CLUBEBIOS

EBIOS : la boîte à outils pour gérer les risques

Approche générique

Date	:	05/09/2018
Statut	:	Approuvé
Classification	:	Public
Nombre de pages	:	27
Responsable des travaux	:	Matthieu GRALL
Validation	:	Groupe de travail
Approbation	:	Conseil d'administration
Licence	:	

Club EBIOS, 72 avenue Gaston Boissier, 78220 VIROFLAY

Avant-propos

Ce document a été réalisé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et le Club EBIOS.

L'ANSSI élabore et tient à jour un important référentiel méthodologique destiné à aider les organismes du secteur public et du secteur privé à gérer la sécurité de leurs systèmes d'informations. Ce référentiel est composé de méthodes, de bonnes pratiques et de logiciels, diffusés gratuitement sur son site Internet (https://www.ssi.gouv.fr).

Le Club EBIOS est une association indépendante à but non lucratif (Loi 1901), composée d'experts individuels et d'organismes. Il regroupe une communauté de membres du secteur public et du secteur privé, supporte et enrichit le référentiel de gestion des risques français depuis 2003, en collaboration avec l'ANSSI. Le Club organise des réunions périodiques pour favoriser les échanges d'expériences, l'homogénéisation des pratiques et la satisfaction des besoins des usagers. Il constitue également un espace pour définir des positions et exercer un rôle d'influence dans les débats nationaux et internationaux.

Historique des modifications

Date	Objet de la modification	Statut
02/1997	Version 1 d'EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)	Approuvé
05/02/2004	Version 2 d'EBIOS : - convergence vers l'ISO/IEC 15408 ; - ajout de l'étape 5 – Détermination des exigences de sécurité ; - clarifications et compléments, *etc*.	Approuvé
25/01/2010	Version 3 ("2010") d'EBIOS : - convergence des concepts vers les normes internationales ; - mise en évidence des parties prenantes, actions de communication et concertation, et actions de surveillance et revue dans les descriptions des activités ; - ajout du cadre de la gestion des risques, de l'estimation et de l'évaluation des événements redoutés, des notions de défense en profondeur, risques résiduels, déclaration d'applicabilité, plan d'action et validation ; - étude des scénarios de menaces par bien support et non plus par vulnérabilité, *etc*.	Approuvé
05/09/2018	Version 4 d'EBIOS[1] : - décomposition en une approche générique et des applications spécifiques ; - focus sur ce qui n'est pas déjà pris en compte par les mesures d'hygiène et les normes légales ou techniques ; - sources de risques comme point de départ de l'étude ; - prise en compte de l'écosystème ; - approche fractale / top-down des risques ; - recherche d'efficacité plutôt que d'exhaustivité (ou *vice versa*, selon le contexte et l'objectif de l'étude), *etc*.	Validé

[1] Voir aussi "Correspondance avec l'ancienne terminologie" et "Correspondance avec les anciens concepts".

Table des matières

1 Introduction

1.1 Qu'est-ce qu'EBIOS ?

EBIOS[2] (Expression des Besoins et Identification des Objectifs de Sécurité) permet d'apprécier et de traiter les risques. Elle fournit également tous les éléments nécessaires à la communication au sein de l'organisme et vis-à-vis de ses partenaires, ainsi qu'à la validation du traitement des risques (voir l'annexe « EBIOS & gestion des risques »). Elle constitue ainsi un outil complet de gestion des risques (au sens normatif, cf. ISO 31000[3]).

Il s'agit d'une véritable boîte à outils, dont on choisit les actions à mettre en œuvre et la manière de les utiliser selon l'objectif de l'étude. Elle permet d'apprécier les risques au travers de scénarios et d'en déduire une politique cohérente, appuyée sur des mesures concrètes et évaluables.

1.2 Une méthodologie générique, des méthodes spécifiques

EBIOS, conçue initialement pour la sécurité de l'information, peut se décliner dans tous les domaines au moyen de techniques et de bases de connaissances adaptées.

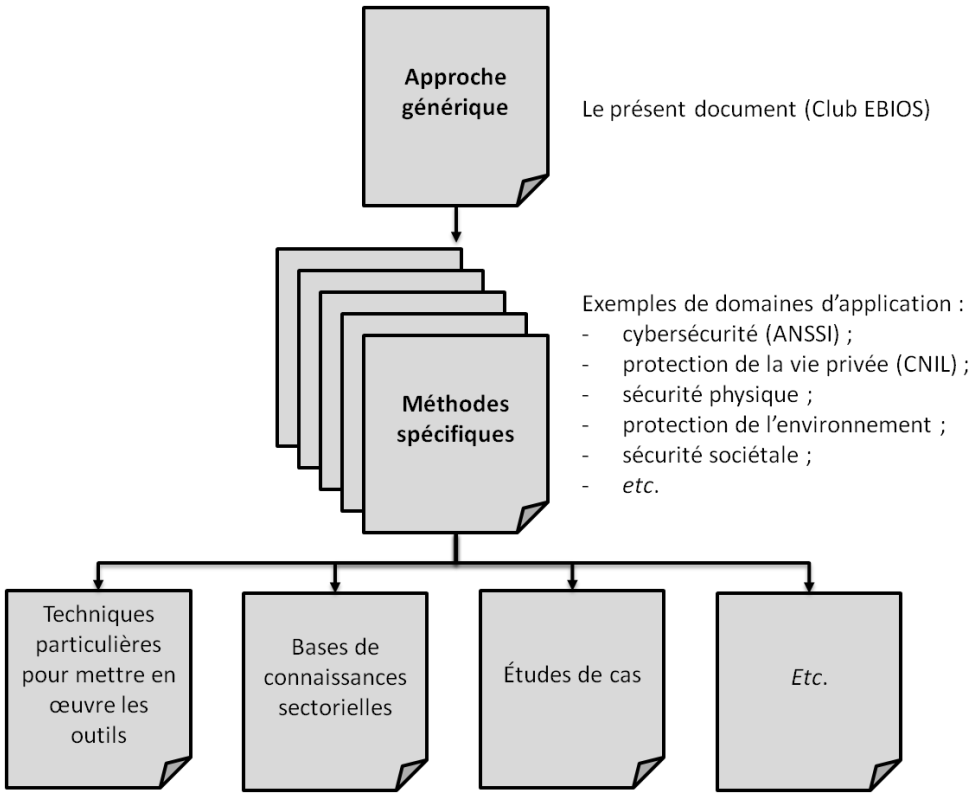

Figure 1 - Déclinaison de la méthodologie générique en méthodes spécifiques

[2] EBIOS est une marque déposée par le Secrétariat général de la défense et de la sécurité nationale.

[3] *Management du risque – Principes et lignes directrices de mise en œuvre*, *International Organization for Standardization* – ISO.

EBIOS est suffisamment souple pour être appliquée à différents domaines. Elle a majoritairement été utilisée pour gérer des risques de sécurité de l'information, mais également ceux sur la vie privée, les infrastructures vitales, l'ergonomie des outils de travail, *etc*. Sa convergence, en termes de concepts et de démarche, vers les normes internationales de systèmes de management et de gestion des risques la rend largement applicable.

L'usage d'EBIOS dans un domaine spécifique est relativement aisé. Il suffit généralement de transposer la terminologie et d'exploiter des techniques et des bases de connaissances spécifiques au domaine concerné si celles-ci ne semblent pas applicables ou comprises (éléments à protéger, critères considérés, impacts potentiels, *etc*.). En effet, chaque domaine d'application (protection de l'environnement, protection des personnes, gestion des risques juridiques, *etc*.) dispose d'un cadre de référence, d'une culture et de connaissances qui lui sont propres. Mais les principes et la démarche de gestion des risques restent globalement les mêmes. Ainsi, l'emploi d'EBIOS dans le cadre de la protection des infrastructures vitales contre le terrorisme a impliqué de transposer le vocabulaire à la terminologie employée dans ce domaine et de créer des bases de connaissances de critères, de sources de risques, de supports, d'actions élémentaires spécifiques, et d'intégrer les plans de prévention et de réaction gouvernementaux en guise de bases de mesures.

En outre, différentes techniques et bases de connaissances peuvent être utilisées pour chaque module d'EBIOS, ce qui facilite l'intégration d'EBIOS aux pratiques de l'organisme.

1.3 Domaine d'application

La démarche de gestion des risques présentée dans ce guide peut s'appliquer :

- à tout domaine (historiquement employée dans le domaine de la sécurité de l'information, elle a été utilisée dans plusieurs autres domaines) ;
- à des systèmes en cours d'élaboration et à des systèmes existants ;
- au secteur public et au secteur privé ;
- à des petites structures (petites et moyennes entreprises, collectivités territoriales, *etc*.) et à des grandes structures (ministères, organisations internationales, entreprises multinationales, *etc*.).

1.4 Objectifs du document

Les principaux objectifs du présent document sont :

- fournir une base commune de concepts et d'activités pragmatiques à toute personne impliquée dans la gestion des risques, notamment pour créer des méthodes spécifiques à partir de cette approche générique ;
- satisfaire les exigences de gestion des risques de tout système de management[4] ;
- définir une démarche méthodologique complète en cohérence et en conformité avec les normes internationales de gestion des risques (ISO 31000, ISO 27005[5], *etc*.) ;
- établir une référence pour la certification de compétences liées à EBIOS.

[4] Cf. l'annexe SL des directives de l'ISO, qui définit le plan et le contenu communs à tout système de management *(Directives ISO/IEC, Partie 1 – Supplément ISO consolidé — Procédures spécifiques à l'ISO*).

[5] *Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information*.

2 Les grands principes

2.1 EBIOS est une boîte à outils à usage variable

Comme toute véritable approche de gestion des risques, EBIOS permet d'identifier des risques, de les analyser, de les évaluer et de les traiter dans le cadre d'une amélioration continue.

La spécificité d'EBIOS réside dans sa souplesse d'utilisation : il s'agit d'une véritable boîte à outils, dont les activités à réaliser, leur niveau de détail et leur séquencement doivent être adaptés à l'usage désiré.

En effet, la boîte à outils n'est pas utilisée de la même manière selon le sujet étudié, les livrables attendus, les destinataires et l'objectif de cette communication (prise de décision, sensibilisation, *etc.*) pour choisir les activités de la démarche à réaliser et présenter les résultats directement sous la forme la plus appropriée, mais aussi le degré de connaissance du périmètre de l'étude, le domaine auquel on l'applique, *etc.*

2.2 Variation de la focale selon le sujet étudié

EBIOS permet de gérer de manière adaptée les risques portant sur des sujets de taille et de nature variables.

EBIOS peut être utilisée pour gérer les risques portant sur un secteur d'activités, un organisme dans son intégralité, une sous-partie ou des processus particuliers de celui-ci, un système d'information, un système informatique, une interconnexion de systèmes, une application, un produit de sécurité, un composant de produit, *etc.*

Il est bien évident qu'une telle diversité de sujets n'est pas abordée de manière uniforme si l'on souhaite des résultats pertinents. C'est ici le niveau de détail qui varie : plus le sujet est large, moins le niveau de détail est important, et inversement. Ainsi, une étude de haut niveau d'abstraction pourrait porter sur des éléments à protéger et des supports macroscopiques, comme les grandes activités d'un organisme et les logiciels dans leur ensemble ; alors qu'une étude focalisée devrait porter sur des éléments à protéger et des supports détaillés, par exemple les données et une version spécifique de système de gestion de base de données.

La boîte à outils peut également être employée pour étudier d'abord un sujet global (ex : un organisme ou un système complexe composé de plusieurs sous-systèmes), et ensuite se focaliser sur un sous-ensemble (ex : quelques processus de l'organisme jugés critiques ou des sous-systèmes). Il convient de veiller à la cohérence d'une étude d'ensemble avec les études de ses sous-ensembles et entre les études des différents sous-ensembles.

2.3 Variation de la profondeur selon le cycle de vie du sujet de l'étude

EBIOS permet de gérer les risques dans toutes les phases de vie du sujet de l'étude ; elle se prête notamment à un usage précoce dans le cadre d'un processus de développement.

Il est conseillé de gérer les risques depuis les premières réflexions relatives à un nouveau service ou un nouveau système. Cela permet d'orienter la conception et la réalisation, et de faire des choix en amont avant d'avoir trop investi pour faire machine arrière.

Le peu de connaissances que l'on a d'un sujet dans les premières phases de son cycle de vie ne permet qu'une étude peu approfondie. La réflexion se fait au fur et à mesure de l'avancement des travaux sur le sujet, par raffinements successifs, en fonction de ce qu'on est capable de connaître et de modéliser. Dans un premier temps, on s'intéresse aux grands enjeux pour identifier des « risques liés aux sources de risques », dans un second temps on peut affiner la description du sujet et élaborer des « risques au niveau des éléments à protéger », puis on peut étudier les « risques au niveau des supports » pour obtenir des risques détaillés et des mesures, *etc*. C'est donc en réalisant des itérations successives et des activités supplémentaires que la gestion des risques accompagne le cycle de vie du sujet.

Ainsi, par exemple, lors des études d'opportunité et de faisabilité d'un système d'information, il est possible d'étudier son contexte, d'identifier les enjeux du système, de faire émerger les fonctionnalités ou les processus essentiels, d'exprimer leurs besoins, d'estimer les impacts potentiels et d'identifier des sources de risques. Une seconde itération de la démarche a lieu lors de la conception générale et de la conception détaillée : les grandes fonctionnalités seront décomposées en fonctions plus détaillées et en informations manipulées (ou autres éléments à protéger, selon le domaine d'application), les supports seront identifiés, les impacts seront affinés, les sources de risques développées et consolidées, les risques au niveau des supports étudiés, les objectifs identifiés, les mesures déterminées et les risques résiduels mis en évidence. Lors de la phase de réalisation, une autre itération permet de rectifier et de compléter l'ensemble de l'étude, notamment au niveau des mesures et des risques résiduels. Enfin, en phase d'exploitation et jusqu'à la fin de vie du système, les évolutions du contexte (supports, sources de risques, risques au niveau des supports, *etc*.) permettent d'ajuster l'étude et de gérer les risques en continu.

2.4 Une démarche générale par itérations successives

La démarche de gestion des risques est découpée en cinq modules :

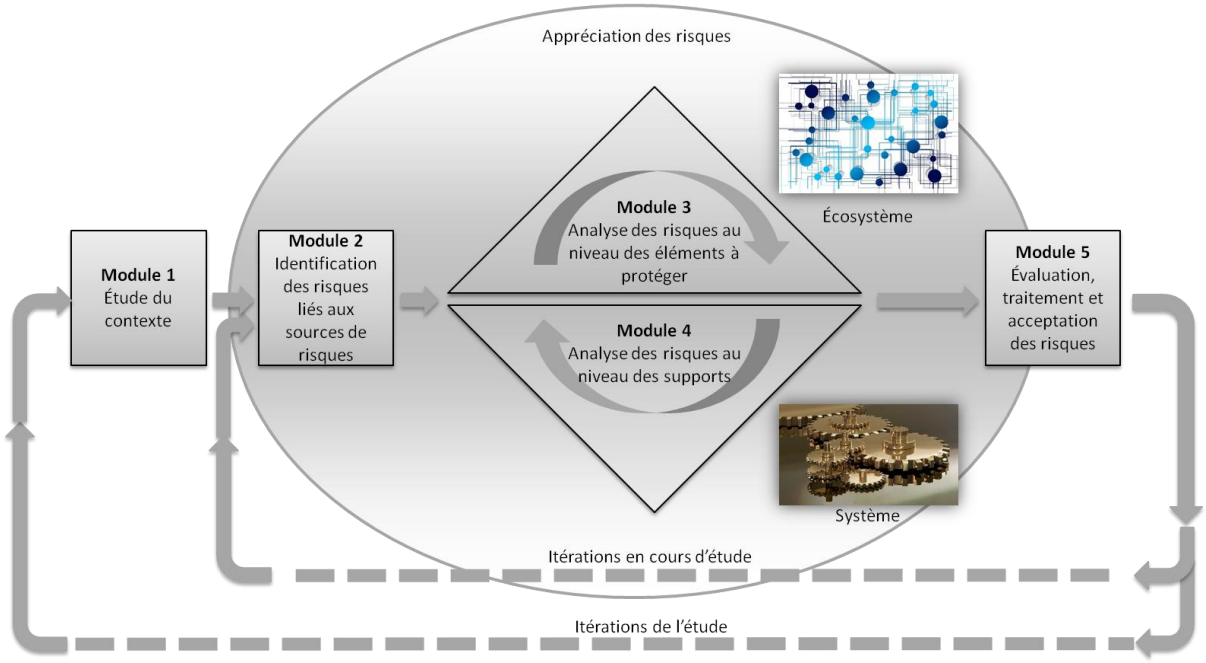

Figure 2 - Démarche générale

La démarche d'EBIOS est itérative : il sera fait appel plusieurs fois à chaque module afin d'en améliorer progressivement le contenu.

En particulier :

- tout d'abord, les Modules 3 et 4 sont construits par itérations successives ;
- si les risques ne sont pas jugés comme acceptables à l'issue du Module 5, de nouvelles itérations doivent permettre de mieux les comprendre et donc de mieux les traiter ;
- enfin, la démarche globale est affinée et tenue à jour au moyen de cycles de mise à jour ; en outre, elle s'inscrit dans une logique d'évaluation de performance et d'amélioration continue de l'ensemble de l'étude.

2.5 Une appréciation des risques par raffinements successifs

L'appréciation des risques d'EBIOS se déroule de manière « fractale » afin de comprendre respectivement les enjeux de haut niveau et leurs fondements pratiques :

- on identifie tout d'abord des risques au niveau le plus macroscopique (« risques liés aux sources de risques », dans le Module 2) ;
- on analyse ensuite les risques en affinant les scénarios par des événements intermédiaires et redoutés (« risques au niveau des éléments à protéger », dans le Module 3) ;
- on termine l'analyse des risques en affinant encore les scénarios par des actions intermédiaires et redoutées (« risques au niveau des supports », dans le Module 4).

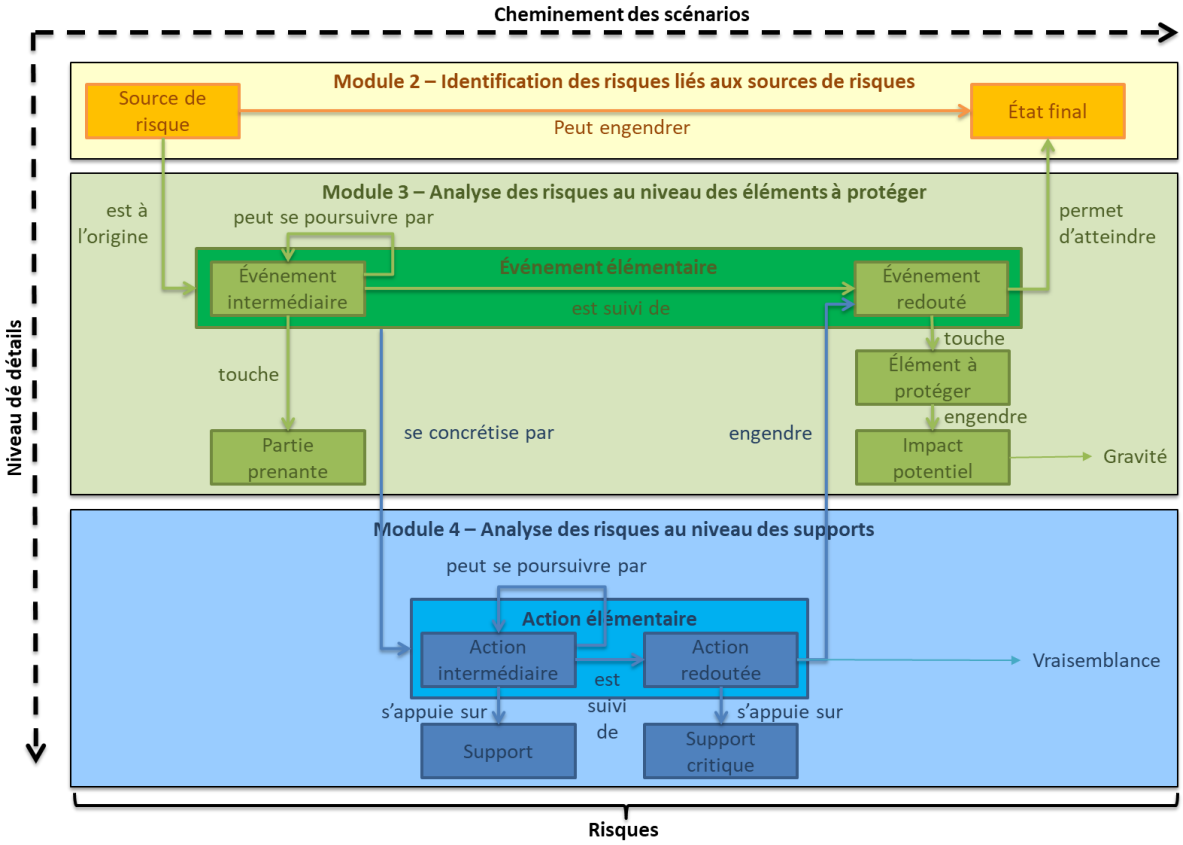

Figure 3 - Appréciation des risques par raffinements successifs

Les risques ainsi affinés sont enfin évalués et traités (dans le Module 5).

Notes : ces éléments sont définis dans l'annexe « Termes et définitions »[6] et utilisés dans les chapitres suivants.

[6] Voir aussi les annexes « Correspondance avec l'ancienne terminologie » et « Correspondance avec les anciens concepts ».

3 Description de la démarche

Module 1 – Étude du contexte

Ce module fournit des outils pour cadrer l'étude des risques, identifier, délimiter et décrire l'objet de l'étude, ainsi que son écosystème.

Outil 1.1. Cadrer l'étude des risques

- Quel est le domaine d'application de l'étude (cybersécurité, protection de la vie privée, sécurité physique, protection de l'environnement, sécurité sociétale, *etc.*) ?
- Quels sont les critères que l'on souhaite protéger selon le domaine d'application (ex : disponibilité, intégrité et confidentialité pour la sécurité de l'information) ?
- Quel est la finalité de l'étude (définition ou mise à jour d'une politique, élaboration d'un cahier des charges, homologation, sensibilisation des utilisateurs ou de la direction, maîtrise des risques de l'organisme, mise en conformité, *etc.*) ?
- Quelles sont les contraintes (techniques, organisationnelles, financières, temporelles, *etc.*) à prendre en compte ?
- Quels sont les acteurs à intégrer à la démarche de gestion des risques ? Comment ?
- Comment les informations seront-elles recueillies, recoupées, formalisées et validées ? Comment est-il prévu de répondre aux questions des outils suivants ?
- Quels éléments est-il possible de réutiliser depuis des études précédentes ?
- Quelles sont la durée de validité de l'étude et la fréquence des révisions prévues ?

Outil 1.2. Identifier et décrire l'objet de l'étude

- Quel est l'objet de l'étude ?
- Quelle est sa finalité ? Quels sont ses enjeux (bénéfices attendus) ?
- Quelles sont ses grandes fonctions ? Peut-on schématiser une description fonctionnelle (en termes de processus) ?

Outil 1.3. Identifier les référentiels à respecter

- Le cas échéant, quels sont les référentiels à respecter (normes juridiques ou techniques, référentiels sectoriels, politiques internes, *etc.*) ?
- Quel est leur état d'application ? Les écarts sont-ils identifiés ? Ont-ils fait l'objet d'un arbitrage ?

Outil 1.4. Identifier les composants de l'écosystème

- Quelles sont les parties prenantes avec lesquelles l'objet de l'étude est en interaction ? Quels sont leurs liens (entre elles et avec l'objet de l'étude, ex : organisationnel, technique, fonctionnel, contractuel, *etc.*) ?
- Si possible, quelles sont leurs caractéristiques (dépendance, maturité, *etc.*) ?
- Lesquelles retient-on dans la suite de l'étude (selon leur pertinence, dans le cas où l'on souhaite aller vite à l'essentiel) ?

Module 2 – Identification des risques liés aux sources de risques

Ce module fournit des outils pour identifier et caractériser les risques à un niveau macroscopique, sous la forme de couple {source de risques présente dans l'écosystème / état final qu'elle peut provoquer sur l'objet de l'étude ou sur l'écosystème}. Ces couples {source de risque / état final} ainsi identifiés constituent des scénarios de risques de haut niveau, qui seront appréciés dans les modules 3 et 4 par raffinements successifs.

Outil 2.1. Identifier les sources de risques pertinentes pour l'objet de l'étude

- Quelles sont les sources de risques pertinentes pour l'objet de l'étude ?
- Comment peut-on les caractériser (interne ou externe, nature humaine, naturelle, ou autre ; origine accidentelle ou intentionnelle ; *etc*.) ?
- Lesquelles retient-on dans la suite de l'étude (selon leur pertinence, dans le cas où l'on souhaite aller vite à l'essentiel) ?

Outil 2.2. Déterminer les états finaux qu'elles peuvent provoquer

- Quels états finaux peuvent-elles provoquer (ou rechercher, dans le cas de sources de risques agissant de manière délibérée) sur l'objet de l'étude ou sur l'écosystème ?
- Lesquels retient-on dans la suite de l'étude (selon leur pertinence, dans le cas où l'on souhaite aller vite à l'essentiel) ?

Outil 2.3. Évaluer la pertinence des risques liés aux sources de risques

- Si possible, quelles sont les capacités des sources de risques à engendrer chaque état final (selon leurs ressources, leur expertise, leur dangerosité, leur contexte professionnel ou personnel pour les sources humaines, leurs motivations pour celles agissant de manière délibérée, *etc*.) ?
- Si possible, quels sont les modes opératoires (actions nécessaires à l'obtention d'un résultat) habituellement associés à ces sources de risques pour ces états finaux ?
- Quels risques liés aux sources de risques (couples {source de risques / état final}) retient-on dans la suite de l'étude (selon leur pertinence, dans le cas où l'on souhaite aller vite à l'essentiel) ?

Module 3 – Analyse des risques au niveau des éléments à protéger

Ce module fournit des outils pour commencer à analyser les risques retenus dans le Module 2. L'analyse est effectuée au niveau des éléments à protéger et non de leurs supports. Elle consiste à étudier les scénarios « fonctionnels » des sources de risques. Ils peuvent comprendre une succession d'événements intermédiaires sur différentes parties prenantes et d'événements redoutés sur des éléments à protéger, ou au moins un événement redouté sur un élément à protéger. Les risques ainsi analysés sont estimés en termes de gravité.

Outil 3.1. Identifier les éléments à protéger

- Quels sont les éléments à protéger (selon le domaine d'application de l'étude et le niveau de détail souhaité, ex : fonctions, informations, personnes, biens, *etc*.) ?
- Lesquels retient-on dans la suite de l'étude (selon leur pertinence, dans le cas où l'on souhaite aller vite à l'essentiel) ?

Outil 3.2. Analyser le scénario « fonctionnel » des sources de risques

- Si les sources de risques devaient passer par des parties prenantes, par lesquelles passeraient-elles pour mener à chaque état final et selon quel enchainement ?
- Que pourraient-elles faire sur chaque partie prenante (événements intermédiaires) ?
- Que pourraient-elles faire sur les éléments à protéger (événements redoutés et critères affectés) ?
- Quels sont les impacts potentiels de chaque événement redouté ainsi constitué (plusieurs types d'impacts peuvent être considérés) ?

Outil 3.4. Estimer la gravité de chaque risque au niveau des éléments à protéger

- Quelle est l'échelle pertinente dans le contexte de l'étude pour estimer la gravité (une échelle globale ou une échelle pour chaque type d'impacts, ex : négligeable, significative, importante, maximale) ?
- Quelles sont les mesures existantes ou prévues contribuant à réduire la gravité de chaque risque au niveau des éléments à protéger ?
- À quel niveau de l'échelle de gravité chaque risque correspond-il, notamment en fonction des impacts potentiels, mais aussi des sources de risques (motivations, potentiel de nuisance, *etc*.) et des mesures existantes ou prévues ?
- Si possible, comment peut-on justifier chaque estimation (illustrations, exemples d'impacts potentiels, volumes concernés, mesures existantes ou prévues, *etc*.) ?

Module 4 – Analyse des risques au niveau des supports

Ce module fournit des outils pour approfondir l'analyse des risques du Module 3. L'analyse est effectuée au niveau des supports et non plus des éléments à protéger. Elle consiste à étudier les scénarios « pratiques » des sources de risques. Ils peuvent comprendre une succession d'actions intermédiaires sur différents supports et d'actions redoutées sur des supports critiques, ou au moins une action redoutée sur un support critique. Les risques ainsi analysés sont estimés en termes de vraisemblance.

Outil 4.1. Identifier les supports

- Quels sont les supports sur lesquels reposent les éléments à protéger ?
- Quels sont ceux que l'on juge comme critiques ? Pourquoi ?
- Lesquels retient-on dans la suite de l'étude (selon leur pertinence, dans le cas où l'on souhaite aller vite à l'essentiel) ?

Outil 4.2. Analyser le scénario « pratique » des sources de risques

- Par quels supports passeraient-elles pour engendrer chaque événement redouté et selon quel enchainement ?
- Que pourraient-elles faire sur chaque support (actions intermédiaires) ?
- Que pourraient-elles faire sur les supports critiques (actions redoutées) ?
- Quelles sont les vulnérabilités des supports, exploitables dans le cadre de chaque action redoutée ainsi constituée ?

Outil 4.4. Estimer la vraisemblance de chaque risque au niveau des supports

- Quelle est l'échelle pertinente dans le contexte de l'étude pour estimer la vraisemblance (ex : négligeable, significative, importante, maximale) ?
- Quelles sont les mesures existantes ou prévues contribuant à réduire la vraisemblance de chaque risque au niveau des supports ?
- À quel niveau de l'échelle de vraisemblance chaque risque correspond-il, notamment au regard des vulnérabilités des supports, mais aussi des sources de risques (proximité de l'objet de l'étude, effort nécessaire, motivations, capacités, sentiment d'impunité, retour attendu, *etc.*) et des mesures existantes ou prévues ?
- Si possible, comment peut-on justifier chaque estimation (illustrations, incidents ayant eu lieu, mesures existantes ou prévues, *etc.*) ?

Module 5 – Évaluation, traitement et acceptation des risques

Ce module fournit des outils pour évaluer les risques qui ont été identifiés au Module 2 et analysés successivement dans les Modules 3 et 4, déterminer les moyens de les traiter et décider d'accepter ou non les risques résiduels.

Outil 5.1. Évaluer les risques

- Quel est le niveau de détail pertinent pour présenter les risques (par risque lié aux sources de risques, par risque au niveau des éléments à protéger, par risque au niveau des supports, par événement redouté, *etc.*) selon le contexte de l'étude et les personnes à qui elle est destinée ?
- Quels sont les risques selon le niveau de détail choisi ? (ex : risques au niveau des éléments à protéger, avec pour chacun la liste des risques au niveau des supports qui permettent sa réalisation, leur gravité étant égale à celle du risque au niveau des éléments à protéger, et leur vraisemblance étant égale à la vraisemblance maximale des risques au niveau des supports)
- Si possible, comment peut-on les représenter visuellement ? (ex : en positionnant chaque risque sur un graphique avec sa vraisemblance en abscisse et sa gravité en ordonnée, ou bien sur un radar avec les risques les plus élevés proches du centre) Comment illustrer chaque risque par un exemple explicite ?
- Quelle est l'échelle pertinente dans le contexte de l'étude pour évaluer les risques ? (ex : négligeable, significatif, important, maximal)
- À quel niveau de l'échelle d'évaluation chaque risque correspond-il au regard de sa gravité et de sa vraisemblance ?

Outil 5.2. Identifier les objectifs

- Quelle est la forme pertinente des objectifs (tactique à privilégier pour traiter chaque risque[7] et/ou objectifs généraux au niveau de l'écosystème et/ou état souhaité de chaque support à l'issue du traitement des risques, *etc.*) selon le contexte de l'étude et les personnes à qui elle est destinée ?
- Quels sont les objectifs que l'on identifie au regard des risques ? Ces objectifs peuvent-ils être contractualisés avec ceux qui devront les satisfaire ?

Outil 5.3. Démontrer la satisfaction des référentiels à respecter

- Le cas échéant, les exigences de chaque référentiel à respecter sont-elles satisfaites (ex : expliquer comment elles le sont ou justifier pourquoi elles ne le sont pas) ?

[7] Plusieurs tactiques sont envisageables :

- par types de mesures à privilégier (prévention, protection, récupération, *etc.*) ;
- par composants des risques à traiter en priorité (sources de risques, supports, éléments à protéger, risques au niveau des supports, impacts potentiels, *etc.*) ;
- par options de traitement du risque (le réduire, le partager, le refuser, le maintenir) ;
- *etc.*

Outil 5.4. Déterminer les mesures complémentaires à mettre en œuvre

- Pour chaque objectif identifié, quelles sont les mesures complémentaires (aux référentiels à respecter et aux mesures existantes ou prévues, le cas échéant) qu'il conviendrait de mettre en œuvre pour l'atteindre ?
- Quelle est, pour chaque mesure déterminée, le plan d'action concret prévu pour la mettre en œuvre (responsable, difficulté, coût financier, terme, *etc*.) ?

Outil 5.5. Accepter les risques résiduels

- Quels sont les risques résiduels (ré-estimer la gravité et la vraisemblance de chaque risque, compte tenu des mesures complémentaires déterminées) ?
- Les risques résiduels et la manière dont il est prévu de traiter les risques sont-ils jugés comme acceptables ? Sinon, reprendre les étapes précédentes !

Outil 5.6. Assurer le suivi des risques et l'amélioration continue

- Quels sont les indicateurs pertinents pour mesurer l'évolution et/ou la réalisation de chaque risque résiduel ?
- Chaque mesure a-t-elle été mise en œuvre ? Quelle est son efficacité réelle ?
- Comment gère-t-on le processus de retour d'expérience et l'amélioration continue ?
- Les cycles de mise à jour définis en début d'étude sont-ils pertinents ?

Annexes

Termes et définitions

Action élémentaire *(Single action)*	Action unitaire exécutée par une source de risque dans le cadre d'un risque au niveau des supports. *Exemple(s) : exploiter une vulnérabilité logicielle, copier des fichiers, effacer des traces.*
Action intermédiaire *(Intermediate action)*	Action élémentaire touchant un support.
Action redoutée *(Feared action)*	Action élémentaire touchant un support critique. *Note(s) :* - *constituant le fondement technique d'un événement redouté, elle décrit le point de vue de l'organisme face à un risque au niveau des supports ;* - *elle représente l'action d'une source de risque sur un support critique et les critères touchés sur l'élément à protéger associé ;* - *elle est estimée en termes de vraisemblance.*
Critère *(Criterion)*	Propriété à garantir. *Exemple(s) : disponibilité, intégrité, confidentialité.* *Note(s) :* - *le critère s'applique à un élément à protéger ;* - *il est affecté par une action sur un support.*
Écosystème *(Ecosystem)*	Ensemble constitué des parties prenantes en interaction avec l'objet de l'étude. *Note(s) :* - *on entend par "interaction" toute relation intervenant dans le fonctionnement normal de l'objet de l'étude ;* - *les sources de risque ne sont pas considérées a priori comme parties prenantes, sauf si elles sont par ailleurs en interaction légitime avec l'objet de l'étude.*
Élément à protéger *(Primary asset)*	Élément présentant un caractère essentiel dans le cadre de l'objet de l'étude selon son domaine d'application. *Exemple(s) : informations (ex : factures, coordonnées, prix, etc.), processus (ex : passer une commande client, gérer le stock, etc.),*

	données à caractère personnel (ex : identifiant, adresse électronique, adresse IP, etc.), personnes (ex : employés, visiteurs, etc.), lieux (ex : site, habitations, voie navigable, etc.).
État final *(Final state)*	Situation ultime de l'objet de l'étude et/ou de l'écosystème, résultant d'actions d'une source de risque. *Exemple(s) : données commerciales volées et revendues, activité principale de l'entreprise interrompue, parts de marché perdues, climat de peur obtenu, sinistre réalisé, etc.* *Note(s) : il peut constituer un but (dans le cas d'une source de risque agissant de manière délibérée) ou survenir de manière fortuite (dans le cas d'une source de risque agissant de manière accidentelle).*
Événement élémentaire *(Single event)*	Événement unitaire causé par une source de risque dans le cadre d'un risque sur les éléments à protéger. *Note(s) :* - *il résulte concrètement de la réalisation d'un risque au niveau des supports par une source de risques.*
Événement intermédiaire *(Intermediate event)*	Événement élémentaire sur une partie prenante.
Événement redouté *(Feared event)*	Événement élémentaire sur un élément à protéger. *Note(s) :* - *il décrit le point de vue de l'organisme face à un risque au niveau des éléments à protéger ;* - *il représente l'action d'une source de risque sur un critère d'un élément à protéger et ses impacts potentiels ;* - *il est estimé en termes de gravité.*
Gravité *(Severity)*	Estimation de la hauteur des effets d'un risque. *Exemple(s) : négligeable, limitée, importante, maximale.* *Note(s) : la gravité d'un risque est généralement celle du risque au niveau des éléments à protéger concerné.*
Impact potentiel *(Potential impact)*	Conséquence potentielle d'un risque sur l'objet de l'étude et/ou son écosystème. *Note(s) :* - *l'impact peut être direct ou indirect ;* - *il peut concerner l'image de marque, des pertes financières, des*

atteintes à la vie privée, etc.

Mesure *(Control)*	Moyen de traiter un risque. *Note(s) : une mesure peut être multiforme selon le contexte et l'objectif de l'étude.* *Par exemple :* - *l'ensemble des mesures qui composent une politique ;* - *une mesure peut être technique ou organisationnelle ;* - *certaines mesures peuvent se renforcer mutuellement en agissant selon des axes ou dimensions complémentaires (notion de défense en profondeur) ;* - *elle s'inscrit dans une option de traitement du risque (réduction, partage, refus, maintien) ayant fait l'objet d'une décision ;* - *une mesure est généralement portée par un support ;* - *une mesure peut agir sur une source de risque, un support, un élément à protéger, ou un impact potentiel.*
Objectif *(Objective)*	Orientation décidée pour traiter un risque. *Note(s) : cette orientation peut s'exprimer tant par un mode de traitement choisi (réduction, partage, refus, maintien) que par un niveau de risque résiduel attendu.*
Objet de l'étude *(Studied object)*	Organisation ou système étudié.
Partie prenante *(Stakeholder)*	Système, personne ou organisation susceptible d'affecter ou d'être affecté par une décision ou une activité dans le cadre de l'objet de l'étude. *Exemple(s) : organisme, prestataire, client.*
Risque *(Risk)*	Scénario de bout en bout, décrivant un risque au niveau des éléments à protéger et tous les risques au niveau des supports susceptibles de l'engendrer. *Note(s) :* - *il est initié par une source de risques et tend à engendrer un état final ;* - *il est estimé en termes de gravité et de vraisemblance.*
Risque au niveau des éléments à protéger *(Risk at the primary assets'*	Mode opératoire décrivant l'enchaînement d'événements élémentaires et de l'événement redouté provoqués par une source de risque dans l'écosystème et susceptible d'engendrer un état final. *Note(s) :* - *il décrit un scénario « fonctionnel » ;*

level)	- *il est composé d'une source de risque, d'éventuels événements élémentaires sur des parties prenantes, d'un événement redouté sur un élément à protéger, et d'un état final ;* - *il est estimé en termes de gravité ;* - *un risque au niveau des éléments à protéger ne sera retenu que s'il contribue réellement à la réalisation d'un état final, i.e. qu'il comporte au moins un événement redouté, contribuant à l'état final.*
Risque au niveau des supports *(Risk at the supporting assets' level)*	Mode opératoire décrivant l'enchaînement d'actions élémentaires et de l'action redoutée réalisées par une source de risque en vue de réaliser un risque au niveau des éléments à protéger. *Note(s) :* - *il décrit un scénario « pratique » ;* - *il est composé d'une source de risque, d'éventuelles actions élémentaires sur des supports et d'une action redoutée sur un support critique ;* - *il est estimé en terme de vraisemblance ;* - *un risque au niveau des supports peut produire des effets correspondant à un risque au niveau des éléments à protéger non visé initialement (notion d'effets collatéraux) ;* - *un risque au niveau des supports ne sera retenu que s'il contribue réellement à la réalisation d'un risque au niveau des éléments à protéger, i.e. qu'il comporte au moins une action redoutée, contribuant à l'événement redouté du risque sur un élément à protéger.*
Source de risque *(Risk source)*	Chose ou personne, groupe de personnes ou organisation, à l'origine d'un ou de plusieurs risque(s). *Exemple(s) : service gouvernemental, pirate, concurrent, employé, animal, eau, feu, temps qui passe.* *Note(s) : dans le cas où des mesures ont déjà été prises pour contrer les risques accidentels, e.g. à travers une étude de sécurité ou de sûreté de fonctionnement, il est possible de se limiter aux sources de risques intentionnelles.*
Support *(Supporting asset)*	Élément du système d'information sur lequel repose un ou plusieurs élément(s) à protéger. *Exemple(s) : sous-système technique, serveur, logiciel métier, réseau, administrateur système.* *Note(s) :* - *il peut s'agir d'un sous-système ou plus précisément d'un matériel, logiciel, réseau, personne, etc. ;* - *le support est la cible pratique de la source de risque ;*

- *un support ciblé doit être observé non seulement au regard de l'atteinte (éventuelle) sur l'élément à protéger qu'il porte, mais aussi au regard de son exploitation possible par la source de risque dans un risque au niveau des supports.*

Support critique *(Critical supporting asset)*	Support jugé par l'organisme comme présentant un caractère critique pour l'(les) élément(s) à protéger qu'il supporte. *Note(s) : la compromission d'un support critique entraîne nécessairement une atteinte sur l'(les) élément(s) à protéger dont il est porteur.*
Vraisemblance *(Likelihood)*	Estimation de la possibilité de réalisation d'un risque. *Exemple(s) : négligeable, limitée, importante, maximale.* *Note(s) : la vraisemblance d'un risque est généralement la vraisemblance maximale des risques au niveau des supports concernés.*

Correspondance avec l'ancienne terminologie

Nouveaux termes	Anciens termes	Terme équivalent dans l'ISO 31000
Action élémentaire	-	-
Action intermédiaire	Menace	-
Action redoutée	-	-
Critère	Critère de sécurité	-
Écosystème	Contexte externe	-
Élément à protéger	Bien essentiel	-
État final	-	-
Événement élémentaire	-	-
Événement intermédiaire	-	-
Événement redouté	[identique]	-
Gravité	[identique]	-
Impact potentiel	Impact	Conséquence
Mesure	Mesure de sécurité	-
Objectif	Objectif de sécurité	-
Partie prenante	[identique]	-
Risque	[identique]	Risque
Risque au niveau des éléments à protéger	-	-
Risque au niveau des supports	Scenario de menace	Événement
Source de risques	Source de menace	Source de risque
Support	Bien support	-
Support critique	-	-
Vraisemblance	[identique]	Vraisemblance

Correspondance avec les anciens concepts

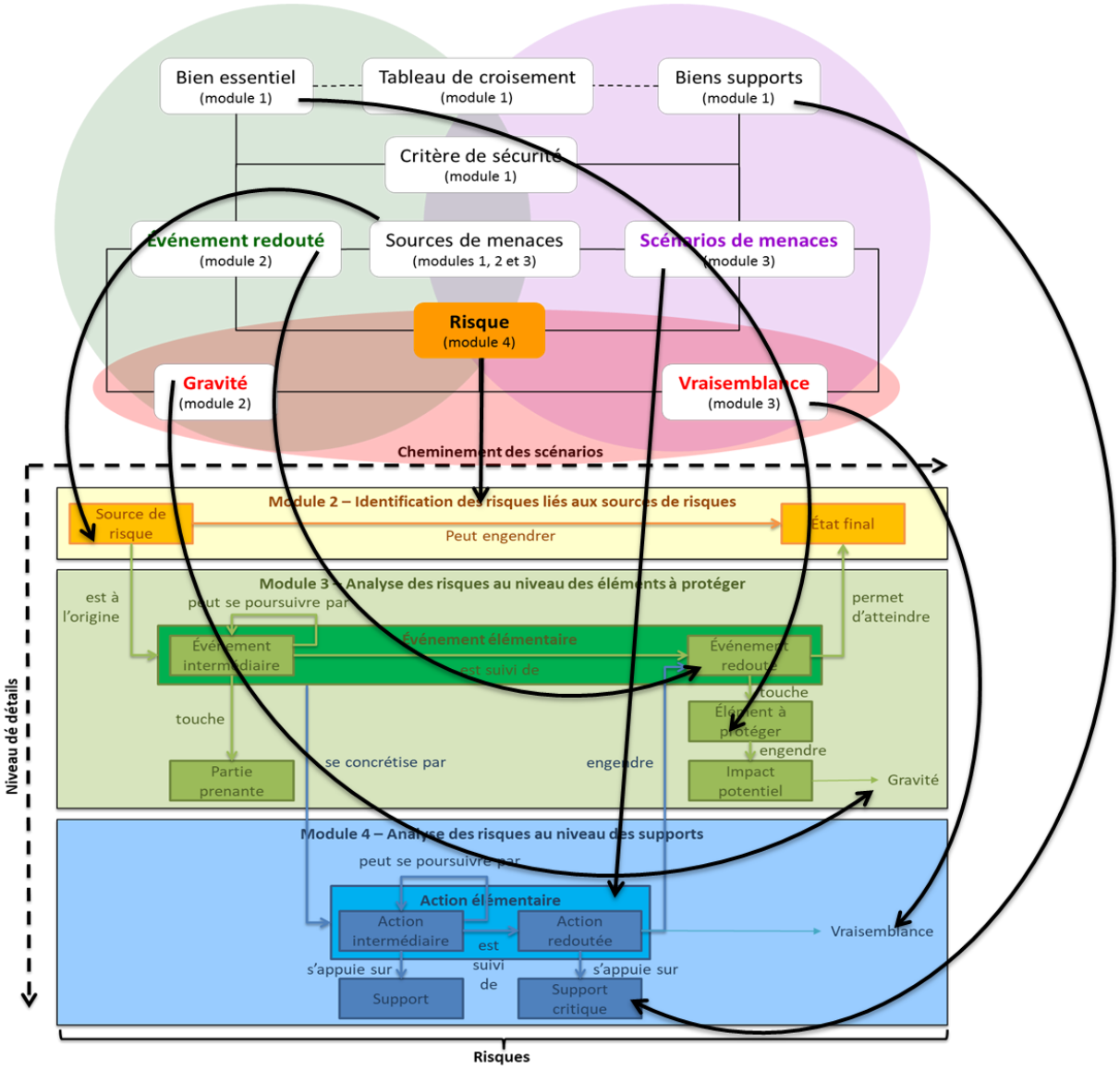

Figure 4 – Correspondance entre les anciens et nouveaux concepts

EBIOS & gestion des risques

L'enjeu : atteindre ses objectifs sur la base de décisions rationnelles

Née dans le domaine financier dans les années 50 et étendue à de nombreux autres domaines tels que la gestion de projet, la sécurité des personnes, la sûreté de fonctionnement, le marketing, l'environnement, la sécurité de l'information ou encore la protection de la vie privée, la gestion des risques a toujours eu pour objectif de rationaliser des situations pour aider à une prise de décision éclairée. Les choix effectués par les décideurs peuvent ainsi être faits au regard des éléments fournis par les *risk managers*. Et ces choix peuvent autant guider l'organisme vers l'atteinte de ses objectifs que faire évoluer sa stratégie.

Des pratiques différentes mais des principes communs

À l'heure actuelle, les principes communs de la gestion des risques se retrouvent dans les normes internationales (notamment ISO 31000) :

- le risque est défini comme l'effet de l'incertitude sur l'atteinte des objectifs. Il est caractérisé par un événement, ses conséquences et sa vraisemblance ;
- le processus de gestion des risques comprend l'établissement du contexte, l'appréciation des risques, le traitement des risques (y compris la validation du traitement des risques), la communication et la concertation relative aux risques, la surveillance et la revue (le contrôle), et l'enregistrement et l'établissement de rapports, dans un cycle d'amélioration continue.

La similitude des concepts et des méthodes d'analyse montre qu'il existe un modèle de gestion des risques suffisamment générique pour être partagé et enrichi par les retours d'expériences interdisciplinaires :

- les risques peuvent être décrits d'après leur cause et leurs impacts directs et indirects pour la sécurité des personnes ;
- par les circonstances à l'origine du risque et leurs conséquences pour les risques juridiques ;
- en termes de scénarios décrivant comment des sources de risques vont pouvoir exploiter les vulnérabilités des systèmes pour atteindre leur objectif et affecter la sécurité des éléments à protéger et l'organisme, comme c'est le cas en cybersécurité ;
- par des scénarios décrivant les actions de sources de risques sur des systèmes traitant des données à caractère personnel et leurs impacts potentiels sur les droits et libertés des personnes dans le domaine de la protection de la vie privée ;
- sans oublier le vocable spécifique à la protection des infrastructures vitales ou aux pratiques de l'intelligence économique.

La gestion des risques doit ainsi permettre de créer de la valeur, être intégrée aux processus organisationnels, être intégrée au processus de prise de décision, traiter explicitement de l'incertitude, être systématique, structurée et utilisée en temps utile, s'appuyer sur la meilleure information disponible, être taillée sur mesure, intégrer les facteurs humains et

culturels, être transparente et participative, être dynamique, itérative et réactive au changement, et faciliter l'amélioration et l'évolution continues de l'organisme.

EBIOS intègre l'ensemble de ces dimensions.

Comment EBIOS permet-elle de gérer les risques ?

L'établissement du contexte

Un contexte bien défini permet de gérer les risques de manière parfaitement appropriée, et ainsi de réduire les coûts à ce qui est nécessaire et suffisant au regard de la réalité du sujet étudié. Pour ce faire, il est essentiel d'appréhender les éléments à prendre en compte :

- le cadre mis en place pour gérer les risques ;
- les modalités d'estimation, d'évaluation et de validation du traitement des risques) ;
- la description du périmètre de l'étude et de son environnement (contexte externe et interne, contraintes, recensement des biens et de leurs interactions, *etc*.).

La boîte à outils EBIOS permet d'aborder tous ces points selon le degré de connaissance que l'on a du sujet étudié. Il sera ensuite possible de l'enrichir, de l'affiner et de l'améliorer à mesure que la connaissance du sujet s'améliore.

L'appréciation des risques

Il y a risque dès lors qu'il y a de l'incertitude sur un événement qui a des conséquences sur les objectifs. Notamment, cela peut se concrétiser dès lors que l'on a conjointement un événement et des conséquences. On peut ainsi comprendre qu'il n'y a plus de risque si l'un de ces facteurs manque (événement redouté ou conséquence). Or, il est extrêmement difficile, voire dangereux, d'affirmer avec certitude qu'un des facteurs est absent. Par ailleurs, chacun des facteurs peut contribuer à de nombreux risques différents, qui peuvent eux-mêmes s'enchaîner et se combiner en scénarios plus complexes, mais tout autant réalistes.

On va donc étudier chacun de ces facteurs, de la manière la plus large possible. On pourra alors mettre en évidence les facteurs importants, comprendre comment ils peuvent se combiner, estimer et évaluer (hiérarchiser) les risques. Un enjeu important est de réussir à obtenir les informations nécessaires qui puissent être considérées comme fiables. C'est la raison pour laquelle il est extrêmement important de veiller à ce que ces informations soient obtenues de manière à limiter les biais et à ce que la démarche soit reproductible.

Pour ce faire, la boîte à outils EBIOS se focalise tout d'abord sur les éléments à protéger (sources de risques, critères et impacts engendrés en cas de non-respect de ces critères), puis sur leurs supports (sources de risques, actions et vulnérabilités). Les risques peuvent alors être identifiés en combinant les événements redoutés et les modes opératoires, puis estimés et évalués afin d'obtenir une liste hiérarchisée selon leur importance.

Le traitement des risques

Les risques appréciés permettent de prendre des décisions objectives en vue de les maintenir à un niveau acceptable, compte-tenu des spécificités du contexte.

Pour ce faire, EBIOS permet de choisir le traitement des risques appréciés au travers des objectifs : il est ainsi possible, pour tout ou partie de chaque risque, de le réduire, de le partager (confier une partie du risque à un tiers plus à même de le traiter), de de refuser (se mettre en situation où le risque n'existe pas) ou de le maintenir (ne mettre aucune mesure supplémentaire en œuvre). Des mesures peuvent alors être proposées et négociées afin de satisfaire ces objectifs.

La manière dont les risques ont été gérés et les risques résiduels subsistants à l'issue du traitement doivent être validés, si possible formellement, par une autorité responsable du périmètre de l'étude. Cette validation se fait sur la base d'un dossier dont les éléments sont issus de l'étude réalisée.

La communication et la concertation relatives aux risques

Obtenir des informations pertinentes, présenter des résultats, faire prendre des décisions, valider les choix effectués, sensibiliser aux risques et aux mesures de sécurité à appliquer, correspondent à des activités de communication qui sont réalisées auparavant, pendant et après l'étude des risques.

Ce processus de communication et concertation relatives aux risques est un facteur crucial de la réussite de la gestion des risques. Si celle-ci est bien menée, et ce, de manière adaptée à la culture de l'organisme, elle contribue à l'implication, à la responsabilisation et à la sensibilisation des acteurs. Elle crée en outre une synergie autour de la sécurité de l'information, ce qui favorise grandement le développement d'une véritable culture de sécurité et du risque au sein de l'organisme.

L'implication des acteurs dans le processus de gestion des risques est nécessaire pour définir le contexte de manière appropriée, s'assurer de la bonne compréhension et prise en compte des intérêts des acteurs, rassembler différents domaines d'expertise pour identifier et analyser les risques, s'assurer de la bonne prise en compte des différents points de vue dans l'évaluation des risques, faciliter l'identification appropriée des risques, l'application et la prise en charge sécurisée d'un plan de traitement.

La surveillance et la revue des risques

Le cadre mis en place pour gérer les risques, ainsi que les résultats obtenus, doivent être pertinents et tenus à jour afin de prendre en compte les évolutions du contexte et les améliorations précédemment identifiées. Cette démarche d'amélioration continue doit s'appuyer sur des indicateurs de performance et, le cas échéant, permettre son intégration dans un cadre contractuel.

L'enregistrement et l'établissement de rapports

La démarche et les outils choisis doivent être formalisés. Ils peuvent faire l'objet de documents diffusables et de documents non diffusables, selon d'une part la volonté d'apporter la confiance par la transparence, et d'autre part le besoin de protéger les secrets industriels et la sécurité de l'organisme.

Couverture de la norme ISO 31000

Le schéma suivant montre la correspondance entre les outils d'EBIOS et la norme ISO 31000 :

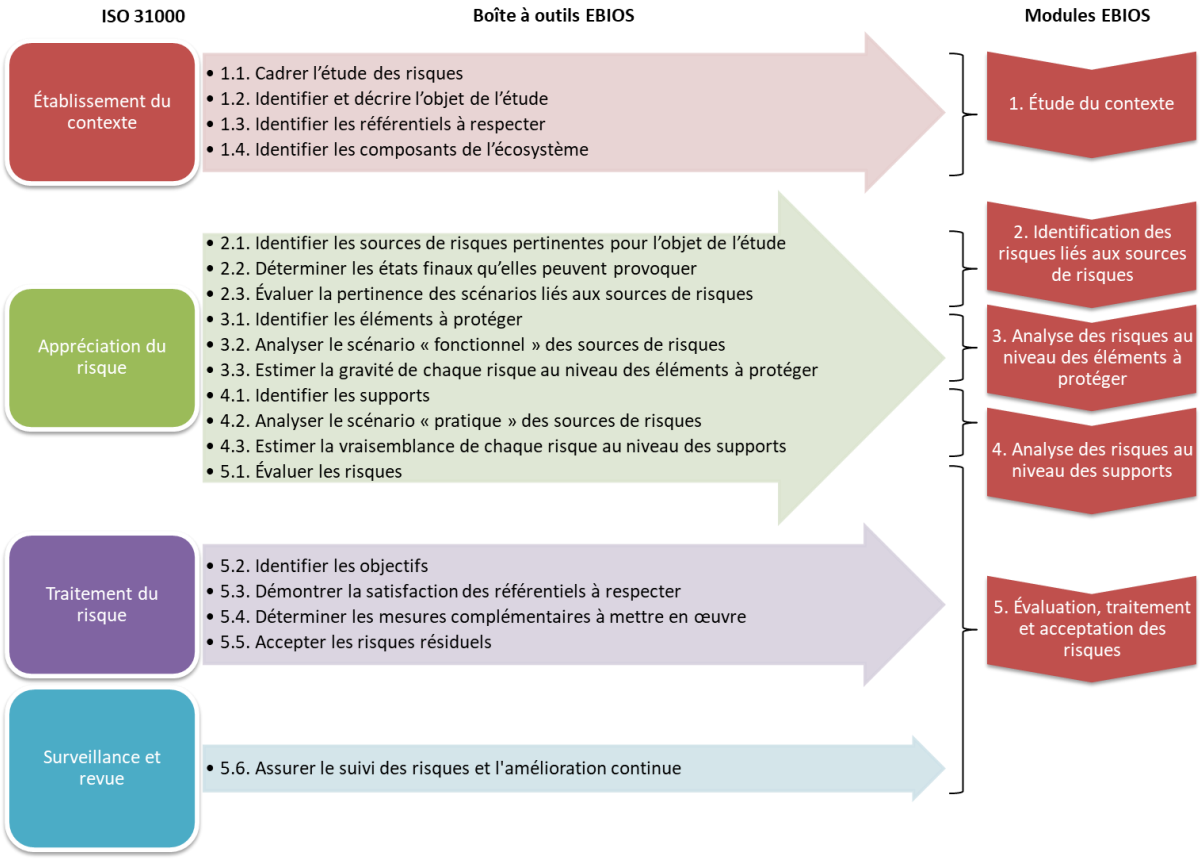

Figure 5 - Correspondance entre les outils d'EBIOS et ISO 31000