PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 23 septembre 2021

N° **2389/ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CCN-MQ_v5.0**

MANUEL QUALITE

Application **:** Dès son approbation.

Diffusion **:** Publique.

Le sous-directeur « Expertise » de l'Agence nationale de la sécurité des systèmes d'information

Renaud LABELLE
[ORIGINAL SIGNE]

SÉCURITÉ Ti CERTIFICATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

SUIVI DES MODIFICATIONS

Version	Date	Modifications
1.0	01/12/2003	Création
2.0	08/03/2016	Refonte du document
3.0	27/05/2019	Mise en conformité avec la norme EN ISO/IEC 17065
3.1	28/08/2019	Précisions dans l'annexe C pour faciliter la lecture Mise à jour du calcul des priorités de l'analyse de risque
3.2	29/1/2020	Suite audit interne : Le « comté des utilisateurs » devient « groupe des utilisateurs » Ajout de dispositions de préservation de l'impartialité Mise en cohérence du §7.8 avec le §9.1 de CER-P-01 Ajout de précisions dans la matrice de conformité EN ISO/IEC 17065
4.0	26/01/2021	Ajout de la publication des rapports de surveillance et gestion de la date de validité des certificats. Correction d'erreurs de typographie et ajouts de précisions Suppression du paragraphe « utilisation des certificats et usage de la marque » pour mettre son contenu dans le chapitre traitant de ce sujet Ajout d'un paragraphe traitant des mesures dérogatoires Prise en compte de la nouvelle charte graphique
5.0	23/09/2021	Précisions sur les organismes apparentés Correction pour indiquer que les CESTI sont des sous-traitants de l'ANSSI et non des organismes apparentés Précision concernant la délégation de signature du DG

En application du décret n° 2002-535 du 18 avril 2002 modifié, le présent manuel a été soumis, lors de sa création, au comité directeur de la certification qui a donné un avis favorable.

Ce document est également soumis pour avis lors de chaque modification majeure. Les évolutions mineures, quant à elles, ne sont pas soumises au comité directeur de la certification.

Le présent manuel est disponible en ligne sur le site institutionnel de l'ANSSI (www.ssi.gouv.fr).

TABLE DES MATIERES

Chapitre 1
Le Manuel Qualité

1.1. Objet du manuel

Le manuel qualité a pour objet de présenter les méthodes et les procédures de l'organisme de certification (Centre de certification national) en vue d'assurer et de maintenir la qualité et la continuité de ses prestations en matière de certification de la sécurité des produits et des systèmes des technologies de l'information, des profils de protection et des sites indifféremment appelés « objets à certifier » ou « objets à évaluer » dans la suite de ce document.

Le manuel qualité constitue la référence pour :

- toute entité tierce faisant appel aux prestations de certification de l'ANSSI ;
- toute personne ou entité de l'ANSSI exerçant une fonction relative à l'activité de certification, quant à son rôle et à ses responsabilités ;
- toute personne nouvellement recrutée au centre de certification pour l'informer de la politique de l'ANSSI et faciliter son intégration ;
- l'évaluation réciproque entre l'ANSSI et les autres organismes, étrangers notamment, en vue d'une reconnaissance mutuelle.

Note : pour les besoins du présent document, les termes « organisme de certification » et « centre de certification » seront indifféremment utilisés.

1.2. Élaboration, mise à jour et diffusion

Ce présent manuel est élaboré et maintenu à jour par le responsable qualité ou son suppléant, vérifié par le Chef du centre de certification puis validé et signé par l'organe de gouvernance[1]. Il est soumis à l'avis du Comité directeur de la certification.

Le responsable qualité ou son suppléant assure la diffusion du manuel qualité : les règles de diffusion du manuel sont les mêmes que celles des autres documents du système qualité.

Toutes les versions sont conservées sous forme électronique. Toutefois, seule la version française originale sous forme papier constitue la version de référence.

[1] L'organe de gouvernance est composé de tous les membres de la hiérarchie de l'ANSSI externes au centre de certification. Pour plus de détails, voir paragraphe « Interfaces de l'organisme de certification ».

Chapitre 2
Le schéma de certification

2.1. Contexte réglementaire

Le décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information précise le contexte réglementaire et l'organisation nécessaire à la conduite d'une évaluation par une tierce partie et à son contrôle, conduisant à la délivrance de certificats.

Ces règles sont mises en œuvre dans un schéma de certification tierce partie.

2.2. Le comité directeur de la certification

L'article 15 du décret 2002-535 modifié indique que le Comité directeur de la certification en sécurité des technologies de l'information a pour mission :

- de formuler des avis ou des propositions sur la politique de certification, sur les règles et normes utilisées pour les procédures d'évaluation et de certification et sur les guides techniques mis à la disposition du public ;
- d'émettre un avis sur la délivrance et le retrait des agréments aux centres d'évaluation ;
- d'examiner, à des fins de conciliation, tout litige relatif aux procédures d'évaluation organisées par le décret 2002-535 modifié qui lui est soumis par les parties ;
- d'émettre un avis sur les accords de reconnaissance mutuelle conclus avec des organismes étrangers.

Le comité directeur se réunit au moins une fois par an. Il est présidé par le secrétaire général de la défense et de la sécurité nationale ou son représentant.

2.3. Le Groupe des utilisateurs

Le Groupe des utilisateurs du schéma français de certification est constitué de différents types d'acteurs, principalement les commanditaires des évaluations et les développeurs des produits certifiés, mais aussi des donneurs d'ordre qui s'appuient sur la certification afin de spécifier les exigences de sécurité des produits qu'ils utilisent ou recommandent. Les membres de ce groupe sont invités à se réunir à l'initiative du centre de certification, leur présence reste cependant facultative. Cette rencontre est un lieu d'échange d'informations qui peuvent être partagées librement entre tous les membres compte tenu de leur caractère général.

Le Groupe des utilisateurs a pour objectifs, entre autres, de permettre à l'ANSSI :

- de présenter les évolutions des règles et normes ;
- d'identifier les besoins et attentes des utilisateurs du schéma ;
- d'échanger à propos des perspectives d'évolution.

De plus, certains membres du Groupe des utilisateurs peuvent être consultés en fonction de leurs domaines d'activité et leurs intérêts pour étayer un document en cours de finalisation. Les propositions retournées par les membres peuvent ou non être retenues, la décision finale revenant au centre de certification.

2.4. Le centre de certification

2.4.1. Statut

L'ANSSI, créée par le décret n° 2009-834 du 7 juillet 2009, instruit les certifications (voir article 4).

L'ANSSI est rattachée au secrétaire général de la défense et de la sécurité nationale, lui-même rattaché au Premier ministre. A ce titre, le centre de certification bénéficie des assurances, voire de provisions pour couvrir les responsabilités résultant de ses opérations. La stabilité financière du centre de certification est également garantie puisque ses ressources sont assurées par l'État.

Le centre de certification ne commercialise pas les résultats de ses travaux et n'effectue pas de conseil aux commanditaires ou aux développeurs.

Le centre de certification est rattaché à la division produits et services de sécurité de la sous-direction expertise de l'ANSSI.

2.4.2. Dispositions de préservation de l'impartialité

Le dispositif de préservation de l'impartialité du centre de certification repose sur l'application de politiques et de principes appliqués à la fois au centre de certification, à son personnel, aux laboratoires d'évaluation et aux personnes externes afin de garantir une totale indépendance de la décision de certification.

Politiques et principes du centre de certification :

- les travaux du centre de certification sont réalisés dans le cadre du décret 2002-535 du 18 avril 2002 modifié et non au travers de contrats commerciaux ;
- le centre de certification est une subdivision d'une administration de l'État ;
- les ressources financières sont assurées par l'État. Les services proposés par le centre de certifications sont libres du paiement de tout droit ;
- le centre de certification ainsi que l'ANSSI ne sont ni des concepteurs, ni des fabricants, ni des installateurs, ni des responsables de l'entretien de produits certifiés ;
- le centre de certification ne délivre aucune information confidentielle durant les réunions regroupant l'ensemble des membres du Groupe des utilisateurs ;
- le centre de certification ne fait pas appel à du personnel externe au centre pour assurer les activités de certification ;
- le centre de certification n'accepte pas de mettre en commun son personnel avec une entité susceptible de porter atteinte à son impartialité ;
- le centre de certification ne fournit pas de prestation de conseil ou de formation visant à l'obtention ou au maintien d'une certification ;
- le centre de certification ne fournit pas de prestation de conseil pour la conception, la fabrication, l'installation et la distribution d'un produit en cours de certification ou déjà certifié ;
- le centre de certification répond à des critères qui permettent de garantir à ses clients, une totale impartialité tant dans l'exécution des travaux que dans la décision finale de certification ou non.

Politiques et principes appliqués au personnel de l'ANSSI intervenant dans un projet de certification :

- chaque personne de l'ANSSI intervenant sur les projets est un agent de la fonction publique[2] habilité au minimum au niveau Secret. Il s'engage entre autres, à respecter le secret le plus absolu sur les informations sensibles qui lui sont confiées dans l'exercice de ses fonctions et à déclarer tout fait qui pourrait remettre en cause son impartialité ;

[2] Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.

- chaque certificateur intervenant sur des projets de certification déclare à sa hiérarchie tout fait antérieur, présent ou à venir qui pourrait remettre en cause son indépendance lorsqu'un projet lui est proposé ;
- chaque personne du centre de certification doit refuser toute sollicitation, promesse, don, présent ou avantage quelconque, soit directement, soit par personne interposée qui pourrait nuire à son indépendance de jugement ;
- les recommandations techniques publiées par les experts techniques de l'ANSSI ne mettent pas en cause les fondements de l'impartialité puisqu'elles s'adressent à l'ensemble de la communauté et non à un développeur particulier ;
- un membre du centre de certification qui a fourni des conseils ou qui a été employé du plaignant ne peut pas participer à la revue, ni approuver la solution apportée à la plainte et ce, durant les deux années qui suivent la fin d'activités de conseil ou de l'emploi chez ce plaignant ;
- la décision permettant d'apporter une solution à une plainte doit être prise, revue et approuvée par un membre du centre de certification non engagé dans les activités liées à la plainte. Par contre, un membre lié à la plainte peut intervenir dans l'élaboration de la réponse.

Politiques et principes appliqués aux laboratoires d'évaluation :

- le laboratoire s'engage à ne pas faire intervenir du personnel qui aurait au préalable promulgué des conseils au développeur pour le produit évalué (rédaction de la cible de sécurité ou la spécification cryptographique par exemple) ;
- le laboratoire s'assure de l'indépendance et de l'impartialité de son personnel vis-à-vis des commanditaires ou des développeurs ;
- les laboratoires d'évaluation peuvent être amenés à donner des conseils et recommandations à leurs clients. Toutefois, un cloisonnement, vérifié lors des audits COFRAC, est assuré entre les acteurs intervenant pour donner du conseil et ceux réalisant les travaux d'évaluation.

Politiques et principes appliqués aux personnes externes :

- si un audit du centre de certification est réalisé par des intervenants externes (société tierce qui a contractualisé avec l'ANSSI, ou membres du COFRAC), les auditeurs techniques sont habilités au moins au niveau Secret et signent un engagement de confidentialité lors de chaque nouvel audit ;
- les auditeurs des centres de certification étrangers n'ont accès qu'aux informations préalablement autorisées par les commanditaires des produits évalués.

Ces intervenants extérieurs n'accèdent aux informations qu'en présence d'une personne du centre de certification et ne sont pas autorisés à les sortir à l'extérieur du centre de certification.

Conformément à l'article 16 du décret 2002-535 modifié, la désignation des membres composant le comité directeur permet d'assurer une large représentation des parties ayant un intérêt significatif notamment lors du traitement des litiges. La politique appliquée est la suivante :

- les membres du comité directeur de la certification sont tenus à la confidentialité et à l'impartialité au travers du « règlement intérieur du comité directeur de la certification » signé par les parties ;
- les membres du comité directeur ont accès à toutes les informations nécessaires à l'exercice de leurs missions.

Politiques liées aux organismes apparentés :

- le *webmaster* est employé par le SGDSN, il est donc soumis aux mêmes règles que les membres du centre de certification et est habilité au minimum au niveau Secret. Il s'engage, entre autres, à respecter le secret le plus absolu sur les informations sensibles qui lui sont confiées dans l'exercice de ses fonctions ;

- le personnel de ménage intervient dans les bureaux durant les heures ouvrées et en présence au moins d'une personne de l'ANSSI. La sélection de la société de ménage et de son personnel fait l'objet du plus grand soin par le SGDSN dans la mesure où les locaux dans lesquels ces personnes interviennent se trouvent dans une zone protégée au sens de [IGI 1300] ;
- le bailleur des locaux dans lesquels sont exercées les activités du centre de certification n'a que très rarement des relations avec les membres du centre de certification;
- les services généraux n'ont également que très rarement des relations avec les membres du centre de certification;
- les gendarmes qui assurent les missions d'accueil et de sécurité, de par leur statut, ne présentent que peu de risque ;
- les membres de l'Opérateur des Systèmes d'Information Interministériels Classifiés (OSIIC) sont soumis aux mêmes règles que les membres du centre de certification et sont habilités au moins au niveau Secret. A ce titre, cet opérateur est en charge d'assurer la sécurité des informations du SGDSN et donc celles liées aux travaux effectués par l'organisme de certification. Cet opérateur a également la charge d'assurer la sauvegarde, la conservation et la destruction des documents numériques produits par l'organisme de certification.

2.4.3. Missions de l'organisme de certification

L'organisme de certification a pour principales missions :

- de mettre en œuvre la stratégie de certification définie par l'ANSSI ;
- d'assurer l'instruction des dossiers d'évaluation ainsi que la mise en œuvre des processus de maintenance et de surveillance des certificats délivrés ;
- d'assurer l'instruction des demandes d'agréments des candidats comme centres d'évaluation nationaux ;
- d'effectuer des audits d'agrément des centres d'évaluation pour s'assurer de leurs niveaux de compétence pour leur domaine considéré ;
- de représenter l'ANSSI dans les instances nationales et internationales traitant des sujets de certification ;
- de définir des référentiels d'évaluation de sécurité adaptés à des catégories de produits en liaison avec les utilisateurs du schéma national ;
- d'assurer la promotion de l'utilisation du schéma national d'évaluation et de certification.

2.4.4. Organisation

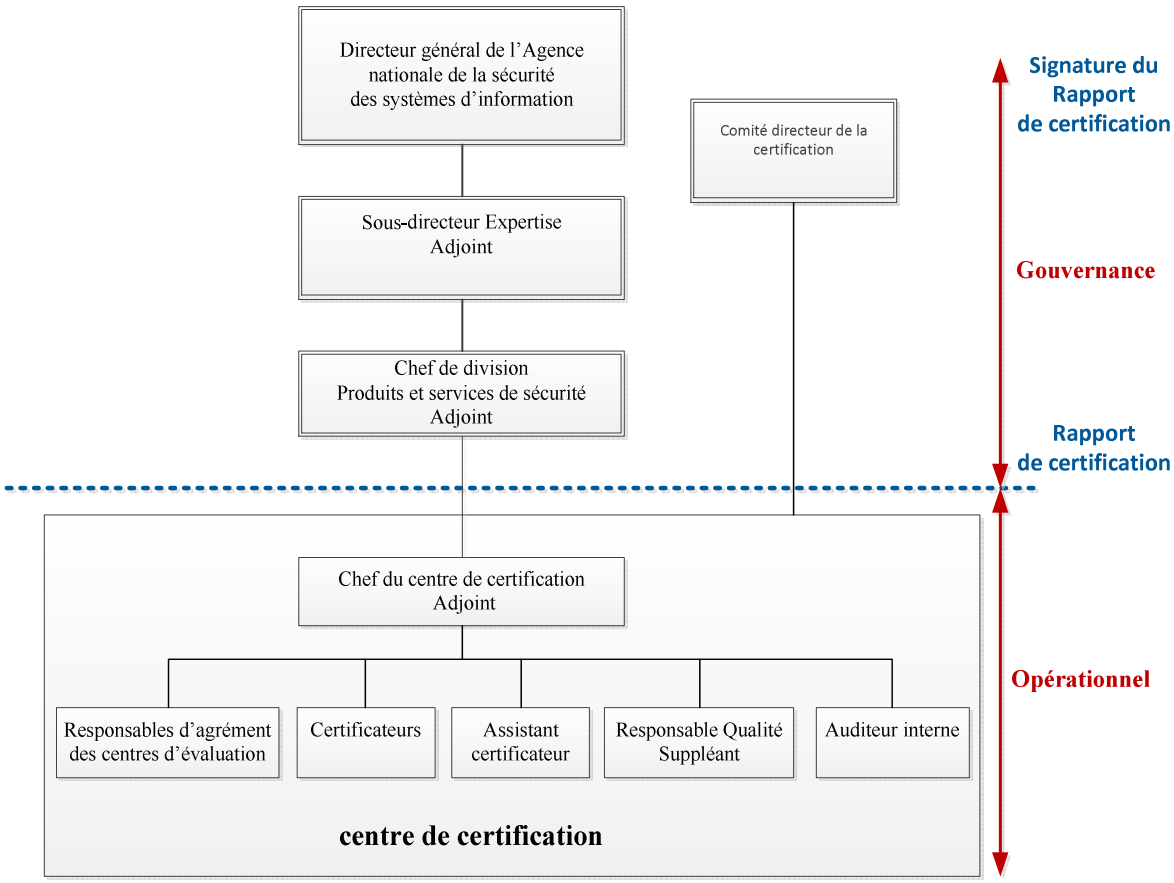


Figure 1 – Organigramme fonctionnel du centre de certification

Les responsabilités pour l'activité de certification sont réparties de la façon suivante :

- **le directeur général de l'Agence nationale de la sécurité des systèmes d'information** pour délivrer les certificats et les agréments des centres d'évaluation. Le directeur préside également le comité directeur de la certification. Par note de délégation, le directeur peut déléguer certaines de ses prérogatives ;
- **le sous-directeur Expertise** a autorité sur le centre de certification mais n'intervient pas dans la décision de certification ;
- **le chef de division « Produits et Services de Sécurité » ou son adjoint** a autorité sur le centre de certification mais n'intervient pas dans la décision de certification. Dans le processus de certification, le chef de division assure la cohérence rédactionnelle de l'ensemble des rapports de certification, de surveillance et de maintenance ;
- **le chef du centre de certification ou son adjoint** a pour fonction la gestion et le contrôle opérationnels du centre de certification. Il définit les besoins en ressources, participe au recrutement de son personnel et s'assure de sa compétence pour les fonctions occupées en tenant à jour un dossier relatif à l'expérience et à la formation du personnel. Il est responsable de la définition de la procédure d'agrément des centres d'évaluation. Il s'assure de la reconnaissance des certificats à l'extérieur des frontières et entretient des relations avec ses homologues étrangers. Il participe à la gestion des critères d'évaluation et de certification. Il est responsable de la proposition de certification (positive ou négative) qu'il transmet pour signature au directeur général ;
- **les responsables d'agrément des centres d'évaluation** sont chargés de s'assurer du respect, par les centres d'évaluation, des normes et standards en vigueur ainsi que des critères d'agrément. Ils s'assurent également de la compétence des évaluateurs, du bon niveau d'équipement et du

plan de développement des centres d'évaluation. Ils instruisent les dossiers d'agrément des CESTI ;

- **le responsable qualité** est chargé de la mise en place, du maintien et de l'amélioration continue du système qualité. Il assure également la formation qualité du personnel du centre de certification ;
- **les certificateurs** sont chargés de suivre les évaluations afin de vérifier le respect des règles, et procédures de certification et, d'appliquer les procédures qualité en vigueur. Ils interviennent entre autres, dans les travaux d'évaluation et dans la décision finale de certification ;
- Certains certificateurs, qualifiés pour cette activité, sont amenés également à réaliser des audits internes planifiés et gérés par le responsable qualité. Cependant, il convient de noter que la plupart des audits internes sont effectués par des entités extérieures à l'ANSSI ;
- **l'assistant certificateur** est chargé d'assurer le suivi administratif des documents du centre de certification et d'assister le chef de centre et les certificateurs dans l'enregistrement, la rédaction et la logistique liés à leurs fonctions.

2.4.5. Interfaces de l'organisme de certification

L'organisme de certification ou le centre de certification national a pour interlocuteurs internes, notamment :

- l'organe de gouvernance qui est composé de tous les membres de la hiérarchie de l'ANSSI externes au centre de certification. Leurs rôles sont notamment les suivants :
    - pour le directeur général[3] :
        - délivrer les rapports de certification, surveillance et maintenance, tant Critères communs que Certification de sécurité de premier niveau,
        - délivrer les agréments aux laboratoires d'évaluation après avoir recueilli l'avis du comité directeur de la certification,
        - retirer les agréments des laboratoires d'évaluation après avis du comité directeur de la certification,
        - signer les notes d'application utilisées pour les procédures d'évaluation et de certification,
        - signer les accords de reconnaissance mutuelle conclus avec les organismes étrangers,
        - signer une partie des documents du processus « qualité »,
        - solliciter le comité directeur de la certification,
        - convoquer le comité directeur à chaque fois que nécessaire ;
    - pour le sous-directeur « Expertise » (SDE) :
        - présider les réunions de revue de direction de la qualité,
        - signer certains documents liés au processus « qualité »,
        - par note de délégation du directeur général, gérer les relations avec le comité directeur de la certification ;
    - pour le chef de division « Produits et Services de Sécurité » (PSS) :
        - assurer la cohérence de qualité de tous les rapports de certification,
        - valider certains documents liés au processus « qualité » ;
    - les différents laboratoires internes à l'ANSSI qui peuvent être sollicités par les certificateurs pour rendre des avis sur des sujets techniques particuliers. Dans tous les cas, les

[3] le directeur général peut être amené à déléguer sa signature, notamment au sous-directeur « Expertise » ou au chef de bureau du centre de certification.

certificateurs sont totalement libres de les solliciter, d'apprécier et de tenir compte ou non des avis rendus ;

- les « Ressources humaines » qui interviennent sur tous les sujets qui traitent de la gestion du personnel du centre de certification (recrutement, gestion des entretiens individuels, suivi des formations, etc.) ;
- les « Affaires juridiques » qui sont sollicitées par l'organisme de certification pour tous les sujets nécessitant des avis juridiques (*Memorandum Of Understanding, Non Disclosure Agreement*, etc.) ;
- les donneurs d'ordre[4] internes, notamment le « Bureau Qualification et Agrément » (BQA) de l'ANSSI qui a pour missions de qualifier et agréer les produits et prestataires de service de confiance. Ces donneurs d'ordre internes n'interviennent dans le processus de certification que pour valider les problématiques de sécurité décrites dans les cibles de sécurité pour s'assurer qu'elles répondent aux besoins de l'Etat.

Les interlocuteurs <u>externes</u> du centre de certification sont :

- les laboratoires d'évaluation (CESTI[5]) agréés par l'organisme de certification qui sont en charge de procéder à l'évaluation des produits conformément aux Critères communs ou à la Certification de sécurité de premier niveau. Ces laboratoires sont en charge de remettre des rapports d'évaluation à l'organisme de certification qui se charge de les valider. Ces laboratoires sont considérés comme des sous-traitants du centre de certification et doivent se conformer aux différents documents sur lesquels ils sont amenés à s'engager ; les commanditaires et/ou développeurs qui sont les demandeurs pour que leurs produits entrent dans un processus de certification ;
- les donneurs d'ordre externes qui sont en charge de valider que les cibles de sécurité soumises avec les dossiers d'évaluation répondent à leurs besoins propres ;
- les schémas homologues d'autres organisations ou d'autres pays dans le but d'harmoniser les pratiques et référentiels internationaux ainsi que de procéder aux audits CCRA et SOG_IS (revue par les pairs) ;
- les organismes apparentés conformément à la doctrine « CERT-REF-04 » éditée par le COFRAC.

2.4.6. <u>Personnel du centre de certification</u>

La direction de l'organisme de certification fixe les exigences en termes de recrutement et de suivi des compétences de son personnel.

On distingue notamment quatre niveaux de qualification :

- le niveau « théorique » : le certificateur acquiert les connaissances de base soit suite à des actions de formations externes ou internes, soit dans le cadre d'auto-formations ;
- le niveau « connaissance » : le certificateur est encadré par un tuteur pour chacun des projets afin de mettre en pratique ses connaissances acquises. A ce stade, il n'est toujours pas autorisé à suivre seul des projets d'évaluation ou à mener des groupes de travail. Il réalise chacune de ces missions sous le contrôle d'un tuteur-projet qui est chargé de statuer sur la bonne réalisation de sa mission ;
- le niveau « autonome » : le certificateur est autorisé à suivre seul les projets d'évaluation. Des formations complémentaires lui sont dispensées pour lui permettre de consolider ses compétences ;
- le niveau « expert » : le certificateur est un référent dans son domaine de compétence.

[4] Le terme « Donneur d'ordre » utilisé dans les bases de données des projets est inapproprié car il ne traduit en rien une quelconque relation de subordination. Cette information sert uniquement aux statistiques du centre pour identifier l'usage des produits certifiés.

[5] Centre d'Evaluation de la Sécurité des Technologies de l'Information.

Dans tous les cas, le certificateur ne pourra en aucun cas prendre en charge un projet pouvant remettre en cause son impartialité. À titre d'exemple, son impartialité pourrait être remise en cause si le projet qui lui était proposé émanait de son employeur précédent, s'il détenait des parts significatives dans le capital de la société à l'origine du projet, s'il avait fourni avant sa venue au Centre de certification des conseils pour le produit concerné, ou s'il l'avait développé. Le Centre de certification n'affecte donc pas, durant les 12 mois suivant son embauche, un certificateur à un projet qui serait lié à son employeur précédent.

Le centre de certification n'emploie pas de personnel temporaire pour les activités de certification.

Chapitre 3
Système qualité

3.1. Politique qualité

3.1.1. Objectif

Le centre de certification évolue dans un milieu où confiance, rigueur et continuité prennent tout leur sens. De par l'étendue géographique de ses activités et la dispersion culturelle de ses clients, le centre de certification doit, au travers de son système qualité, donner la plus grande confiance dans les travaux qu'il mène afin d'assurer la reconnaissance de ses certificats, notamment en raison du cadre international dans lequel il s'inscrit.

Ses objectifs sont axés sur la reconnaissance des certificats émis, à savoir :

- une reconnaissance nationale, pour établir la confiance dans les travaux de certification qu'il mène auprès de toutes les parties concernées ;
- une reconnaissance internationale, afin d'entrer dans le cadre des accords de reconnaissance mutuelle qui l'engagent.

3.1.2. Exigences

Pour obtenir et conserver durablement cette reconnaissance, le centre de certification doit prouver qu'il répond aux exigences de la norme EN ISO/IEC 17065 notamment :

- la traçabilité : toute évaluation doit être reproductible et l'ensemble des éléments de preuves lié à la délivrance du certificat doit être identifié et conservé ;
- la continuité : le centre de certification doit pouvoir assurer ses missions quels que soient les changements internes (organisation, personnel) ;
- l'homogénéité : les certificats doivent rendre compte d'un niveau d'assurance comparable, quel que soit le personnel chargé du suivi et quel que soit le centre d'évaluation qui a mené l'évaluation ;
- la confidentialité : le centre de certification doit assurer le respect de la confidentialité des informations sensibles qui lui sont confiées ou qu'il élabore dans le cadre de la certification ;
- l'impartialité : le centre de certification doit régulièrement s'assurer que ses membres opèrent en toute impartialité.

Le centre de certification doit se conformer aux exigences des accords CCRA et SOG-IS et au référentiel EN ISO/IEC 17065.

3.2. Système qualité

Le système qualité se veut être conforme aux exigences des accords CCRA et SOG-IS pour la reconnaissance internationale des certificats, à la norme EN ISO/IEC 17065 et respecte les textes réglementaires qui instituent les missions du centre de certification.

L'organisme de certification s'engage à :

- publier et tenir à jour les règles et exigences relatives au schéma d'évaluation et de certification ;
- publier et tenir à jour la liste des certificats et des centres d'évaluation agréés ;
- s'assurer des compétences des centres d'évaluation qui procèdent à l'évaluation ;
- n'agréer que des laboratoires accrédités selon la norme EN ISO/IEC 17025 pour les travaux Critères Communs entrant dans le cadre du décret 2002-535 modifié ;

- travailler avec du personnel compétent et qualifié dans son domaine.

3.3. Planification de la qualité

3.3.1. Audits internes

Des audits périodiques du système qualité sont organisés par le responsable qualité ou son suppléant et conduits par des auditeurs qualifiés et indépendants des fonctions auditées conformément au plan d'audits établi en début d'année.

Le responsable qualité ou son suppléant planifient et gèrent les audits de manière à ce que les exigences de la norme EN ISO/IEC 17065 soient auditées au moins une fois par an et veillent dans le cas où l'audit serait segmenté à ce qu'il soit achevé dans un délai de 12 mois.

3.3.2. Analyse de risques

L'organisme de certification prend en compte, à chaque fois que nécessaire, les risques susceptibles de nuire à ses activités et à son impartialité.

L'analyse des risques qui en découle ainsi que les actions prises pour maîtriser voire éliminer les risques identifiés est revue annuellement et approuvée dans le cadre des revues de direction de la qualité. L'analyse des risques fait également l'objet d'une approbation par le comité directeur de la certification.

Le processus adopté pour effectuer l'analyse de risques consiste à recenser les risques bruts suivant la perception des acteurs concernés (personnel de l'organisme de certification, l'organe de gouvernance, clients, etc.) puis à évaluer pour chacun des risques, sa gravité et sa probabilité de survenir ceci sur une échelle de 1 à 4.

GRAVITE		
Échelle	**Caractérisation**	**Description**
1	Non significatif	Dérive ou évènement mineur ne remettant pas en cause l'atteinte des objectifs
2	Peu grave	Risque occasionnel remettant en cause l'atteinte des objectifs
3	Grave	Risque avéré pouvant perturber le fonctionnement global du processus
4	Très grave	Risque mettant en péril le fonctionnement d'un ou plusieurs processus

PROBABILITE		
Échelle	**Caractérisation**	**Description**
1	Peu probable / Rare	Une fois par an au plus
2	Probable / Occasionnelle	Une fois par mois au plus
3	Très probable / Fréquent	une fois par semaine au plus
4	Extrêmement probable / Très Fréquent	Une ou plusieurs fois par jour

Le résultat de ces cotations permet d'identifier le niveau de risque brut.

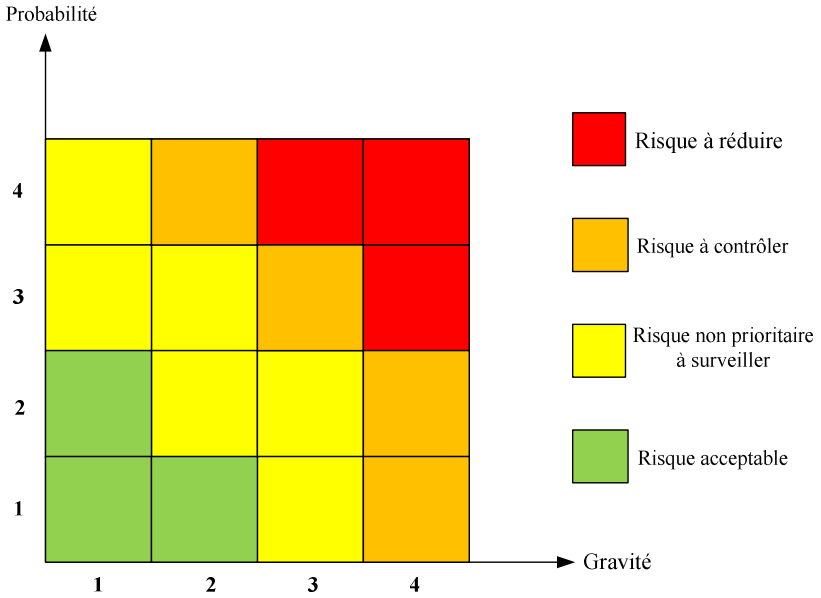


Figure 2 : niveaux de risques

Le niveau de risque brut associé à la cotation des éléments de maitrise permet de déterminer le niveau de priorité pour mener chacune des actions permettant de réduire ou maitriser le risque. Certains risques sont considérés comme acceptables, ils ne nécessitent alors pas d'action de maîtrise de réduction du risque.

Les risques sont ensuite catégorisés de la façon suivante :

RISQUES		
Échelle	**Caractérisation**	**Description**
1	« acceptables »	Risques résiduels connus mais ne nécessitent pas de mesures particulières
2	« non prioritaires à surveiller »	Risques qui doivent faire l'objet de mesures de prévention pour minimiser leurs éventuelles apparitions
3	« à contrôler »	Risques qui doivent faire l'objet d'actions de renforcement pour assurer leur maîtrise
4	« à réduire »	Risques qui doivent faire l'objet d'actions et de mesures de prévention pour les faire passer au minimum, dans la catégorie « à contrôler »

L'efficacité des éléments permettant de maîtriser le risque est appréciée de la manière suivante :

EFFICACITE		
Échelle	**Caractérisation**	**Description**
1	« Inefficace »	Le ou les éléments de maîtrise sont inefficaces et ne permettent pas de couvrir le risque identifié
2	« Minimale »	Le ou les éléments de maîtrise sont peu efficaces et ne couvrent pas suffisamment le risque identifié
3	« Moyenne »	Le ou les éléments de maîtrise sont partiels et ne couvrent pas intégralement le risque identifié
4	« Totale »	Le ou les éléments de maîtrise sont efficaces et couvrent totalement le risque identifié

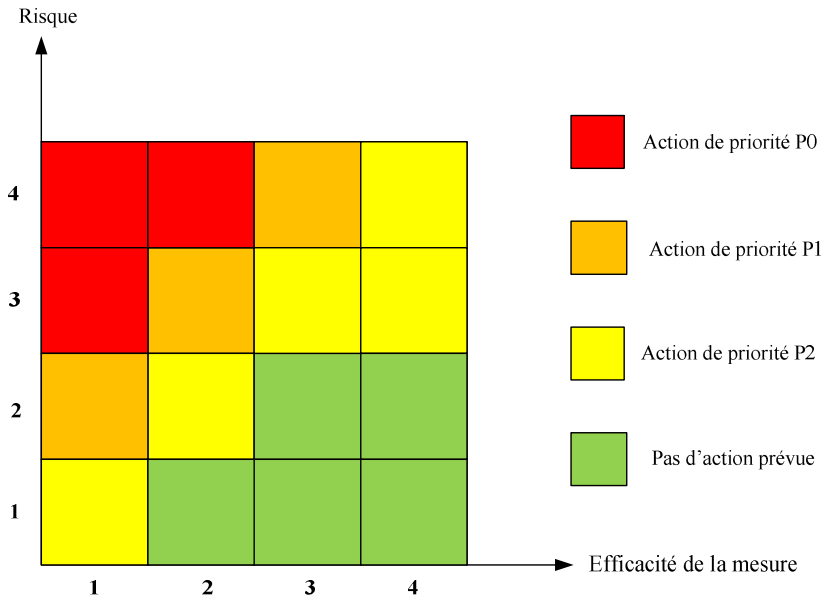


Figure 3 : Niveaux de priorité

Le niveau de priorité de mise en place des actions est déterminé à l'aide des critères suivants :

- mesure de maîtrise du risque inexistante ou non mise en œuvre : action prioritaire qui doit être prise en compte rapidement et planifiée (P0) ;
- mesure inadaptée ou partielle : mesure qui doit être prise en compte une fois les actions P0 prises en compte et planifiées (P1) ;
- mesure adaptée et mise en œuvre mais quelques défaillances possibles : mesure à prendre en compte une fois les actions de P0 et P1 prises en compte et planifiées (P2) ;
- mesure parfaitement adaptée : pas d'action prévue.

Le centre de certification réalise une revue interne :

- semestrielle des actions de priorité P0 et P1 ;
- annuelle toutes les actions.

3.3.3. Revue de direction

Lors de la réunion annuelle de revue de direction de la qualité organisée par le responsable qualité ou son suppléant, la gouvernance du centre de certification s'assure que le système de management de la qualité demeure pertinent, adéquat et efficace, qu'il est maintenu à jour et disponible à l'ensemble des intervenants du centre de certification. A cette occasion, il est notamment fait part à l'organe de gouvernance des résultats des audits internes et externes, des nouveaux points de l'analyse des risques, des appels et plaintes des clients.

Durant l'année, d'autres revues peuvent être organisées à la demande de la direction ou de l'organisme de certification.

3.4. Architecture documentaire

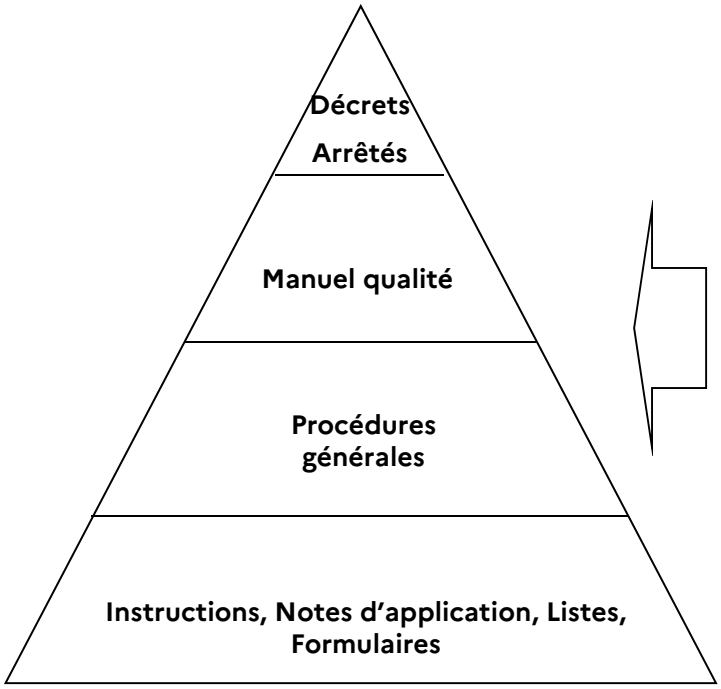
Le centre de certification dispose d'une collection documentaire couvrant l'ensemble de l'activité de certification et répondant aux exigences de la norme EN ISO/IEC 17065.

Au moins une fois par an, une revue documentaire du système de management de la qualité est effectuée afin de s'assurer notamment pour les documents externes mis à disposition des membres du centre de certification et des autres utilisateurs du schéma correspondent bien à leurs dernières versions.

3.4.1. Structure documentaire

La structure de cette collection documentaire est la suivante :

Organisation



Référentiels :
CCRA
SOG-IS
EN ISO/IEC 17065,
EN ISO/IEC 17025

Critères d'évaluation :
Critères Communs
ITSEC
EN ISO/IEC 15408
Certification Sécurité de Premier Niveau (CSPN)

	Entrées	Sorties	
Application	Demandes de certification Rapports d'évaluation Enquêtes de satisfaction à remplir	Lettres d'enregistrement Revues des rapports d'évaluation Rapports de certification et certificats Rapports d'audits d'agrément Décisions d'agrément Enquêtes de satisfaction remplie par le commanditaire / développeur	Enregistrements relatifs à la certification et à l'agrément. Enquête de satisfaction
	Présentations pour « revue de direction de la qualité » Programmes d'audits internes et externes Plans d'audits	Comptes rendus de la revue de direction de la qualité Rapports d'audits internes et externes Fiches d'anomalies	Enregistrements relatifs au système qualité

3.4.2. Maîtrise de la documentation

Le centre de certification possède des règles d'élaboration et de maîtrise de la documentation liées à son activité de certification[6].

Le responsable qualité ou son suppléant tiennent à jour la liste de tous ces documents qualité établis par le centre de certification.

[6] Procédure ANSSI-CC-DOC-P-01 « Elaboration et mise à jour de la documentation du système qualité du centre de certification ».

3.4.3. Enregistrements liés à la certification

Il existe trois types d'enregistrements démontrant que toutes les procédures et instructions relatives à l'activité de certification ont bien été appliquées :

- les enregistrements sur support papier conservés au centre de certification ou dans un local d'archives ;
- les enregistrements stockés sur support informatique ;
- les échantillons remis par les commanditaires, conservés au centre de certification.

La durée de conservation des enregistrements est de dix ans au minimum.

Chapitre 4
Modalités de la certification

4.1. Accès et traitement non discriminatoires

Tous les développeurs et commanditaires d'objets à évaluer ont accès aux services du centre de certification de l'ANSSI et ce, sans aucun caractère discriminant de quelque nature qu'il soit.

Le centre de certification de l'ANSSI veille à l'égalité de traitement entre les différents objets à certifier et limite ses exigences, son évaluation, sa revue, sa décision et sa surveillance aux éléments spécifiquement en rapport avec la portée de la certification « Critères communs » ou celle de la « Certification de sécurité de premier niveau ».

L'attribution de la certification n'est subordonnée qu'au respect des règles de fonctionnement du schéma et à la satisfaction des critères d'évaluation.

4.2. Documents de référence

L'ensemble des documents publics relatifs à la certification est disponible ou référencé sur le site Internet de l'ANSSI.

Ces documents sont notamment :

- les textes réglementaires relatifs à la certification de la sécurité des produits et des systèmes des technologies de l'information ;
- les documents de fonctionnement (procédures, instructions, formulaires et notes d'application) du centre de certification ;
- le formulaire « Demande d'évaluation » tant pour les Critères communs que pour la Certification de sécurité de premier niveau ;
- les critères d'évaluation.

4.3. Critères d'évaluation

Les critères et méthodologies d'évaluation utilisés sont approuvés par le Comité directeur de la certification.

Ces critères d'évaluation sont susceptibles d'évoluer ou d'être complétés par des guides techniques en fonction de la technologie considérée ou de contextes particuliers.

4.4. Modification des exigences de certification[7]

Les exigences relatives à la certification peuvent être amenées à évoluer dans le temps, elles sont communiquées aux intéressés.

Ces évolutions peuvent être :

- des évolutions des critères d'évaluation provenant des instances normatives internationales ou nationales : elles sont directement disponibles sur les sites Internet de ces instances de normalisation ;

7 Procédure ANSSI-CC-MOD-P-01 « Modification des exigences de certification ».

- des adaptations d'exigences pour un domaine particulier : si elles sont obligatoires ou dépendantes du schéma national, elles sont notifiées par une note d'application du schéma qui précise son délai d'application ;
- des évolutions de pratiques du schéma de certification : en cas d'évolutions majeures, elles nécessitent l'avis du Comité directeur de la certification.

Chapitre 5
Demande de certification

5.1. Contenu du dossier d'évaluation

Le commanditaire, après avoir sélectionné un centre d'évaluation agréé par l'organisme de certification, demande l'ouverture d'un dossier de certification « Critères communs » ou de « Certification de sécurité de premier niveau » au centre de certification par le biais d'un dossier d'évaluation disponible sur le site de l'ANSSI.

Le dossier d'évaluation comprend notamment :

- les conditions générales de la certification ;
- l'engagement du commanditaire et du centre d'évaluation à respecter les règles de certification ;
- une description de l'objet à évaluer (incluant sa cible de sécurité) ;
- le programme de travail prévisionnel élaboré par le centre d'évaluation lors de la préparation de l'évaluation « Critères communs » ;
- le planning prévisionnel de livraison des fournitures délivrées par le commanditaire ou développeur au laboratoire d'évaluation et à l'ANSSI.

5.2. Enregistrement de la demande

Sur la base du dossier d'évaluation, le centre de certification :

- vérifie que la signature de la demande vaut engagement de la société ;
- procède à une revue documentaire approfondie, notamment de la cible de sécurité et du programme de travail prévisionnel. Si le centre de certification estime que les objectifs de sécurité ne sont pas définis de manière pertinente au regard des normes, prescriptions techniques ou règles de bonne pratique applicables au moment où commence l'évaluation, il notifie au commanditaire qu'il ne pourra pas en l'état du dossier procéder à la certification envisagée ;
- vérifie la pertinence des charges prévues pour l'évaluation ;
- vérifie que la portée d'agrément du laboratoire lui permet d'évaluer le produit considéré ;
- indique le nom du certificateur désigné pour assurer le suivi de l'évaluation.

Par défaut, l'existence même de l'évaluation est considérée comme confidentielle, elle ne fait donc l'objet d'aucune publicité par le centre de certification, sauf demande du commanditaire, approuvée par l'organisme de certification.

Chapitre 6
Évaluation

6.1. Les centres d'évaluation

6.1.1. Rôles et responsabilités

Les centres d'évaluation réalisent les évaluations : ils constituent une tierce partie indépendante des développeurs de produits et des commanditaires et sont considérés comme des sous-traitants du centre de certification.

Les centres d'évaluation sont agréés par l'ANSSI après avis du comité directeur de la certification et, à ce titre, sont tenus de respecter toutes les règles du schéma[8]. Le centre de certification intervient dans cette démarche d'agrément notamment au travers d'audits techniques pour s'assurer de la capacité du centre d'évaluation à mener à bien ses missions dans son ou ses domaine(s) de compétence revendiquée.

Les centres d'évaluation sont constitués d'équipes d'experts et de responsables, intégrés le plus souvent dans un organisme à vocation plus large. Toutefois, les critères d'agrément imposent un cloisonnement vis-à-vis des autres activités de l'organisme auquel le centre d'évaluation est rattaché.

6.1.2. Procédure d'agrément

Les critères d'agrément Critères communs comprennent, entre autres, l'accréditation des laboratoires d'évaluation par le COFRAC (COmité FRançais d'ACcréditation) selon la norme EN ISO/IEC 17025 lorsqu'ils effectuent des évaluations Critères communs. Des guides techniques d'accréditation, élaborés par le COFRAC, précisent le domaine particulier de l'évaluation de la sécurité des technologies de l'information.

L'agrément impose des exigences qui permettent de s'assurer de la maîtrise par le laboratoire de certaines techniques particulières ainsi que de sa capacité à traiter des informations sensibles.

L'agrément d'un centre d'évaluation est ensuite accompagné d'une procédure de suivi qui permet de s'assurer de la pérennité du respect des exigences d'agrément.

6.1.3. Réalisation des travaux d'évaluation par le centre d'évaluation

Le centre d'évaluation mène les travaux d'évaluation conformément aux critères d'évaluation choisis. Ces travaux sont suivis par le certificateur désigné.

Le commanditaire de l'évaluation est responsable de la livraison des fournitures nécessaires à l'évaluation. La liste exacte des fournitures à livrer au centre d'évaluation et au centre de certification dépend des critères d'évaluation choisis.

Le centre d'évaluation analyse l'objet à évaluer et sa documentation afin de vérifier que les exigences spécifiées dans les critères d'évaluation sont satisfaites. Certains critères d'évaluation peuvent exiger une visite des sites de développement ou de production de l'objet à évaluer.

6.1.4. Le Rapport Technique d'Évaluation

Le centre d'évaluation rédige un rapport technique d'évaluation (RTE) qui décrit les travaux effectués lors de l'évaluation et expose les résultats obtenus. Ce RTE est transmis :

- au centre de certification et au commanditaire dans le cadre des évaluations CC ;
- uniquement au centre de certification qui donne son accord avant transmission au commanditaire dans le cadre des évaluations CSPN.

[8] Procédures ANSSI-CC-AGR-P-01 « Agrément des centres d'évaluation » et ANSSI-CSPN-AGR-P-01 « Agrément des centres d'évaluation en vue de la certification de sécurité de premier niveau ».

Le RTE est soumis pour validation au certificateur en charge du projet.

Lorsque toutes les tâches d'évaluation ont été menées par le centre d'évaluation et que l'ensemble des travaux a été validé par le centre de certification, l'évaluation est considérée comme terminée.

Le RTE contient une conclusion statuant sur la Réussite ou l'Echec de l'évaluation.

Le RTE contient des données sensibles couvertes par le secret industriel et commercial. Sa diffusion est contrôlée : les clauses de confidentialité imposées par l'ANSSI peuvent être précisées contractuellement entre le centre d'évaluation et le commanditaire lors de la phase de préparation de l'évaluation.

Chapitre 7
Certification

7.1. Préambule

La certification est un processus global qui permet, par un ensemble d'actions, de s'assurer que l'évaluation s'est déroulée avec la compétence et l'impartialité requises[9].

7.2. Rapport de certification

Après validation d'un RTE positionné à « Réussite », le certificateur rédige un rapport de certification qui propose la certification. Le rapport de certification est, avec la cible de sécurité, le seul document produit dans le cadre de l'évaluation qu'un acheteur potentiel est normalement amené à consulter.

Le rapport de certification décrit fidèlement l'objet évalué, l'environnement d'évaluation considéré et recommande éventuellement la mise en œuvre de mesures nécessaires à une utilisation sûre de l'objet certifié.

Le rapport de certification constitue, avec la cible de sécurité éventuellement expurgée de certaines informations propriété du commanditaire/développeur, la documentation minimale à fournir pour la reconnaissance internationale du certificat.

7.3. Décision de certification

Dans le cas où le centre de certification décide de certifier l'objet évalué, il transmet les projets de rapport de certification et de certificat, au directeur général de l'Agence de la sécurité des systèmes d'information. Le directeur général de l'Agence de la sécurité des systèmes d'information qui en a reçu délégation par le Premier ministre signe le certificat et le rapport de certification.

7.4. Maîtrise des enregistrements

Toutes les fournitures et documents électroniques délivrés par les commanditaires et les laboratoires d'évaluation, ainsi que ceux produits par l'organisme de certification, sont systématiquement enregistrés, stockés et conservés sur les réseaux homologués du Secrétariat général de la défense et de la sureté nationale.

Les originaux signés des documents papier spécifiques aux processus de certification sont conservés par l'organisme de certification dans un lieu sécurisé au minimum durant dix ans.

7.5. Publication du certificat

Si le commanditaire en fait la demande, le rapport de certification et la cible de sécurité correspondante sont publiés sur le site Internet de l'ANSSI (.

Passée leur date de validité, les documents publiés sur le site de l'ANSSI sont déplacés dans une liste de produits certifiés archivés si le commanditaire n'a pas, entre temps, obtenu une extension de sa durée via le processus de surveillance de produit.

[9] Procédures ANSSI-CC-CER-P-01 « Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection » et ANSSI-CSPN-CER-P-01 « Certification de sécurité de premier niveau ».

7.6. Indice de satisfaction

Aux termes de la certification, le commanditaire et/ou le développeur a la possibilité de remplir un questionnaire de satisfaction, qui lui est soumis par le centre de certification, et qui vise à l'amélioration des services rendus.

7.7. Suspension, retrait du certificat

Le centre de certification de l'ANSSI peut être amené à suspendre, voire retirer un certificat pour diverses raisons techniques (découverte d'une vulnérabilité, fin de période de validité du certificat, suite à une surveillance, etc.) ou de communication incomplète, voire frauduleuse.

Chapitre 8
Utilisation du certificat et de la marque

Le centre de certification engage contractuellement les parties impliquées à respecter scrupuleusement l'usage des certificats et de la marque.

8.1. Règles de communication

Le commanditaire et, le cas échéant, les développeurs, ont le devoir d'informer fidèlement et honnêtement les utilisateurs de produits certifiés et l'ANSSI. En particulier, le commanditaire a le devoir de :

- fournir le rapport de certification et la cible de sécurité chaque fois qu'un donneur d'ordre en fait la demande. Les copies de documents de certification à autrui doivent être conformes en tout point aux originaux délivrés. Les destinataires des copies peuvent vérifier leur exactitude auprès de l'organisme de certification de l'ANSSI ;
- ne pas faire d'annonce trompeuse sur le produit en laissant entendre par exemple que le produit est certifié alors qu'il n'est qu'en cours d'évaluation ou qu'un produit est certifié alors qu'il ne s'agit pas de la version exacte certifiée ;
- informer ses utilisateurs si une vulnérabilité susceptible d'impacter une ou des versions déjà déployées est découverte au cours de l'évaluation ;
- signifier systématiquement et sans délais à l'ANSSI (CERT-FR[10]) toute vulnérabilité avec son analyse d'impact associée afin de permettre son instruction pour qu'elle soit corrigée ou contournée et permettre l'établissement d'un message vers les utilisateurs des produits certifiés.

8.2. Règles d'utilisation de la marque

La marque « certification sécurité TI » reproduite ci-dessous est la marque de certification française de la sécurité offerte par les technologies de l'information accordée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Cette marque est déposée à l'Institut national de la propriété industrielle sous le numéro 023 175 658.

Elle identifie les produits et systèmes certifiés dans le cadre du décret 2002-535 modifié. Son usage est défini dans une procédure spécifique[11].

L'usage des logotypes des accords CCRA et SOG-IS pour la reconnaissance internationale des certificats est également décrit dans une procédure spécifique[12].

[10] *Computer Emergency Response Team* ; Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatique.

[11] Procédures ANSSI-CC-MAR-P-01 « Règles d'utilisation de la marque « Certification Sécurité TI ».

[12] Procédures ANSSI-CC-MAR-P-02 « Utilisation des logotypes CCRA et SOG-IS ».

Chapitre 9
Surveillance et continuité de l'assurance

Le certificat atteste, au moment de sa signature, de la conformité d'un produit ou d'un système aux exigences listées dans sa cible de sécurité. Pour prolonger la confiance dans cette conformité ou faciliter la prise en compte des évolutions d'un produit précédemment certifié, le centre de certification propose des programmes de surveillance et de continuité de l'assurance.

9.1. Surveillance[13]

Le centre de certification propose un programme de surveillance des certificats qui consiste à effectuer un suivi du produit pour maintenir la confiance dans le certificat émis.

Ce suivi, laissé à l'initiative du commanditaire, consiste à réaliser régulièrement (la période est définie par le commanditaire) des travaux de mise à jour de l'analyse de vulnérabilité du produit certifié et à effectuer d'éventuels tests de pénétration. Le centre de certification peut publier les résultats de la surveillance des produits sur le site de l'ANSSI à la demande des commanditaires. Ces publications conditionnent les dates de validité des certificats des produits et l'archivage des certificats.

9.2. Continuité de l'assurance[14]

Un certificat s'applique uniquement à la version et à la configuration évaluée du produit. Or, il est probable que le produit, son environnement de développement ou de production soient amenés à évoluer.

Le commanditaire peut alors demander un avis sur les nouvelles versions du produit dans le cadre de la « continuité de l'assurance ». Le rapport produit par l'organisme de certification dans le cadre de ce processus ne se substitue pas à une réévaluation ou à une surveillance de la nouvelle version du produit qui seule permet de maintenir le niveau de confiance dans le temps.

[13] Procédure ANSSI-CC-SUR-P-01 « Surveillance des produits certifiés ».

[14] Procédures ANSSI-CC-MAI-P-01 « Continuité de l'assurance » et ANSSI-CSPN-MAI-P-01 « Maintien de la confiance : continuité de l'assurance ».

Chapitre 10
Confidentialité des informations traitées

10.1. Accès aux locaux

Le centre de certification dispose du même niveau de sécurité que celui appliqué au Secrétariat général de la défense et de la sécurité nationale ; il bénéficie donc des mesures de protection et de sécurité élevées de ce dernier.

10.2. Confidentialité de l'information

L'ensemble des personnes impliqué dans les dossiers de certification est habilité. Le personnel de l'organisme de certification s'engage par écrit à respecter la confidentialité des informations échangées dans le cadre du schéma d'évaluation et de certification de la sécurité des technologies de l'information.

Le personnel de l'organisme de certification traite également avec le même soin de confidentialité toute information relative à un client obtenue par d'autres sources.

Toutefois, en cas de procédure de justice, l'organisme de certification peut être amené à fournir des informations confidentielles sans que l'aval du client ait été demandé. Dans la mesure du possible, le client sera informé de cette mise à disposition.

10.3. Accès aux informations

Les informations échangées pendant l'évaluation présentent le plus souvent un caractère sensible. Le centre de certification traite ces informations selon des règles de protection adéquates[15].

Dans le cadre de l'agrément, le centre de certification s'assure que les centres d'évaluation appliquent des règles similaires pour la gestion des informations sensibles qu'ils traitent.

Le personnel de l'organisme de certification a accès à l'ensemble des documents clients. D'autres intervenants peuvent également avoir accès à certains documents « client » concernant le produit en cours d'évaluation ou certifié. Il s'agit notamment :

- des experts techniques de l'ANSSI ayant signé les engagements de confidentialité de la certification ;
- du personnel de BQA si une demande de qualification du produit a été demandée par le commanditaire ou le développeur ;
- des membres de la hiérarchie impliqués dans la revue des rapports techniques et certificats ;
- du directeur général de l'ANSSI ;
- de la DSI pour assurer les enregistrements et sauvegardes des dossiers.

10.4. Enregistrement et durée de conservation

Tous les documents et fournitures utilisés durant l'évaluation sont enregistrés et conservés avec des exigences fortes de confidentialité (voir [SECU-P-01]).

[15] Procédure ANSSI-CC-SECU-P-01 « Gestion de la confidentialité au centre de certification » disponible sur demande.

Chapitre 11
Anomalies, réclamations

11.1. Auprès du centre de certification

11.1.1. Enregistrement et traitement

Le centre de certification conserve un enregistrement des anomalies en matière de certification afin de prendre les mesures qui s'imposent et agir sur la cause et les facteurs précurseurs ou prédisposant[16].

11.1.2. Litiges

Le Comité directeur de la certification examine, à des fins de conciliation, tout litige relatif aux procédures d'évaluation organisées par le décret 2002-535 modifié qui lui est soumis par les parties.

11.2. Auprès des commanditaires

Le centre de certification exige pour les objets certifiés que le commanditaire l'avise de toute plainte portée à sa connaissance à propos de la conformité de l'objet aux exigences listées dans la cible de sécurité correspondante.

[16] Procédure ANSSI-CC-ANO-P-01 « Traitement des anomalies ».

Chapitre 12
Mesures dérogatoires

Dans le cas où le centre de certification serait amené, dans des circonstances exceptionnelles, à déroger aux règles préconisées dans son processus qualité, le centre de certification ne pourra prendre aucune mesure dérogatoire sans avoir évalué au préalable les risques encourus par une telle décision, notamment ceux ayant attrait à l'impartialité. Dans ce dernier cas, les risques éventuels seront tracés dans l'analyse de risques (voir §3.3.2).

Annexe A
Documents de référence

Textes réglementaires

Certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, version consolidée au 27 décembre 2010.
Arrêté du 28 février 2003 portant nomination au comité directeur de la certification en sécurité des technologies de l'information.
Arrêté du 1er avril 2014 portant délégation de signature (secrétariat général de la défense et de la sécurité nationale).

SGDSN/ANSSI

Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »	
Décret n° 2014-845 du 28 juillet 2014 modifiant le décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information	
IGI 1300	Instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 13 novembre 2020 sur la protection du secret de la défense nationale

Textes relatifs à l'accréditation

EN ISO/IEC 17065	Exigences pour les organismes certifiant les produits, les procédés et les services.
CPS-Ref-02	Critères d'accréditation concernant les organismes de certification procédant à la certification de produits et de services, révision 01, novembre 2002.
EN ISO/IEC 17025	Exigences générales concernant la compétence des laboratoires d'étalonnage et d'essais.

Accords de reconnaissance

CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security.
SOG-IS	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Management Committee.

Critères d'évaluation

ITSEC	Critères d'évaluation de la sécurité des systèmes informatiques (ITSEC).
ITSEM	Manuel d'évaluation de la sécurité des technologies de l'information (ITSEM).
JIL	ITSEC Joint Interpretation Library (ITSEC JIL).
CC	Common Criteria for Information Technology Security Evaluation : Part 1 : Introduction and general model ; Part 2 : Security functional requirements ; Part 3 : Security assurance requirements.
CEM	Common Methodology for Information Technology Security Evaluation: Part 1 : Introduction and general model ; Part 2 : Evaluation Methodology.
CSPN	Certification de Sécurité de Premier Niveau

Annexe B
Définitions et acronymes

Définitions

Centre de certification national	Bureau de l'ANSSI institué par le décret 2001-693 et les arrêtés 15-02-2002-1 et 15-02-2002-2, dont les membres instruisent les dossiers de certification.
Centre d'évaluation	Organisme accrédité selon le référentiel EN ISO/IEC 17025 et agréé par le centre de certification pour conduire des évaluations de la sécurité en vue d'une certification dans le cadre du décret 2002-535 modifié.
Certificateur	Personnel du centre de certification chargé de l'instruction des dossiers de certification.
Certificat	Il atteste que l'exemplaire d'un produit ou d'un système répond aux exigences de sécurité spécifiées dans sa cible de sécurité. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8 du décret 2002-535 modifié).
Certification	Action de fournir l'assurance de conformité à des normes et autres documents normatifs.
Commanditaire	Personne ou organisme qui demande l'évaluation en vue de la certification.
Comité directeur de la certification	Comité directeur de la certification en sécurité des technologies de l'information défini par le Chapitre III du décret 2002-535 modifié.
Cible de sécurité	Ensemble d'exigences de sécurité constituant le référentiel de certification pour les évaluations ITSEC, Critères communs, Certification de sécurité de premier niveau.
Organisme de certification	Autre dénomination du centre de certification national.

Acronymes et abréviations

SGDSN	Secrétariat général de la défense et de la sureté nationale
ANSSI	Agence nationale de la sécurité des systèmes d'information
SOG-IS	Senior Officer Group Information Security
RTE	Rapport technique d'évaluation
CC	Critères communs
CSPN	Certification de sécurité de premier niveau

Annexe C
Couverture de la norme EN ISO/IEC 17065

Paragraphe de la norme	Documents
4 - Exigences générales	
4.1 - Domaine juridique et contractuel	
4.1.1 - Responsabilité juridique	MQ - §2.4.1 "Statut" : le centre de certification est gouvernemental donc bénéficie d'un statut particulier
4.1.2 - Contrat de certification	
4.1.2.1 – L'organisme de certification doit disposer d'un contrat juridiquement applicable de fourniture d'activités de certification à ses clients. Les contrats de certification doivent tenir compte des responsabilités de l'organisme de certification et de celles de ses clients.	Le contrat juridique applicable est constitué de plusieurs documents, notamment le formulaire CER-F-01 signé par les parties prenantes.
4.1.2.2 – l'organisme de certification doit s'assurer que le contrat de certification engage le client à se conformer au moins aux points suivants :	
a) Répondre en permanence aux exigences de certification incluant la mise en œuvre des changements appropriés qui sont communiqués par l'organisme de certification.	ANSSI-CC-CER-F-01 - § "Droits et obligations du commanditaire et des développeurs" ANSSI-CSPN-CER-F-01 - § "Droits et obligations du commanditaire et des fournisseurs"
b) Si la certification s'applique à une production de série, s'assurer que le produit certifié continue de répondre aux exigences du produit	
c) Prendre toutes les dispositions nécessaires pour :	
1) La conduite de l'évaluation et la surveillance, y compris la fourniture d'éléments en vue de leur examen tels que : de la documentation et des enregistrements, l'accès au matériel, aux sites, aux zones, aux personnels et sous-traitants du client concernés	
2) L'instruction des réclamations	
3) La participation d'observateurs, le cas échéant.	
d) Faire les déclarations sur la certification en cohérence avec la portée d'accréditation.	

e) Ne pas utiliser la certification de ses produits d'une façon qui puisse nuire à l'organisme de certification ni faire de déclaration sur la certification de ses produits que l'organisme de certification puisse considérer comme trompeuse ou non autorisée.	
f) En cas de suspension, de retrait ou à l'échéance de la certification, cesser d'utiliser l'ensemble des moyens de communication qui y fait référence et remplir toutes les exigences prévues par le programme de certification et s'acquitter de toute autre mesure exigée.	
g) Si le client fournit des copies de documents de certification à autrui, il doit les reproduire dans leur intégralité ou tel que spécifié par le programme de certification.	
h) En faisant référence à la certification de ses produits dans ses supports de communication, tels que documents, brochures ou publicité, se conformer aux exigences de l'organisme de certification et/ou aux spécifications du programme de certification.	
i) Se conformer à toutes les exigences qui peuvent être prescrites dans le programme de certification du produit relatives à l'utilisation des marques de conformité et aux informations relatives au produit.	
j) Conserver un enregistrement de toutes les réclamations dont il a eu connaissance concernant la conformité aux exigences de certification et mettre ces enregistrements à la disposition de l'organisme de certification sur demande, et	
1) Prendre toute action appropriée en rapport avec ces réclamations et les imperfections constatées dans les produits qui ont des conséquences sur leur conformité aux exigences de certification	
2) Documenter les actions entreprises	
k) Informer, sans délais, l'organisme de certification des changements qui peuvent avoir des conséquences sur sa capacité à se conformer aux exigences de certification.	
4.1.3 - Utilisation de licences, de certificats et de marque de conformité	
4.1.3.1 – L'organisme de certification doit exercer le contrôle tel que spécifié par le programme de certification sur la propriété, l'utilisation et l'affichage des licences, des certificats, des marques de conformité, ainsi que tout autre dispositif destiné à indiquer la certification d'un produit.	MQ - §7.7 "Suspension, retrait du certificat" ANSSI-CC-MAR-P-02 : Utilisation des logotypes CCRA et SOGIS ANSSI-CC-MAR-P-01 : Règles d'utilisation de la marque Certification TI

4.1.3.2 – Des références erronées au programme de certification ou une utilisation trompeuse des licences, des certificats, des marques ou de tout autre indiquant qu'un produit est certifié, figurant dans la documentation ou d'autres outils publicitaires doivent être corrigées par une action appropriée.	ANSSI-CC-CER-P-01 v4.0 - §9 ANSSI-CSPN-CER-P-01 v3.0 - §13
4.2 - Gestion de l'impartialité	
4.2.1 - Activités de certification menées de manière impartiale	MQ - §2.4.2 "Dispositions de préservation de l'impartialité"
4.2.2 - OC responsable de l'impartialité	MQ - §2.4.2 "Dispositions de préservation de l'impartialité" ANSSI-CC-PER-F-03 : Engagement du personnel
4.2.3 - OC doit identifier les risques	MQ - §3.3.2 "Analyse de risques"
4.2.4 - OC élimine ou maîtrise le risque identifié	MQ - §3.3.2 "Analyse de risques"
4.2.5 - OC s'engage en matière d'impartialité	ANSSI-CC-MQ-ANN-1 v1.0 : Engagement qualité du DG
4.2.6 - Restriction des activités de l'OC	MQ - §2.4.2 "Dispositions de préservation de l'impartialité" ANSSI-CC-CER-F-01 Dossier d'évaluation - § "Droits et obligations du laboratoire d'évaluation" ANSSI-CSPN-CER-F-01 Dossier d'évaluation CSPN - § "Droits et obligations du laboratoire d'évaluation"
4.2.7 - Entités juridiques séparées de l'OC ne compromettent pas l'impartialité	MQ - §2.4.2 "Dispositions de préservation de l'impartialité "
4.2.8 - OC et son personnel non impliqués dans entité juridique séparée.	MQ - §2.4.2 "Dispositions de préservation de l'impartialité"
4.2.9 - Activités de l'OC pas commercialisées ou liées à un organisme de conseil.	MQ - §2.4.1 "Statut"
4.2.10 - Période de carence de certification pour le personnel de l'OC	MQ - §2.4.6 "Personnel du centre de certification"
4.2.11 - OC prend des mesures quand l'impartialité menacée	MQ - §3.3.2 "Analyse de risques"
4.2.12 - Personnel de l'OC agit de manière impartiale	ANSSI-CC-SECU-P-01 v3.0 : Gestion de la confidentialité à CCN - §3
4.3 Responsabilité et financement	
4.3.1 - OC doit couvrir les responsabilités liées à ses opérations.	MQ - §2.4.1 "Statut"
4.3.2 - OC doit avoir une stabilité financière et les ressources nécessaires à ses opérations	MQ - §2.4.1 "Statut" MQ - §2.4.4 "Organisation" (partie chef de centre de certification)

4.4 Conditions non discriminatoires	
4.4.1 - Politiques et procédures de l'OC non discriminatoires	Articles 2 et 7 du décret n°2002-535 MQ - §4.1 "Accès et traitement non discriminatoires"
4.4.2 - OC doit rendre ses services accessibles	Site Web de l'ANSSI
4.4.3 - Accès au processus de certification ouvert à tous et non abusif	MQ - §4.1 "Accès et traitement non discriminatoires" ANSSI-CC-CER-F-01 : Dossier d'évaluation - § "Frais liés à la certification" ANSSI-CSPN-CER-F-01 : Dossier d'évaluation CSPN § - "Frais liés à la certification"
4.4.4 - Exigences de l'OC limitées à la portée de certification	MQ - §4.3 "Critères d'évaluation" MQ - §4.4 "Modification des exigences de certification" ANSSI-CC-CER-P-01 - §4.3 ANSSI-CSPN-CER-P-01 - § 9.1
4.5 Confidentialité	
4.5.1 - OC doit manager les informations obtenues pendant la certification de manière confidentielles	MQ - §10.2 "Confidentialité de l'information" ANSSI-CC-CER-F-01 : Dossier d'évaluation - § "Confidentialité" ANSSI-CSPN-CER-F-01 : Dossier d'évaluation CSPN - § "Confidentialité" ANSSI-CC-SECU-01 pour l'OC ANSSI-CC-AGR-P-02 pour les CESTI CC ANSSI-CCPN-AGR-P-01 pour les CESTI CSPN
4.5.2 - Diffusion d'information obligatoire par l'OC	MQ - §10.2 "Confidentialité de l'information"
4.5.3 - Informations visant un client obtenues par d'autres sources sont confidentielles	MQ - §10.2 "Confidentialité de l'information"
4.6 Informations accessibles au public	
a) Informations sur le programme de certification des produits	Les documents "PUBLIC" sont publiés sur le site de l'ANSSI
b) Moyens d'obtention d'appuis financiers et info tarif	L'OC dispose des moyens financiers du SGDSN, lui-même tributaire de certains ministères Services de l'OC non facturés
c) Description des droits et devoirs des demandeurs et clients	ANSSI-CC-CER-F-01 : Dossier d'évaluation - § "Conditions générales de la certification" ANSSI-CSPN-CER-F-01 : Dossier d'évaluation CSPN - § "Conditions générales de la certification"
d) Processus traitement des plaintes et appels	ANSSI-CC-ANO-P-01 : Traitement des anomalies
5 - Exigences structurelles	
5.1 - Organisation et direction	

5.1.1 - Les activités de l'OC doivent être gérées et structurées pour préserver l'impartialité	MQ - §2.4.5 "Interfaces de l'organisme de certification" ANSSI-CC-QUA-F-05 : Analyse de risques
5.1.2 - OC doit documenter son organisation	MQ - §2.4.3 "Organisation" MQ - §2.4.5 "Interfaces de l'organisme de certification"
5.1.3 - OC doit identifier le comité, le groupe de personnes ou la personne ayant des pouvoirs de décision et la responsabilité de :	
a) l'élaboration de politiques relatives au fonctionnement de l'OC	MQ - Chapitre 2 "Le schéma de certification" MQ - §2.4.4 "Organisation" ANSSI-CC-PER-P01 : Recrutement et qualification du personnel - Fiche de poste du "Chef du centre de certification"
b) la supervision de la mise en œuvre des politiques et procédures	MQ - §3.3.3 "Revue de direction" ANSSI-CC-QUA-P-01 : Revues de direction ANSSI-CC-QUA-P-03 : Audits internes
c) la supervision de la situation financière de l'OC	MQ - §2.4.1 "Statut"
d) le développement des prestations de certification	MQ - §2.2 "Le comité directeur de la certification"
e) le développement des exigences de certification	ANSSI-CC-PER-P01 : Recrutement et qualification du personnel - Fiche de poste "Certificateur ou Ingénieur au centre de certification "
f) l'évaluation	MQ - §2.4.5 "Interfaces de l'organisme de certification" (laboratoires d'évaluation)
g) la revue	ANSSI-CC-PER-P01 : Recrutement et qualification du personnel - Fiche de poste "Certificateur ou Ingénieur au centre de certification"
h) la décision en matière de certification	MQ - §7.3 "Décision de certification"
i) la délégation des pouvoirs à des comités ou à du personnel	Fiche de poste "Chef du centre de certification"
j) les dispositions contractuelles	MQ - §2.4.5 "Interfaces de l'organisme de certification" (affaires juridiques)
k) la fourniture des ressources appropriées pour les activités de certification	MQ - §2.4.5 "Interfaces de l'organisme de certification" (ressources humaines) ANSSI-CC-PER-P01 Recrutement et qualification du personnel - Fiche de poste du "Chef du centre de certification" MQ - §3.3.3 "Revue de direction"
l) la prise en charge des plaintes et des appels	ANSSI-CC-ANO-P-01 : Traitement des anomalies
m) les exigences en matière de compétences du personnel	ANSSI-CC-PER-P-01 : Recrutement et qualification du personnel - Fiche de poste du "Chef du centre de certification"

n) le système de management de l'OC	MQ - §2.2 "Le comité directeur de la certification" MQ - §3.3.3 "Revue de direction" ANSSI-CC-PER-P-01 : Recrutement et qualification du personnel
5.1.4 - L'OC doit disposer de règles formelles régissant la désignation, la mission et le fonctionnement de tous les comités engagés dans le processus de certification.	Décret 2002-535 du 18 avril 2002 modifié Règlement intérieur du comité directeur de la certification
5.2 - Dispositif de préservation de l'impartialité	
5.2.1 - L'OC doit disposer d'un DPI qui doit fournir des données d'entrée sur :	
a) les politiques et les principes relatifs à l'impartialité de ses activités de certification	MQ - §2.4.2 "Dispositions de préservation de l'impartialité" MQ - §2.4.5 "Interfaces de l'organisme de certification" ANSSI-CC-PER-F-03 : Engagement du personnel ANSSI-CC-QUA-F-05 : Analyse de risques L'article 25 bis inséré dans la loi de 1983 lors de la loi "déontologie" de 2016
b) toute tendance de l'OC à laisser des considérations commerciales et autres entraver la fourniture objective et fiable des prestations de certification	MQ - §2.4.1 "Statut"
c) les éléments susceptibles d'influencer sur l'impartialité et la confiance dans la certification, notamment la transparence	ANSSI-CC-QUA-F-05 : Analyse de risques
5.2.2 - Le dispositif doit être documenté afin qu'ils soient garantis :	
a) une représentation équilibrée des parties ayant un intérêt significatif, de façon qu'aucun intérêt ne prédomine	MQ - §2.2 "Le comité directeur de la certification"
b) l'accès à toutes les informations nécessaires pour remplir toutes ses fonctions	MQ - 2.4.2 "Dispositions de préservation de l'impartialité"
5.2.3 - Si la direction de l'OC ne suit pas les avis de ce dispositif	MQ - §2.2 "Le comité directeur de la certification"
5.2.4 - OC doit identifier et inviter les parties ayant un intérêt significatif	MQ - §2.2 "Le comité directeur de la certification"
6 - Exigences relatives aux ressources	
6.1 - Personnel de l'organisme de certification	
6.1.1 - Généralités	
6.1.1.1 - L'OC doit employer ou pouvoir faire appel à du personnel en quantité suffisante	MQ - §2.4.5 "Interfaces de l'organisme de certification"

6.1.1.2 - Le personnel doit posséder les compétences correspondant aux fonctions qu'il remplit	ANSSI-CC-PER-P-01 : Recrutement et qualification du personnel
6.1.1.3 - Le personnel, mais aussi tous les membres des comités, le personnel des organismes externes doivent préserver la confidentialité de toutes les informations obtenues ou gérées au cours de certification	Accréditation COFRAC EN ISO/IEC 17025 des CESTI pour les CESTI CC MQ - §2.4.2 "Dispositions de préservation de l'impartialité" MQ - §10.2 "Confidentialité de l'information" ANSSI-CC-SECU-P-01 : Gestion de la confidentialité
6.1.2 - Gestion des compétences du personnel engagé dans le processus de certification	
6.1.2.1 - L'OC doit instaurer, mettre en œuvre et maintenir une procédure de gestion des compétences du personnel	ANSSI-CC-PER-L-02 Liste des qualifications ANSSI-CC-PER-P-01 v6.1 - §4.3
6.1.2.2 – L'OC doit tenir à jour les enregistrements suivants concernant le personnel impliqué dans le processus de certification.	Dossier à l'embauche Dossier d'habilitation Entretien individuel
6.1.3 - Contrat conclu avec le personnel	ANSSI-CC-PER-F-03 : Engagement du personnel
6.2 - ressources pour l'évaluation	
6.2.1 - Ressources internes	Les expertises techniques faites par les laboratoires internes de l'ANSSI sont effectuées à titre d'avis consultatifs
6.2.2 - Ressources externes	
6.2.2.1 - L'OC ne doit externaliser ses activités d'évaluation qu'aux organismes répondant à l'EN ISO/IEC 17025	Les CESTI CC sont accrédités EN ISO/IEC 17025 et répondent à cette exigence dans le cadre du périmètre de l'accréditation
6.2.2.2 - Activités d'évaluation confiées à des organismes non indépendants	Non applicable
6.2.2.3 - L'OC doit disposer d'un contrat juridiquement exécutoire	ANSSI-CSPN-CER-F-01 : Dossier d'évaluation CSPN ANSSI-CC-CER-F-01 : Dossier d'évaluation Décret n°2002-535 ANSSI-CC-AGR-F-01 : Demande d'agrément ANSSI-CSPN-AGR-F-01 : Demande d'agrément ANSSI-CSPN-AGR-F-08 : Décision d'agrément
6.2.2.4 - L'OC doit :	
a) assumer l'entière responsabilité de toutes les activités externalisées auprès d'un autre organisme	L'ANSSI porte l'entière responsabilité puisqu'elle délivre les certificats et qu'elle a le pouvoir de valider les rapports d'évaluation transmis par les CESTI Décret n°2002-535

b) garantir que l'organisme qui assure les prestations externalisées et le personnel qu'il emploie ne sont pas engagés, directement ou par le biais d'un autre employeur, d'une façon qui pourrait compromettre la crédibilité des résultats	ANSSI-CC-AGR-P-01 : Agrément des centres d'évaluation ANSSI-CSPN-AGR-P-01 : Agrément des centres d'évaluation
c) disposer de politiques, de procédures et d'enregistrements sur la qualification, l'évaluation et le contrôle de tous les organismes assurant des prestations externalisées servant à ses activités de certification	ANSSI-CC-AGR-P-01 : Agrément des centres d'évaluation ANSSI-CSPN-AGR-P-01 : Agrément des centres d'évaluation
d) tenir à jour une liste des prestataires de services externalisés habilités	ANSSI-CC-AGR-L-01 : Liste du statut des agréments de CESTI Site Web de l'ANSSI : www.ssi.gouv.fr
e) mettre en œuvre des actions correctives pour tout manquement au contrat de 6.2.2.3 ou à d'autres exigences de 6.2.2 dont il rend compte, et	ANSSI-CC-QUA-F-05 Analyse de risques ANSSI-CC-ANO-L-01 Tableau des Actions du centre
f) informer par avance le client des activités qui sont externalisées, afin de lui donner la faculté d'émettre des objections.	ANSSI-CSPN-CER-F-01 : Dossier d'évaluation CSPN ANSSI-CC-CER-F-01 : Dossier d'évaluation Ces documents sont signés par le client et le laboratoire Décret n°2002-535

7 - Exigences relatives aux processus	
7.1 - Généralités	
7.1.1 - L'OC doit exploiter un ou plusieurs programmes de certification couvrant ses activités de certification	ANSSI-CC-CER-P-01 v4.0 : Certification de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection ANSSI-CSPN-CER-P-01 v3.0 : Certification de sécurité de premier niveau ANSSI-CC-CRY-P-01 : Modalités pour la réalisation des analyses cryptographiques ANSSI-CC-MAR-P-01 : Règles d'utilisation de la marque Certification TI ANSSI-CC-MAR-P-02 : Utilisation des logotypes CCRA et SOGIS ANSSI-CC-SITE-P-02 : Evaluation de composants d'assurance ALC génériques ANSSI-CC-AGR-P-01 : Agrément des centres d'évaluation ANSSI-CC-AGR-P-02 : Sécurité des centres d'évaluation ANSSI-CSPN-AGR-P-01 : Agrément des centres d'évaluation
7.1.2 - Les produits des clients doivent être évalués selon les exigences figurant dans les normes et autres documents normatifs spécifiés.	Les normes (Critères communs) et autres documents normatifs liés aux CC sont disponibles sur les sites du CCRA et du SOG-IS. Les documents "PUBLIC" sont aussi publiés sur le site de l'ANSSI Les documents normatifs liés aux CSPN sont disponibles sur le site de l'ANSSI
7.1.3 - Si des explications concernant l'application de ces documents à un programme de certification spécifique s'avèrent nécessaires, elles doivent être formulées par des personnes ou des comités pertinents et impartiaux, possédant les compétences techniques nécessaires, et elles doivent pouvoir être fournies sur demande par l'OC.	Site de l'ANSSI : Visa de sécurité / Certification / FAQ

7.2 - Demande	
Pour instruire les demandes, l'OC doit recueillir toutes les informations nécessaires pour mener à bien le processus de certification	MQ - §5.1 "Contenu du dossier d'évaluation" ANSSI-CC-CER-P-01 v4.0 - §3.1 ANSSI-CSPN-CER-P-01 v3.0 - §7
7.3 - Revue de demande	
7.3.1 - L'OC doit effectuer une revue des informations obtenues pour garantir que :	
a) les informations sur le client et le produit sont suffisantes pour permettre la réalisation du processus de certification	MQ - §5.2 "Enregistrement de la demande" ANSSI-CC-CER-P-01 v4.0 - §3.2 ANSSI-CSPN-CER-P-01 v3.0 - §8
b) toute divergence d'interprétation identifiée entre l'OC et le client est résolue, y compris l'accord concernant les normes ou les documents normatifs	ANSSI-CC-CER-P-01 v4.0 - §4.1 ANSSI-CSPN-CER-P-01 v3.0 - §8
c) la portée de la certification souhaitée est définie	ANSSI-CC-CER-P-01 v4.0 - §4.1 ANSSI-CSPN-CER-P-01 v3.0 - §8
d) les moyens permettant de réaliser toutes les activités d'évaluation sont disponibles	ANSSI-CC-CER-P-01 v4.0 - §4.1 ANSSI-CC-CER-F-19 : Compte rendu réunion de démarrage ANSSI-CSPN-CER-P-01 v3.0 - §8
e) l'OC a la compétence et la capacité nécessaire pour réaliser l'activité de certification	ANSSI-CC-CER-P-01 v4.0 - §3.2 ANSSI-CSPN-CER-P-01 v3.0 - §8
7.3.2 - L'OC doit disposer d'un processus pour repérer les demandes de certification du client	ANSSI-CC-CER-F-12 : Fiche de revue du dossier de demande de certification
7.3.3 - L'OC doit s'assurer qu'il possède les compétences et les capacités pour toutes les activités de certification qu'il doit entreprendre et tenir à jour un enregistrement justifiant la décision d'entreprendre la certification	ANSSI-CC-CER-F-12 : Fiche de revue du dossier de demande de certification
7.3.4 - L'OC doit refuser d'entreprendre une certification spécifique s'il ne dispose pas des compétences ou des capacités nécessaires pour les activités	ANSSI-CC-CER-F-12 : Fiche de revue du dossier de demande de certification
7.3.5 - Si l'OC s'appuie sur des certifications qu'il a déjà délivrées au client ou qu'il a déjà délivrées à d'autres clients, pour omettre certaines activités, alors l'OC doit faire référence à la ou aux certifications existantes dans ses enregistrements.	ANSSI-CC-CER-F-12 : Fiche de revue du dossier de demande de certification
7.4 - Évaluations	
7.4.1 - L'OC doit avoir un planning des activités d'évaluation pour permettre de gérer les dispositions nécessaires	Echanges avec les laboratoires

7.4.2 - L'OC doit désigner des membres du personnel pour réaliser chacune des tâches d'évaluation	ANSSI-CC-PER-P-01 : Recrutement et qualification du personnel
7.4.3 - L'OC doit veiller à la disponibilité de toutes les informations et/ou documentations nécessaires à la réalisation des tâches d'évaluation	ANSSI-CSPN-CER-F-01 : Dossier d'évaluation CSPN ANSSI-CC-CER-F-01 : Dossier d'évaluation Critères communs Documents publiés sur le site Web de l'ANSSI
7.4.4 - l'OC doit exécuter les activités d'évaluation qu'il entreprend avec ses ressources internes et doit gérer les ressources externalisées conformément au §7.4.1. Les produits doivent être évalués par rapport aux exigences couvertes par la portée de la certification et aux exigences spécifiées dans le programmes de certification.	MQ - §2.4.4 "Organisation" MQ - §2.4.5 "Interfaces de l'organisme de certification" MQ - §5.2 "Enregistrement de la demande" ANSSI-CC-CER-P-01 - §2 et §3 ANSSI-CSPN-CER-P-01 - §2 et §3.1
7.4.5 - l'OC ne doit s'appuyer, sur des résultats obtenus avant la demande certification, que s'il en assure la responsabilité	ANSSI-CC-CER-F-01 - § "Cas d'une réévaluation" ANSSI-CC-CER-F-01 - § "Cas d'une composition" ANSSI-CSPN-CER-F-01 - § "Cas d'une réévaluation"
7.4.6 - l'OC doit informer le client de toutes les non-conformités	MQ - §6.1.4 "Le Rapport Technique d'Évaluation" ANSSI-CC-CER-P-01 v4.0 - §4.3 Non applicable en CSPN
7.4.7 - si une ou plusieurs non-conformités apparaissent et si le client souhaite poursuivre le processus de certification, l'OC doit fournir les informations concernant les taches d'évaluation supplémentaires à la vérification de la correction des non-conformités	ANSSI-CC-CER-P-01 v4.0 - §4.4 Non applicable en CSPN
7.4.8 - Si le client donne son accord pour la réalisation des tâches d'évaluation supplémentaires, le processus spécifié en 7.4 doit être réitéré pour la réalisation des tâches	ANSSI-CC-CER-P-01 v4.0 - §4.4 Non applicable en CSPN
7.4.9 - Les résultats de toutes les activités d'évaluation doivent être documentés avant de procéder à la revue.	MQ - §6.1.4 "Le Rapport Technique d'Évaluation" ANSSI-CC-CER-P-01 v4.0 - §4.3 ANSSI-CSPN-CER-P-01 v3.0 - §9.6
7.5 - Revue	
7.5.1 - L'OC doit désigner au moins une personne pour prendre la décision de certification	MQ - §2.4.4 "Organisation" MQ - §7.3 "Décision de certification"
7.5.2 - Les recommandations en faveur d'une décision de certification doivent être documentées.	MQ - §7.2 "Rapport de certification"
7.6 - Décision de certification	

7.6.1 - L'OC doit être responsable et doit conserver son pouvoir décisionnel en matière de certification	MQ - §2.4.4 "Organisation" MQ - §7.3 "Décision de certification"
7.6.2 - L'OC doit désigner au moins une personne pour prendre la décision de certification	MQ - §2.4.4 "Organisation" MQ - §7.3 "Décision de certification"
7.6.3 - Les personnes missionnées par l'OC pour prendre une décision de certification doivent être employées par ou sous contrat avec l'OC.	MQ - §2.4.6 "Personnel du centre de certification" MQ - §2.4.2 "Dispositions de préservation de l'impartialité"
7.6.4 - Le contrôle organisationnel de l'OC doit être la propriété totale ou majoritaire d'une autre entité par l'OC	MQ - §2.2 "Le comité directeur de la certification" Décret n°2002-535
7.6.5 - Les personnes employées par des entités sous contrôle opérationnel sont soumises aux mêmes exigences que les personnes employées par l'OC	Non applicable : aucune entité n'est sous le contrôle opérationnel de l'OC
7.6.6 - L'OC doit notifier au client toute décision de refus de certification en précisant le raisons	ANSSI-CC-CER-P-01 v4.0 - §4.3 ANSSI-CSPN-CER-P-01 v3.0 - §10.2
7.7 - Documents de certification	
7.7.1 - L'OC doit fournir au client des documents de certification officiels	MQ - §7.2 "Rapport de certification" ANSSI-CSPN-CER-F-07 ANSSI-CC-CER-F-07
7.7.2 - Les documents officiels de certification doivent comporter la signature de la personne de l'OC habilitée.	ANSSI-CSPN-CER-F-07 ANSSI-CC-CER-F-07
7.7.3 - Les documents officiels de certification ne doivent être émis qu'après ou en même temps que : - la décision de délivrer la certification - la satisfaction aux exigences de certification - la signature du contrat de certification	ANSSI-CC-CER-P-01 v4.0 - §5 ANSSI-CSPN-CER-P-01 v3.0 - §10
7.8 - Annuaire des produits certifiés	
L'OC doit tenir à jour des informations sur les produits certifiés.	MQ - §7.4 "Maîtrise des enregistrements"
7.9 - Surveillance	
7.9.1 - Si une surveillance est requise par le programme de certification ou dans les cas prévus aux articles 7.9.3 ou 7.9.4, l'OC doit mettre en place une surveillance des produits couverts par la décision de certification	Point 7.9.3 applicable
7.9.2 - Quand le processus de surveillance recourt à l'évaluation, la revue ou la décision de certification, les exigences de 7.4, 7.5 et 7.6 doivent être respectées	Non applicable : la surveillance de l'usage des marques ne recourt pas à l'évaluation, la revue ou la décision de certification

7.9.3 - Lorsqu'est accordée une autorisation d'utilisation permanente d'une marque de certification sur un produit certifié, une surveillance périodique doit être mise en place	ANSSI-CC-CER-P-01 v4.0 - §8 et 9 ANSSI-CSPN-CER-P-01 v3.0 - §12 et 13
7.9.4 - Quand l'utilisation d'une marque de certification est accordée pour un processus ou un service, une surveillance doit être instaurée	Non applicable : le périmètre de l'OC ne couvre pas les processus et les services
7.10 - Changements ayant des conséquences sur la certification	
7.10.1 - Quand le programme de certification introduit des exigences nouvelles qui ont une incidence pour le client, l'OC doit s'assurer que tous les clients en sont informés. L'OC doit vérifier que ses clients mettent en œuvre les changements et doit prendre en compte les actions exigées par le programme de certification.	MQ - §4.4 "Modification des exigences de certification"
7.10.2 - L'OC doit étudier les autres changements ayant des conséquences sur la certification, y compris les changements à l'initiative du client et arrêter les mesures appropriées.	ANSSI-CC-CER-P-01 v4.0 - §9 ANSSI-CSPN-CER-P-01 v3.0 - §13
7.10.3 - Les actions pour traiter les changements ayant des conséquences sur la certification.	ANSSI-CC-CER-P-01 v4.0 - §9 ANSSI-CSPN-CER-P-01 v3.0 - §13
7.11 - Résiliation, réduction, suspension ou retrait de la certification	
7.11.1 - Lorsqu'une non-conformité aux exigences de la certification est avérée que ce soit à la suite d'une surveillance ou par tout autre moyen, l'OC doit examiner la non-conformité et arrêter des mesures appropriées.	ANSSI-CC-CER-P-01 v4.0 - §9 ANSSI-CSPN-CER-P-01 v3.0 - §13
7.11.2 - Lorsque les mesures appropriées comportent une évaluation, une revue ou une décision de certification, les exigences de 7.4, 7.5 et 7.6 doivent être remplies.	ANSSI-CC-CER-P-01 v4.0 - §9 ANSSI-CSPN-CER-P-01 v3.0 - §14.2.1
7.11.3 - Si la certification est résiliée (à la demande du client), suspendue ou retirée, l'OC doit prendre les actions spécifiques et apporter toutes les informations au public.	ANSSI-CC-CER-P-01 v4.0 - §9 ANSSI-CSPN-CER-P-01 v3.0 - §13
7.11.4 - Si la certification est suspendue, l'OC doit faire en sorte d'informer le client et lui communiquer les actions pour lever et rétablir la certification et toutes autres actions exigées par le programme.	ANSSI-CC-CER-P-01 v4.0 - §9 ANSSI-CSPN-CER-P-01 v3.0 - §13
7.11.5 - Toutes évaluations, revues ou décisions nécessaires à la levée de suspension ou qui exigées par le programme de certification doivent être assurées conformément aux parties applicables des §7.4, 7.5, 7.6, 7.7, 7,9 et 7.11.3	ANSSI-CC-CER-P-01 v4.0 - §9 ANSSI-CSPN-CER-P-01 v3.0- §13

7.11.6 - Si la certification est rétablie après une suspension, l'OC doit apporter toutes les modifications nécessaires aux documents officiels de certification, aux informations destinées au public, aux autorisations d'utilisation des marques, etc. pour garantir l'existence de toutes les indications pertinentes confirmant que le produit continue d'être certifié.	ANSSI-CC-CER-P-01 v4.0 - §9 ANSSI-CSPN-CER-P-01 v3.0- §13
7.12 - Enregistrements	
7.12.1 - L'OC doit conserver les enregistrements prouvant que toutes les exigences du processus de certification ont été effectivement respectées.	MQ - §7.4 "Maîtrise des enregistrements"
7.12.2 - L'OC doit préserver la confidentialité des enregistrements.	MQ - §7.4 "Maîtrise des enregistrements"
7.12.3 - Si le programme de certification implique une réévaluation complète du ou des produits dans un cycle déterminé, les enregistrements doivent être conservés au moins pour le cycle en cours et le cycle précédent.	MQ - §7.4 "Maîtrise des enregistrements"
7.13 - Plaintes et appels	
7.13.1 - L'OC doit avoir un processus documenté lui permettant de recevoir, d'évaluer et de prendre des décisions relatives aux plaintes et appels. L'OC doit enregistrer et tracer les plaintes et appels, ainsi que les actions entreprises pour y apporter des solutions.	ANSSI-CC-ANO-P-01 v5.1 : Traitement des anomalies
7.13.2 - A réception d'une plainte ou d'un appel, l'OC doit confirmer si la plainte ou l'appel est lié aux activités de certification dont il a la responsabilité, et dans l'affirmative, il doit les traiter.	ANSSI-CC-ANO-P-01 v5.1
7.13.3 - L'OC doit accuser réception d'une plainte ou d'un appel.	ANSSI-CC-ANO-P-01 v5.1
7.13.4 - L'OC doit être responsable de la collecte et de la vérification de toutes les informations nécessaires pour que la plainte ou l'appel aboutisse à une décision.	ANSSI-CC-ANO-P-01 v5.1
7.13.5 - La décision permettant d'apporter une solution à la plainte ou à l'appel doit être prise, ou revue et approuvée par une ou des personnes non engagées dans les activités de certification liées à la plainte ou à l'appel.	ANSSI-CC-ANO-P-01 v5.1

7.13.6 - Pour garantir l'absence de tout conflit d'intérêt, le personnel qui a fourni des conseils ou qui a été employé par un client, y compris les personnes qui ont assuré des activités de conseil en système de management, ne doit pas participer, pour le compte de l'OC, à la revue, ni approuver la solution apportée à une plainte ou un appel de ce client dans les deux ans suivant la fin des activités de conseil ou de l'emploi chez ce client.	ANSSI-CC-ANO-P-01 v5.1
7.13.7 - Dans la mesure du possible, l'OC doit dûment aviser le plaignant de la conclusion du processus de traitement de la plainte qu'il a formulée.	ANSSI-CC-ANO-P-01 v5.1
7.13.8 - L'OC doit dûment aviser le requérant de la conclusion du processus de traitement de l'appel qu'il a formulé.	ANSSI-CC-ANO-P-01 v5.1
7.13.9 - L'OC doit prendre toutes les actions consécutives nécessaires pour résoudre la plainte ou l'appel.	ANSSI-CC-ANO-P-01 v5.1
8 - Exigences du système de management	
8.1 - Options	
8.1.2 - Option A	Les paragraphes concernés ont été traités précédemment
8.2 - Documentation générale du système de management	
8.2.1 - La direction de l'OC doit instaurer, documenter et maintenir des politiques et des objectifs en vue de répondre à la norme ISO/CEI 17065.	Le corpus documentaire de l'OC couvre les politiques et objectifs en vue de répondre à la norme ISO/CEI 17065 : il est régulièrement revu et maintenu à jour
8.2.2 – La direction de l'OC doit fournir la preuve de son engagement dans le développement et la mise en œuvre du système de management, ainsi que l'efficacité avec laquelle elle parvient à répondre aux exigences de la norme ISO/CEI 17065.	La direction au travers des revues de direction qualité, des validations à tous les niveaux de documents qualité est engagée dans le développement et la mise à œuvre du système de management
8.2.3 – La direction de l'OC doit nommer un membre de l'encadrement qui, nonobstant d'autres responsabilités, doit avoir notamment la responsabilité et l'autorité pour : a) s'assurer que les processus et les procédures nécessaires au système de management sont instaurés, mis en œuvre et maintenus, et b) rendre compte à la direction de la performance du système de management et de toute nécessité d'amélioration.	Le responsable qualité ou son suppléant remplit les exigences demandées Les performances du système de management et de toute nécessité d'amélioration sont revues annuellement lors de « revues de direction du système qualité du centre de certification »

8.2.4 – Tous les documents, processus, systèmes, enregistrement, etc. liés à la réalisation des exigences de la norme ISO/CEI 17065 doivent être inclus, référencés dans la documentation du système de management ou y être reliés.	ANSSI-CC-DOC-L-01 : Liste des documents de référence
8.2.5 – Toutes les personnes impliquées dans les activités de certification doivent avoir accès aux éléments de la documentation du système de management.	Les documents qualité validés sont tous disponibles aux membres de l'OC
8.3 - Maîtrise des documents	
8.3.1 – L'OC doit établir des procédures lui permettant de maîtriser les documents liés au respect de la norme ISO/CEI 17065.	L'OC dispose de procédures tant publiques, qu'internes pour maîtriser les exigences de la norme EN ISO/IEC 17065
8.3.2 – Ces procédures doivent définir les mesures nécessaires pour : a) approuver l'adéquation des documents avant diffusion ; b) revoir, mettre à jour si nécessaire et approuver de nouveaux documents ; c) s'assurer que les modifications et le statut de la version en vigueur des documents sont identifiés ; d) assurer la disponibilité sur les lieux d'utilisation des versions pertinentes des documents applicables ; e) s'assurer que les documents restent lisibles et facilement identifiables ; f) s'assurer que les documents d'origine extérieure sont identifiés et que leur diffusion est maîtrisée, et ; g) empêcher toute utilisation non intentionnelle de documents périmés et les identifier de manière adéquate s'ils sont conservés dans un but quelconque.	a) ANSSI-CC-DOC-P-01 v4.1 - §6.1 b) ANSSI-CC-DOC-P-01 v4.1 - §11 pour la revue documentaire et §6 pour l'approbation des documents c) Tous les documents en vigueur sont accessibles depuis ANSSI-CC-DOC-L-01 d) Idem c) e) Les documents sont identifiables conformément à ANSSI-CC-DOC-P-01 v4.1 - §3. Ces documents sont lisibles soit en version électronique, soit en version papier (original) f) ANSSI-CC-DOC-P-01 v4.1 - §12 pour la gestion des documents externes g) ANSSI-CC-DOC-P-01 v4.1 - §7
8.4 - Maîtrise des enregistrements	
8.4.1 – L'OC doit instaurer des procédures pour assurer l'identification, le stockage, la protection, l'accessibilité, la durée de conservation et l'élimination des enregistrements générés dans le cadre des exigences de la norme ISO/CEI 17065.	L'OC bénéficie des moyens de stockage, de protection, d'accessibilité et de durée de conservation du SGDSN ANSSI-CC-DOC-P-01 v4.1 Document système qualité MQ - §7.4 "Maîtrise des enregistrements"
8.4.2 – L'OC doit établir des procédures définissant une période de conservation des enregistrements qui soit cohérente avec ses obligations contractuelles et légales. L'accès à ces enregistrements doit être conforme aux dispositions en matière de sécurité.	Idem précédent
8.5 - Revue de direction	

8.5.1 - Généralités	
8.5.1.1 – L'OC doit établir des procédures pour revoir, à intervalles planifiés, son système de management pour garantir qu'il demeure pertinent, adéquat et efficace, y compris les politiques et les objectifs déclarés relatifs au respect des exigences de la norme ISO/CEI 17065.	MQ - §3.3.3 "Revue de direction"
8.5.1.2 – Ces revues doivent être réalisées au moins un fois par an. Il est également possible de procéder à une revue complète en plusieurs parties, celle-ci devant être menée à son terme dans une période de douze mois. Les enregistrements des revues doivent être tenus à jour.	ANSSI-CC-DOC-P-01 - §11 ANSSI-CC-DOC-L-01 : Liste des documents de référence
8.5.2 - Éléments d'entrée de la revue	ANSSI-CC-QUA-F-04 : Compte-rendu revue de direction
8.5.3 - Éléments de sortie de la revue	ANSSI-CC-QUA-F-04
8.6 - Audits internes	
8.6.1 – L'OC doit instaurer des procédures relatives aux audits internes […]	ANSSI-CC-QUA-P-03 v3.3 : Audits internes
8.6.2 – Un programme d'audits doit être planifié […]	ANSSI-CC-QUA-P-03 v3.3 - §2.2
8.6.3- Les audits internes doivent normalement être réalisés une fois par an […]	ANSSI-CC-QUA-P-03 v3.3
8.6.4 – Les audits internes sont réalisés par un personnel qualifié […]	ANSSI-CC-QUA-P-03 v3.3
8.7 - Actions correctives	
8.7.1 – L'OC doit établir des procédures pour identifier et gérer les non-conformités de ses opérations.	ANSSI-CC-ANO-P-01 v5.1 :Traitement des anomalies
8.7.2 – L'OC doit également, si nécessaire, entreprendre des actions pour éliminer les causes de non-conformités afin d'éviter qu'elles ne se reproduisent	ANSSI-CC-ANO-L-01 - feuille "Actions et vérifications"
8.7.3 – Les actions correctives doivent être adaptées aux effets des non-conformités rencontrées	ANSSI-CC-ANO-P-01 v5.1-- §7
8.7.4 – Les procédures doivent définir les exigences pour	
a) Procéder à l'identification des non-conformités	ANSSI-CC-ANO-P-01 v5.1- §5.1 et §8
b) Déterminer les causes de non-conformité	ANSSI-CC-ANO-P-01 v5.1 - §5.2 et §8
c) Corriger les non-conformités	ANSSI-CC-ANO-P-01 v5.1 - §5.3 et §8
d) Évaluer le besoin d'entreprendre des actions pour garantir que les non-conformités ne se reproduisent pas	ANSSI-CC-ANO-P-01 v5.1 - §7 et §8

e) Déterminer et mettre en œuvre en temps opportun, les actions nécessaires	ANSSI-CC-ANO-P-01 v5.1 - §7 et §8
f) Enregistrer les résultats des actions mises en œuvre	ANSSI-CC-ANO-P-01 v5.1 - §7
g) Procéder à la revue de l'efficacité des actions correctives mises en œuvre.	ANSSI-CC-ANO-P-01 v5.1 - §7 et §8
8.8 - Actions préventives	
8.8.1 – L'OC doit instaurer des procédures relatives à la mise en place d'actions préventives permettant d'éliminer les causes de non-conformités potentielles	ANSSI-CC-ANO-P-01 v5.1 - §7
8.8.2 – Les actions préventives doivent être adaptées aux effets probables des problèmes potentiels	ANSSI-CC-ANO-L-01 v5.1 - §7
8.8.3 – Les procédures relatives aux actions préventives doivent définir les exigences pour déterminer […]	ANSSI-CC-ANO-P-01 v5.1 - §9