Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Procédure pour l'obtention du label « Logiciel EBIOS *Risk Manager* »

Labellisation des solutions logicielles EBIOS *Risk Manager*

Version 1.1 du 16/01/2019

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
28/12/2018	1.0	Première version applicable	ANSSI
16/01/2019	1.1	Mise à jour. Modification principales: • Ajout d'une durée limitée pour le prêt du logiciel à l'ANSSI. La durée correspond à la durée nécessaire pour effectuer les tests de conformité.	ANSSI

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de la Tour-Maubourg
75700 Paris 07 SP

ebios@ssi.gouv.fr

1 Préambule

Depuis 1995, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ses partenaires ont fait évoluer EBIOS, la méthode de référence pour l'analyse des risques relatifs à la sécurité du numérique. Une nouvelle version de la méthode EBIOS, intitulée EBIOS *Risk Manager*, a été publiée en octobre 2018 pour répondre de façon agile, réaliste et collaborative aux évolutions de la menace, au plus près des besoins des organisations.

Forte d'une expérience riche et d'une communauté d'utilisateurs et de contributeurs engagée au sein du Club EBIOS, cette nouvelle édition de la méthode permet une approche concrète et actuelle du management du risque numérique, adaptée à toutes les organisations.

EBIOS *Risk Manager* est une méthode d'analyse et de traitement qui a pour but de permettre aux dirigeants d'appréhender le risque cyber, au même titre que d'autres menaces stratégiques pour leur organisation, avec une compréhension partagée entre le niveau décisionnel et opérationnel.

Afin d'outiller cette nouvelle méthode, l'ANSSI souhaite permettre une identification par l'utilisateur des solutions logicielles proposées qui sont conformes à la méthode publiée. La mise à disposition d'une ou plusieurs solutions logicielles conformes à l'esprit de la méthode apparaît comme un complément attendu qui facilitera son adoption par le plus grand nombre.

Dans cette logique, l'ANSSI a mis en place un label de conformité EBIOS *Risk Manager*, accessible à tout éditeur souhaitant développer une solution logicielle conforme aux principes et aux concepts de la méthode EBIOS *Risk Manager* (cf. www.ssi.gouv.fr). Ce document accompagne la charte d'engagements pour une demande de labellisation de conformité à la méthode d'analyse de risque EBIOS *Risk Manager* par l'ANSSI.

Pour être labellisé, un éditeur de logiciel doit développer une solution logicielle conforme :
- au guide EBIOS *Risk Manager* et aux fiches méthodes associées ;
- au cahier des charges pour la labellisation ;
- à la charte d'engagements.

Ce document précise les modalités à respecter pour obtenir le label EBIOS *Risk Manager*.

2 Références

[Demande] : Formulaire de demande de labellisation.

[Procédure] : Procédure pour l'obtention du label (le présent document).

[Charte] : Charte d'engagements.

[Méthode EBIOS *Risk Manager*] : Guide EBIOS *Risk Manager* et fiches méthodes associées.

[Cahier des charges] : Cahier des charges pour la labellisation des solutions logicielles EBIOS *Risk Manager*.

[Confidentialité] : Accord de confidentialité.

Tous ces documents sont disponibles sur le site Internet de l'ANSSI, www.ssi.gouv.fr.

3 Description du processus pour une demande de labellisation

3.1 Demande de labellisation

3.1.1 Formulation de la demande de labellisation

L'éditeur de logiciel, ou candidat, qui souhaite obtenir la labellisation EBIOS *Risk Manager* de son application doit constituer un dossier de demande de labellisation, composé du formulaire [Demande] et de la [Charte].

Une fois constitué, l'éditeur transmet le dossier complété et signé à l'ANSSI par courriel à l'adresse suivante : ebios@ssi.gouv.fr.

La [Demande] doit être fournie au format modifiable (Word, OpenOffice, LibreOffice, etc.). Un original signé de la [Charte] doit être envoyé par courrier papier à l'adresse suivante :

ANSSI
Sous-Direction Stratégie – EBIOS *Risk Manager*
51, Bd de la Tour Maubourg
75700 PARIS 07 SP

3.1.2 Enregistrement de la demande par l'ANSSI

L'ANSSI accuse réception auprès de l'éditeur par voie postale ou électronique, du dossier de demande de labellisation puis désigne un chargé de labellisation au sein de la sous-direction Stratégie en charge de l'instruction de la demande.

L'accusé de réception du dossier de demande ne vaut pas acceptation de la demande de labellisation.

3.1.3 Décision d'acceptation de demande de labellisation

Après vérification de la cohérence de la demande de labellisation, de la signature de la [Charte] et de la [Demande] dument complétée, l'ANSSI se prononce sur l'acceptation du dossier de demande de labellisation.

Si la demande est estimée non cohérente avec la labellisation, ou si les éléments demandés ne sont pas correctement renseignés, le chargé de labellisation sollicite le candidat pour apporter les corrections nécessaires aux éléments demandés sous 15 jours ouvrés.

3.2 Évaluation de la conformité des solutions logicielles aux exigences du [Cahier des charges]

Le chargé de labellisation est en charge de l'instruction du dossier. Il s'assure que la solution logicielle soumise à labellisation est conforme à la [Méthode EBIOS *Risk Manager*], ainsi qu'à l'ensemble des exigences du [Cahier des charges].

Pour être évalué, la solution logicielle concernée avec le scénario « Société de biotechnologie fabricant des vaccins », (évoqué dans le guide EBIOS Risk Manager) implémenté et son guide d'utilisation doivent être envoyé par tout moyen après que l'ANSSI se soit prononcé sur l'acceptation du dossier de demande de labellisation. La solution logicielle est conservé par l'ANSSI jusqu'à la décision de labellisation. En cas de recours gracieux, le logiciel devra être renvoyé dans les mêmes conditions pour permettre son réexamen. »

Le chargé de labellisation peut, en tant que de besoin, s'appuyer sur un ou plusieurs experts de l'ANSSI pour valider la pertinence de certains points du dossier.

Des demandes de compléments d'informations peuvent être formulées au candidat (par exemple, informations manquantes ou ambiguës par rapport aux exigences). Ce dernier dispose de 15 jours ouvrés pour y répondre. A défaut, la labellisation sera rejetée.

Des demandes de corrections de la solution logicielle peuvent être formulées au candidat. Le chargé de labellisation sollicite le candidat pour apporter les corrections nécessaires aux éléments demandés sous 2 mois. A défaut, la labellisation sera rejetée.

3.3 Décision de labellisation

Le sous-directeur Stratégie de l'ANSSI transmet un avis sur la labellisation au directeur général de l'ANSSI, qui prononce la décision de labellisation ou son refus. La décision est envoyée par courrier à la personne en charge du dossier chez le candidat. Elle peut être de deux natures :

- **décision de labellisation de la solution logicielle** : une référence de label est attribuée et les informations sur la solution logicielle sont publiées sur le site Internet de l'ANSSI sous le statut « labellisée » ;
- **décision de non labellisation** : le demandeur est informé des raisons pour lesquelles la solution logicielle ne répond pas aux exigences de labellisation. Il est informé des voies et délais de recours.

3.4 Validité d'une labellisation

La labellisation est valable trois ans.

3.5 Contestation suite à un refus de labellisation

Un éditeur de logiciel recevant un avis négatif pour une solution logicielle qu'il a proposée peut contester cet avis par un recours gracieux dans les deux mois qui suivent la réception de l'avis par courrier papier ou courriel aux mêmes coordonnées que pour la demande initiale en précisant les éléments qu'il conteste.

En l'absence de réponse de l'ANSSI sous deux mois calendaires, la demande est considérée comme rejetée.

Le fait pour un candidat d'avoir eu un avis négatif n'empêche pas le dépôt d'une nouvelle [Demande] par ce candidat dans la limite d'une demande par année calendaire pour une même version d'un logiciel.

4 Suivi de la labellisation

L'ANSSI peut vérifier à tout moment que les exigences du [Cahier des charges] et de la [Méthode EBIOS *Risk Manager*] continuent d'être respectées par chaque logiciel labellisé.

Cette vérification peut se faire par demande d'informations et/ou par entretien avec le candidat.

Si le logiciel ne respecte plus les exigences du [Cahier des charges] ou de la [Méthode EBIOS *Risk Manager*], ou en cas d'absence de réponse suite à une demande d'information ou d'entretien avec le candidat, l'ANSSI déclenche le processus de retrait de la labellisation.

5 Modifications des éléments de labellisation d'un logiciel labellisé

En cas de modification des éléments entrant dans les conditions de la labellisation tels qu'ils ont été décrits précédemment, il appartient au candidat de les signaler à l'ANSSI au plus tôt et si possible, avant que ces modifications prennent effet.

Le signalement des modifications se fait par renvoi d'un formulaire de demande de labellisation [Demande], dans lequel doivent apparaitre la description des modifications ainsi que les évolutions mineures et majeures par rapport à la version labellisée.

La [Demande] indique pour chaque élément si la modification concernée est mineure ou majeure :

- les modifications mineures font l'objet d'un traitement simplifié et ne modifient pas la référence de la labellisation ;
- les modifications majeures font l'objet d'un traitement équivalent à une labellisation initiale et peuvent modifier la référence de la labellisation initiale.

L'ANSSI fait connaitre sa décision quant à la conséquence des modifications selon les modalités suivantes :

- par simple courriel pour confirmer la prise en compte d'une modification mineure ou la requalification d'une modification majeure en modification mineure ;
- par courrier signifiant que le dossier est enregistré et en cours de traitement pour une modification majeure ou la requalification d'une modification mineure en modification majeure.

6 Renouvellement de la labellisation

Il appartient à l'éditeur qui développe un logiciel labellisé de demander le renouvellement de sa labellisation.

Pour ce faire, il adresse sa demande à l'ANSSI, dans les mêmes conditions qu'une demande initiale, **au plus tard trois mois avant l'échéance de la validité de sa labellisation en cours**.

Le dossier de demande de renouvellement est identique à celui de la demande initiale. Afin de faciliter le traitement de la demande, les modifications entre le dossier initial ou précédent et le dossier de renouvellement doivent être clairement indiquées par tout moyen (descriptions détaillées, changement de couleur dans le texte modifié, etc.).

Le traitement de la demande de renouvellement est identique à la demande initiale.

7 Procédure de retrait de la labellisation

Si l'ANSSI considère, au cours de la période de validité du label, que la solution logicielle labellisée ne répond plus aux exigences du [Cahier des charges] ou de la [EBIOS *Risk Manager*], elle peut prononcer le retrait du label.

Pour ce faire, l'ANSSI adresse un courrier à l'éditeur concerné pour lui notifier son intention d'engager une procédure de retrait de la labellisation.

L'éditeur dispose alors de quinze jours calendaires, à compter de la réception du courrier de l'ANSSI, pour faire valoir ses observations.

Après étude des observations et éventuelle demandes d'informations et/ou entretiens avec le candidat, l'ANSSI informe l'éditeur par courrier de sa décision concernant la procédure de retrait de labellisation initialement engagée.

8 Fin de la labellisation

Il est mis fin à la labellisation d'un logiciel lorsque :

1. l'éditeur qui développe la solution logicielle le demande explicitement par courrier signé et transmis par voie postale ;
2. l'éditeur n'a pas sollicité de renouvellement auprès de l'ANSSI à la date d'échéance de la labellisation ;
3. l'ANSSI prononce le retrait du label dans les conditions prévues au paragraphe 7.

Dans les deux premiers cas, l'ANSSI adresse un courrier à l'éditeur, lui confirmant ou l'informant du retrait de la labellisation du logiciel concerné.

Dans tous les cas, lorsqu'il est mis fin à la labellisation, les droits et obligations imposés par la labellisation à l'ANSSI et à l'éditeur cessent. L'éditeur cesse sans délai toute utilisation du nom EBIOS *Risk Manager* ou de son visuel.