

Gestion de l'impartialité



Cybeval

Version du document	Date de modification	Objet de la modification	Editeur	Approbateur	Date d'approbation
V1.0	22/06/2024	Création	Guillaume CARAT	Mathieu BAUDAIS	30/08/2024
V1.1	31/10/2024	Modifications mineures	Guillaume CARAT	Mathieu BAUDAIS	31/10/2024
V1.2	13/03/2025	Modifications mineures	Guillaume CARAT	Mathieu BAUDAIS	13/03/2025
V1.3	22/07/2025	Changement de charte	Guillaume CARAT	Mathieu BAUDAIS	27/07/2025

Table des matières

1. Objet	3
2. Références	3
2.1. Norme NF EN ISO/IEC 17021-1 : 2015 - §5.2.3.....	3
2.2. COFRAC, CERT-REF-04, Révision 8, note de doctrine n°3.....	3
3. Processus d'évaluation des risques	3
3.1. Identification des relations entre l'organisme certificateur et des organismes apparentés	3
3.2. Analyse et documentation des conflits d'intérêts par l'organisme certificateur	3
3.3. Modalités internes à l'organisme certificateur.....	3
3.3.1. Concernant les auditeurs de l'organisme certificateur	3
3.3.2. Concernant les entreprises clientes.....	4
3.3.2.1. Questionnaire préalable envoyé au client candidat	4
3.3.2.2. Validation des auditeurs par le client candidat	4
3.3.3. Interdiction interne.....	4
3.3.4. Restrictions	4
3.3.5. Comité d'impartialité	4

1. Objet

Ce document vise à identifier les risques liés à l'impartialité et à l'indépendance entre l'organisme certificateur et une entité (*organisme ou personne apparentée*), qu'il s'agisse de liens directs ou indirects.

2. Références

2.1. Norme NF EN ISO/IEC 17021-1 : 2015- §5.2.3

2.2. COFRAC, CERT-REF-04, Révision 8, note de doctrine n°3.

3. Processus d'évaluation des risques

3.1. Identification des relations entre l'organisme certificateur et des organismes apparentés

Le processus d'évaluation des risques se matérialise par l'identification des relations entre l'organisme certificateur et les organismes apparentés.

Ces organismes sont listés au sein d'une liste documentée mise à jour régulièrement en fonction des évolutions des parties prenantes, ou dès qu'une suspicion de conflit d'intérêt apparaît, quelle que soit la source d'information, par catégories (*CYB-LIS-INT-Entites-apparentees.xlsx*).

3.2. Analyse et documentation des conflits d'intérêts par l'organisme certificateur

La liste citée au §3.1 comporte les éléments suivants :

- Organismes apparentés
- Nature du conflit d'intérêt par rapport à la certification ;
- Niveau du risque (*1=risque minime, 2=risque potentiel, 3=risque élevé, 4=risque inacceptable*) ;
- Dispositions prises pour maîtriser le risque.

3.3. Modalités internes à l'organisme certificateur

L'organisme certificateur dispose d'un processus lui permettant d'identifier, d'analyser, d'évaluer, de traiter, de surveiller et de documenter les risques liés aux conflits d'intérêts.

Ce processus est piloté par le directeur de l'organisme certificateur, avec des informations provenant de sources diverses : auditeurs, clients candidats et clients certifiés, comité d'impartialité notamment, et toute source pertinente permettant d'identifier un potentiel conflit d'intérêt.

3.3.1. Concernant les auditeurs de l'organisme certificateur

Contrôle n°1

L'organisme certificateur, avant chaque mission d'audit, demande aux auditeurs de l'équipe d'évaluation de déclarer explicitement si un conflit d'intérêt peut potentiellement exister avec le client audité.

Si la réponse est positive, il appartient au directeur d'apprécier le niveau de risque lié à cette évaluation en procédant à un entretien avec l'auditeur potentiel, et éventuellement avec le client audité, et de prendre une décision favorable ou défavorable quant à sa participation à l'audit, en documentant la décision et en apportant la preuve documentant le risque résiduel (*conformément au §5.2.3. de la norme ISO17021-1*).

Si la réponse est négative, le directeur peut assigner l'auditeur à la mission d'audit considérée.

3.3.2. Concernant les entreprises clientes

3.3.2.1. Questionnaire préalable envoyé au client candidat

Contrôle n°2

L'organisme certificateur, dans son questionnaire préalable envoyé au client candidat à la certification, demande si le client candidat a bénéficié de prestations de conseil de la part d'une entité (*organisme ou personne*).

Si, parmi les entités citées par le client candidat, un organisme apparenté de l'organisme certificateur est présent, il appartient au directeur d'évaluer le risque lié à ce cas de figure, quitte à indiquer, si le risque est considéré comme inacceptable, que l'organisme certificateur n'est pas en mesure d'effectuer l'audit de certification, conformément à sa politique d'impartialité, en documentant ce point, conformément au §5.2.3 de la norme ISO17021-1.

3.3.2.2. Validation des auditeurs par le client candidat

Contrôle n°3

L'organisme certificateur doit faire valider par le client candidat le profil des auditeurs pressentis pour réaliser la certification.

Pour ce faire, les éléments suivants sont envoyés au client, sur sa demande :

- CV de l'auditeur ;
- Attestation de compétence sur le domaine de certification souhaité si disponible ;
- NDA signé entre l'organisme certificateur et l'auditeur (*s'il s'agit d'un freelance*).

3.3.3. Interdiction interne

L'organisme certificateur s'interdit toute pratique laissant supposer que la certification sera plus simple, moins chère, ou plus rapide, si elle est précédée par des missions de conseil réalisées par des entités apparentées.

Cette mention est explicitement indiquée dans les conditions générales de ventes.

3.3.4. Restrictions

Conformément aux §5.2.5 à §5.2.13 de la norme ISO17021-1, CYBEVAL et toutes les entités sous son contrôle opérationnel s'interdisent de :

- Certifier le Système de management d'un autre organisme de certification ;
- Fournir des prestations de conseil en matière de système de management ;
- Certifier le système de management d'un client pour lequel un audit interne aurait été réalisé par une entité sous le contrôle opérationnel de CYBEVAL, sauf après une période d'exclusion de 2 ans ;
- Sous-traiter des audits à un organisme de conseil en matière de système de management (à l'exception des auditeurs individuels, sous contrat adapté avec CYBEVAL) ;
- Employer des personnes ayant effectué une prestation de conseil sur le même système de management que celui visé par l'activité de certification, sauf après une période d'exclusion de 2 ans.

Par ailleurs, CYBEVAL exige du personnel interne ou externe de l'informer de toute situation dont il a connaissance et qui pourrait créer un conflit d'intérêt. Ces données sont conservées par CYBEVAL.

3.3.5. Comité d'impartialité

Compte-tenu des spécificités de l'actionnariat de l'organisme certificateur, un comité d'impartialité composé de personnalités de références dans le domaine de la cybersécurité est mis en place, qui se réunit de manière annuelle, afin d'assurer la déconfliction éventuelle entre les clients certifiés ou candidats à la certification, et les entités apparentées de l'organisme certificateur.

Les compte-rendu de ce comité permettront de faire apparaître les conflits d'intérêt éventuels et de garantir la tenue à jour de la liste (*CYB-LIS-INT-Entites-apparentees.xlsx*).

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