Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Cahier des charges

Labellisation des solutions logicielles EBIOS *Risk Manager*

Version 2.0 du 24/10/2019

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
28/12/2018	1.0	Première version applicable pour le mode standalone	ANSSI
24/10/2019	2.0	Exigences complémentaires pour le mode client/serveur	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

Sommaire

1. Introduction

Ce document a pour but de rassembler les exigences de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en vue de la labellisation d'un logiciel qui instancie la méthode EBIOS *Risk Manager*.

Il détaille les attentes de l'ANSSI par rapport au projet et décrit les besoins fonctionnels et non fonctionnels.

La première partie du document présente le contexte et l'objectif de la labellisation.

La seconde décrit les spécifications à respecter pour l'obtention du label EBIOS *Risk Manager*.

Une annexe donne des recommandations relatives à l'application et à son ergonomie.

2. Description du projet

2.1 Présentation du contexte

L'ANSSI est rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDSN), service du Premier ministre chargé d'assister le chef du Gouvernement dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

Elle a notamment pour mission d'apporter son concours aux administrations, aux opérateurs d'importance vitale et aux opérateurs de services essentiels dans la sécurisation et la défense de leurs systèmes d'information. Ainsi, tient-elle à jour un important référentiel méthodologique et technique aidant à la spécification et à la mise en œuvre de systèmes et de produits sécurisés.

Dans ce cadre, l'ANSSI a élaboré la méthode EBIOS *Risk Manager* qui permet d'étudier les risques relatifs à la sécurité numérique. En 2018, une nouvelle version de la méthode a été publiée dans le but de la rendre plus souple, de prendre en compte les retours d'expérience accumulés depuis ces dernières années, notamment grâce au Club EBIOS, et de l'adapter aux évolutions de la menace cyber.

Afin d'outiller cette nouvelle méthode, l'ANSSI souhaite s'appuyer sur des partenaires externes, éditeurs de logiciels. 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.

L'attribution d'un label de conformité EBIOS *Risk Manager* est accessible à tout éditeur ayant développé une solution logicielle conforme aux principes et aux concepts de la méthode EBIOS *Risk Manager*.

Le présent cahier des charges précise les exigences à respecter.

L'ensemble du référentiel EBIOS *Risk Manager* (guide et fiches méthodes associées) est disponible sur le site Internet de l'ANSSI, www.ssi.gouv.fr.

Toutes les notions utilisées dans le présent cahier des charges sont à comprendre dans le sens que leur donne le guide EBIOS *Risk Manager* publiée par l'ANSSI.

2.2 Objectif de la labellisation

La labellisation consiste à valider un outil fonctionnel, simple et ergonomique qui permet la mise en œuvre complète de la méthode EBIOS *Risk Manager*.

Le logiciel labellisé devra avoir la capacité :

- de réaliser l'ensemble des ateliers, activités et actions de la méthode ;
- d'adapter la démarche et les métriques en fonction du sujet étudié et de l'objectif attendu ;
- de collecter, importer les données d'entrée nécessaires à une étude ;

- de faciliter le déroulement de la méthode de bout-en-bout par une ergonomie pensée et adaptée;
- de permettre le suivi des révisions successives d'une analyse de risques ;
- d'apposer une mention de protection à l'analyse de risques comme prévue par l'instruction interministérielle 901[1] ;
- de produire des livrables et d'exporter les données de sortie à l'issue de chaque atelier ;
- de produire aisément les livrables issus d'une étude ;
- de respecter la sémantique du guide ;
- d'assurer un niveau minimal de sécurité pour les données stockées dans la solution logicielle labélisée.

Pour sa labellisation, la solution logicielle devra être fournie à l'ANSSI et l'exemple fictif qui sert de fil conducteur dans le guide (société de biotechnologie fabriquant des vaccins) devra être implémenté afin que chaque point de la méthode puisse être contrôlé.

2.3 Synthèse des exigences applicables

Le label EBIOS *Risk Manager* se décline selon deux types de labellisation en fonction du mode de fonctionnement du logiciel.

- Le logiciel fonctionnant de manière autonome sur une station de travail est soumis aux exigences relevant du mode « standalone ».
- Le logiciel fonctionnant au sein d'une infrastructure réseau privée et dans un environnement client–serveur est soumis aux exigences relevant du mode « Client-Serveur ».

La grille ci-dessous décline les exigences décrites dans la suite du document, et applicables au logiciel en fonction de son mode de fonctionnement.

Exigences	**Label EBIOS *Risk Manager***	
	Standalone	**Client-Serveur**
Spécifications générales		
Spécifications logicielles	X	X
Classification de l'analyse de risque	X	X
Guide d'utilisation	X	X
Gestion des versions des analyses des risques	X	X
Spécifications détaillées		
Atelier 1 – Cadrage et socle de sécurité	X	X
Atelier 2 – Sources de risque	X	X
Atelier 3 – Scénarios stratégiques	X	X
Atelier 4 – Scénarios opérationnels	X	X
Atelier 5 – Traitement du risque	X	X
Exigences de sécurité		
Mécanismes d'identification et d'authentification et de cloisonnement des profils		X

[1] https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-interministerielle-n-901/

Exigences	Label EBIOS *Risk Manager*	
	Standalone	**Client-Serveur**
Confidentialité des données		X
Journalisation		X
Revue des politiques internes de développement		X
Maintien en condition de sécurité		X
Conditions générales d'emploi et d'usage		X

3. Spécifications générales

3.1 Spécifications logicielles

Le logiciel devra fonctionner de manière autonome sur une station de travail (format « standalone ») ou selon un environnement client/serveur. Il devra permettre de dérouler de bout-en-bout les 5 ateliers de la méthode EBIOS *Risk Manager*:

- Atelier 1 – Cadrage et socle de sécurité ;
- Atelier 2 – Sources de risque ;
- Atelier 3 – Scénarios stratégiques ;
- Atelier 4 – Scénarios opérationnels ;
- Atelier 5 – Traitement du risque.

Il doit être possible de travailler de façon agile, c'est-à-dire itérative et incrémentale et d'exporter des livrables pour chacune des étapes.

Leur contenu est détaillé, pour chaque atelier, dans le guide EBIOS *Risk Manager* (« Les données de sortie »).

3.2 Mention de protection de l'analyse de risque

L'application permet de porter une mention (obligatoire) de protection à l'analyse de risque. Par exemple, non protégée, sensible, restreinte ou confidentielle.

3.3 Guide d'utilisation

L'éditeur de l'application met à disposition un guide d'utilisation pour l'installation du logiciel, le lancement des fonctions de base, et propose des recommandations d'utilisation (en particulier lorsque des données sensibles ou devant porter une mention de protection seront utilisées pour produire l'analyse de risque).

3.4 Gestion des versions des analyses des risques

L'application devra pouvoir gérer les versions successives d'une même analyse de risque :

- en permettant à un utilisateur qui ouvrirait une analyse de risque de choisir s'il souhaite la mettre à jour dans le cadre d'un cycle opérationnel ou stratégique (exemple : case à cocher) ;
- en incrémentant la version x.y de l'analyse de risque (par exemple incrément du « y » pour une mise à jour opérationnelle et du « x » pour une mise à jour stratégique) ;
- en demandant à l'utilisateur quelles sont les modifications majeures apportées lors d'une mise à jour (exemple : champ texte renseigné librement) et quels ateliers sont concernés (exemple : cases à cocher) ;
- en proposant une synthèse des mises à jour effectuées (*à minima* identification des ateliers et activités ayant fait l'objet de modifications).

4. Spécifications fonctionnelles

4.1 Atelier 1 – Cadrage et socle de sécurité

Activité 1.1 : Définir le cadre de l'étude

Référence	Exigence
EXI_M1_01	L'application permet de renseigner les éléments du cadre de l'étude : - les objectifs de l'étude ; - les participants à l'étude (par exemple sous forme de matrice de type RACI) ; - le cadre temporel de l'étude (durée des cycles opérationnel et stratégique) ; - les éléments de planning projet (par exemple date des ateliers, contraintes du projet).
EXI_M1_02	L'utilisateur peut ajouter, modifier, supprimer les éléments du cadre de l'étude.
EXI_M1_03	L'application prévoit d'éditer ou d'exporter les éléments du cadre de l'étude.

Activité 1.2 : Définir le périmètre métier et technique

(Cf. fiche méthode n°1 EBIOS *Risk Manager*: définir le périmètre métier et technique et fiche méthode n°2 EBIOS *Risk Manager*: identifier les biens supports)

Référence	Exigence
EXI_M1_04	L'application permet de recenser les missions de l'objet étudié. Pour chaque mission, il est possible de saisir une description.
EXI_M1_05	L'application permet de recenser les valeurs métier associées à l'objet de l'étude. Pour chaque valeur métier, l'utilisateur peut saisir sa dénomination, la nature de la valeur métier (par exemple : processus ou information), et une description. A cette valeur métier, est associée une entité ou une personne responsable (interne ou externe à l'organisme).
EXI_M1_06	L'application recense les biens supports associés à chaque valeur métier définie. Pour chaque bien support, l'utilisateur saisit sa dénomination et sa description détaillée. A ce bien support, est associée une entité ou une personne responsable (interne ou externe à l'organisme).
EXI_M1_07	L'utilisateur peut ajouter, modifier, supprimer des éléments du périmètre métier technique.
EXI_M1_08	L'application prévoit d'éditer, d'importer ou d'exporter les éléments du périmètre métier et technique. (Optionnel) Des options de filtre sont proposées (ex : ne faire apparaitre que les biens supports associés à une valeur métier choisie). Un exemple figure en p.22-23 du guide EBIOS *Risk Manager* v1.1.

Activité 1.3 : Identifier les événements redoutés et évaluer leur niveau de gravité

(Cf. fiche méthode n°3 : évaluer la gravité des impacts des événements redoutés)

Référence	Exigence
EXI_M1_09	L'application prévoit d'ajouter, modifier et supprimer des événements redoutés.
EXI_M1_10	L'application permet d'associer à chaque valeur métier un ou plusieurs événements redoutés.
EXI_M1_11	L'application prévoit une échelle de gravité décrivant des niveaux et pour chacun d'entre eux une description. Des fonctionnalités permettent la création, la mise à jour et la suppression d'échelles de gravité. Un exemple figure en p.26 du guide EBIOS *Risk Manager* v1.1.
EXI_M1_12	A une valeur métier et un événement redouté peuvent être associés un ou plusieurs impacts (par exemple : juridique, financier, image).
EXI_M1_13	L'application permet d'associer à chaque couple valeur métier / événement redouté un niveau de gravité de l'échelle de gravité.
EXI_M1_14	L'application prévoit d'éditer ou d'exporter les évènements redoutés. Un exemple figure en p.27 du guide EBIOS *Risk Manager* v1.1.

Activité 1.4 : Déterminer le socle de sécurité

Référence	Exigence
EXI_M1_15	L'application permet à l'utilisateur de renseigner lui-même les référentiels et les exigences de sécurité associées. (Optionnel) L'utilisateur peut importer des référentiels de sécurité, à partir de fichiers.
EXI_M1_16	Pour chaque référentiel de sécurité, l'application propose de sélectionner des exigences de sécurité respectées (à l'aide, par exemple, de cases à cocher à choix multiples afin de permettre à l'utilisateur de sélectionner/désélectionner l'intégralité du référentiel ou chacune des exigences du référentiel indépendamment, s'il/elle est appliqué(e)).
EXI_M1_17	L'application permet à l'utilisateur de rendre visible ou non le détail des exigences de chaque référentiel de sécurité par simple clic.
EXI_M1_18	Un indicateur permet à l'utilisateur de visualiser rapidement l'état d'application des référentiels listés (exemple : indicateur de couleur : vert pour « appliqué sans restriction », orange pour « appliqué avec restrictions », rouge pour « non appliqué »)
EXI_M1_19	Pour chaque exigence du référentiel, l'utilisateur peut saisir des commentaires ou des informations de justification de la dérogation dans un champ texte.
EXI_M1_20	L'utilisateur peut ajouter, modifier, supprimer les référentiels de sécurité. Il peut modifier leur état d'application. Les indicateurs peuvent être modifiés.

Référence	Exigence
EXI_M1_21	L'application prévoit d'éditer ou d'exporter le socle de sécurité. (Optionnel) Des options de filtre sont proposées (exemple : ne faire apparaitre que les exigences non respectées). Un exemple d'état figure en p.29 du guide EBIOS *Risk Manager* v1.1.

4.2 Atelier 2 – Sources de risque

Activité 2.1 : Identifier les sources de risque et les objectifs visés

(Cf. fiche méthode n°4 : identifier et caractériser les sources de risque)

Référence	Exigence
EXI_M2_01	L'application propose par défaut des catégories génériques de sources de risques et d'objectifs visés.
EXI_M2_02	L'application permet de compléter ou modifier ces catégories (exemple : ajouter, supprimer, renommer une catégorie de source de risque).
EXI_M2_03	L'utilisateur saisit manuellement les objectifs visés pour chaque source de risque identifiée. Un exemple figure en p.35 du guide EBIOS *Risk Manager* v1.1. (Optionnel) L'utilisateur peut importer et fusionner des bases de connaissances de catégories de source de risques et d'objectifs visés, à partir de fichiers.

Activité 2.2 : Evaluer les couples source de risque/objectif visé

Référence	Exigence
EXI_M2_04	A chaque couple source de risque/objectif visé sont associés des critères de caractérisation comme le degré de motivation, le niveau des ressources, le niveau d'activité.
EXI_M2_05	L'application évalue selon une métrique le niveau de pertinence du couple source de risques/objectif visé ou permet de saisir directement la pertinence de chaque couple.
EXI_M2_06	L'application prévoit d'éditer et d'exporter les couples source de risque/objectif visé et leur évaluation. Un exemple figure en p.37 du guide EBIOS *Risk Manager* v1.1. (Optionnel) Des options de filtre sont proposées (exemple : ne faire apparaitre que certaines sources de risque).

Activité 2.3 : Sélectionner les couples source de risque/objectif visé jugés prioritaires

Référence	Exigence
EXI_M2_07	L'application propose de sélectionner les couples source de risque/objectif visé retenus pour la suite de l'analyse.
EXI_M2_08	L'application permet de représenter les couples source de risque/objectif visé sur des cartographies visuelles de type radar. (Optionnel) Des options de filtre sont proposées (exemple : ne faire apparaitre que des éléments associés à certaines catégories).

4.3 Atelier 3 – Scénarios stratégiques

Activité 3.1 : Construire la cartographie de menace numérique de l'écosystème

(Cf. fiche méthode n°5 : construire la cartographie de menace numérique de l'écosystème)

Référence	Exigence
EXI_M3_01	L'application propose par défaut des catégories génériques de parties prenantes tant internes qu'externes (par exemple, les parties prenantes externes pourront être de type clients, fournisseurs, partenaires).
EXI_M3_02	L'utilisateur peut ajouter, modifier, supprimer les catégories des parties prenantes.
EXI_M3_03	(Optionnel) L'application permet d'importer et fusionner des bases de connaissances de catégories de parties prenantes
EXI_M3_04	L'utilisateur recense les parties prenantes de l'écosystème de l'objet étudié. Chaque partie prenante est caractérisée par un nom, une description et est associée à une catégorie (cf. EXI_M3_01).
EXI_M3_05	A chaque partie prenante de l'écosystème sont associées deux valeurs, correspondant au niveau de menace initial et résiduel de celle-ci.
EXI_M3_06	L'application permet de calculer le niveau de menace initial de chaque partie prenante sur la base de critères et de métriques d'évaluation.
EXI_M3_07	L'application propose par défaut une grille d'évaluation sur la base des quatre critères suivants : dépendance, pénétration, maturité SSI, confiance.
EXI_M3_08	L'ajout, la modification, la suppression des métriques de cotation est rendue possible. (Optionnel) L'application permet d'importer et fusionner des bases de connaissances contenant des critères et métriques d'évaluation de la menace.
EXI_M3_09	Le niveau de menace d'une partie prenante est calculé selon la formule : (Dépendance x Pénétration) / (Maturité SSI x Confiance). La formule de calcul du niveau de menace peut être modifiée afin de pondérer chacun des critères si nécessaire.
EXI_M3_10	La valeur du niveau de menace initial de chaque partie prenante peut être « forcée ».

Référence	Exigence
EXI_M3_11	Une fonctionnalité rend possible la saisie des valeurs de seuils correspondant à la zone de danger, à la zone de contrôle et à la zone de veille.
EXI_M3_12	L'application permet de représenter le niveau de menace des parties prenantes sur une cartographie visuelle de type radar (appelée « cartographie de menace initiale »). Un exemple figure en p.45 du guide EBIOS *Risk Manager* v1.1.
EXI_M3_13	L'application permet de sélectionner les parties prenantes estimées comme critiques par l'utilisateur. Les parties prenantes considérées comme critiques peuvent être distinguées des autres, visuellement, sur la cartographie de menace.
EXI_M3_14	L'utilisateur peut ajouter, modifier, supprimer les parties prenantes, les valeurs des critères d'évaluation et les valeurs de seuil des différentes zones. L'application devra permettre de distinguer visuellement une modification des valeurs faite de manière intentionnelle par l'utilisateur.
EXI_M3_15	L'application prévoit d'éditer et d'exporter la cartographie de menace initiale. (Optionnel) Des options de filtre sont proposées.

Action 3.2 : Elaborer des scénarios stratégiques

Référence	Exigence
EXI_M3_16	L'application permet de construire des scénarios stratégiques et de distinguer les chemins d'attaque qui les constituent. Pour chaque scénario stratégique peuvent être associés un nom et une description dans des champs texte. Il en est de même pour les chemins d'attaque des scénarios.
EXI_M3_17	Chaque scénario stratégique est associé à un couple source de risque / objectif visé sélectionné dans l'atelier 2. Il se présente sous la forme d'un séquencement d'événements soit liés à une partie prenante de l'écosystème (événements intermédiaires), soit liés à une valeur métier de l'objet de l'étude (événements redoutés). L'application facilite la construction des scénarios en permettant d'associer chaque événement intermédiaire à une partie prenante (liste, cf. activité 3.1) et chaque événement redouté à une valeur métier (liste, cf. atelier 1). Des exemples figurent en p.48-49 du guide EBIOS *Risk Manager* v1.1.
EXI_M3_18	(Optionnel) L'espace de construction des scénarios peut être rempli grâce à des glisser-déposer d'évènements proposés sur le côté de l'espace de travail.
EXI_M3_19	La gravité d'un scénario stratégique correspond à la gravité des événements redoutés impliqués dans les chemins d'attaque du scénario.
EXI_M3_20	Il est possible de « forcer » le niveau de gravité d'un scénario stratégique.

Référence	Exigence
EXI_M3_21	L'application prévoit d'éditer et d'exporter les scénarios stratégiques avec leurs chemins d'attaque associés. Un exemple figure en p.50 du guide EBIOS *Risk Manager* v1.1. (Optionnel) Des options de filtre peuvent être proposées.

Action 3.3 : Définir des mesures de sécurité sur l'écosystème

(Cf. fiche méthode n°6 : définir des mesures de sécurité pour l'écosystème)

Référence	Exigence
EXI_M3_22	Il est possible d'associer à chaque partie prenante des mesures de sécurité ou un niveau cible à atteindre, en lien avec les critères d'évaluation retenus pour l'étude (par exemple : abaisser le niveau « pénétration » de la partie prenante de 4 à 3).
EXI_M3_23	A chaque partie prenante de l'écosystème est associé un niveau de menace résiduel (suite à l'application des mesures de sécurité). Cette valeur est calculée selon la formule choisie pour établir le niveau de menace initial.
EXI_M3_24	L'application permet de représenter le niveau de menace résiduel des parties prenantes sur une cartographie visuelle de type radar (appelée « cartographie de menace résiduelle »), selon le même modèle que la cartographie de menace initiale.
EXI_M3_25	Les valeurs de seuils correspondant à la zone de danger, à la zone de contrôle et à la zone de veille sont identiques sur les cartographies de menace initiale et résiduelle.
EXI_M3_26	L'application prévoit d'éditer et d'exporter la cartographie de menace résiduelle, ainsi que le tableau de synthèse des mesures de sécurité sur l'écosystème. (Optionnel) Des options de filtre peuvent être proposées.

4.4 Atelier 4 – Scénarios opérationnels

Activité 4.1 : Elaborer les scénarios opérationnels

(Cf. fiche méthode n°7 : construire des graphes d'attaque)

Référence	Exigence
EXI_M4_01	L'application permet de construire des scénarios opérationnels associés aux scénarios stratégiques. Pour chaque scénario opérationnel, il est possible d'associer un nom, une description dans des champs texte et un scénario stratégique (via une liste déroulante par exemple). Il en est de même pour les modes opératoires des scénarios. Un exemple figure en p.61 du guide EBIOS *Risk Manager* v1.1.
EXI_M4_02	(Optionnel) La construction des scénarios opérationnels devra être simple et intuitive. Par exemple, l'espace de construction des scénarios pourra être rempli grâce à des glisser-déposer d'actions élémentaires proposées sur le côté de l'espace de travail.

Référence	Exigence
EXI_M4_03	L'application propose par défaut une liste d'actions élémentaires, organisées selon des catégories d'actions d'une séquence d'attaque type. Il est possible de modifier cette base (exemple : modifier l'intitulé d'une action élémentaire ou d'une phase de la séquence d'attaque, ajouter une phase et l'associer à des actions élémentaires existantes, créer des actions élémentaires et les associer à une phase, ajouter une catégorie d'actions élémentaires, etc.).
EXI_M4_04	(Optionnel) Il est possible d'importer et fusionner des bases de connaissances structurées d'actions élémentaires associées à une séquence d'attaque type.
EXI_M4_05	Chaque action élémentaire d'un scénario opérationnel est associée à un bien support sur lequel elle s'applique.

Activité 4.2 : Evaluer la vraisemblance des scénarios opérationnels

(Cf. fiche méthode n° 8 : évaluer la vraisemblance des scénarios opérationnels)

Référence	Exigence
EXI_M4_06	L'application permet de sélectionner la méthode d'évaluation de vraisemblance souhaitée (expresse, standard, avancée) qui s'appliquera à l'ensemble des scénarios opérationnels de l'analyse de risque. Selon le choix de la méthode d'évaluation, l'application propose les critères et métriques de cotation associés (voir ci-après). 1) Méthode expresse ; 2) Méthode standard ; 3) Méthode avancée.
EXI_M4_07	L'application permet de changer à tout moment (en cours d'analyse) la méthode d'évaluation de la vraisemblance des scénarios opérationnels.
EXI_M4_08	Méthode expresse : l'application permet d'associer une vraisemblance globale au scénario, et si l'utilisateur le souhaite à chacun des modes opératoires du scénario.
EXI_M4_09	Méthode standard : l'application permet d'associer une probabilité de succès à chaque action élémentaire.
EXI_M4_10	Méthode avancée : l'application permet d'associer une probabilité de succès et une difficulté technique à chaque action élémentaire.
EXI_M4_11	L'application propose par défaut des grilles génériques de cotation de la vraisemblance globale, de la probabilité de succès et de la difficulté technique. Il est possible de modifier ces grilles (exemple : modifier l'intitulé des classes de vraisemblance, modifier l'intitulé ou le seuil des niveaux de vraisemblance). Un exemple d'échelle de vraisemblance globale figure en p.64 du guide EBIOS *Risk Manager* v1.1. Des métriques détaillées sont proposées dans la fiche méthode n°8.
EXI_M4_12	(Optionnel) Il est possible d'importer des métriques de cotation.

Référence	Exigence
EXI_M4_13	Méthodes standard et avancée : l'application propose des algorithmes de calcul de la vraisemblance globale d'un scénario à partir de la cotation des actions élémentaires, selon le choix de la méthode d'évaluation standard/avancée. Si plusieurs algorithmes de calculs sont proposés, l'utilisateur peut sélectionner l'algorithme de son choix dans une liste déroulante par exemple.
EXI_M4_14	L'application permet de faciliter la cotation des actions élémentaires ou des modes opératoires en éditant une base de connaissances telle que celle qui figure à la fin de la fiche méthode n°8. L'application permet de modifier cette base de connaissance.
EXI_M4_15	La vraisemblance globale d'un scénario opérationnel peut être « forcée ».
EXI_M4_16	Méthodes standard et avancée : l'application permet d'identifier et visualiser les actions élémentaires les plus critiques (les plus probables et/ou faciles), ainsi que le mode opératoire le plus vraisemblable (celui de moindre effort).
EXI_M4_17	L'application permet d'éditer et d'exporter les scénarios opérationnels, ainsi qu'un tableau de synthèse des scénarios, et si l'utilisateur le souhaite, des modes opératoires. Des exemples figurent en p.65 du guide EBIOS *Risk Manager* v1.1 et au chapitre 4 de la fiche méthode n°8. (Optionnel) Des options de filtre peuvent être proposées (par exemple : ne faire apparaitre que les scénarios dont la vraisemblance dépasse un seuil donné).

4.5 Atelier 5 – Traitement du risque

Activité 5.1 : Réaliser la synthèse des scénarios de risque

Référence	Exigence
EXI_M5_01	L'application permet de visualiser la cartographie du risque initial des scénarios de risque selon leur gravité et vraisemblance globale. Un exemple figure en p.70 du guide EBIOS *Risk Manager* v1.1.
EXI_M5_02	L'application permet d'éditer et d'exporter la cartographie du risque initial, ainsi que le tableau de synthèse des scénarios de risque. (Optionnel) Des options de filtre sont proposées (par exemple n'exporter que les scénarios relatifs à une catégorie de source de risque et de gravité supérieure à un seuil donné).
EXI_M5_03	(Optionnel) L'application permet d'éditer une matrice de traçabilité/couverture entre les événements redoutés de l'atelier 1 et les scénarios de risque traités dans les ateliers 3 et 4. L'application met en évidence les éventuels événements redoutés (et valeurs métier associées) qui n'apparaissent dans aucun scénario de risque.

Activité 5.2 : Définir la stratégie de traitement du risque et les mesures de sécurité

Référence	Exigence
EXI_M5_04	Pour chaque scénario de risque, on associe un indicateur de couleur représentant la stratégie de traitement du risque (exemple : vert pour « acceptable en l'état » orange pour « tolérable sous contrôle », rouge pour « inacceptable »). Un exemple figure en p.72-73 du guide EBIOS *Risk Manager* v1.1. (Optionnel) La coloration est rendue possible directement, par clic, depuis la cartographie du risque initial.
EXI_M5_05	L'application permet d'associer aux scénarios de risque des mesures de sécurité. Ces mesures s'appliquent à l'objet de l'étude (valeur métier, bien support) ou à des parties prenantes de l'écosystème.
EXI_M5_06	L'application permet d'associer à chaque mesure de sécurité : - une catégorie (gouvernance, protection, défense, résilience : cf. fiche méthode n°9 : structurer les mesures de traitement du risque), - l'élément concerné (valeur métier, bien support, partie prenante d'écosystème), - un responsable, - un coût, - une échéance - un pourcentage d'avancement de la mise en œuvre - des commentaires additionnels L'ensemble des mesures de sécurité est ainsi formalisé dans un plan d'amélioration continue de la sécurité (sous la forme d'un tableau par exemple). Un exemple figure en p.75 du guide EBIOS *Risk Manager* v1.1.
EXI_M5_07	L'application permet l'édition et l'exportation de tout ou partie du plan d'amélioration continue de la sécurité. La liste des mesures peut être triée ou filtrée par catégorie, responsable, coût, échéance, etc.

Activité 5.3 : Evaluer et documenter les risques résiduels

Référence	Exigence
EXI_M5_08	A chaque scénario de risque sont associées une gravité et une vraisemblance résiduelles suite à l'application des mesures de sécurité. Cette réévaluation s'effectue soit à partir de la cartographie du risque initial (en « glissant » manuellement les risques concernés de leur position initiale gravité/vraisemblance à la position résiduelle), soit depuis le tableau de synthèse des scénarios de risque (colonnes gravité et vraisemblance résiduelles). La cartographie du risque résiduelle et le tableau de synthèse des scénarios de risque sont mis à jour automatiquement selon les modifications apportées à l'un ou à l'autre.
EXI_M5_09	Il est possible pour l'utilisateur de s'affranchir des calculs automatiques des valeurs de gravité et vraisemblance résiduelles, et de renseigner les valeurs qui pourraient lui sembler plus pertinentes.

Référence	Exigence
EXI_M5_10	L'application permet de visualiser la cartographie du risque résiduel représentant les scénarios de risque selon leur gravité et vraisemblance résiduelles. Les échelles de représentation sont identiques à celles de la cartographie du risque initial. Un exemple figure en p.77 du guide EBIOS *Risk Manager* v1.1.
EXI_M5_11	L'application permet d'éditer et d'exporter la cartographie du risque résiduel, ainsi que le tableau de synthèse associé.
EXI_M5_12	L'application permet de documenter les risques résiduels, selon le modèle proposé en page 76 du guide EBIOS *Risk Manager* v1.1. L'application permet d'éditer et d'exporter la liste des risques résiduels. (Optionnel) Des options de filtre sont proposées (ex : n'exporter que les risques résiduels relatifs à une catégorie d'impact et de gravité supérieure à un seuil donné).

5. Exigences de sécurité

5.1 Mécanismes d'identification et d'authentification et de cloisonnement des profils

Référence	Exigence
EXI_S1_01	L'application devra prévoir un compte d'administration dédié et distinct des comptes utilisateurs. Le compte administrateur permet d'accéder aux ressources et interfaces d'administration, qui ne seront visible que par l'administrateur.
EXI_S1_02	Le compte administrateur devra permettre la gestion des différents profils utilisateurs tel qu'ils sont décrits dans la méthode EBIOS *Risk Manager*.
EXI_S1_03	La création des profils devra être nominative, non générique et basée sur un identifiant unique et individuel.
EXI_S1_04	L'authentification des profils administrateurs et utilisateurs devra être à minima basée sur l'usage de mot de passe.
EXI_S1_05	L'attribution des droits en lecture et/ou écriture devra être paramétrable par profils utilisateurs et par analyses de risques.
EXI_S1_06	La gestion des droits doit permettre de gérer le besoin d'en connaitre au niveau d'un utilisateur ou groupe d'utilisateurs. A minima, la granularité des autorisations permettra de restreindre l'accès à une analyse, un groupe d'analyse ou à toutes les analyses de risques.
EXI_S1_07	La validation de l'authentification sur la base d'un couple identifiant/authentifiant devra être réalisée par la partie serveur de l'application ou par l'intermédiaire d'un annuaire externe à l'application.
EXI_S1_08	L'application doit assurer la confidentialité et l'intégrité des informations d'identification et d'authentification des profils administrateurs et utilisateurs.

5.2 Confidentialité des données

Référence	Exigence
EXI_S2_01	L'application devra garantir la confidentialité et l'intégrité des données qui y sont stockées.
EXI_S2_02	L'application devra garantir la confidentialité et l'intégrité des données lors de leurs transits.
EXI_S2_03	La mise en œuvre des mécanismes de sécurité lors du transit des données devra être conformes aux guides de bonnes pratiques de l'ANSSI relatifs aux protocoles TLS, IPSEC ou SSH (www.ssi.gouv.fr/bonnes-pratiques).

5.3 Journalisation

Référence	Exigence
EXI_S3_01	L'application devra mettre en œuvre les mécanismes de journalisation et d'imputabilité des actions effectuées par chacun des profils administrateurs et utilisateurs.
EXI_S3_02	Une journalisation des évènements d'identification et d'authentification liés aux profils administrateurs et utilisateurs devra être mise en œuvre. Cette journalisation peut être locale au serveur applicatif ou déportée.
EXI_S3_03	Si l'identification et l'authentification des profils sont gérées par un annuaire externe à l'application, alors la journalisation des profils administrateurs et utilisateurs devra être recommandée dans les conditions générales d'emploi et d'usage de la solution logicielle (cf. § 2.3).
EXI_S3_04	Si l'identification et l'authentification des profils administrateurs et utilisateurs sont gérées par l'application, la journalisation devra porter à minima sur les éléments suivants : - ouverture et fermeture de session ; - verrouillage des comptes (si cette protection est mise en œuvre) ; - gestion des comptes administrateurs et utilisateurs (création, suppression ou modification) ; - accès en lecture ou écriture d'une analyse de risques ; - manipulation des journaux ; - des évènements applicatif : monté de version, arrêt, relance, etc.
EXI_S3_05	L'application devra assurer la protection des données journalisées, à minima en générant un évènement lié à l'effacement des journaux.

5.4 Revue des politiques internes de développement

La revue des politiques internes de développement de l'éditeur de l'application a pour objectif de promouvoir des pratiques à l'état de l'art en matière de développement sécurisé et d'en identifier les écarts afin d'évaluer la surface d'exposition et de tendre à limiter l'apparition de vulnérabilités dans la solution logicielle.

Référence	Exigence
EXI_S4_01	L'éditeur de l'application devra présenter les politiques et processus internes de développement relevant du cloisonnement des environnements de développement liés à l'application ;
EXI_S4_02	L'éditeur de l'application devra présenter les politiques et processus internes de développement relevant de la revue et de l'audit de code liés à l'application ;
EXI_S4_03	L'éditeur de l'application devra présenter les politiques et processus internes de développement relevant du contrôle d'innocuité de l'application avant livraison ;
EXI_S4_04	L'éditeur de l'application devra présenter les politiques et processus internes de veille sur les modules et briques applicatifs tiers (versions, support, vulnérabilités) liés à l'application.

5.5 Maintien en conditions de sécurité

Référence	Exigence
EXI_S5_01	Les engagements pris par l'éditeur au titre des exigences EXI_S5_01 à EXI_S5_06 devront être clairement spécifiés dans sa politique de maintien en conditions de sécurité.
EXI_S5_02	L'éditeur de l'application devra afficher sa politique en matière de versions (mineures et majeures) supportées et maintenues de l'application, en fonction des systèmes d'exploitation et des plateformes d'intégrations supportés.
EXI_S5_03	L'éditeur devra préciser si sa politique en matière de version supportées diffère selon qu'il s'agit de correctifs fonctionnels (MCO) ou de sécurité (MCS).
EXI_S5_04	En cas de faille, de vulnérabilité ou d'incident concernant l'application, l'éditeur s'engage, dès qu'il en a connaissance, à notifier le CERT-FR (www.cert.ssi.gouv.fr/contact) et à émettre un avis de sécurité auprès des utilisateurs.
EXI_S5_05	L'éditeur devra s'engager sur le délai de correction maximal des failles et vulnérabilités logicielles concernant les versions supportées et maintenues de l'application.
EXI_S5_06	Dès publication d'un correctif de sécurité, l'éditeur s'engage à publier un avis de sécurité à destination des clients finaux de l'application, ainsi qu'au CERT-FR.

5.6 Conditions générales d'emploi et d'usage

Référence	Exigence
EXI_S6_01	L'éditeur devra faire apparaitre dans les conditions générales d'emploi et d'usage de l'application, sous la forme d'un encart d'avertissement ou de « *disclaimer* » les exigences EXI_S6_02 à EXI_S6_04.
EXI_S6_02	L'évaluation de conformité réalisée par l'Agence au titre du Label EBIOS *Risk Manager* se restreint aux aspects fonctionnels de la solution vis-à-vis de la méthode EBIOS *Risk Manager*.
EXI_S6_03	Le Label EBIOS *Risk Manager* ne se substitue pas aux démarches de certification ou de qualification, tel que décrites sur le site de l'Agence (www.ssi.gouv.fr/visa-de-securite).
EXI_S6_04	Le Label EBIOS *Risk Manager* ne garantit en aucun cas la robustesse de l'application face à des actions malveillantes.
EXI_S6_05	Afin de déterminer les mesures de sécurité nécessaires à la protection de l'application et des données qui y sont contenues, l'éditeur recommande à l'utilisateur d'entreprendre une démarche d'homologation de sécurité tel que décrite par l'Agence (www.ssi.gouv.fr/guide-homologation-securite).

Référence	Exigence
EXI_S6_06	Afin d'orienter l'utilisateur dans sa démarche d'homologation et de sécurisation de l'application, l'éditeur devra faire apparaitre une matrice affichant l'état de conformité de l'application vis-à-vis des guides et bonnes pratiques (www.ssi.gouv.fr/bonnes-pratiques) publiés par l'Agence (tel que l'exemple ci-après).

Guides & Bonnes pratiques	Implémenté	Partiellement implémenté	A implémenter via l'homologation	Non Applicable
Recommandations pour la mise en place de cloisonnement système - v.1	✓			
Recommandations de configuration d'un système Gnu/linux				✓
Recommandations relatives à l'administration sécurisée des systèmes d'information		✓	✓	
….				

Exemple de matrice de conformité « Application / Guides ANSSI »

Annexe A - Recommandations portant sur l'application

Il est recommandé de proposer une solution logicielle ergonomique et adaptée à la production d'analyses de risque.

1. L'interface de l'application s'adapte automatiquement à la taille de l'écran. Cet écran peut être redimensionné par l'utilisateur en suivant le fonctionnement des interfaces graphiques prévues par les environnements MS Windows, Mac OS ou LINUX.

2. Il est possible de travailler à l'aide de la souris, mais également par des raccourcis clavier.

3. L'application permet de réaliser une sauvegarde manuelle et automatique périodique de l'étude.

4. Le contenu des champs de saisie est contrôlé par l'application (par exemple : un champ date permet uniquement la saisie d'une date selon un format prédéfini dans le code de l'application).

5. L'application permet la mise en forme enrichie des champs de saisie de texte : gras, italique, souligné, centrer, puces, taille de police de caractère, couleur du texte et surlignage.

6. Les visuels de restitution et de manipulation d'informations (représentations graphiques des risques, tableaux des événements redoutés, etc.) facilitent l'exploitation de l'analyse (ex. : les titres des colonnes/lignes restent visibles même en se déplaçant dans le tableau, les lignes sont alternativement de tonalités différentes, le texte s'adapte au conteneur).

7. L'utilisateur identifie facilement l'atelier et l'activité en cours dans le processus d'analyse (par exemple en faisant apparaître en permanence le schéma p.6-7 du guide EBIOS *Risk Manager* v1.1 et en mettant en surbrillance l'atelier en cours).

8. L'utilisateur peut accéder à tout moment aux différents ateliers et activités : l'application permet facilement de naviguer d'un atelier ou d'une activité à une autre, par exemple à partir du schéma du processus général de la méthode et/ou d'une arborescence des activités accessible facilement.

9. L'application propose uniquement les métriques et éléments d'analyse qui sont nécessaires pour réaliser l'atelier (par exemple, dans l'atelier 4 si l'utilisateur choisit une évaluation expresse de la vraisemblance, il n'est pas utile de proposer les grilles de probabilité de succès et de difficulté technique, ni la grille de croisement).

10. L'application permet d'annuler les actions précédentes.

11. L'application permet l'utilisation de la roulette de la souris dans les listes déroulantes.

12. Les listes déroulantes utilisées sont triées par ordre alphabétique et permettent la saisie prédictive.

13. L'application devra s'installer le plus simplement possible (type installeur automatisé).