



Certification EBIOS Risk Manager

Exigences relatives au schéma

Date : 01/08/2020

Statut : Approuvé

Classification : Public

Nombre de pages : 5

Responsable des travaux : Philippe LOUDENOT

Validation : Groupe de travail

Approbation : Conseil d'administration

Licence :



Historique des modifications

Date	Objet de la modification	Auteur(s)	Statut
18/12/2012	Création du document sur la base des travaux du groupe des travaux du Club EBIOS relatifs à la certification de compétences EBIOS.	Matthieu GRALL	Document de travail
09/07/2017	Adaptation du document aux évolutions de contexte à l'aide des commentaires des administrateurs. Intégration des contributions des organismes de certification (LSTI et PECB). Modification du document pour que le schéma ne nécessite plus l'accréditation par le COFRAC.	Matthieu GRALL	Approuvé
01/08/2020	Mise en cohérence avec EBIOS <i>Risk Manager</i> et prise en compte des retours de CERTI-TRUST.	Matthieu GRALL	Approuvé

Sommaire

Introduction	3
1 Exigences relatives à l'ANSSI	3
2 Exigences relatives au Club EBIOS	3
3 Exigences relatives aux organismes certificateurs	4
Références	5

Introduction

Le présent document constitue le référentiel d'**[Exigences relatives au schéma de certification]** pour une certification de personnes portant sur leurs compétences relatives à la pratique de la méthode EBIOS *Risk Manager*¹.

Il définit les exigences relatives aux principales parties prenantes :

- l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ;
- le Club EBIOS ;
- les organismes certificateurs.

Avertissement : le schéma de certification défini par les présentes exigences est valable tant qu'il n'existe pas de schéma de certification accrédité par le Comité français d'accréditation (COFRAC). Dans le cas contraire, le schéma de certification accrédité sera privilégié.

1 Exigences relatives à l'ANSSI

Exigence 1. L'ANSSI² dépose la marque « EBIOS ».

Exigence 2. L'ANSSI publie la méthode EBIOS *Risk Manager* sur Internet.

Exigence 3. L'ANSSI définit et maintient le **[Référentiel de compétences]**.

Exigence 4. L'ANSSI publie le **[Référentiel de compétences]** sur son site internet.

Exigence 5. L'ANSSI donne son avis sur les **[Exigences relatives au schéma de certification]**.

Exigence 6. L'ANSSI donne son avis sur les **[Exigences relatives aux compétences]**.

2 Exigences relatives au Club EBIOS

Exigence 7. Le Club EBIOS définit et maintient les **[Exigences relatives au schéma de certification]**.

Exigence 8. Le Club EBIOS publie les **[Exigences relatives au schéma de certification]** sur son site internet.

Exigence 9. Le Club EBIOS définit et maintient les **[Exigences relatives aux compétences]**.

Exigence 10. Le Club EBIOS publie les **[Exigences relatives aux compétences]** sur son site internet.

Exigence 11. Le Club EBIOS agréé les organismes certificateurs à délivrer des certifications de compétences EBIOS *Risk Manager* qui en font la demande et qui respectent d'une part les **[Exigences relatives au schéma de certification]** qui les concernent, et d'autre part les **[Exigences relatives aux compétences]** pour évaluer les candidats à la certification de compétences EBIOS *Risk Manager*.

Exigence 12. Dans un souci de confidentialité, et afin d'éviter tout conflit d'intérêt, les informations transmises au Club EBIOS dans le cadre du processus d'agrément d'un candidat ne seront accessibles qu'aux administrateurs du Club EBIOS ayant le besoin d'en connaître.

Exigence 13. Le Club EBIOS publie la liste des organismes certificateurs qu'il a agréés sur son site Internet.

¹ [EBIOS Risk Manager](#) est la méthode de gestion des risques numériques de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

² En pratique, la marque est actuellement déposée par l'État français, représenté par le Secrétariat général de la défense et de la sécurité nationale (SGDSN), dont l'ANSSI dépend.

- Exigence 14. Le Club EBIOS autorise les organismes certificateurs agréés à utiliser une référence textuelle à la méthode EBIOS *Risk Manager*, de type "Organisme agréé par le Club EBIOS pour procéder à la certification de compétences EBIOS *Risk Manager*".
- Exigence 15. Le Club EBIOS se réserve la possibilité de faire référence à la liste des organismes certificateurs agréés sur son site internet ou dans toute autre présentation dont il est l'auteur, sans engagement d'exhaustivité.
- Exigence 16. Le Club EBIOS retire l'agrément des organismes certificateurs qui ne respectent plus les **[Exigences relatives au schéma de certification]** ou les **[Exigences relatives aux compétences]**.
- Exigence 17. Le Club EBIOS traite les demandes de recours adressées à un organisme certificateur agréé.

3 Exigences relatives aux organismes certificateurs

- Exigence 18. Les organismes certificateurs sont accrédités par un organisme d'accréditation³ membre de l'IAF (*International Accreditation Forum*), conformément à la norme ISO/IEC 17024, dans un domaine relatif à la sécurité de l'information ou connexe à celle-ci, à délivrer des certifications de compétences.
- Exigence 19. Les organismes certificateurs développent et maintiennent leur matériel d'évaluation et documentation descriptive de leur mise en œuvre (règles de certification). Les organismes certificateurs agréés doivent développer et tenir à jour, au moins, deux jeux d'examen.
- Exigence 20. En cas de changements effectués sur la méthode EBIOS *Risk Manager*, les organismes certificateurs s'engagent à soumettre dans un délai de six mois une version à jour de leur matériel d'évaluation et des règles de certification.
- Exigence 21. Les organismes certificateurs doivent démontrer la compétence du personnel intervenant dans les activités de certification (*a minima* pour le responsable du programme de certification, le responsable des processus d'examens, ainsi que les correcteurs). Les CV du responsable du programme de certification et du responsable des processus d'examens doivent être transmis lors de la demande d'agrément. Les organismes certificateurs agréés informent le Club EBIOS du changement à ces deux postes.
- Exigence 22. Les organismes certificateurs qui demandent à être agréés fournissent au Club EBIOS un dossier comprenant :
- l'attestation d'accréditation ISO/IEC 17024 ;
 - un extrait K-bis ou équivalent ;
 - un document qui présente le programme de certification.
- Exigence 23. Les organismes certificateurs qui demandent à être agréés autorisent l'accès gratuit du Club EBIOS à leur matériel d'évaluation et fournissent, sur sa demande, la documentation descriptive de leur mise en œuvre (règles de certification), ainsi que toute autre information nécessaire.
- Exigence 24. Les organismes certificateurs agréés respectent les **[Exigences relatives au schéma de certification]** qui les concernent.
- Exigence 25. Les organismes certificateurs agréés respectent les **[Exigences relatives aux compétences]** pour évaluer les candidats à la certification de compétences EBIOS *Risk Manager*.
- Exigence 26. Les organismes certificateurs agréés respectent les dispositions prévues par le Club EBIOS pour la mise en œuvre de l'agrément.

³ En France, le Comité français d'accréditation (COFRAC).

Exigence 27. Les organismes certificateurs agréés informent l'ANSSI et le Club EBIOS de toute difficulté rencontrée dans l'application des **[Exigences relatives au schéma de certification]** qui les concernent ou dans l'application des **[Exigences relatives aux compétences]**.

Exigence 28. Les organismes certificateurs délivrent une « certification en gestion des risques numériques à l'aide de la méthode EBIOS *Risk Manager* » (libellé long) ou « certification de compétence EBIOS *Risk Manager* » (libellé court) aux candidats qui ont été évalués comme ayant atteint le niveau 2 (« Application ») du **[Référentiel de compétences]**⁴. Pour cela, deux grades sont créés :

- a. un grade « probatoire / *provisional* » est attribué au candidat en cas de succès à l'examen de certification. Cet examen, d'une durée minimale de 2h30, doit valider la connaissance de l'ensemble des exigences des thèmes 1 et 2 du **[Référentiel de compétences]** et les parties pertinentes du thème 3. Les pré-requis pour le passage de l'examen sont un diplôme universitaire ou une expérience professionnelle pertinente d'au moins 2 ans ;
- b. un grade « confirmé » est attribué à une personne certifiée au grade « probatoire / *provisional* » quand :
 - i. l'organisme de certification établit et enregistre avec la confiance suffisante que le candidat a bien suivi une part significative de la méthode en conditions réelles au moins une fois dans les trois ans précédant la demande ;
 - ii. le candidat apporte la preuve qu'il a suivi une formation de compétences EBIOS *Risk Manager* ou qu'il possède une expérience professionnelle pertinente d'au moins 2 ans.

Le maintien de la certification au niveau « confirmé » est subordonné au suivi d'une part significative de la méthode en conditions réelles au moins une fois dans les trois ans.

Exigence 29. Les organismes certificateurs agréés invitent à leur comité de certification un membre du Club EBIOS et de l'ANSSI.

Exigence 30. Les organismes certificateurs agréés font parvenir au Club EBIOS un rapport annuel d'activité sur la certification EBIOS *Risk Manager*.

Exigence 31. Les organismes certificateurs agréés font parvenir au Club EBIOS les plaintes et recours à leur encontre.

Références

[Référentiel de compétences]	<i>Certification EBIOS Risk Manager – Référentiel de compétences</i> , version du 1 ^{er} août 2020, Club EBIOS. https://club-ebios.org/site/wp-content/uploads/site-documents/ClubEBIOS-Certification-Referentiel-Competences.pdf
[Exigences relatives au schéma de certification]	<i>Certification EBIOS Risk Manager – Exigences relatives au schéma</i> , version du 1 ^{er} août 2020, Club EBIOS. https://club-ebios.org/site/wp-content/uploads/site-documents/ClubEBIOS-Certification-Referentiel-ExigencesSchema.pdf
[Exigences relatives aux compétences]	<i>Certification EBIOS Risk Manager – Exigences relatives aux compétences</i> , version du 1 ^{er} août 2020, Club EBIOS. https://club-ebios.org/site/wp-content/uploads/site-documents/ClubEBIOS-Certification-Referentiel-ExigencesCompetences.pdf

⁴ Ce niveau exige une pratique de la méthode en conditions réelles.