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 28 Avril 2025

N° **772 /ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CC-ANO-P-01_v5.2**

PROCEDURE

TRAITEMENT DES ANOMALIES

Application **:** A compter de sa publication.

Diffusion **:** Publique.

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

Renaud LABELLE

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

SUIVI DES MODIFICATIONS

Versions	Date	Modifications
1	13/01/2004	Création
2.0	07/03/2011	Mise à jour du document
3.0	08/03/2016	Refonte document et diffusion publique
4.0	21/11/2017	Mise à jour : - des documents de référence - du vocabulaire (harmonisation avec la norme NF EN ISO/CEI 17065) Prise en compte de la fusion des documents ANSSI-CC-CPP-P-01, ANSSI-CC-SITE-P-01 et ANSSI-CC-CER-P-01 dans ANSSI-CC-CER-P-01
5.0	29/01/2019	Ajouts de précision pour être conforme aux exigences de la norme NF EN ISO/CEI 17065
5.1	13/1/2020	Ajout de signataires pour réponses aux plaintes Précision concernant le traitement des non-conformités et des actions préventives. Ajout de la gestion des points sensibles
5.2	28/04/2025	Correction du rôle de l'agent traitant les appels et plaintes

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

Cette procédure est également soumise pour avis lors de chaque modification majeure conformément au manuel qualité du centre de certification. Les évaluations mineures ne sont pas soumises au comité directeur de la certification.

La présente procédure est disponible en ligne sur le site institutionnel de l'ANSSI (www.cyber.gouv.fr).

TABLE DES MATIERES

1 Objet de la procédure

Cette procédure définit le processus mis en œuvre pour résoudre les anomalies et les améliorations de toutes origines et concerne l'ensemble de l'activité de certification Critères communs, de Certification de sécurité de premier niveau et du système qualité du centre de certification.

Le décret relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information définit le cadre réglementaire applicable à ce processus de certification (voir [DECRET]) qui régit à la fois le schéma national et la mise en œuvre au niveau national du schéma européen de certification de cybersécurité fondé sur les critères communs (voir [EUCC]).

Ce décret définit l'organisation nécessaire à la conduite d'une évaluation par une tierce partie et à son contrôle, conduisant à la délivrance de certificats attestant qu'un objet répond aux exigences de sécurité listées dans sa cible de sécurité.

Le centre de certification s'appuie sur cette même organisation pour certifier la conformité des profils de protection aux exigences de la classe APE définie dans les Critères Communs [CC]. Les certificats correspondants sont également émis au titre du décret 2002-535 modifié.

2 Définitions

Le terme « anomalie » est le terme générique pour désigner les « appels », les « plaintes », ou les « écarts ».

Un « appel » est une demande adressée à l'organisme de certification par un commanditaire pour que cet organisme reconsidère une décision déjà prise relative à la certification d'un objet évalué ou à l'agrément d'un CESTI[1].

Par exemple :

- un commanditaire peut émettre un appel après émission de la décision de certification ;
- un centre d'évaluation peut émettre un appel en cas de refus de son agrément.

Une « plainte » est l'expression d'un mécontentement relatif aux activités de l'organisme de certification, autre qu'un appel, émis par une personne ou une organisation.

Par exemple :

- la non-réaction du centre de certification suite à la commercialisation d'un produit avec les marques de certification alors qu'il ne correspondant pas à celui certifié ;
- la non-réaction du centre de certification suite à une communication mensongère sur un statut de certification d'un produit.

Un « écart » est une non-conformité des exigences applicables au centre de certification (système qualité, norme ISO 17065, accord de reconnaissance [CCRA] et [SOG-IS], [EUCC]) identifiée lors d'un audit (interne ou externe) ou remontée de façon spontanée par le personnel de l'organisme de certification.

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

Un « litige » au sens du [DECRET] - Article 15 est un appel qui a dû être soumis au Comité Directeur de la Certification pour y être tranché.

Une « amélioration » est un conseil d'évolution n'émanant pas d'une anomalie.

Un « point à surveiller » parfois appelé « point sensible » est un point spécifique, identifié lors d'un audit, qui n'engendre pas un écart au moment de l'audit mais qui doit être corrigé malgré tout pour éviter que ce ne soit le cas lors de l'audit suivant.

Une « action corrective » est une action entreprise pour éliminer la cause d'une anomalie détectée ou d'une autre situation indésirable.

Une « action préventive » est une action entreprise pour éliminer la cause d'une anomalie potentielle ou d'une autre situation potentielle indésirable.

Un « plaignant » est une personne morale ou physique qui dépose une plainte auprès du centre de certification.

Un « requérant » est une personne morale ou physique qui adresse un appel au centre de certification.

3 Enregistrement et traçabilité

Toutes les anomalies, améliorations, points sensibles, actions correctives et préventives du centre, quelles que soient leurs provenances, sont systématiquement enregistrés dans le tableau de suivi [ANO-L-01]. Ce dernier, trace également toutes les analyses de causes des anomalies. Il est régulièrement sauvegardé et archivé.

La durée et les conditions de sécurité de conservation du tableau [ANO-L-01] respectent les mêmes exigences que celles mises en place pour les autres documents gérés par le centre de certification.

3.1 Traitement des anomalies

Quelle que soit la source de l'anomalie considérée (appels, les plaintes, ou écarts), chaque anomalie est enregistrée avec un numéro unique dans l'onglet « Anomalie » de [ANO-L-01].

La cause de chaque anomalie est recherchée. Dans la mesure du possible, une action temporaire est prise visant à parer dans l'immédiat à la non-conformité, elle doit être obligatoirement suivie d'une action corrective afin de remédier définitivement à l'écart.

Les anomalies liées à un non-respect des clauses d'impartialité ou qui nuisent par exemple à l'image du centre de certification sont insérés dans l'analyse de risques permettant ainsi leur révision régulière.

3.2 Enregistrement d'une anomalie

Une plainte émanant d'une source externe à l'ANSSI peut être portée à la connaissance du centre de certification en remplissant le formulaire [ANO-F-03] disponible sur le site web www.cyber.gouv.fr. Elle doit être adressée au centre de certification soit par courriel (certification@ssi.gouv.fr), soit par courrier postal.

Une plainte interne peut être également émise par un membre de l'ANSSI en remplissant le formulaire [ANO-F-01]. Il doit être adressé par email soit directement au responsable qualité, soit à certification@ssi.gouv.fr.

Avant d'enregistrer une plainte ou un appel, le centre de certification s'assure qu'il est bien lié à ses activités de certification.

Une personne du centre, qui n'a pas pris part initialement au traitement du dossier est alors désignée pour assurer le suivi de cette anomalie particulière ; toutefois, par défaut, ces anomalies sont traitées par le chef du centre ou responsable qualité.

Dans tous les cas, le centre de certification ou le responsable qualité accuse réception de la plainte ou de l'appel reçu en indiquant :

- Si la plainte ou l'appel relèvent des activités de certification, le nom de la personne en charge de suivre le dossier, et ce :
    - via un courrier papier ou électronique quand il s'agit d'une plainte externe ;
    - via un courriel en cas de plainte interne.
- Si la plainte ou l'appel ne relève pas des activités de certification, les raisons du rejet de traitement au titre de la procédure de gestion des plaintes et appels du centre de certification.

3.3 Analyse des causes d'une anomalie

Le responsable du suivi d'une anomalie a la charge de collecter tous les éléments nécessaires à son traitement afin d'en déterminer les causes et permettre de proposer une priorité de traitement des actions correctives associées (voir 7). Il doit nécessairement informer le plaignant, dans le cas d'une plainte, ou le requérant, dans le cas d'un appel, de l'évolution du traitement de l'anomalie. Le responsable qualité ou son suppléant doivent être tenu informés de l'avancement de traitement du dossier.

Les informations recueillies sont enregistrées avec le même niveau de confidentialité et avec la même durée de conservation que les autres documents du centre de certification. Le tableau [ANO-L-01] trace également les analyses des causes et les actions entreprises pour remédier à l'anomalie.

L'analyse des causes et les propositions d'actions correctives associées à une anomalie sont validées par le chef de centre ou son adjoint, exceptées celles liées à la qualité qui peuvent être traitées par le responsable qualité ou son suppléant sans validation préalable du chef de centre ou son adjoint.

3.4 Correction d'une anomalie

Une fois une anomalie identifiée, dans la mesure du possible une action visant à y parer dans l'immédiat est prise. Cependant, cette action est temporaire, elle doit être obligatoirement suivie d'une action corrective afin de remédier définitivement à l'anomalie.

4 Traitement des améliorations et des points sensibles

Chaque amélioration et chaque point sensible est enregistré avec un numéro unique dans l'onglet « Améliorations-points sensibles » de [ANO-L-01].

Une amélioration possible, formulée lors d'un audit interne ou externe, ou par un membre du centre de certification par exemple, peut donner lieu à une action. Une amélioration correspondant à un point sensible doit quant à elle donner lieu systématiquement à une action préventive.

Une amélioration est close quand :

- le besoin d'entreprendre une action pour éviter l'apparition d'une non-conformité est non avéré ;
- une action préventive a été appliquée et son efficacité pour couvrir l'amélioration a été vérifiée.

5 Traitement des actions correctives et préventives

Les actions correctives et préventives sont enregistrées avec un numéro unique dans l'onglet « Actions et vérifications » de [ANO-L-01]. Chacune des actions proposées est validée par le chef de centre ou le responsable qualité, exceptées celles liées à la qualité qui peuvent être traitées par le responsable qualité ou son suppléant sans validation préalable du chef de centre ou son adjoint.

Des priorités de traitement sont systématiquement affectées aux actions correctives.

Le traitement des actions correctives et préventives s'effectue suivant la priorité qui lui est affectée dans l'onglet « Actions et vérifications » de [ANO-L-01].

A l'issue du traitement d'une action lié à la qualité, le responsable qualité ou son suppléant sont en charge de l'approbation de l'efficacité du traitement de l'action pour procéder à la clôture de l'action ; pour les autres actions, le chef de centre ou son adjoint sont en charge de cette approbation de l'efficacité.

La vérification de l'efficacité consiste à s'assurer que les actions prises permettent de couvrir l'anomalie afin qu'elle ne se reproduise plus. Dans le cas d'une amélioration, la vérification de l'efficacité consiste à s'assurer que les mesures prises répondent à l'objectif d'amélioration. Dans les deux cas, les mesures prises doivent être conforme aux référentiels qualité. Si toutes ces exigences sont remplies, il est alors possible de clore définitivement l'anomalie ou l'amélioration.

5.2 Particularités du traitement des actions correctives

Dans le cas d'un écart, le délai de mise en œuvre de l'action corrective doit, dans la mesure du possible, être tel qu'il puisse être clos avant le début de l'audit interne suivant.

5.3 Particularités du traitement des actions préventives

Le traitement d'une action préventive est effectué lorsque le centre de certification le juge opportun, excepté pour une action préventive émanant d'un point sensible où une priorité est alors affectée.

6 Préservation de l'impartialité

Pour éviter un éventuel conflit d'intérêt :

- aucun membre du centre de certification ne peut intervenir sur le dossier, si dans les deux années précédant la date du dépôt de la plainte ou de l'appel, cette personne a fourni des conseils sur le produit ou a été salariée du plaignant ;
- un membre du centre de certification qui a participé aux activités initiales de certification concernées peut être impliqué dans l'élaboration de la solution pour remédier à une plainte ou un appel externe mais ne peut ni décider de la solution, ni procéder à sa revue ;
- les travaux de vérification et d'approbation des bonnes pratiques, effectués normalement par le responsable qualité ou son suppléant, sont exceptionnellement confiés à un autre membre du centre dans le cas où le responsable qualité et son suppléant sont également partie prenante dans la mise en œuvre de la correction apportée.

7 Information externe lié au traitement d'une plainte ou d'un appel

Le centre de certification informe par écrit (courriel ou voie postale) le plaignant ou le requérant des conclusions du processus et des décisions prises. Lorsque la plainte ou l'appel émane d'une entité externe à l'ANSSI, la réponse rédigée par le centre de certification est signée par le Sous-directeur

Expertise ou son adjoint. En cas de plainte interne, la validation de la proposition de réponse est effectuée par le chef de bureau ou son adjoint.

A ce stade, deux cas peuvent alors survenir :

- le plaignant ou le requérant est satisfait des corrections apportées, la plainte ou l'appel peut alors être définitivement clos. Le responsable qualité ou son suppléant renseigne alors le fichier de suivi des anomalies.
- le plaignant ou le requérant n'est pas satisfait des conclusions, la plainte ou l'appel devient alors un litige.

Le responsable qualité du centre de certification ou son suppléant informe alors le plaignant ou le requérant qu'il peut saisir le président du comité directeur de la certification et son adjoint afin que l'article 10 du [REGLEMENT] soit mis en œuvre.

Nota : une correction apportée à une plainte ou un appel peut nécessiter d'être surveillée dans la durée, un risque lié à la plainte ou à l'appel est alors inséré dans l'analyse de risques permettant ainsi sa revue régulière.

ANNEXE A. Références

Référence	Document
[DECRET]	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.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the fields of Information Technology Security*, 2 juillet 2014, www.commoncriteriaportal.org,
[SOGIS]	*Mutual Recognition Agreement of Information Technology Security Evaluation*, version 3,0, 8 janvier 2010, www.sogis.eu.
[EUCC]	Schéma européen de certification de cybersécurité fondé sur les critères communs (règlement d'exécution (UE) 2024/482) et ses amendements.
[17025]	Norme EN ISO/IEC 17025 : Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais, version en vigueur.
[REGLEMENT]	ANSSI-CC-REG-01 Règlement intérieur du Comité directeur de la certification, version en vigueur.
[ANO-F-03]	ANSSI-CC-ANO-F-03 Fiche d'anomalie externe, version en vigueur.
[ANO-F-01]	ANSSI-CC-ANO-F-03 Fiche d'anomalie interne, version en vigueur.
[ANO-L-01]	ANSSI-CC-ANO-L-01 Modèle de TAC, version en vigueur.

La plupart de ces documents peuvent être consultés et téléchargés depuis le site de l'ANSSI (www.cyber.gouv.fr).