus d'audit. CYBEVAL est responsable de ses décisions en matière de certification, incluant l'octroi, le refus, le maintien de la certification, l'extension ou la réduction du périmètre de la certification, le renouvellement, la suspension ou le rétablissement après la suspension, ou le retrait de la certification.

5. Informations

5.1. Modifications émanant de CYBEVAL

Exigences supplémentaires propres à l'HDS

Lorsque le Client dispose d'un document de certification pour la certification ISO 27001 établit par un autre organisme de certification accrédité, CYBEVAL est tenu d'informer ce confrère en cas de non-conformité relative à une exigence de l'ISO 27001 constatée à l'occasion d'un audit HDS.

Lorsqu'une modification des exigences de CYBEVAL en matière de certification a lieu, CYBEVAL informe chacun de ses Clients de ces évolutions, et met en place un formulaire de recueil de prise en compte de ces modifications par les Clients.

5.2. Modifications émanant d'un Client certifié

Le Client à la certification est avisé que toute modification pouvant compromettre la capacité de son système de management à se conformer aux exigences de la norme doit être indiquée le plus rapidement possible à CYBEVAL, par le moyen de son choix (mail, téléphone), dans les Conditions Générales de Certification.

Cela concerne notamment :

- Le statut juridique, commercial, l'actionnariat, l'organisation
- Changement de dirigeant, de personne-clé
- Coordonnées de la personne à contacter et les sites principaux
- Périmètre des opérations réalisées dans le cadre du système de management certifié
- Modifications importantes apportées au système de management et aux processus

Exigences supplémentaires propres à l'HDS

Lorsque le Client dispose d'un document de certification pour la certification ISO 27001 établi par un autre organisme de certification accrédité, le client a l'obligation d'informer immédiatement CYBEVAL de toute mesure de suspension, retrait, résiliation ou transfert de son certificat ISO 27001. Cet engagement fait l'objet d'une vérification lors des audits de surveillance.

6. Processus de certification

L'ensemble des dispositions à venir s'applique également pour le référentiel ISO27001 et HDS quel que soit le type d'audit considéré, et la typologie de l'audit dans le cycle de certification.

6.1. Demande de certification

6.1.1. Demande de certification d'un Client titulaire d'un document de certification ISO/IEC 27001 et/ou HDS

Dans le cas d'un transfert de certification vers CYBEVAL, le Client demandeur doit fournir à CYBEVAL les rapports d'audit précédents ainsi que les éléments de suivi des non-conformités éventuelles.

CYBEVAL demandera également à l'organisme émetteur le dossier de certification et le statut de la certification, conformément à la procédure de transfert CYB-PRO-INT.

Tant que CYBEVAL n'est pas accrédité, CYBEVAL doit proposer un audit de certification initial en indiquant au Client les raisons de ce choix imposé par les exigences applicables (Cf. Références), ou inviter le Client à se tourner vers un centre d'évaluation déjà accrédité sur le programme concerné. C'est pourquoi CYBEVAL applique les dispositions applicables pour tout nouveau Client non certifié décrites ci-après, pour tout Client titulaire d'un document de certification émis par un autre organisme de certification accrédité.

Exigences supplémentaires propres à l'HDS

Si le Client souhaite faire prévaloir la certification selon la norme NF ISO 27001 qu'il a déjà obtenue, cette certification doit remplir toutes les conditions ci-dessous :

- Le périmètre d'application de la certification dont dispose l'hébergeur doit inclure le périmètre pour lequel il demande une certification HDS
- Les rapports d'audit : le rapport d'audit initial et les rapports d'audit de surveillance de la certification dont l'équivalence est demandée doivent être fournis à CYBEVAL
- Pour un Client candidat disposant d'une certification ISO 27001, la déclaration d'applicabilité (DDA) du système de gestion de la sécurité des informations de l'organisation doit expressément inclure :
 - La justification détaillée de toute exclusion de contrôles de l'ISO 27001
 - La justification détaillée de tout contrôle non applicable

- La certification doit être en cours de validité et avoir été délivrée par un organisme de certification accrédité par une instance nationale d'accréditation telle que définie dans le règlement (CE) n° 765/2008 pour la délivrance de ces certificats et dont l'accréditation doit être en cours de validité (le COFRAC en France ou son équivalent dans les autres pays signataires des accords multilatéraux de reconnaissance internationaux)
 - Ne pas faire l'objet d'une procédure de suspension ou de retrait
 - Ne pas faire l'objet d'une demande de transfert

Les certifications obtenues selon des normes internationales équivalentes aux normes françaises pourront être reconnues selon les mêmes conditions. Il s'agit notamment des certifications de conformité aux normes ISO 27001 et ISO 17021 dans d'autres langues que le français.

6.1.2. Demande de certification d'un Client non certifié

La première étape d'une certification nécessite la réponse à plusieurs questions, de la part du Client candidat à la certification :

- Le périmètre souhaité pour la certification
- Les détails pertinents du Client candidat (raison sociale, adresse du (des) site(s), les ressources humaines et techniques, ses fonctions, ses processus et opérations, et toutes les obligations juridiques applicables)
- L'identification des processus externalisés utilisés par l'organisme qui peuvent affecter potentiellement la conformité aux exigences
- Les normes ou les autres exigences par rapport auxquelles le Client candidat souhaite être certifié
- Si des prestations de conseil pour la certification ont été fournies au Client candidat, et si oui, par qui
- Le contexte, les aspects métiers spécifiques, le secteur professionnel et si ce dernier impacte le SMSI les types de produits ou de processus et si ces derniers ont un impact sur le SMSI

La liste suivante énumère de manière non exhaustive des éléments supplémentaires pouvant être précisés :

- Type d'audit : combiné, intégré, conjoint
- Données de performance du Client (niveaux des indicateurs clés de l'organisation par exemple)
- Préoccupations pertinentes des parties intéressées
- Organisation interne des équipes du Client, notamment dans le cas de rotation d'équipes

Ces questions sont envoyées au Client candidat par l'intermédiaire d'un formulaire spécifique (CYB-FOR-PUB-Demande-Certification.docx).

Les réponses peuvent directement être fournies par le Client candidat via le formulaire disponible en ligne sur le site Internet de CYBEVAL.

Exigences supplémentaires propres à l'HDS

Le Client précise également la liste des activités du référentiel HDS afin de déterminer le type de certification HDS :

Est considérée comme une activité d'hébergement de données de santé à caractère personnel sur support numérique au sens du II de l'article L. 1111-8, le fait d'assurer pour le compte du responsable de traitement mentionné au 1° du I de l'article R. 1111-8-8 ou du patient mentionné au 2° du I de ce même article, tout ou partie des activités suivantes :

1° La mise à disposition et le maintien en condition opérationnelle de sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;

2° La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;

3° La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;

4° La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;

5° L'administration et l'exploitation du système d'information contenant les données de santé ;

6° La sauvegarde des données de santé.

Un Client candidat souhaitant obtenir une certification HDS devra répondre aux exigences du référentiel de certification HDS.

La certification d'un hébergeur nécessite :

- Qu'il ait mis en œuvre un Système de Management de la Sécurité de l'Information (SMSI) certifié selon la norme ISO 27001, complétée des exigences définies au chapitre 5 du référentiel de certification HDS
- Que le domaine d'application de ce SMSI couvre l'ensemble des activités d'hébergement de données de santé de l'Hébergeur
- Que les contrats conclus avec ses clients répondent aux exigences définies au chapitre 6 du référentiel de certification HDS
- Qu'il respecte les exigences relatives à la souveraineté définies au chapitre 7 du référentiel de certification HDS
- Qu'il communique à ses clients la présentation des garanties formalisée conformément au chapitre 8 du référentiel de certification HDS

10

En cas de recours à des sous-traitants par l'hébergeur, la représentation des garanties décrite au chapitre 8 du référentiel de certification HDS s'applique.

Un hébergeur qui a déjà obtenu une certification ISO 27001 peut faire prévaloir cette certification s'il remplit les conditions citées dans le chapitre 6.1.1.

6.2. Revue de la demande de certification

CYBEVAL effectue une revue de la candidature et des informations fournies pour s'assurer que :

- Les informations fournies sont suffisantes pour élaborer un programme d'audit
- Il ne subsiste aucun malentendu entre le Client candidat et CYBEVAL
- CYBEVAL dispose bien de la capacité et la compétence d'effectuer la prestation demandée
- Le périmètre souhaité et l'ensemble des éléments influant sur les activités de certification sont pris en compte (langue, sécurité, impartialité, etc . . .)

Suite à la revue de la demande, CYBEVAL peut soit accepter, soit refuser la demande de certification.

- Lorsque CYBEVAL refuse une demande de certification suite à la revue de la demande, CYBEVAL documentera les raisons de son refus et les indiquera clairement au Client candidat.
- Lorsque CYBEVAL accepte la demande de certification, il élabore un programme d'audit afin d'établir un contrat de certification.

Exigences supplémentaires propres à l'HDS

Les conditions décrites au 6.1.1. font l'objet d'une vérification et CYBEVAL enregistre les informations reçues (copies des certificats notamment) et justifie les résultats de cette vérification en indiquant quelle(s) certification(s) est (sont) acceptée(s).

6.3. Programme d'audit de certification

Le programme d'audit d'un cycle complet de certification est élaboré pour identifier clairement les activités d'audit requises afin de démontrer que le système de management du Client répond aux exigences de la certification suivant les documents normatifs choisis. Il couvre l'ensemble des exigences relatives au système de management.

Le programme d'audit de certification initiale se décompose comme suit :

- Audit initial en 2 étapes, suivi d'une décision de certification
- Audits de surveillance la première et deuxième année après la décision de certification, dans un délai maximal de 12 mois à compter de la date de décision de certification ; toutefois, la fréquence de surveillance peut être réduite à 3 ou 6 mois en fonction des résultats des audits précédents.
- Audit de renouvellement la troisième année avant l'expiration de la certification

Le premier cycle de certification de trois ans commence avec la date de la décision de certification.

Les cycles suivants commencent avec la date de la décision de renouvellement de la certification.

Les audits de surveillance sont effectués au moins une fois par année civile. La date du premier audit de surveillance suivant la certification initiale doit être fixée dans un délai entre 10 et 12 mois à compter de la date de certification.

La date de l'audit de renouvellement doit être fixée de manière à ce que toutes les activités de renouvellement soient débutées, et dans la mesure du possible achevées, afin de pouvoir renouveler le certificat avant sa date d'expiration.

Le programme d'audit d'une certification renouvelée se décompose comme suit :

- Audits de surveillance la première et deuxième année après la décision de renouvellement
- Audit de renouvellement la troisième année avant l'expiration de la certification

Lors de l'élaboration du programme d'audit, CYBEVAL détermine les besoins spécifiques en termes de compétences afin de désigner l'équipe d'audit adéquate. CYBEVAL identifie les compétences spécifiques nécessaires le cas échéant au regard :

- Des aspects métiers spécifiques suivant le domaine d'activité à auditer (dépend des auditeurs, dépend des clients)
- De la connaissance des exigences légales et réglementaires dans le domaine correspondant de la sécurité de l'information, dans la zone géographique et la juridiction concernée
- Des risques de sécurité de l'information de différents secteurs professionnels
- De la terminologie générique des processus et des technologies de différents secteurs professionnels
- Des pratiques pertinentes dans différents secteurs professionnels
- De l'incidence du type de l'organisation, de sa taille, sa gouvernance, sa structure, ses fonctions et ses relations sur le développement et la mise en œuvre du SMSI et des activités de certification, y compris l'externalisation

- Des exigences légales et réglementaires applicables à divers produits ou services

CYBEVAL convient à l'avance avec le client des dates d'audit au regard de ce programme.

CYBEVAL conserve le programme d'audit et la grille de sélection de l'équipe d'audit au regard des besoins spécifiques en termes de compétences.

Exigences supplémentaires propres à l'HDS

Avant toute intervention de la part de l'équipe d'audit, CYBEVAL s'assure avec le Client que les informations qui seront communiquées durant l'audit ne contiennent aucune donnée de santé à caractère personnel, ni aucune donnée confidentielle ou sensible. Le cas échéant, CYBEVAL et son Client définissent les modalités d'accès au système devant être audité (engagement de confidentialité, etc.).

Dans le cas d'une incapacité à auditer le système d'information sans accéder à des données de santé à caractère personnel ou d'autres données confidentielles ou sensibles, CYBEVAL en informe le Client. Un accord de confidentialité est alors établi et un professionnel de santé intervenant sous la responsabilité du client est informé.

La description du périmètre de certification doit préciser la liste des activités de certification pour lesquelles le Client demande une certification afin de déterminer le type de certification HDS.

Un Client disposant déjà de cette certification est évalué sur le périmètre des exigences du référentiel de certification non couvertes par la certification.

6.4. Contrat de certification

CYBEVAL établit un contrat de certification juridiquement exécutoire afin de cadrer l'ensemble de la démarche de certification entre le Client et CYBEVAL.

Le contrat doit être signé par les deux parties avant de pouvoir entrer dans la phase de planification opérationnelle et de réalisation des activités d'audit.

6.5. Cas de l'audit à blanc ou pré-audit

Dans le cas d'un audit à blanc (ou pré-audit), le processus d'audit est exactement le même qu'un processus d'audit de certification classique, sans revue de certification ni prise de décision relative à la certification. Cet audit ne donne pas lieu à la délivrance de conseil et ne peut donc être assimilé à une prestation de conseil, ni à un audit interne.

Les règles suivantes s'appliquent :

1. Les pré-audits n'ont d'autre but que d'effectuer une évaluation factuelle de l'état de préparation d'une entité au regard des critères de la certification souhaitée, en décelant des écarts éventuels sans préconiser les solutions pour les résoudre, ni suivre leur résolution ;
2. L'activité de pré-audit est réservée aux clients non encore certifiés (en demande de certification initiale pour une norme donnée ou en transition vers une nouvelle version d'une norme pour laquelle le client est certifié) ;
3. Les règles de déontologie pour le pré-audit sont les mêmes que pour une certification classique ;
4. Le pré-audit est limité à une seule intervention par site et par domaine de certification avant un audit de certification ;
5. La durée du pré-audit est nettement inférieure à la durée d'un audit initial de certification : elle est de 1/3 de la charge d'un audit initial. En conséquence, le pré-audit ne peut pas être considéré comme une évaluation exhaustive de son système qualité ;
6. Tout pré-audit donne lieu à un rapport, adressé au client, et consultable lors des évaluations du COFRAC, permettant de s'assurer que les intervenants ne se sont pas écartés de leur mission ;
7. Un pré-audit ne peut être assimilé à l'étape 1 d'un audit de certification initiale, ni à un audit interne.

6.6. Audit de certification initial

Les audits sont réalisés conformément à la norme ISO / IEC 19011 « lignes directrices pour l'audit des systèmes de management ».

L'audit de certification initiale d'un SMSI est mené en deux étapes : étape 1 et étape 2.

CYBEVAL fournit au Client le nom et, lorsque cela est demandé, les informations nécessaires concernant chacun des membres de l'équipe d'audit dans un délai suffisant pour permettre à ce dernier de formuler une objection à la désignation d'un membre particulier de l'équipe d'audit et ainsi permettre à CYBEVAL de reformer l'équipe en réponse à toute objection valide.

Exigences supplémentaires propres à l'HDS

Des représentants de l'Agence du Numérique en Santé peuvent assister en tant qu'observateurs à la réalisation d'un audit.

6.6.1. Audit Etape 1

L'audit d'étape 1 a pour objectifs :

- De revoir les informations documentées du système de management du Client
- D'évaluer les conditions spécifiques au site du Client, échanger avec le personnel du Client, et évaluer le niveau de préparation du Client pour l'audit d'étape 2
- De procéder à une revue de l'état de l'organisme du Client et de sa compréhension des exigences de la norme, notamment en ce qui concerne l'identification des performances clés ou des aspects, des processus, des objectifs et du fonctionnement significatifs du système de management
- D'obtenir les informations nécessaires permettant de valider le périmètre de certification cible (sites, processus et équipements utilisés, niveaux de maîtrise, exigences légales et réglementaires)
- De déterminer si les audits internes et les revues de direction ont été planifiés et réalisés, et si le niveau de mise en œuvre du système de management atteste que l'organisme Client est prêt pour l'étape 2
- De procéder à une revue de l'affectation des ressources pour l'étape 2 et faire le point avec le Client sur les détails de l'étape 2
- De permettre la planification de l'étape 2 avec l'ensemble des points de compréhension précédents

Au cours de cet audit, les conclusions, ainsi que les potentielles non-conformités doivent être notifiées au Client.

Le délai entre l'audit d'étape 1 et l'audit d'étape 2 dépend des modifications éventuelles à apporter par CYBEVAL au plan d'audit, suite aux conclusions de l'audit d'étape 1, et également de la durée éventuellement nécessaire au Client pour modifier son système de management afin de corriger un certain nombre de points observés lors de l'étape 1 qui pourraient impacter l'audit d'étape 2.

Pour réaliser cet audit d'étape 1, afin de rester en cohérence avec la politique de confidentialité, CYBEVAL ne demande pas au Client de lui envoyer sa documentation par mail ou d'une quelconque autre manière.

Plusieurs modalités sont possibles :

- Présentation de la documentation via un outil de visioconférence si le niveau de confidentialité des documents le permet
- Accès à une plateforme maîtrisée par le Client, avec des droits d'accès limités dans le temps et les fonctionnalités (lecture seule, pas de possibilité de téléchargement)
- Consultation physique des documents par l'auditeur, chez le Client

Un rapport d'audit d'étape 1 est réalisé par CYBEVAL afin de documenter les résultats de cet audit.

6.6.2. Audit Étape 2

L'audit d'étape 2 a pour objectif d'évaluer la mise en œuvre et l'efficacité du système de management du Client.

Le Responsable d'audit établit un plan d'audit et le communique à CYBEVAL et au Client.

L'équipe d'audit analyse l'ensemble des informations et des preuves réunies au cours de l'étape 1 et de l'étape 2, afin de passer en revue les résultats et de déterminer les conclusions d'audit. L'équipe d'audit présente oralement ces conclusions lors d'une réunion de clôture. Le cas échéant, chaque non-conformité constatée est présentée et discutée lors de cette réunion de clôture afin que le Client et l'équipe d'audit puissent faire leurs commentaires. Le Responsable d'audit consolide ces constats dans un fichier de suivi des non-conformités.

6.6.3. Traitement des non-conformités, le cas échéant

L'organisme dispose de 2 semaines pour retourner au Responsable d'audit, ce fichier d'écarts renseigné de l'analyse des causes, des plans d'actions et délais de mise en œuvre proposés pour corriger les écarts.

Si les plans d'action proposés ne sont pas jugés pertinents par le Responsable d'audit ou par CYBEVAL, un nouveau délai de 2 semaines est accordé pour obtenir un nouveau plan d'actions.

Si l'organisme ne retourne pas au Responsable d'évaluation les non-conformités complétées des plans d'actions proposés pour corriger les écarts dans les délais impartis ou s'il ne répond pas favorablement à la demande de modifier son plan d'action, la procédure de certification continue en prenant en compte cet élément, ce qui pourra conduire à une décision défavorable.

Les écarts majeurs en statut non maîtrisé font obstacle à l'octroi de la certification. La certification de l'organisme est suspendue, ou non octroyée, tant qu'il n'a pas apporté des preuves d'implémentation des corrections et des actions correctives (Cf. § 6.8 Décision).

Les écarts mineurs sont levés lors des évaluations suivantes. Un écart mineur non traité conformément au plan d'action proposé par l'Organisme peut être classifié plus sévèrement lors de l'évaluation suivante.

L'équipe d'audit passe en revue les causes identifiées, les corrections et les actions correctives soumises par le Client pour déterminer si elles sont acceptables.

Si des non-conformités ne sont pas traitées ou ne sont pas traitées de manière à y remédier dans un délai de 6 mois, l'audit de certification initial est suspendu. Au-delà de 6 mois, si le Client souhaite maintenir sa demande de certification, CYBEVAL devra établir un nouveau contrat de certification afin de réaliser un nouvel audit initial mené en deux étapes.

6.7. Rapport d'audit

Le rapport d'audit est rédigé sous le pilotage du Responsable d'audit. Il demeure la propriété de CYBEVAL.

Exigences supplémentaires propres à l'HDS

Le rapport d'audit précise que les données de santé à caractère personnel et toutes autres données confidentielles ou sensibles auxquelles CYBEVAL a eu accès dans le cadre de l'audit ne peuvent être divulguées ou réutilisées par CYBEVAL, ni par le Client.

6.8. Décision de certification

6.8.1. Revue de certification

Au sein de CYBEVAL, une revue de certification est réalisée par une personne qualifiée n'ayant pas participé à l'audit afin de prendre la décision d'octroi, de refus de certification, d'extension ou de réduction du périmètre de la certification.

La revue de certification repose sur :

- L'ensemble du dossier du Client, de la demande de certification à la signature du contrat de certification
- Le rapport d'audit initial (étapes 1 & 2)
- La confirmation que les objectifs de l'audit ont été atteints
- La recommandation par l'équipe d'audit relative à la décision de délivrer ou non la certification, accompagnée de réserves éventuelles ou d'observations

Le processus de la revue de dossier vise à vérifier que :

- Les informations fournies sont suffisantes eu égard aux exigences et au périmètre de la certification
- Pour toutes les non-conformités majeures, l'équipe d'audit a examiné, accepté et vérifié les corrections et actions correctives
- Pour toute non-conformité mineure, l'équipe d'audit a examiné et accepté les corrections et actions correctives.

La revue aboutit à :

- Le cas échéant, la modification du rapport d'audit de certification. CYBEVAL adresse alors un courrier justifiant ces modifications ainsi que le rapport d'audit de certification modifié.
- Un avis de décision de certification qui peut être :
 1. L'octroi de la certification sans réserve si le rapport ne fait pas/plus apparaître de non-conformités majeures
 2. L'octroi de la certification sous réserve d'un audit supplémentaire dont le délai de réalisation est fixé par CYBEVAL afin de lever les réserves constatées lors de la revue de certification, et en cas de très nombreuses non-conformités mineures, et/ou de manque de maturité du système sans que cela ne mette en évidence des non-conformités majeures, et/ou de manque de confiance dans les éléments apportés par le Client
 3. Le refus d'octroyer de la certification si le rapport fait apparaître des non-conformités majeures, ou un ensemble de non-conformité mineures qui pourraient avoir un impact significatif sur la sécurité du SMSI. Un avenant au contrat de certification est alors établi par CYBEVAL ; il doit être signé par le Client afin de formaliser la décision du Client de choisir l'une ou l'autre des deux options ci-dessous. En cas de non signature par le Client, le processus de certification est suspendu ; au-delà de 6 mois à compter de la date de la réunion de clôture de l'audit de certification, si le Client souhaite maintenir sa demande de certification, CYBEVAL devra établir un nouveau contrat de certification afin de réaliser un nouvel audit initial mené en deux étapes.

Dans le cas de non-conformités majeures, un audit complémentaire sera réalisé 90 jours suivant la fin de l'audit dans le cas d'un audit initial afin de vérifier la mise en œuvre des corrections et actions correctives, avant la prise de décision de certification, et ce délai est ramené à 60 jours dans le cas d'un audit de surveillance ou de renouvellement.

Dans le cas d'un ensemble significatif de non-conformités mineures, un audit supplémentaire sera réalisé dans les 6 mois qui suivent la décision de certification afin de vérifier la mise en œuvre des corrections et actions correctives et de réaliser les investigations qui n'auraient pas pu être menées dans le cas d'un audit incomplet. Au-delà du délai de 6 mois, si l'audit supplémentaire n'a pas eu lieu ou n'est pas concluant, la certification est immédiatement

retirée. Le Client souhaitant obtenir à nouveau la certification devra émettre une nouvelle demande de certification.

Pour chaque audit complémentaire ou supplémentaire, CYBEVAL établit un devis afin d'apporter toute transparence au Client.

6.8.2. Décision de certification

Les décisions de certification sont prises par un personnel qualifié n'ayant pas participé à l'audit, et ne peuvent être prises par le Président de CYBEVAL.

A l'issue de la revue de décision, le Président de CYBEVAL signe, ou ne signe pas le certificat correspondant en suivant strictement l'avis rendu lors de la revue de certification.

Toutefois, si le Président de CYBEVAL constate une irrégularité manifeste dans les conclusions, et qu'il décide de pas suivre strictement l'avis rendu lors de la revue de certification, il doit immédiatement avertir le Comité d'Impartialité, de Stratégie et de Déontologie de CYBEVAL en justifiant sa décision.

Si nécessaire, une seconde revue de certification contradictoire réalisée par un autre personnel qualifié peut être réalisée.

Un registre de suivi des certificats et des décisions rendues permet de retracer l'ensemble de ces éléments.

Le Président de CYBEVAL peut également consulter ce Comité d'Impartialité, de Stratégie et de Déontologie dès qu'il souhaite recueillir son avis au cours du processus de certification ou lors de la prise de décision.

Suite à la revue de décision, CYBEVAL peut décider d'octroyer, d'octroyer sous réserve ou de refuser d'octroyer la certification.

- Lorsque CYBEVAL refuse d'octroyer la certification suite à la revue de décision, CYBEVAL documente les raisons de son refus et les indique clairement au Client candidat.
- Lorsque CYBEVAL octroie avec ou sans réserve la certification, il élabore un document de certification.

16

6.8.3. Document de certification

CYBEVAL émet un document de certification qui précise la portée de la certification.

La durée de validité de la certification est de trois ans à compter de la décision d'octroi de la certification. Elle est subordonnée au respect du programme d'audit pour un cycle complet de certification.

Dès émission du document de certification et envoi au Client, ce dernier doit appliquer strictement le document de politique générale d'utilisation de la marque CYBEVAL et des logos correspondants (CYB-POL-PUB-Utilisation-Marque).

6.9. Activités de certification post octroi de la certification

6.9.1. Activités de surveillance de la certification

Des audits de surveillance de la certification sont conduits sur site de manière à vérifier que le système de management est toujours conforme aux exigences certifiées.

Ces audits, qui ne sont pas forcément des audits du système complet portent notamment sur :

- Le respect des exigences des référentiels de certification
- La maîtrise opérationnelle continue du système
- Les éventuelles modifications apportées au système
- L'audit interne
- La revue de direction
- La revue des actions entreprises vis-à-vis des non-conformités identifiées au cours de l'audit précédent
- Le traitement des plaintes
- L'efficacité du système de management (indicateurs au regard des objectifs)

- L'avancement des actions planifiées visant à l'amélioration continue
- L'utilisation des marques et/ou toute autre référence à la certification
- Le respect des exigences stipulées dans le présent programme

Les activités de surveillance de CYBEVAL peuvent également porter sur :

- Les enquêtes de CYBEVAL adressées au Client sur des aspects liés à la certification
- La vérification des déclarations du Client liées à la certification
- La fourniture des documents et des enregistrements en réponse à la demande de CYBEVAL
- La revue du matériel promotionnel du Client, site Web
- Tout autre moyen de surveillance, adapté au cœur de métier du Client certifié

L'équipe d'audit mène l'audit comme un audit étape 2 (§6.6.2) et CYBEVAL applique le processus de certification tel que défini du § 6.5.3 au § 6.8.2.

Sauf modification de la portée de la certification, le document de certification reste inchangé.

6.9.2. Activités de renouvellement de la certification

Le Client doit demander le renouvellement de la certification au plus tard 3 mois avant la date de fin de validité de la certification.

Les activités de renouvellement de la certification suivent le processus de certification tel que défini du § 6.1 au § 6.8.3. Elles doivent être planifiées avant l'expiration du cycle de certification précédent.

L'audit de renouvellement consiste à effectuer un audit sur site (étape 2) afin de vérifier si le système de management de l'Organisme, dans sa totalité, est conforme, efficace et cohérent au regard de toutes les exigences de la norme applicable et du périmètre certifié.

Si des modifications significatives sont apportées au système de management de l'organisme Client au moment de cet audit, il peut être nécessaire de réaliser un audit en 2 étapes tel que prévu aux § 6.6.1 & 6.6.2.

Les audits de renouvellement sont des audits complets qui incluent les points spécifiés pour les audits de surveillance (Cf. § 6.9.1) et ainsi que la revue des rapports des audits de surveillance précédents, notamment pour s'assurer de la revue exhaustive de toutes les exigences applicables sur le cycle complet de certification, ce qui permet le cas échéant d'ajuster le plan d'audit en conséquence.

L'équipe d'audit mène l'audit comme un audit étape 2 (§6.6.2) et CYBEVAL applique le processus de certification tel que défini du § 6.6.3 au § 6.8.3.

Lorsque les activités de renouvellement de la certification sont terminées avec succès avant la date d'expiration de la certification existante, la date d'expiration de la nouvelle certification peut être basée sur la date d'expiration de la certification existante. La date de délivrance indiquée sur le nouveau document de certification doit correspondre à la date de la décision de renouvellement de la certification ou à une date ultérieure.

Si CYBEVAL n'a pas terminé l'audit de renouvellement de la certification ou s'il n'est pas en mesure de vérifier la mise en œuvre des corrections et actions correctives pour toute non-conformité majeure avant la date d'expiration de la certification, alors le renouvellement de la certification n'est pas recommandé et la validité de la certification n'est pas être prolongée. Le Client en est informé et les conséquences lui sont expliquées.

CYBEVAL peut rétablir une nouvelle certification dans les 6 mois qui suivent l'expiration de la certification, sous réserve que les activités de renouvellement de la certification non résolues soient terminées, à défaut un audit d'étape 2 doit au minimum être réalisé. La date d'entrée en vigueur figurant sur le nouveau document de certification doit correspondre à la date de la décision de renouvellement de la certification ou à une date ultérieure et la date d'expiration doit être basée sur le cycle de certification antérieur.

6.9.3. Audits particuliers

6.9.3.1. Extension du périmètre

En réponse à une demande d'extension du périmètre d'une certification déjà accordée, CYBEVAL entreprend une revue de la demande.

CYBEVAL établit un rapport d'extension dans lequel il analyse les impacts de la demande et détermine toute activité de certification nécessaire pour décider de la possibilité ou non d'accorder l'extension.

La demande d'extension fait donc l'objet d'un devis qui s'appuie sur ces différentes activités de certification. Une fois ce devis signé par le Client, CYBEVAL entreprend les activités qui mènent jusqu'à l'émission d'un nouveau document de certification tel que prévu au § 6.8.3.

6.9.3.2. Audits avec un préavis très court

CYBEVAL peut être amené à réaliser des audits de Clients certifiés avec un très court préavis ou inopinés afin d'instruire des plaintes ou suite à des modifications ou pour effectuer un suivi des Clients suspendus.

Dans ces cas précis :

- CYBEVAL doit décrire et porter préalablement à la connaissance des Clients certifiés les conditions dans lesquelles ces audits seront conduits
- CYBEVAL doit apporter un soin particulier à la désignation de l'équipe d'audit du fait de l'impossibilité pour le Client de formuler une objection relative aux membres de l'équipe d'audit

CYBEVAL établit d'un devis qui s'appuie sur les différentes activités de certification à réaliser, afin d'apporter toute transparence au Client. Une fois ce devis signé par le Client, CYBEVAL entreprend les activités prévues qui peuvent mener jusqu'à une nouvelle revue, une nouvelle décision de certification et jusqu'à l'émission d'un nouveau document de certification tels que prévus aux § 6.8.1, 6.8.2 & 6.8.3.

6.9.4. Cas de l'audit à distance

Lorsque des technologies d'information et de communication sont proposées pour les activités d'audit, la revue de la demande inclut la vérification que le client dispose de l'infrastructure nécessaire pour soutenir l'utilisation des TIC.

Dans le cas d'un audit à distance, une analyse de risque est réalisée sur les éléments suivants :

1. Infrastructure disponible de CYBEVAL et du client
2. Secteur d'activité du client
3. Type d'audit considéré
4. Compétences des personnes du client qui participent à l'audit à distance
5. Retour d'expérience et performances du client sur le sujet de l'audit à distance
6. Domaine d'application de la certification

Des preuves documentées sont conservées dans le plan d'audit et le rapport d'audit.

6.9.5. Suspension, retrait ou réduction du périmètre de la certification

CYBEVAL procède à la suspension de la certification dans les cas cités dans le présent règlement (Cf. §6) et dans les cas suivants :

- Le système de management a constamment ou gravement manqué au respect des exigences de la certification
- Le Client certifié n'a pas permis la réalisation des audits de surveillance ou de renouvellement de la certification selon la périodicité requise
- Le contexte du Client le conduit à demander une suspension (changement de structure juridique, cessation d'activité, déménagement, modification majeure...)
- Le Client n'a pas corrigé les écarts notifiés lors des activités de certification dans les délais impartis

CYBEVAL prononce la suspension de certification conformément au § 6.8. La certification est alors considérée comme provisoirement invalidée.

Sauf cas de force majeure (accident sur un site, plan social, liquidation judiciaire), la suspension ne doit pas dépasser 6 mois.

Pendant la période de suspension, le Client doit strictement respecter le document de politique générale d'utilisation de la marque CYBEVAL et des logos correspondants (CYB-POL-PUB-Utilisation-Marque) et par conséquent, cesser immédiatement tout usage de la marque de certification et toute promotion de la certification.

Quel que soit le motif et le contexte de la suspension, CYBEVAL réalise un audit supplémentaire conformément au § 6.8 afin de pouvoir établir une revue avant de prendre la décision de levée d'une suspension de certification. CYBEVAL établit alors un devis afin d'apporter toute transparence au Client.

CYBEVAL rétablit la certification suspendue si le problème qui a abouti à la suspension a été résolu dans les délais impartis. Dans le cas contraire, CYBEVAL procède au retrait de la certification, ou alors à la réduction du périmètre, afin d'exclure les éléments ne satisfaisant plus aux exigences, dans la limite des critères de la norme de certification.

En cas de retrait de la certification, le Client doit strictement respecter le document de politique générale d'utilisation de la marque CYBEVAL et des logos correspondants (CYB-POL-PUB-Utilisation-Marque) et par conséquent, cesser immédiatement et définitivement tout usage de la marque de certification et toute promotion de la certification. Le Client retourner immédiatement à CYBEVAL le document de certification.

Les décisions de certification, réduction ou retrait sont prises conformément au § 6.8.

7. Modalités d'échange d'informations entre CYBEVAL et l'autorité compétence, dans le cas d'une certification HDS

7.1. Rapport de suspension HDS

CYBEVAL doit communiquer en français ou en anglais à l'autorité compétente toute décision de suspension de certification d'un hébergeur de données de santé.

Les informations ci-dessous relatives à l'hébergeur de données de santé dont la certification a été suspendue doivent être communiquées :

- Désignation ou raison sociale de l'hébergeur de données de santé pour lequel la certification a été suspendue
- Numéro d'identifiant du certificat suspendu
- Date de suspension du certificat
- Raisons de la suspension de la certification HDS

L'envoi des informations sera réalisé par voie électronique en complétant le modèle proposé en Annexe I (Échanges d'informations entre CYBEVAL et l'autorité compétente).

7.2. Rapport de retrait HDS

CYBEVAL doit communiquer en français ou en anglais à l'autorité compétente toute décision de retrait de certification d'un hébergeur de données de santé.

Les informations ci-dessous relatives à l'hébergeur de données de santé dont la certification a été retirée doivent être communiquées :

- Désignation ou raison sociale de l'hébergeur de données de santé pour lequel la certification a été retirée
- Numéro d'identifiant du certificat retiré
- Date de retrait du certificat

- Raisons du retrait de la certification HDS

L'envoi des informations doit être réalisé par voie électronique en complétant le modèle de l'Annexe I.

7.3. Répertoire Clients HDS

CYBEVAL doit fournir, a minima une fois par mois, un rapport des certifications valides, suspendues et retirées, à l'autorité compétente. Ce rapport, en français ou en anglais, doit contenir les données suivantes pour chaque hébergeur de données de santé :

- Désignation ou raison sociale de l'hébergeur de données de santé
- Numéro d'identifiant du certificat
- Périmètre de la certification (liste des activités)
- Adresse du site certifié et dans le cas d'une certification multi sites, indiquer l'adresse du siège social, ainsi que celles de tous les sites rattachés
- État de la certification (valide, suspendue ou retirée)
- Date de la certification
- URL ou contact afin de permettre la vérification du certificat auprès de l'OC
- URL de la page de déclaration des transferts des DSCP conformément à l'exigence 31 du référentiel de certification

L'envoi du répertoire doit être réalisé par voie électronique en complétant le modèle de l'Annexe I.

7.4. Rapport annuel HDS

Chaque année, CYBEVAL doit fournir à l'autorité compétente un rapport annuel en français ou en anglais comprenant :

- Une synthèse anonymisée des certifications HDS, des audits réalisés et des non conformités relevées
- Une synthèse des difficultés rencontrées lors de la certification des hébergeurs et des éventuelles propositions de modifications à apporter aux référentiels de certification et d'accréditation
- Des indicateurs sur la procédure de certification HDS, tels que :
 1. Le nombre d'hébergeurs de données de santé en cours de certification
 2. Le nombre d'hébergeurs de données de santé ayant échoué à la certification
 3. Le nombre de renouvellements de certification
 4. La durée moyenne des audits

L'envoi du rapport annuel doit être réalisé par voie électronique entre le 1er et le 31 janvier de l'année suivante, en complétant le modèle proposé en Annexe I.

8. Appels

Une décision de certification peut faire l'objet d'un recours, nommé « appel ».

Le Client doit formuler par écrit son appel et l'adresser à CYBEVAL dans les plus brefs délais et au maximum dans les 3 mois qui suivent une décision de certification.

CYBEVAL accuse réception de cet appel et l'enregistre.

L'appel est ensuite soumis à une personne qualifiée n'ayant pas participé à l'audit & à la revue de certification qui ont conduit à la prise de décision de certification.

Cette personne examine le bien-fondé de l'appel, réalise une nouvelle revue de certification conformément au § 6.8.1 et émet un avis au regard de l'appel prononcé par le Client.

Au regard de l'avis rendu lors de la seconde revue de certification, le Président de CYBEVAL suit strictement cette décision par défaut. Si le Président de CYBEVAL ne suit pas cet avis, il doit immédiatement avertir le Comité d'Impartialité, de Stratégie et de Déontologie de CYBEVAL en justifiant sa décision.

Suite à la décision de certification, CYBEVAL informe le Client du résultat du traitement de l'appel.

Le Client peut alors renouveler son appel s'il dispose de nouveaux éléments venant compléter son 1er appel.

CYBEVAL doit accuser réception de cet appel.

CYBEVAL enregistre ensuite l'appel et transmet toutes les informations au Comité d'Impartialité, de Stratégie et de Déontologie de CYBEVAL. Le Comité examine le bien fondé du 2nd appel en consultant l'ensemble du dossier (1er et 2nd appel comprenant les éléments nouveaux apportés par le Client). Le Comité émet un avis au regard du 2nd appel prononcé par le Client. CYBEVAL informe le Client de l'avis rendu par le Comité d'Impartialité, de Stratégie et de Déontologie de CYBEVAL.

En aucun cas, l'appel n'est suspensif de l'application de la décision de certification initialement prononcée qui fait l'objet de l'appel.

9. Plaintes

Une plainte est une réclamation émise par toute personne ou organisation contre un Client certifié de CYBEVAL ou contre CYBEVAL lui-même. Elle peut par exemple concerner un dysfonctionnement, un mécontentement, le non-respect des exigences contractuelles ou du présent programme de certification.

CYBEVAL accuse réception de cette plainte et l'enregistre.

CYBEVAL examine l'objet de la plainte.

Si la plainte concerne un Client certifié par CYBEVAL, CYBEVAL peut décider de réaliser un audit avec un préavis très court conformément au § 6.9.3.2.

Si la plainte concerne CYBEVAL, CYBEVAL l'analyse pour déterminer si elle est recevable et le cas échéant, analyse les causes du problème et y remédier dans les plus brefs délais.

CYBEVAL informe le Client du résultat de l'analyse de la plainte et le cas échéant, des actions permettant d'y remédier et de toute autre action vis-à-vis du plaignant.

21

10. Enregistrements relatifs au Client

CYBEVAL conserve l'ensemble des enregistrements relatifs à l'audit et aux activités de certification de tous ses Clients, tels que :

- La demande de certification
- Les rapports d'audit
- Le contrat de certification
- Le programme d'audit et les plan d'audit
- La justification de la méthodologie utilisée pour l'échantillonnage des sites, le cas échéant
- La justification pour le calcul du temps d'audit par auditeur
- Le traitement des non-conformités
- Les revues de décisions de certification et décisions de certification
- Les documents de certification
- L'enregistrement des plaintes et des appels, leur analyse et leur traitement

CYBEVAL conserve les enregistrements au sein de partitions chiffrées, accessibles aux seuls auditeurs ayant réalisés les audits correspondants, en respectant les principes du besoin d'en connaître et des moindres privilèges.

Les échanges d'information avec les Clients se font en utilisant des containers chiffrés. CYBEVAL utilise la solution ZED ! par défaut, mais peut s'adapter aux différentes exigences des Clients. La seule contrainte imposée par CYBEVAL est que les échanges soient chiffrés par un procédé reconnu comme robuste par la communauté cyber et à l'état de l'art de la sécurité, si possible, ou assumé par le Client.

Les enregistrements sont conservés depuis le précédent cycle de certification et pendant la durée du cycle en cours, soit une durée maximum de 6 ans, par enregistrement, sauf évènement imprévu dans le processus de certification.

-----FIN DU DOCUMENT-----

ANNEXE I : Échanges d'informations entre CYBEVAL et l'autorité compétente

Rapport Annuel HDS					
Nom de l'organisme de certification : CYBEVAL			Date : jj/mm/aaaa		
Synthèse des certifications HDS, des audits réalisés et des non-conformités relevées					
XXX					
Synthèse des difficultés rencontrées lors de la certification HDS					
XXX					
Propositions d'amélioration de la certification HDS					
XXX					
Indicateurs sur la procédure de certification HDS					
Nombre de certification délivrées	Nombre d'échecs	Nombre de renouvellements	Nombre de suspensions	Nombre de retraits	Nombre de certifications transférées
XXX	XXX	XXX	XXX	XXX	XXX

Répertoire Clients HDS							
Nom de l'organisme de certification : CYBEVAL					Date : jj/mm/aaaa		
Identifiant du certificat	Nom hébergeur de données de santé	Périmètre de la certification (liste des activités)	URL de la page de déclaration des risques de transfert des DSCP conformément à l'exigence 31	Adresse des sites	Date de certification	Etat du certificat	URL de publication du certificat ou contact CYBEVAL
	XXX		XXX	XXX	XXX	XXX	XXX