Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Sous-direction assistance, conseil et expertise
Bureau assistance et conseil

Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS

MÉTHODE DE GESTION DES RISQUES

Version du 25 janvier 2010

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 65 - Fax 01 71 75 84 90

Historique des modifications

Date	Objet de la modification	Statut
02/1997	Publication du guide d'expression des besoins et d'identification des objectifs de sécurité (EBIOS)	Validé
05/02/2004	Publication de la version 2 du guide EBIOS (convergence vers l'ISO 15408, ajout de l'étape 5 – Détermination des exigences de sécurité, clarifications et compléments)	Validé
25/01/2010	Amélioration du guide EBIOS : ❑ Prise en compte des nombreux retours d'expériences de l'ANSSI et du Club EBIOS ❑ Convergence des concepts vers les normes internationales relatives au système de management de la sécurité de l'information et à la gestion des risques ([ISO 27001], [ISO 27005], [ISO Guide 73] et [ISO 31000]) ❑ Regroupement des sections 1 (Présentation), 2 (Démarche) et 3 (Techniques) en un seul guide méthodologique ❑ Refonte complète de la présentation de la méthode ❑ Révision du contenu de la démarche méthodologique o Mise en évidence des avantages, des parties prenantes, des actions de communication et concertation, et des actions de surveillance et revue dans les descriptions des activités o Module 1 : ajout de la définition du cadre de la gestion des risques (vision projet, étude des sources de menaces…), étude du contexte plus souple et davantage liée aux processus métiers, regroupement de toutes les métriques au sein de la même activité, mise en évidence de l'identification des sources de menaces et des mesures de sécurité existantes o Module 2 : expression des besoins selon les processus métiers, développement de l'analyse des impacts, lien avec les sources de menaces afin de disposer d'événements redoutés complets au sein du même module, ajout de l'estimation et de l'évaluation des événements redoutés o Module 3 : étude des scénarios de menaces par bien support et non plus par vulnérabilité, lien avec les sources de menaces afin de disposer de scénarios de menaces complets au sein du même module, ajout de l'estimation et de l'évaluation des scénarios de menaces o Module 4 : mise en évidence de l'appréciation des risques, hiérarchisation explicite des risques, changement de forme des objectifs de sécurité (notions de réduction, transfert, refus, prise de risques) o Module 5 : ajout explicite des notions de défense en profondeur, de risques résiduels, de déclaration d'applicabilité, de plan d'action et de la validation	Validé

Table des matières

Note : les libellés entre crochets […] correspondent à des références bibliographiques en annexe.

Avant-propos

L'Agence nationale de la sécurité des systèmes d'information (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 meilleures pratiques et de logiciels, diffusés gratuitement sur son site Internet (http://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, français et européens. Il 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.

Ce document a été réalisé par le bureau assistance et conseil de l'ANSSI, avec la collaboration du Club EBIOS. La communauté des utilisateurs d'EBIOS enrichit régulièrement le référentiel complémentaire à ce document (techniques de mise en œuvre, bases de connaissances, guides d'utilisations spécifiques de la méthode, documents relatifs à la communication, à la formation, à la certification, logiciels…).

Introduction

Qu'est-ce qu'EBIOS ?

La méthode EBIOS[1] (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. Elle constitue de ce fait un outil complet de gestion des risques.

Objectifs du document

Les principaux objectifs du présent document sont :

- de fournir une base commune de concepts et d'activités pragmatiques à toute personne impliquée dans la gestion des risques, notamment dans la sécurité de l'information ;
- de satisfaire les exigences de gestion des risques d'un système de management de la sécurité de l'information ([ISO 27001]) ;
- de définir une démarche méthodologique complète en cohérence et en conformité avec les normes internationales de gestion des risques ([ISO 31000], [ISO 27005]…) ;
- d'établir une référence pour la certification de compétences relatives à la gestion des risques.

Domaine d'application

La démarche de gestion des risques présentée dans ce guide peut s'appliquer au secteur public et au secteur privé, à des petites structures (petites et moyennes entreprises, collectivités territoriales…) et à des grandes structures (ministère, organisation internationale, entreprise multinationale…), à des systèmes en cours d'élaboration et à des systèmes existants.

Historiquement employée dans le domaine de la sécurité de l'information, elle a été exploitée dans d'autres domaines.

EBIOS fait aujourd'hui figure de référence en France, dans les pays francophones et à l'international.

Références réglementaires et normatives

Le présent document décline les normes internationales [ISO 27005] et [ISO 31000], tout en satisfaisant les exigences de gestion des risques de l'[ISO 27001]. Aucune de ces normes n'est indispensable à l'utilisation de ce document.

Par ailleurs, il permet de mettre en œuvre les pratiques préconisées dans la réglementation ([RGS], [IGI 1300]…).

Structure du document

Après avoir présenté la problématique de la gestion des risques, notamment dans le domaine de la sécurité de l'information (chapitre 1), ce document explique ce qu'est EBIOS et son fonctionnement général (chapitre 2), puis décrit chaque activité de la démarche (chapitre 3).

Une démonstration de la couverture des normes internationales (annexe A) et les références utiles (annexe B) complètent le document.

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

1 Gérer durablement les risques sur le patrimoine informationnel

1.1 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 ou encore la sécurité de l'information, 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.

1.2 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 Guide 73]) :

- le risque est décrit par un événement, ses conséquences et sa vraisemblance ;
- le processus de gestion des risques comprend une étude du contexte, l'appréciation des risques, le traitement des risques, la validation du traitement des risques, la communication relative aux risques, le contrôle, dans une 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 :

- qu'ils soient 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 l'origine des menaces, de vulnérabilités exploitables, de sinistres et d'impacts comme c'est le cas en sécurité de l'information ;
- sans oublier le vocable spécifique à la protection des infrastructures vitales ou aux pratiques de l'intelligence économique.

Selon l'[ISO 31000], qui décrit la gestion des risques quel que soit le domaine d'application, elle devrait :

- 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 ;
- faciliter l'amélioration et l'évolution continues de l'organisme.

1.3 La spécificité de la sécurité de l'information : le patrimoine informationnel

La sécurité de l'information a pour but de protéger le patrimoine informationnel de l'organisme. Celui-ci permet son bon fonctionnement et l'atteinte de ses objectifs.

La valeur de ce patrimoine, dit informationnel, peut en effet être appréciée au regard des opportunités qu'il offre quand on l'utilise correctement et des conséquences négatives dans le cas contraire.

1.4 La difficulté : appréhender la complexité

Le patrimoine informationnel naît, vit et disparaît dans le cadre des différents systèmes d'information[2] qui l'entourent. Ceux-ci ont un but, des moyens, et sont organisés pour créer, exploiter, transformer et communiquer le savoir (informations) et le savoir-faire (fonctions, processus…). Ils sont par nature complexes, changeants et interfacés avec d'autres, chacun ayant ses propres contraintes.

De plus, ces systèmes d'information peuvent être confrontés à des problèmes variés, sont en évolution constante, sont parfois liés les uns aux autres, et sont difficiles à mettre objectivement en évidence.

Il est donc nécessaire d'employer des moyens rationnels pour appréhender la protection du patrimoine informationnel de manière à la fois globale et dynamique.

1.5 Le besoin d'une méthode

L'adoption de démarches et d'outils de prise de décision rationnelle et de gestion de la complexité apparaît aujourd'hui comme une condition nécessaire à la sécurité de l'information. Il convient pour cela d'utiliser des approches de gestion des risques structurées, éprouvées, tout en prenant garde aux illusions de scientificité et à la manipulation de chiffres, offertes par de nombreuses méthodes.

D'une manière générale, une approche méthodologique permet de :

- disposer d'éléments de langage communs ;
- disposer d'une démarche claire et structurée à respecter ;
- se baser sur un référentiel validé par l'expérience ;
- s'assurer d'une exhaustivité des actions à entreprendre ;
- réutiliser la même approche en amélioration continue et sur d'autres périmètres…

En matière de gestion des risques de sécurité de l'information, une approche méthodologique permet également de :

- établir le contexte en prenant en compte ses spécificités (contexte interne et externe, enjeux, contraintes, métriques…) ;
- apprécier les risques (les identifier au travers des événements redoutés et des scénarios de menaces, les estimer et les évaluer) ;
- traiter les risques (choisir les options de traitement à l'aide d'objectifs de sécurité, déterminer des mesures de sécurité appropriées et les mettre en œuvre) ;
- valider le traitement des risques (valider formellement le plan de traitement des risques et les risques résiduels) ;
- communiquer sur les risques (obtenir les informations nécessaires, présenter les résultats, obtenir des décisions et faire appliquer les mesures de sécurité) ;
- suivre les risques (veiller à ce que les retours d'expériences et les évolutions du contexte soient prises en compte dans le cadre de gestion des risques, les risques appréciés et les mesures de sécurité).

[2] On parle évidemment ici de la notion de système d'information correspondant à l'ensemble de biens supports (organisations, lieux, personnels, logiciels, matériels et réseaux) organisé pour traiter des biens essentiels (informations, processus, fonctions…). Cette notion est encore parfois confondue avec celle de système informatique, principalement du fait que la sécurité des systèmes d'information (SSI) a ses origines dans le domaine informatique. Afin d'éviter les confusions encore trop fréquentes, le libellé "sécurité de l'information" a donc été préféré à celui de "SSI" dans ce guide.

2 EBIOS : la méthode de gestion des risques

2.1 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 dans la réflexion :

- le cadre mis en place pour gérer les risques ;
- les critères à prendre en considération (comment estimer, évaluer et valider le 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…).

La méthode 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 de sécurité de l'information dès lors qu'on a conjointement :

- une source de menace ;
- une menace ;
- une vulnérabilité ;
- un impact.

On peut ainsi comprendre qu'il n'y a plus de risque si l'un de ces facteurs manque. 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. Le principal enjeu reste, par conséquent, 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 méthode EBIOS se focalise tout d'abord sur les événements redoutés (sources de menaces, besoins de sécurité et impacts engendrés en cas de non respect de ces besoins), puis sur les différents scénarios de menaces qui peuvent les provoquer (sources de menaces, menaces et vulnérabilités). Les risques peuvent alors être identifiés en combinant les événements redoutés et les scénarios de menaces, 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 de sécurité : il est ainsi possible, pour tout ou partie de chaque risque, de le réduire, de le transférer (partage des pertes), de l'éviter (se mettre en situation où le risque n'existe pas) ou de le prendre (sans rien faire). Des mesures de sécurité peuvent alors être proposées et négociées afin de satisfaire ces objectifs.

La validation du traitement des risques

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, généralement appelé homologation de sécurité, 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.

EBIOS propose ainsi des actions de communication à réaliser dans chaque activité de la démarche.

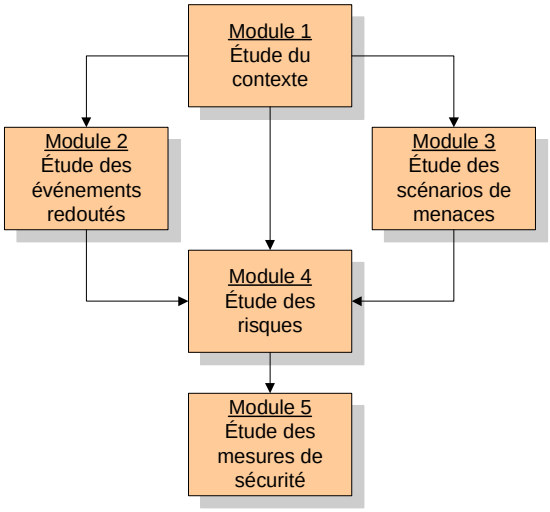
La surveillance et la revue des risques

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.

Pour ce faire, la méthode EBIOS prévoit les principaux éléments à surveiller lors de la réalisation de chaque activité et lors de toute évolution du contexte afin de garantir de bons résultats et de les améliorer en continu.

2.2 Une démarche itérative en cinq modules

La méthode formalise une démarche de gestion des risques découpée en cinq modules représentés sur la figure suivante :



La démarche est dite itérative. En effet, il sera fait plusieurs fois appel à chaque module afin d'en améliorer progressivement le contenu, et la démarche globale sera également affinée et tenue à jour de manière continue.

Module 1 – Étude du contexte

À l'issue du premier module, qui s'inscrit dans l'établissement du contexte, le cadre de la gestion des risques, les métriques et le périmètre de l'étude sont parfaitement connus ; les biens essentiels, les biens supports sur lesquels ils reposent et les paramètres à prendre en compte dans le traitement des risques sont identifiés.

Module 2 – Étude des événements redoutés

Le second module contribue à l'appréciation des risques. Il permet d'identifier et d'estimer les besoins de sécurité des biens essentiels (en termes de disponibilité, d'intégrité, de confidentialité…), ainsi que tous les impacts (sur les missions, sur la sécurité des personnes, financiers, juridiques, sur l'image, sur l'environnement, sur les tiers et autres…) en cas de non respect de ces besoins et les sources de menaces (humaines, environnementales, internes, externes, accidentelles, délibérées…) susceptibles d'en être à l'origine, ce qui permet de formuler les événements redoutés.

Module 3 – Étude des scénarios de menaces

Le troisième module s'inscrit aussi dans le cadre de l'appréciation des risques. Il consiste à identifier et estimer les scénarios qui peuvent engendrer les événements redoutés, et ainsi composer des risques. Pour ce faire, sont étudiées les menaces que les sources de menaces peuvent générer et les vulnérabilités exploitables.

Module 4 – Étude des risques

Le quatrième module met en évidence les risques pesant sur l'organisme en confrontant les événements redoutés aux scénarios de menaces. Il décrit également comment estimer et évaluer ces risques, et enfin comment identifier les objectifs de sécurité qu'il faudra atteindre pour les traiter.

Module 5 – Étude des mesures de sécurité

Le cinquième et dernier module s'inscrit dans le cadre du traitement des risques. Il explique comment spécifier les mesures de sécurité à mettre en œuvre, comment planifier la mise en œuvre de ces mesures et comment valider le traitement des risques et les risques résiduels.

2.3 Différents usages d'EBIOS

EBIOS est une boîte à outils à usage variable

Comme toute véritable méthode de gestion des risques, EBIOS permet d'analyser des risques, 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 seront adaptés à l'usage désiré. En effet, la méthode ne sera pas utilisée de la même manière selon le sujet étudié, les livrables attendus, le degré de connaissance du périmètre de l'étude, le secteur auquel on l'applique…

Variation de la focale selon le sujet étudié

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, ou même un composant de produit.
La méthode peut également être employée pour étudier dans un premier temps un sujet global (par exemple un organisme ou un système complexe composé de plusieurs sous-systèmes), pour ensuite se focaliser sur un sous-ensemble (par exemple quelques processus de l'organisme jugés critiques ou des sous-systèmes).

Il est bien évident qu'une telle diversité de sujets ne sera pas abordée de manière uniforme si l'on souhaite des résultats pertinents. C'est ici le niveau de détail qui variera : plus le sujet est large, moins le niveau de détail est important, et inversement.

Ainsi, une étude de haut niveau d'abstraction portera sur des biens essentiels (par exemple les grandes activités d'un organisme) et des biens supports (par exemple les logiciels dans leur ensemble) macroscopiques, et une étude focalisée portera sur des biens essentiels (par exemple un champ d'une base de données) et des biens supports (par exemple une version spécifique de système de gestion de bases de données) détaillés.
Il conviendra 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.

Variation des outils et du style selon les livrables attendus

La gestion des risques permettant de rationaliser de nombreuses activités, la méthode EBIOS permet d'élaborer ou de contribuer à l'élaboration de nombreux documents livrables :

- des documents fondateurs (schémas directeurs, politiques de sécurité de l'information, notes de cadrage, stratégies de sécurité, plans de continuité d'activités…) ;
- des spécifications (fiches d'expression rationnelle des objectifs de sécurité – FEROS au sens du [Guide 150], profils de protection – PP au sens de l'[ISO 15408], cibles de sécurité au sens de l'[ISO 15408] ou au sens général, cahiers des charges, plans de traitement au sens de l'[ISO 27001]…) ;
- d'autres livrables de sécurité de l'information (cartographie des risques, référentiels d'audit, tableaux de bord…).

La manière d'utiliser la méthode EBIOS doit être adaptée au(x) livrable(s) que l'on souhaite produire afin de ne réaliser que les activités nécessaires et suffisantes et d'en exploiter directement les résultats. Il convient dès lors de bien définir le(s) livrable(s) attendu(s), les destinataires et l'objectif de cette communication (prise de décision, sensibilisation…) pour choisir les activités de la démarche à réaliser et présenter les résultats directement dans la forme la plus appropriée.

Ainsi, la rédaction d'une FEROS dans le but d'homologuer un système d'information ne requiert pas de réaliser les dernières activités de la démarche EBIOS et doit être suffisamment synthétique et claire pour être lue dans le cadre d'une commission d'homologation ; l'étude pourra être détaillée, mais le style rédactionnel sera adapté en ce sens. Une politique de sécurité de l'information d'un organisme peut ne pas demander à étudier les scénarios de menaces, mais uniquement les événements redoutés ; le style de rédaction sera adapté aux personnes qui devront appliquer cette politique. L'élaboration d'une déclaration d'applicabilité et d'un plan de traitement (au sens de l'[ISO 27001]) requiert l'emploi de l'[ISO 27002] dans les dernières activités de la démarche…

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

Il est conseillé de gérer les risques depuis les premières réflexions relatives à un nouveau service ou un nouveau système. En effet, cela permet le cas échéant 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 fera 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'intéressera aux grands enjeux, dans un second temps on pourra affiner la description du sujet et élaborer des scénarios d'événements redoutés, puis on pourra étudier les scénarios de menaces pour obtenir de véritables risques et des mesures de sécurité… C'est donc en réalisant des itérations successives et des activités supplémentaires que la gestion des risques accompagnera le cycle de vie du sujet.

Ainsi, lors des études d'opportunité et de faisabilité d'un système d'information, il sera possible d'étudier son contexte, d'identifier les enjeux du système, de faire émerger les fonctionnalités ou les processus essentiels, d'exprimer leurs besoins de sécurité, d'estimer les impacts et d'identifier des sources de menaces. Une seconde itération de la démarche aura lieu lors de la conception générale et de la conception détaillée : les grandes fonctionnalités seront décomposées en fonctions plus détaillées et en informations manipulées, les biens supports seront identifiés, les besoins et les impacts seront affinés, les sources de menaces développées et consolidées, les menaces et les vulnérabilités étudiées, les risques appréciés, les objectifs identifiés, les mesures de sécurité déterminées et les risques résiduels mis en évidence. Lors de la phase de réalisation, une autre itération permettra de rectifier et de compléter l'ensemble de l'étude, notamment au niveau des mesures de sécurité et des risques résiduels. Enfin, en phase d'exploitation et jusqu'à la fin de vie du système, les évolutions du contexte (biens supports, sources de menaces, vulnérabilités…) permettront d'ajuster l'étude et de gérer les risques en continu.

Variation du cadre de référence selon le secteur

La méthode EBIOS est suffisamment générique pour être appliquée à différents secteurs. Elle a majoritairement été utilisée dans le secteur de la sécurité de l'information, mais également dans le secteur des infrastructures vitales, de l'ergonomie des outils de travail… La convergence de la méthode, en termes de vocabulaire et de démarche, vers les plus récents travaux de normalisation internationale ([ISO Guide 73], [ISO 31000]…) la rend applicable encore plus largement.

L'usage d'EBIOS dans un autre secteur que celui de la sécurité de l'information est en effet relativement aisé. Il suffit éventuellement de transposer la terminologie et d'exploiter des bases de connaissances du secteur concerné si celles-ci ne semblent pas applicables ou comprises. En effet, chaque secteur (protection de l'environnement, protection des personnes, gestion des risques juridiques…) dispose d'un cadre de référence, d'une culture et de connaissances qui lui sont propres. Les principes et les activités 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 de la méthode à la terminologie employée dans ce secteur et de créer des bases de connaissances de critères de sécurité, de sources de menaces, de biens supports, de menaces et de vulnérabilités spécifiques, et d'intégrer les plans de prévention et de réaction gouvernementaux en guise de bases de mesures de sécurité.

Une réflexion préalable sur la stratégie de mise en œuvre est nécessaire

La méthode EBIOS est donc une véritable boîte à outils, qu'il convient d'utiliser de manière appropriée au sujet étudié, aux livrables attendus, à la phase du cycle de vie et au secteur dans lequel les risques doivent être gérés. On définit ainsi la stratégie de gestion des risques de sécurité de l'information.

Il est par conséquent important de bien cerner ces paramètres avant d'initier la démarche pour :

- prévoir l'éventuelle décomposition du périmètre en sous-périmètres ;
- prévoir les éventuelles itérations de la méthode ;
- choisir le niveau de détail approprié ;
- choisir les activités pertinentes, la manière de les réaliser et les résultats à produire ;
- prévoir les éventuels ajustements de terminologie et des bases de connaissances…

2.4 Fiabiliser et optimiser la prise de décision

Un outil de négociation et d'arbitrage

En fournissant les justifications nécessaires à la prise de décision (descriptions précises, enjeux stratégiques, risques détaillés avec leur impact sur l'organisme, objectifs et exigences de sécurité explicites), EBIOS est un véritable outil de négociation et d'arbitrage.

Un outil de sensibilisation

EBIOS permet de sensibiliser toutes les parties prenantes d'un projet (direction générale, financière, juridique ou des ressources humaines, maîtrise d'ouvrage, maîtrise d'œuvre, utilisateurs), d'impliquer les acteurs du système d'information et d'uniformiser le vocabulaire.

Un outil compatible avec les normes internationales

La méthode EBIOS contribue à la reconnaissance internationale des travaux de sécurité en assurant la compatibilité avec les normes internationales. Elle permet en effet de mettre en œuvre l'[ISO 31000] et l'[ISO 27005]. Elle constitue en outre le cœur du système de management de la sécurité dé l'information de l'[ISO 27001]. Elle peut exploiter les mesures de sécurité de l'[ISO 27002]…

Une souplesse d'utilisation et de multiples livrables

La démarche peut être adaptée au contexte de chacun et ajustée à sa culture et à ses outils. Sa flexibilité en fait une véritable boîte à outils pour de nombreuses finalités, dans le cadre de projets ou d'activités existantes, dans d'autres domaines que celui de la sécurité de l'information…

Une méthode rapide

La durée de réalisation d'une étude EBIOS est optimisée car elle permet d'obtenir les éléments nécessaires et suffisants selon le résultat attendu.

Un outil réutilisable

EBIOS favorise la pérennité des analyses de risques et la cohérence globale de la sécurité. En effet, l'étude spécifique d'un système peut être basée sur l'étude globale de l'organisme ; une étude peut être régulièrement mise à jour afin de gérer les risques de manière continue ; l'étude d'un système comparable peut aussi être utilisée comme référence.

Une approche exhaustive

Contrairement aux approches d'analyse des risques par catalogue de scénarios prédéfinis, la démarche structurée de la méthode EBIOS permet d'identifier et de combiner les éléments constitutifs des risques. Cette construction méthodique garantit l'exhaustivité de l'analyse des risques.

Un référentiel complet

La méthode dispose de bases de connaissances riches et adaptables (types de biens supports, menaces, vulnérabilités, mesures de sécurité…), d'un logiciel libre et gratuit, de formations de qualité pour le secteur public et le secteur privé et de documents de communication variés.

Une expérience éprouvée

Créée en 1995, EBIOS repose sur une expérience éprouvée en matière de conseil et d'assistance à maîtrise d'ouvrage. Elle contribue à la notoriété des outils méthodologiques de l'ANSSI.

De nombreux utilisateurs

Elle est largement utilisée dans le secteur public (l'ensemble des ministères et des organismes sous tutelle), dans le secteur privé (cabinets de conseil, industriels, petites et grandes entreprises), en France et à l'étranger (Union européenne, Québec, Belgique, Tunisie, Luxembourg…). L'association Club EBIOS réunit régulièrement la communauté d'experts et d'utilisateurs soucieux de contribuer au développement de la méthode et de disposer des dernières informations à son sujet.

2.5 Rigueur de la méthode EBIOS

EBIOS met en œuvre des contrôles méthodologiques afin d'assurer d'une part la validité interne et externe de la démarche, et d'autre part que les résultats de l'étude sont fidèles à la réalité. Il en résulte ainsi un outil méthodologique rigoureux.

Une méthode valide : la démarche peut être reproduite et vérifiée

La méthodologie, science de la méthode, est une méta-méthode que l'on peut voir comme une sorte de boîte à outils. Dans cette boîte, chaque outil est un processus, une technique ou une technologie appropriée à résoudre un problème particulier. Elle permet de le résoudre de manière plus efficace et de systématiser l'étude, indépendamment du périmètre de l'étude lui-même, en établissant une suite d'actions à mener, de questions à se poser, de choix à faire…

Ceci permet d'obtenir des résultats qui ont une rigueur démontrable par une démarche qui peut être reproduite et vérifiée.

Sur le plan scientifique, cette validité se décompose en validité interne et en validité externe.
La validité interne fait référence à l'exactitude des résultats. Il y a validité interne lorsqu'il y a concordance entre les données et leur interprétation. Une étude peut ainsi être considérée pour sa validité interne, c'est-à-dire que les résultats correspondent à ce qui a été étudié pour des individus et un moment donnés.
La validité externe réfère à la possibilité de généraliser des résultats, c'est ce qui permet d'en tirer des conclusions impartiales au sujet d'une population cible plus grande que l'ensemble des individus ayant participé à l'étude. Par exemple, les résultats d'une étude menée avec un échantillon de sept participants dans une unité d'affaires peuvent être généralisés à l'ensemble de l'organisation lorsque l'étude a un niveau adéquat de validité externe.

Une méthode fidèle : la démarche retranscrit la réalité

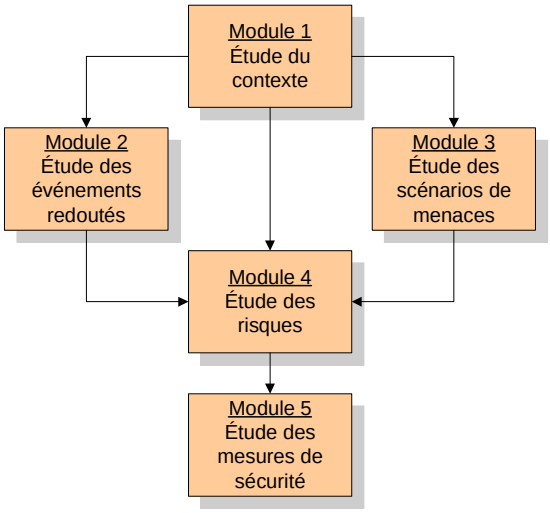
La méthode peut s'avérer un outil efficace lorsqu'elle est utilisée diligemment dans un contexte bien déterminé (avec des contraintes et des besoins particuliers). Néanmoins, comme d'autres méthodologies servant à répondre à des questionnements, elle doit tenir compte de plusieurs sources d'erreur et de biais, en relation à la sélection des participants, aux mesures utilisées, à l'analyse (explicative ou statistique) ou à l'interprétation des résultats… Elle doit également donner aux personnes réalisant l'étude des moyens pour limiter l'impact de ces sources d'erreurs et de ces biais.

Afin d'assurer que la méthode est fidèle à la réalité, il convient de respecter un ensemble de critères :

- la crédibilité : les résultats de l'analyse des données recueillies reflètent l'expérience des participants ou le contexte avec crédibilité ;
- l'authenticité : la perspective émique (intérieure des participants) présentée dans les résultats de l'analyse démontre une conscience des différences subtiles d'opinion de tous les participants ;
- le criticisme : le processus d'analyse des données recueillies et des résultats montre des signes d'évaluation du niveau de pertinence de ces informations ;
- l'intégrité : l'analyse reflète une validation de la validité répétitive et récursive associée à une présentation simple ;
- l'explicité : les décisions et interprétations méthodologiques, de même que les positions particulières de ceux qui réalisent l'étude, sont considérées ;
- le réalisme : des descriptions riches et respectant la réalité sont illustrées clairement et avec verve dans les résultats ;
- la créativité : des méthodes d'organisation, de présentation et d'analyse des données créatives sont incorporées à l'étude ;
- l'exhaustivité : les conclusions de l'étude couvrent l'ensemble des questions posées au départ de façon exhaustive ;
- la congruence : le processus et les résultats sont congruents, ils vont de pair les uns avec les autres et ne s'inscrivent pas dans un autre contexte que celui de la situation étudiée ;
- la sensibilité : l'étude a été faite en tenant compte de la nature humaine et du contexte socioculturel de l'organisation étudiée.

3 Description de la démarche

Ce chapitre présente les cinq modules de la méthode EBIOS :



Chaque activité des cinq modules est décrite sous la forme d'une fiche selon le même formalisme :

Objectif
But et description de l'activité, replacée dans un contexte général.

Avantages
Liste des principaux avantages apportés par la mise en œuvre de l'activité.

Données d'entrée
Liste des informations d'entrée, nécessaires à la mise en œuvre de l'activité.

Actions préconisées et rôle des parties prenantes
Liste des actions préconisées et responsabilités génériques pour réaliser l'activité :
- "R" = Responsable de la mise en œuvre de l'activité
- "A" = Autorité légitime pour approuver l'activité (imputable)
- "C" = Consulté pour obtenir les informations nécessaires à l'activité
- "I" = Informé des résultats de l'activité

Les fonctions génériques, qui peuvent endosser ces responsabilités, sont les suivantes :
- Responsable = Responsables du périmètre de l'étude
- RSSI = Responsable de la sécurité de l'information
- *Risk manager* = Gestionnaire de risques
- Autorité = Autorités de validation
- Dépositaire = Dépositaire de biens essentiels (utilisateurs ou maîtrises d'ouvrage)
- Propriétaire = Propriétaire de biens supports

Données produites
Liste des informations de sortie, produites par les actions de l'activité.

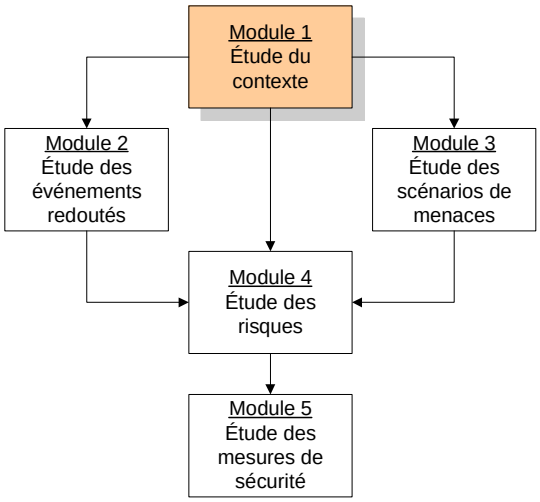
Communication et concertation
Liste des principales idées pour obtenir de l'information (techniques à employer) et la restituer (présentation des résultats, représentations graphiques…).

Surveillance et revue
Liste des points de contrôle pour vérifier la qualité de la réalisation de l'activité et la tenue à jour des informations résultantes.

Propositions pour mettre en œuvre les actions préconisées
Description détaillée de la (des) manière(s) possible(s) de procéder pour mettre en œuvre les actions préconisées.

Module 1 – Étude du contexte

Ce module a pour objectif de collecter les éléments nécessaires à la gestion des risques, afin qu'elle puisse être mise en œuvre dans de bonnes conditions, qu'elle soit adaptée à la réalité du contexte d'étude et que ses résultats soient pertinents et utilisables par les parties prenantes.



Il permet notamment de formaliser le cadre de gestion des risques dans lequel l'étude va être menée. Il permet également d'identifier, de délimiter et de décrire le périmètre de l'étude, ainsi que ses enjeux, son contexte d'utilisation, ses contraintes spécifiques…

À l'issue de ce module, le champ d'investigation de l'étude est donc clairement circonscrit et décrit, ainsi que l'ensemble des paramètres à prendre en compte dans les autres modules.

Le module comprend les activités suivantes :

- Activité 1.1 – Définir le cadre de la gestion des risques
- Activité 1.2 – Préparer les métriques
- Activité 1.3 – Identifier les biens

Activité 1.1 – Définir le cadre de la gestion des risques

Objectif

Cette activité fait partie de l'établissement du contexte. Elle a pour but de circonscrire le périmètre d'étude et de définir le cadre dans lequel la gestion des risques va être réalisée.

Avantages

- Permet de circonscrire objectivement le périmètre de l'étude
- Permet de s'assurer de la légitimité et de la faisabilité des réflexions qui vont être menées
- Permet d'orienter les travaux et les livrables en fonction des objectifs réels

Données d'entrée

- Données concernant le contexte du périmètre de l'étude (documents stratégiques, documents relatifs aux missions, les attributions et l'organisation, politique de gestion des risques…).
- Données concernant le contexte de la gestion des risques et la structure de travail

Actions préconisées et rôle des parties prenantes

Actions : \ Parties prenantes :	Responsable	RSSI	*Risk manager*	Autorité	Dépositaire	Propriétaire
Action 1.1.1. Cadrer l'étude des risques	R	C	C	I		
Action 1.1.2. Décrire le contexte général	R			I		
Action 1.1.3. Délimiter le périmètre de l'étude	R			A		
Action 1.1.4. Identifier les paramètres à prendre en compte	R			I		
Action 1.1.5. Identifier les sources de menaces	R	C	C	I		

Données produites

- Synthèse relative au cadre de la gestion des risques
- Paramètres à prendre en compte
- Sources de menaces

Communication et concertation

- Les données sont obtenues à l'aide de documents et d'entretiens avec les parties prenantes
- Les données produites peuvent faire l'objet d'une note de cadrage
- Elles peuvent utilement être intégrées à la politique de sécurité de l'information

Surveillance et revue

- Le périmètre de l'étude (toute l'organisation, une unité d'affaires, un processus…) est défini et délimité de façon claire et explicite
- La définition du risque est adaptée au contexte particulier de l'organisation et délimitée de façon claire et explicite
- La population à l'étude est définie
- Le type d'échantillonnage (probabiliste, non probabiliste ou autre) est identifié et justifié en fonction de la population à l'étude, du contexte et de la portée de l'étude
- Les critères de sélection (inclusion et exclusion) des participants à l'étude sont choisis afin de représenter de façon équilibrée l'ensemble de l'organisation dans laquelle est réalisée l'étude
- Des processus sont mis en place pour vérifier qu'on a bien considéré toutes les informations nécessaires (par rapport à l'état de l'art, aux organismes dans le même secteur d'activités…). Par exemple, l'identification à priori des principaux éléments qui devront être considérés dans l'étude permettra de faire une validation post-étude de résultats afin de s'assurer que rien n'a été omis. Dans le cas de variance entre les attentes définies à priori et l'analyse post-étude, l'organisation pourra évaluer les causes de cette variance afin de s'assurer que celle-ci fut exhaustive et, au besoin, prendre des actions correctives.

Propositions pour mettre en œuvre les actions préconisées

Action 1.1.1. Cadrer l'étude des risques

Description

Cette action consiste à formaliser le but de l'étude (en termes d'intention et de livrables) et à définir la manière dont elle va être menée. En effet, la démarche qui va être employée (actions à entreprendre parmi l'ensemble des actions de la méthode EBIOS, particularités de mise en œuvre, niveau de détail, parties prenantes à impliquer…) dépend essentiellement de l'objectif de l'étude.

Il convient tout d'abord de formaliser le but de l'étude, comme par exemple :
- d'optimiser les processus métiers en maîtrisant les risques de sécurité de l'information ;
- de mettre en place un système de management de la sécurité de l'information ;
- d'homologuer un système d'information ;
- d'élaborer d'une politique de sécurité de l'information ;
- de contribuer à la gestion globale des risques de l'organisme…

Ensuite, il convient d'identifier clairement les livrables attendus, comme par exemple :
- une politique de sécurité de l'information, à destination de tout le personnel ;
- un cahier des charges à soumettre pour un appel d'offres ;
- une cartographie des risques pour le *risk manager* ;
- une fiche d'expression rationnelle des objectifs de sécurité (FEROS), à destination d'une commission d'homologation ;
- une cible de sécurité en vue d'une évaluation de produit de sécurité ;
- des orientations stratégiques en matière de sécurité de l'information pour la direction…

Enfin, il convient de planifier la structure de travail pour cadrer l'étude qui va être réalisée :
- les actions à entreprendre (choix des activités ou des actions, particularités d'application…) ;
- les ressources à prévoir et le rôle des parties prenantes ;
- le calendrier prévisionnel ;
- les documents à produire (enregistrements, livrables intermédiaires et finaux) ;

On peut également préciser :
- les chemins de décision à emprunter ;
- les mécanismes de communication interne et externe ;
- la population à l'étude ;
- les critères de sélection des personnes participant à l'étude ;
- la méthode selon laquelle les performances de la gestion des risques sont évaluées.

Conseils

- Formuler un objectif explicite et en lien avec les objectifs de l'organisme.
- Identifier clairement le(s) livrable(s) attendu(s) et les personnes à qui il(s) est(sont) destiné(s).
- S'interroger sur l'utilité de chaque activité de la méthode et sur la manière de la réaliser (quelles actions ? quelles parties prenantes ?...) pour satisfaire l'objectif de l'étude et/ou pour élaborer le(s) livrable(s). Le niveau de maturité de l'organisme constitue également un élément à considérer.
- Afin de dimensionner convenablement les charges nécessaires à la réalisation des activités, il convient de ne pas négliger les réunions impliquant de nombreux participants.

Exemple

L'objectif de l'étude : gérer les risques SSI sur le long terme et élaborer une politique
Le Directeur de la société @RCHIMED souhaite que les risques de sécurité de l'information qui pourraient empêcher l'organisme d'atteindre ses objectifs soient gérés, et ce, de manière continue, afin d'être au plus proche d'une réalité en mouvement.

Une politique de sécurité de l'information doit ainsi être produite, appliquée et contrôlée.

Par ailleurs, il n'exclut pas l'idée de faire certifier à terme les principales activités du cabinet selon l'ISO 27001 et reconnaît l'intérêt d'exploiter des meilleures pratiques reconnues internationalement (ISO 27002). Par conséquent, une déclaration d'applicabilité devrait être produite ultérieurement.

Le plan d'action : une réflexion sur 15 jours qui requiert la participation de tous
Pour ce faire, le cabinet @RCHIMED prévoit la structure de travail suivante :

Activités d'EBIOS	***Directeur***	***Directeur adjoint***	***Comité de suivi***	***Secrétariat***	***Service commercial***	***Bureau d'études***	***Service comptabilité***	***Documents à produire en plus de l'étude des risques***	***Consignes particulières***	***Ressources estimées (en h.j)***	***Durée (en jours)***
Activité 1.1 – Définir le cadre de la gestion des risques		*R*	*C*	*I*	*I*	*I*	*I*			*2*	*2*
Activité 1.2 – Préparer les métriques		*R*	*C*	*I*	*I*	*I*	*I*		*Vérifier l'uniformité de la compréhension*	*2*	*2*
Activité 1.3 – Identifier les biens	*A*	*R*	*C*	*C*	*C*	*C*	*I*	*Note de cadrage*	*Ne pas trop détailler*	*6*	*2*
Activité 2.1 – Apprécier les événements redoutés		*R*	*C*	*C*	*C*	*C*	*I*		*Utiliser les bases génériques*	*6*	*2*
Activité 3.1 – Apprécier les scénarios de menaces		*R*	*C*	*C*	*C*	*C*	*I*		*Utiliser les bases génériques*	*6*	*2*
Activité 4.1 – Apprécier les risques		*R*	*C*	*I*	*I*	*I*	*I*			*1*	*1*
Activité 4.2 – Identifier les objectifs de sécurité	*A*	*R*	*C*	*I*	*I*	*I*	*I*	*Note de stratégie*		*2*	*1*
Activité 5.1 – Formaliser les mesures de sécurité à mettre en œuvre	*A*	*R*	*C*	*C*	*C*	*C*	*I*	*Politique de sécurité de l'information*		*15*	*3*
Activité 5.2 – Mettre en œuvre les mesures de sécurité	*A*	*R*	*I*	*C*	*C*	*C*	*I*	*Homologation*	*Cette activité ne sera réalisée de suite*	*0*	*0*

Légende : R = Réalisation ; A = Approbation ; C = Consultation ; I = Information

Action 1.1.2. Décrire le contexte général

Description

Cette action consiste à se familiariser avec l'environnement et la conjoncture du périmètre de l'étude, de manière à inscrire la gestion de risques dans sa réalité et à identifier les éléments pouvant impacter la manière de gérer les risques de sécurité de l'information.

Le but est ici de faciliter l'intégration de la gestion des risques dans la culture, la structure et les processus de l'organisme en mettant en évidence les éléments qu'il conviendra de considérer dans la réflexion de sécurité de l'information. L'étude pourra ainsi être adaptée à son contexte spécifique afin que les objectifs et préoccupations de toutes les parties prenantes puissent être pris en compte.

On peut ainsi utilement collecter les informations suivantes :

- sur le contexte externe :
  - l'environnement social et culturel, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local ;
  - les facteurs et tendances ayant un impact déterminant sur les objectifs ;
  - les relations avec les parties prenantes externes, leurs perceptions et leurs valeurs ;
- sur le contexte interne :
  - la description générale de l'organisme ;
  - les aptitudes en termes de ressources (capital, personnels, technologies…) ;
  - les missions (ce que l'organisme doit faire) ;
  - les valeurs (ce que l'organisme fait bien) ;
  - les métiers (ce que l'organisme sait faire) et la culture ;
  - l'organisation, et les principaux processus métiers, rôles et responsabilités ;
  - les politiques, les objectifs et les stratégies mises en place pour les atteindre ;
  - les systèmes d'information, flux d'information et processus de prise de décision ;
  - les normes, principes directeurs et modèles adoptés par l'organisme ;
  - les relations avec les parties prenantes internes ;
  - la forme et l'étendue des relations contractuelles ;
  - des éléments de conjoncture internes ;
  - des éléments de contexte socioculturel.

Il convient également de replacer la gestion des risques dans la gestion de l'organisme et l'atteinte de ses objectifs, en formalisant par exemples :

- la définition du risque, adaptée au contexte ;
- l'organisation générale en matière de gestion des risques :
  - les interfaces de la gestion des risques avec les processus de l'organisme ;
  - la politique générale de gestion des risques ;
  - l'engagement de la hiérarchie ;
  - une éventuelle définition particulière du risque ;
- l'organisation spécifique à l'étude :
  - les personnes interrogées par module ;
  - l'(les)autorité(s) de validation ;
  - les interfaces.

Conseils

- Cette action peut être préparée à l'aide de documents publics (présentation des activités, bilan annuel…), stratégiques (schéma directeur, orientations…), d'organisation…
- Parce qu'il s'agit d'effectuer une étude des risques, il est essentiel que l'organisme détermine ce qui consiste un risque pour lui. Par exemple, une réduction de l'utilité attendue (perte de revenus, perte de clientèle, diminution de la productivité) d'un système d'information ou d'un processus d'affaire.
- Le résultat de cette action doit être synthétique : il suffit de faire prendre conscience, de manière simple et concise, du contexte dans lequel l'étude va être réalisée.

Exemple

L'organisme étudié est la société @RCHIMED. Il s'agit d'une PME toulonnaise constituée d'une douzaine de personnes. C'est un bureau d'ingénierie en architecture qui réalise des plans d'usines et d'immeubles. Sa vocation principale est de vendre des services pour les professionnels du bâtiment.

@RCHIMED compte de nombreux clients, privés ou publics, ainsi que quelques professionnels du bâtiment.

Son capital s'élève à xxxxx € et son chiffre d'affaires à yyyyy €.
Ses missions consistent principalement à élaborer des projets architecturaux, ainsi que des calculs de structures et la création de plans techniques.
Ses valeurs sont la réactivité, la précision des travaux, la créativité architecturale et la communication.
Les principaux métiers représentés sont l'architecture et l'ingénierie du bâtiment.
Sa structure organisationnelle est fonctionnelle avec une direction, un service commercial, un bureau d'études, un service comptabilité et un service de gestion de site internet.
Ses axes stratégiques sont d'une part l'utilisation des nouvelles technologies (Internet, Intranet) dans un but d'ouverture vers l'extérieur et d'optimisation des moyens, et d'autre part la consolidation de l'image de marque (protection des projets sensibles).

Ses principaux processus métiers sont les suivants :

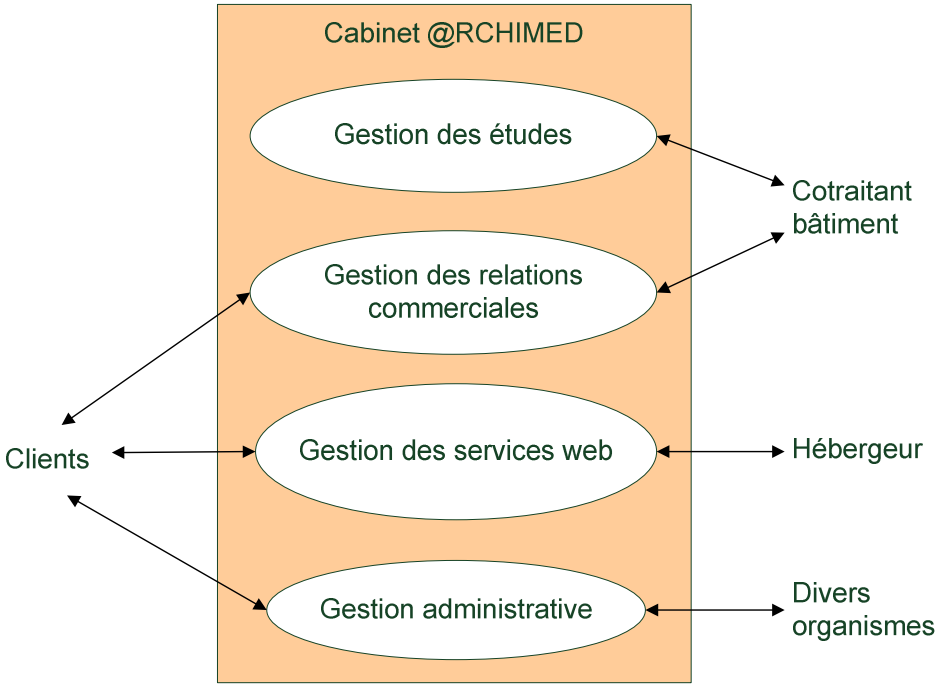


Figure 1 - *Les principaux processus métiers de la société*

Plusieurs éléments de conjoncture ont été identifiés :

- *la mise en réseau des systèmes informatiques s'est effectuée avec succès et a permis de réduire encore plus les délais de réalisation des travaux ;*
- *l'entreprise a dernièrement perdu un marché : la rénovation de la mairie de Draguignan. Lors de la présentation des projets, il est apparu de curieuses similitudes entre la maquette virtuelle d'@RCHIMED et la proposition d'un concurrent de Nice. Le directeur d'@RCHIMED soupçonne une compromission du projet qu'il avait présenté. Il a maintenant des craintes sur la confidentialité de certains projets ;*
- *l'arsenal de Toulon semble vouloir rénover certaines installations servant à la maintenance des bâtiments de la marine nationale. @RCHIMED souhaiterait pouvoir se présenter à d'éventuels appels d'offres ;*
- *une rude concurrence, dépendant des appels d'offres, s'exerce dans le secteur ;*
- *seule une crise très grave dans le bâtiment pourrait affecter le fonctionnement du cabinet d'architecture.*

Une gestion des risques intégrée

Le risque est défini comme un "scénario, avec un niveau donné, combinant un événement redouté par @RCHIMED sur son activité, et un ou plusieurs scénarios de menaces. Son niveau correspond à l'estimation de sa vraisemblance et de sa gravité".

En matière de gestion des risques, les rôles et responsabilités sont les suivants :

- *le Directeur d'@RCHIMED est pleinement responsable des risques pesant sur sa société ;*
- *le Directeur adjoint a été mandaté pour animer la gestion des risques de sécurité de l'information ; il est ainsi responsable de la réalisation des études de risques ;*
- *un comité de suivi, composé d'un membre de chaque service et présidé par le Directeur adjoint, réalisera la première étude de risques et se réunira ensuite tous les six mois afin de faire le point sur les évolutions à apporter à la gestion des risques de sécurité de l'information.*

Les interfaces de la gestion des risques sont les suivantes :

- *la gestion des risques de sécurité de l'information est partie intégrante de la gestion d'@RCHIMED ; à ce titre, ses résultats sont pris en compte dans la stratégie de la société ;*
- *l'ensemble de la société est concerné par la gestion des risques de sécurité de l'information, tant pour apprécier les risques que pour appliquer et faire appliquer des mesures de sécurité.*

Action 1.1.3. Délimiter le périmètre de l'étude

Description

Cette action consiste à circonscrire le périmètre d'étude au sein du contexte général que l'on a décrit précédemment, à expliquer ce qu'est le périmètre de l'étude et ce à quoi il sert. Les participants à l'étude sont également définis.

Pour commencer, on peut formaliser :
- la présentation du périmètre de l'étude ;
- sa fonction ou son objectif ;
- sa contribution aux processus métiers ;
- ses enjeux dans le contexte global ;
- les processus concernés ;
- les interfaces avec les autres processus ;
- les parties prenantes ;
- les éventuels éléments à écarter de la réflexion (types de biens supports, menaces…) ;
- le mode d'exploitation de sécurité.

À l'issue, on doit clairement savoir ce qui fait partie du périmètre et ce qui n'en fait pas partie.

Le découpage du périmètre en sous-périmètres peut être envisagé pour faciliter la suite de l'étude. L'objectif principal de la décomposition en sous-périmètres est de simplifier l'application de la démarche. Il est ensuite possible de déterminer soit plusieurs sous-périmètres plus simples à étudier séparément, soit un seul sous-périmètre sur lequel portera précisément l'étude. L'étude de ces sous-périmètres est généralement plus simple que l'étude globale d'un périmètre multiforme, mais le nombre de sous-périmètres doit rester faible car chacun fera l'objet d'une étude séparée.

La décomposition en sous-périmètres facilite :
- la sélection des axes d'effort : elle peut permettre de mettre en évidence des sous-périmètres pour lesquels une étude est inutile ou moins prioritaire ;
- l'organisation de l'étude : l'étude d'un sous-périmètre peut être confiée à une équipe restreinte.

Il n'y a pas de méthode à proprement parler permettant de décomposer un périmètre en sous-périmètres, mais un ensemble de critères à examiner. Les principaux critères de décomposition applicables sont les suivants :
- au vu de l'architecture matérielle : faire autant de sous-périmètres qu'il y a de machines (ou ensemble de machines) autonomes. Si, dans le cas général, les différentes machines sont reliées les unes aux autres, la décomposition dépend du niveau d'interopérabilité des différentes parties (machines ou ensembles de machines) du périmètre ;
- décomposition par les fonctions ou les informations essentielles : il peut être possible de décomposer un même sous-périmètre physique au vu des fonctions réalisées par telle ou telle machine ou partie du périmètre ou selon la façon dont sont traitées les informations les plus sensibles ;
- autonomie de responsabilité : un ensemble d'entités formant un tout du point de vue de la responsabilité de mise en œuvre (ensemble d'utilisateurs ou mise en œuvre technique), pourra être utilisé comme un sous-périmètre à étudier séparément. Il pourra s'agir d'une partie de périmètre placée sous la responsabilité d'un service dûment identifié sur un organigramme de l'organisme. Ce critère peut également s'appliquer lorsqu'il existe plusieurs documentations séparées ;
- implantation dans des sous-zones distinctes : si les constituants (matériels, supports, personnels) sont implantés dans des sous-zones différentes (bâtiments, sous-zones réservées, sous-sols...), chaque sous-zone est susceptible de constituer un sous-périmètre (à condition que le niveau d'interopérabilité avec l'extérieur soit suffisamment faible) ;
- isolement de "sous-périmètres communs" : les quatre premiers critères ayant été appliqués, certains ensembles d'entités ou des constituants peuvent se trouver à l'intersection de plusieurs sous-périmètres (serveurs communs, réseaux communs, personnels ou sous-zones communes par exemple). Ils sont susceptibles de former des sous-périmètres qu'il est possible d'étudier séparément. Les résultats de ces études étant par la suite reportés sur les sous-périmètres englobant. Il s'agit en quelque sorte d'une factorisation du travail.

Il est également possible d'identifier le mode d'exploitation de sécurité du(des) système(s) informatique(s) présents dans le périmètre de l'étude. Celui-ci définit le contexte de gestion de l'information. Il indique comment le système permet aux utilisateurs de catégories différentes de traiter, transmettre ou conserver des informations de sensibilités différentes. Généralement, il appartient à l'une des catégories suivantes :

- Catégorie 1 – Exclusif : toutes les personnes ayant accès au système sont habilitées au plus haut niveau de classification et elles possèdent un besoin d'en connaître (ou équivalent) identique pour toutes les informations traitées, stockées ou transmises par le système.
- Catégorie 2 – Dominant : toutes les personnes ayant accès au système sont habilitées au plus haut niveau de classification mais elles n'ont pas toutes un besoin d'en connaître (ou équivalent) identique pour les informations traitées, stockées ou transmises par le système.
- Catégorie 3 – Multi-niveaux : les personnes ayant accès au système ne sont pas toutes habilitées au plus haut niveau de classification et elles n'ont pas toutes un besoin d'en connaître (ou équivalent) identique pour les informations traitées, stockées ou transmises par le système.

Pour choisir le mode d'exploitation de sécurité, il est important de savoir s'il existe ou doit exister :

- une classification des informations hiérarchique (ex : confidentiel, secret…) et/ou par compartiment (médical, société, nucléaire…) ;
- des catégories d'utilisateurs ;
- une notion de besoin d'en connaître, d'en modifier, d'en disposer…

Le choix du mode d'exploitation de sécurité peut être reconsidéré au vu des risques identifiés lors des étapes suivantes. Il est cependant important de s'interroger sur cet aspect au plus tôt car sa mise en œuvre a de fortes conséquences sur l'architecture du système informatique.

Une fois le périmètre délimité, il convient de définir les participants à l'étude :

- la population à l'étude, pour adapter les métriques et généraliser les résultats ;
- le type d'échantillonnage (probabiliste, non probabiliste ou autre) selon la population à l'étude, le contexte et la portée de l'étude ;
- les critères de sélection (inclusion et exclusion).

Cette définition permet de mettre en place des critères objectifs de sélection afin de réduire l'impact de la subjectivité et de biais de sélections sur l'étude.

Conseils

- Le résultat de cette action doit être synthétique : il doit permettre de comprendre rapidement et sans ambiguïté ce qu'est le périmètre de l'étude, ce à quoi il sert et ses enjeux pour l'organisme.
- Il n'est pas nécessaire de décrire la composition du périmètre de l'étude de manière détaillée (cela sera demandé dans l'activité suivante), mais il doit être possible de se faire une bonne idée de sa taille et de sa complexité.
- Une attention particulière doit être portée sur les liens avec les objectifs de l'organisme, car c'est en reliant les risques de sécurité de l'information à ces objectifs qu'ils prendront tout leur sens pour les parties prenantes.
- La population à l'étude est liée à celle du périmètre de l'étude, mais il est recommandé de définir cette population de façon explicite afin de permettre une validation des résultats en fonction de critères précis, afin de permettre l'application des résultats à l'ensemble du périmètre visé.

Exemple

Le choix du périmètre d'étude s'est porté sur le sous-ensemble du système d'information du cabinet @RCHIMED correspondant à son cœur de métier :

- *gestion des relations commerciales (gestion des devis, projets…) ;*
- *gestion des études (calculs de structure, plans techniques, visualisations 3D…) ;*
- *gestion des services web (nom de domaine, site Internet, courrier électronique…).*

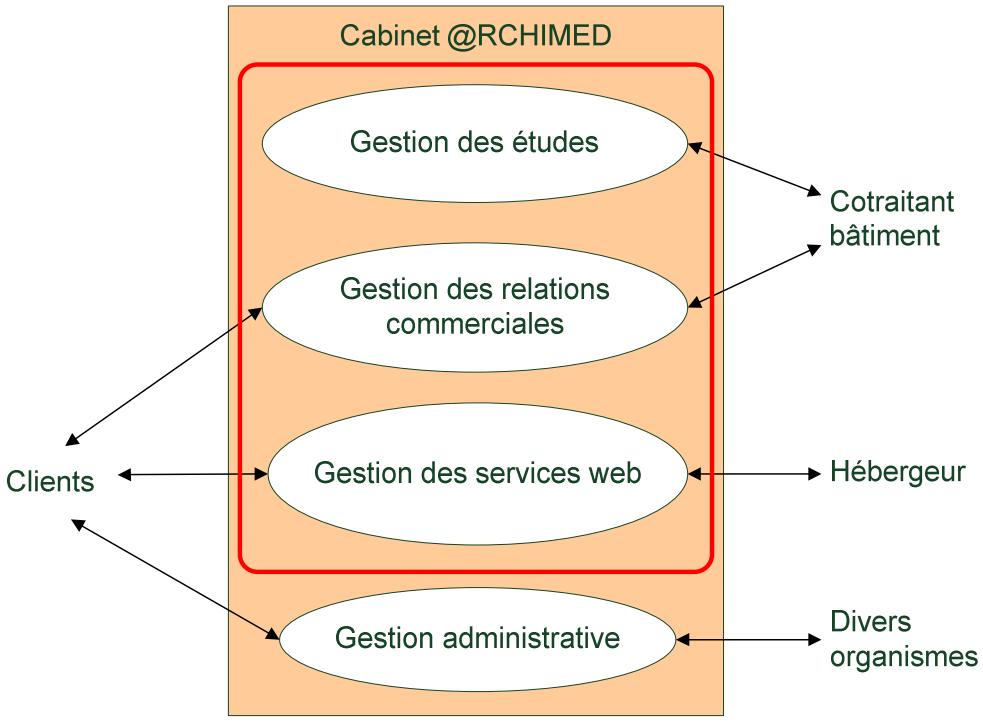


Figure 2 - *Le périmètre d'étude*

La gestion administrative est donc en dehors du périmètre d'étude :

- *gérer la comptabilité ;*
- *gérer les contentieux juridiques et techniques ;*
- *gestion administrative interne (ressources humaines, maintenance, assurances) ;*
- *gestion des permis de construire.*

Les principales interfaces concernent :

- *les clients (de visu, par téléphone, par courrier papier et électronique),*
- *les cotraitants bâtiment (de visu, par téléphone, par courrier papier et électronique),*
- *l'hébergeur du site web (via une connexion Internet, par courrier papier et électronique).*

Le système informatique du cabinet @RCHIMED est composé de deux réseaux locaux, l'un pour le bureau d'études et l'autre pour le reste de la société, sur un seul site et dépendant uniquement de la société, utilisés par une douzaine de personnes manipulant des logiciels métiers.

La gestion du site web est assurée par un poste isolé, en relation avec un hébergeur sur Internet.

Le sujet de l'étude représente la partie du système d'information d'@RCHIMED indispensable pour qu'il exerce son métier. L'ensemble du patrimoine informationnel du cabinet est créé, traité et stocké sur ce système d'information.

Les enjeux suivants ont été identifiés :

- *favoriser l'ouverture du système informatique vers l'extérieur ;*
- *démontrer la capacité du cabinet à protéger les projets sensibles (assurer la confidentialité relative aux aspects techniques…) ;*
- *améliorer les services rendus aux usagers et la qualité des prestations ;*
- *améliorer les échanges avec les autres organismes (fournisseurs, architectes).*

Les participants à l'étude sont définis comme suit :

- *la population à l'étude est l'ensemble des collaborateurs travaillant dans le périmètre choisi (gestion des relations commerciales, gestion des études et gestion des services web) ;*
- *au moins un personnel de chaque catégorie (direction, commercial, ingénieur, technicien) participe à l'étude ; d'autres personnels peuvent également participer à l'étude afin d'apporter un point de vue extérieur ;*
- *les critères de sélection sont les meilleures connaissances du métier en général, et des processus d'@RCHIMED.*

Action 1.1.4. Identifier les paramètres à prendre en compte

Description

Cette action consiste à recenser les éléments qui devraient avoir une incidence sur la gestion des risques (sur l'appréciation et/ou le traitement) :

- les références communautaires, légales et réglementaires à appliquer ;
- les références internes relatives à la sécurité de l'information à appliquer ;
- les contraintes de conformité à des référentiels (ex : ISO 27001, homologations…) ;
- les contraintes qui pèsent sur l'organisme ;
- les contraintes pesant spécifiquement sur le périmètre de l'étude ;
- les hypothèses.

La prise en compte des lois, règles ou règlements peut enfin limiter le choix de solutions matérielles ou procédures et modifier l'environnement ou les habitudes de travail. Il convient par conséquent de recenser les références communautaires, légales et réglementaires applicables au périmètre de l'étude. On ne retiendra que les références susceptibles d'avoir un impact sur l'étude.

Les principales références internes relatives à la sécurité de l'information et applicables au périmètre de l'étude, notamment :

- des politiques de sécurité (globale, de l'information, du système d'information, du patrimoine informationnel…) ou documents d'application (politiques locales, procédures…) ;
- des schémas directeurs traitant de sécurité de l'information ;
- des plans de continuité (des activités, des applications…), de secours ou de reprise ;
- des résultats d'audits relatifs à la sécurité de l'information…

Les contraintes qui pèsent sur l'organisme pourront être identifiées. Elles peuvent être d'origine interne à l'organisme, auquel cas celui-ci peut éventuellement les aménager, ou extérieures à l'organisme, et donc en règle générale, incontournables. Il peut s'agir, par exemples, de :

- contraintes d'ordre politique : elles peuvent concerner les administrations de l'État, les établissements publics ou en règle générale tout organisme devant appliquer les décisions gouvernementales. D'une manière générale, il s'agit de décisions d'orientation stratégique ou opérationnelle, émanant d'une Direction ou d'une instance décisionnelle et qui doivent être appliquées ;
  Par exemple, le principe de dématérialisation des factures ou des documents administratifs induit des problèmes de sécurité.
- contraintes d'ordre stratégique : des contraintes peuvent résulter d'évolutions prévues ou possibles des structures ou des orientations de l'organisme. Elles s'expriment dans les schémas directeurs d'organisation stratégiques ou opérationnels ;
  Par exemple, les coopérations internationales sur la mise en commun d'informations sensibles peuvent nécessiter des accords au niveau des échanges sécurisés.
- contraintes territoriales : la structure et/ou la vocation de l'organisme peut induire des contraintes particulières telles que la dispersion des sites sur l'ensemble du territoire national ou à l'étranger ;
  Par exemple, les agences de la poste, les ambassades, les banques, les différentes filiales d'un grand groupe industriel...
- contraintes conjoncturelles : le fonctionnement de l'organisme peut être profondément modifié par des situations particulières telles que des grèves, des crises nationales ou internationales ;
  Par exemple, la continuité de certains services doit pouvoir être assurée même en période de crise grave.
- contraintes structurelles : la structure de l'organisme peut induire, du fait de sa nature (divisionnelle, fonctionnelle ou autre), une politique de sécurité qui lui est spécifique et une organisation de la sécurité adaptée à ces structures ;
  Par exemple, une structure internationale doit pouvoir concilier des exigences de sécurité propres à chaque nation.
- contraintes fonctionnelles : il s'agit des contraintes directement issues des missions générales ou spécifiques de l'organisme ;
  Par exemple, un organisme peut avoir une mission de permanence qui exigera une disponibilité maximale de ses moyens.

- contraintes relatives au personnel : les contraintes relatives au personnel sont de natures très diverses et liées aux caractéristiques suivantes : niveau de responsabilité, recrutement, qualification, formation, sensibilisation à la sécurité, motivation, disponibilité…
  Par exemple, il peut être nécessaire que l'ensemble du personnel d'un organisme de la défense soit habilité pour des confidentialités supérieures.
- contraintes d'ordre calendaire : elles peuvent résulter de réorganisations de services, de la mise en place de nouvelles politiques nationales ou internationales qui vont imposer des échéances à date fixe ;
  Par exemple, la création d'une direction de la sécurité.
- contraintes relatives aux méthodes : compte tenu des savoir-faire internes à l'organisme, certaines méthodes (au niveau de la planification du projet, des spécifications, du développement…) seront imposées ;
  La contrainte peut être, par exemple, de devoir associer la politique de sécurité aux actions relatives à la qualité, en vigueur dans l'organisme.
- contraintes d'ordre culturel : dans certains organismes les habitudes de travail ou le métier principal ont fait naître une "culture", propre à cet organisme, qui peut constituer une incompatibilité avec les mesures de sécurité. Cette culture constitue le cadre de référence général des personnes de l'organisme et peut concerner de nombreux paramètres tels que les caractères, l'éducation, l'instruction, l'expérience professionnelle ou extra-professionnelle, les opinions, la philosophie, les croyances, les sentiments, le statut social…
- contraintes d'ordre budgétaire : les mesures de sécurité préconisées ont un coût qui peut, dans certains cas, être très important. Si les investissements dans le domaine de la sécurité ne peuvent s'appuyer sur des critères de rentabilité, une justification économique est généralement exigée par les services financiers de l'organisation ;
  Par exemple, dans le secteur privé et pour certains organismes publics, le coût total des mesures de sécurité ne doit pas être supérieur aux conséquences des risques redoutés. La direction doit donc apprécier et prendre des risques calculés si elle veut éviter un coût prohibitif pour la sécurité.

Les contraintes pesant spécifiquement sur le périmètre de l'étude peuvent également être recensées quand elles ont un impact. Il peut s'agir, par exemples, de :

- contraintes d'antériorité : tous les projets d'applications ne peuvent pas être développés simultanément. Certains sont dépendants de réalisations préalables. Un système peut faire l'objet d'une décomposition en sous-systèmes ; un système n'est pas forcément conditionné par la totalité des sous-systèmes (par extension à des fonctions d'un système) d'un autre système ;
- contraintes techniques : elles peuvent provenir des fichiers (exigences en matière d'organisation, de gestion de supports, de gestion des règles d'accès…), de l'architecture générale (exigences en matière de topologie, qu'elle soit centralisée, répartie, distribuée, ou de type client-serveur, d'architecture physique…), des logiciels applicatifs (exigences en matière de conception des logiciels spécifiques, de standards du marché…), des progiciels (exigences de standards, de niveau d'évaluation, qualité, conformité aux normes, sécurité…), des matériels (exigences en matière de standards, qualité, conformité aux normes…), des réseaux de communication (exigences en matière de couverture, de standards, de capacité, de fiabilité…), des infrastructures immobilières (exigences en matière de génie civil, construction des bâtiments, courants forts, courants faibles…)…
- contraintes financières : la mise en place de mesures de sécurité est souvent limitée par le budget que l'organisme peut y consacrer, néanmoins la contrainte financière est à prendre en compte en dernier lieu (la part du budget allouée à la sécurité pouvant être négociée en fonction de l'étude de sécurité) ;
- contraintes d'environnement : elles proviennent de l'environnement géographique ou économique dans lequel le SI est implanté : pays, climat, risques naturels, situation géographique, conjoncture économique…
- contraintes de temps : le temps nécessaire à la mise en place de mesures de sécurité doit être mis en rapport avec l'évolutivité du SI ; en effet, si le temps d'implémentation est très long, la parade peut ne pas être en rapport avec les risques qui auront évolués. Le temps est déterminant dans le choix des solutions et des priorités ;
- contraintes relatives aux méthodes : compte tenu des savoir-faire et des habitudes dans l'organisme, certaines méthodes (au niveau de la planification du projet, des spécifications et du développement…) seront imposées ;
- contraintes organisationnelles : l'exploitation (exigences en matière de délais, de fourniture de résultats, de services, exigences de surveillance, de suivi, de plans de secours, fonctionnement en mode dégradé…), la maintenance (exigences d'actions de diagnostic

d'incidents, de prévention, de correction rapide…), la gestion des ressources humaines (exigences en matière de formation des opérationnels et des utilisateurs, de qualification pour l'occupation des postes tels qu'administrateur système ou administrateur de données…), la gestion administrative (exigences en matière de responsabilités des acteurs…), la gestion des développements (exigences en matière d'outils de développement, AGL, de plans de recette, d'organisation à mettre en place…), la gestion des relations externes (exigences en matière d'organisation des relations tierces, en matière de contrats…)…

Les hypothèses sont le plus souvent imposées par l'organisme responsable de l'étude, pour des raisons de politique interne ou externe de l'organisme, financières ou de calendrier. Les hypothèses peuvent aussi constituer un risque accepté a priori sur un environnement donné.

Conseils

- Enrichir cette action au fur et à mesure de l'étude.
- Une fois ces paramètres identifiés, il peut être utile d'indiquer s'ils vont avoir une incidence sur l'appréciation et/ou sur le traitement des risques, ce qui facilitera la démonstration ultérieure de couverture de ces paramètres.

Exemple

Un ensemble de contraintes à prendre en compte a été identifié :

- *relatives au personnel :*
  - *le personnel est utilisateur de l'informatique, mais pas spécialiste,*
  - *le responsable informatique est l'adjoint du directeur, il est architecte de formation,*
  - *le personnel de nettoyage intervient de 7h à 8h,*
  - *la réception des clients se fait dans les bureaux des commerciaux, mais des visites ont parfois lieu au bureau d'études ;*
- *d'ordre calendaire :*
  - *la période de pointe se situant d'octobre à mai, toute action (installation de système de sécurité, formation et sensibilisation) se fera en dehors de cette période ;*
- *d'ordre budgétaire :*
  - *la société a fait un effort important en matière d'informatisation, tout investissement supplémentaire devra être dûment justifié ;*
- *d'ordre technique :*
  - *les règles de conception architecturale doivent être respectées,*
  - *des logiciels professionnels du domaine architectural doivent être employés ;*
- *d'environnement :*
  - *le cabinet loue deux étages d'un immeuble au centre ville,*
  - *le cabinet est au voisinage de commerces divers,*
  - *aucun déménagement n'est planifié.*

Action 1.1.5. Identifier les sources de menaces

Description

Cette action consiste à déterminer les sources de menaces pertinentes vis-à-vis du contexte particulier du périmètre de l'étude.

Les parties prenantes doivent réfléchir aux origines des risques : qui ou quoi pourrait porter atteinte aux besoins de sécurité exprimés et engendrer les impacts identifiés ?

La réflexion, qui devrait être menée avec l'autorité responsable du périmètre de l'étude du fait qu'elle est la plus à même d'en avoir une vision globale et objective, consiste à sélectionner les sources de menaces les plus pertinentes selon le contexte particulier du périmètre de l'étude. Elle aura essentiellement pour finalité d'apprécier les risques de manière pertinente vis-à-vis de ces sources et de déterminer des mesures de sécurité adaptées à ces sources.

Il convient tout d'abord de choisir une typologie de sources de menaces. Les bases de connaissances de la méthode proposent une liste générique que l'on peut directement utiliser ou que l'on peut ajuster. Cette typologie doit aider les parties prenantes à envisager des origines de différentes natures, auxquelles elles n'auraient peut-être pas songé, et ce, dans leur contexte particulier.

Bien que, potentiellement, n'importe quelle source de menace puisse être considérée, il convient ici d'identifier celles qui sont réellement présentes dans l'environnement du périmètre de l'étude et auxquelles on décide de pouvoir s'opposer. Cela ne signifie pas forcément qu'elles soient visibles, ni même précisément connues. Il s'agit en effet des sources de menaces que l'on peut redouter, selon la conjoncture sociale, politique, économique, géographique, climatique… Ainsi, il conviendra de ne pas retenir les sources de menaces auxquelles on estime ne pas être exposé selon :

- leur origine, humaine ou non humaine ;
- leur lien avec le périmètre de l'étude (interne ou externe) ;
- dans le cas de sources humaines :
  - leur caractère intentionnel (et dans ce cas leur motivation) ou accidentel,
  - leurs capacités (force intrinsèque, selon leurs ressources, leur expertise, leur dangerosité…) ;
- dans le cas de sources non humaines :
  - leur type (naturelle, animale, contingence…).

Les sources de menaces devraient ensuite être caractérisées. Plus la réflexion est poussée, plus l'appréciation des risques sera pertinente et plus les mesures de sécurité destinées à les contrer seront appropriées. Chaque source de menace peut ainsi être illustrée d'exemples représentatifs dans le contexte considéré, et décrite de manière plus ou moins détaillée.

De plus, des valeurs peuvent être estimées pour :

- l'exposition à ces sources de menaces ("fréquence" des incidents ou sinistres SSI liés à ces sources de menaces) ;
- leur potentiel :
  - leur motivation (attraction envers les biens dans le cadre du périmètre de l'étude, jeu, vengeance, agent, effet médiatique, peur…),
  - leur facilité d'accès au périmètre de l'étude,
  - leur capacité à mobiliser de l'énergie,
  - le temps disponible à l'action,
  - les compétences techniques disponibles,
  - les ressources financières ou matérielles ;
- leur capacité de dissimulation…

Conseils

- Une manière de procéder consiste à partir de la typologie proposée dans les bases de connaissances, écarter les sources de menaces qui ne concernent pas le périmètre de l'étude en le justifiant (ne garder que les plus pertinentes), illustrer simplement les sources de menaces retenues (un employé, un concurrent, le personnel d'entretien, un pirate, une forêt…) et les décrire plus précisément afin de sensibiliser et d'impliquer les parties prenantes.
- Ce sont souvent des acteurs externes (par exemple les autorités publiques) qui informent l'organisme des sources de menaces à considérer plus particulièrement à un moment donné.

Exemple

Le cabinet @RCHIMED souhaite s'opposer aux sources de menaces suivantes :

Types de sources de menaces	***Retenu ou non***	***Exemple***
Source humaine interne, malveillante, avec de faibles capacités	*Non, le cabinet n'estime pas y être exposé*	
Source humaine interne, malveillante, avec des capacités importantes	*Non, le cabinet n'estime pas y être exposé*	
Source humaine interne, malveillante, avec des capacités illimitées	*Non, le cabinet n'estime pas y être exposé*	
Source humaine externe, malveillante, avec de faibles capacités	*Oui*	✓ *Personnel de nettoyage (soudoyé)* ✓ *Script-kiddies*
Source humaine externe, malveillante, avec des capacités importantes	*Oui*	✓ *Concurrent (éventuellement en visite incognito)* ✓ *Maintenance informatique*
Source humaine externe, malveillante, avec des capacités illimitées	*Non, le cabinet n'estime pas y être exposé*	
Source humaine interne, sans intention de nuire, avec de faibles capacités	*Oui*	✓ *Employé peu sérieux*
Source humaine interne, sans intention de nuire, avec des capacités importantes	*Non, le cabinet n'estime pas y être exposé*	
Source humaine interne, sans intention de nuire, avec des capacités illimitées	*Oui*	✓ *Employé peu sérieux (ceux qui ont un rôle d'administrateur)*
Source humaine externe, sans intention de nuire, avec de faibles capacités	*Oui*	✓ *Client* ✓ *Cotraitant* ✓ *Partenaire*
Source humaine externe, sans intention de nuire, avec des capacités importantes	*Oui*	✓ *Fournisseur d'accès Internet* ✓ *Hébergeur*
Source humaine externe, sans intention de nuire, avec des capacités illimitées	*Non, le cabinet n'estime pas y être exposé*	
Virus non ciblé	*Oui*	✓ *Virus non ciblé*
Phénomène naturel	*Oui*	✓ *Phénomène naturel (foudre, usure…)*
Catastrophe naturelle ou sanitaire	*Oui*	✓ *Maladie*
Activité animale	*Non, le cabinet n'estime pas y être exposé*	
Événement interne	*Oui*	✓ *Panne électrique* ✓ *Incendie des locaux*

Propositions pour mettre en œuvre les actions préconisées

Action 1.2.1. Définir les critères de sécurité et élaborer les échelles de besoins

Description

Cette action consiste à choisir les critères de sécurité qui seront étudiés, à produire une définition pour chacun d'eux et à élaborer autant d'échelles de besoins que de critères de sécurité retenus.

Les critères de sécurité constituent des facteurs permettant de relativiser l'importance des différents biens essentiels selon les besoins métiers, et serviront ainsi à décrire les conditions dans lesquelles le métier s'exerce convenablement.

Trois critères de sécurité sont incontournables (leur définition figure dans le glossaire de la méthode) :

- la disponibilité : elle reflète le besoin que des biens essentiels soient accessibles ; elle peut correspondre à la durée nécessaire pour avoir accès au bien essentiel (*ex. : 1 heure, 1 journée, 1 semaine…*) et/ou à un taux (*ex. : 99%*) ; on peut même séparer ces deux notions en deux critères de sécurité distincts ;
- l'intégrité : elle reflète le besoin que des biens essentiels ne soient pas altérés ; elle correspond autant à leur niveau de conformité qu'à leur stabilité, leur exactitude, leur complétude… ;
- la confidentialité : elle reflète le besoin que des biens essentiels ne soient pas compromis ni divulgués ; elle correspond au nombre ou catégories de personnes autorisées à y accéder.

Les besoins sont parfois exprimés selon d'autres "critères de sécurité", tels que la preuve, l'imputabilité, l'auditabilité, la fiabilité, la traçabilité… Il ne s'agit évidemment pas de facteurs permettant de refléter des besoins métiers. Il s'agit de différentes fonctions / solutions de sécurité, mises en place pour satisfaire des besoins de disponibilité, d'intégrité ou de confidentialité, et non de véritables critères de sécurité. Néanmoins, on peut les considérer comme tels si ces notions paraissent réellement au cœur du métier de l'organisme, si elles sont ancrées dans sa culture ou si on tient à orienter fortement la communication qui sera faite autour d'une étude sur l'une de ces notions.

Une échelle de besoins est généralement ordinale (les objets sont classés par ordre de grandeur, les nombres indiquent des rangs et non des quantités) et composée de plusieurs niveaux permettant de classer l'ensemble des biens essentiels étudiés. Chaque niveau reflète un besoin métier possible.

Il doit être facile de déterminer le niveau nécessaire pour chaque bien essentiel. Les différents niveaux devraient ainsi être très explicites, non ambigus, et avec des limites claires. On note que le nombre de niveaux des différentes échelles n'est pas nécessairement le même.

Le principal enjeu concernant une échelle de besoins réside dans le fait qu'elle soit comprise et utilisable par les personnes qui vont exprimer les besoins de sécurité des biens essentiels. Cette échelle doit donc être adaptée au contexte de l'étude. Son élaboration peut utilement être réalisée en collaboration avec les personnes qui vont déterminer les besoins. Ainsi, chaque valeur aura une réelle signification pour elles et les valeurs seront cohérentes.

Conseils

- Ne considérer que la disponibilité, l'intégrité et la confidentialité, et se baser sur les définitions fournies dans le glossaire de la méthode.
- S'assurer que les critères de sécurité, les niveaux et leurs descriptions sont bien compris par les parties prenantes et ajuster la terminologie et les descriptions si besoin.
- Chaque niveau doit être décrit en termes fonctionnels de besoins métiers (*le bien essentiel est nécessaire dans l'heure pour que le métier s'exerce de manière acceptable*), et non en termes d'impacts (*ex. : la compromission du bien essentiel peut engendrer une perte importante de chiffre d'affaires*).

Exemple

Afin d'exprimer les besoins de sécurité, les critères de sécurité retenus sont les suivants :

Critères de sécurité	Définitions
Disponibilité	*Propriété d'accessibilité au moment voulu des biens essentiels.*
Intégrité	*Propriété d'exactitude et de complétude des biens essentiels.*
Confidentialité	*Propriété des biens essentiels de n'être accessibles qu'aux utilisateurs autorisés.*

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de disponibilité :

Niveaux de l'échelle	Description détaillée de l'échelle
Plus de 72h	*Le bien essentiel peut être indisponible plus de 72 heures.*
Entre 24 et 72h	*Le bien essentiel doit être disponible dans les 72 heures.*
Entre 4 et 24h	*Le bien essentiel doit être disponible dans les 24 heures.*
Moins de 4h	*Le bien essentiel doit être disponible dans les 4 heures.*

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes d'intégrité :

Niveaux de l'échelle	Description détaillée de l'échelle
Détectable	*Le bien essentiel peut ne pas être intègre si l'altération est identifiée.*
Maîtrisé	*Le bien essentiel peut ne pas être intègre, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée.*
Intègre	*Le bien essentiel doit être rigoureusement intègre.*

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de confidentialité :

Niveaux de l'échelle	Description détaillée de l'échelle
Public	*Le bien essentiel est public.*
Limité	*Le bien essentiel ne doit être accessible qu'au personnel et aux partenaires.*
Réservé	*Le bien essentiel ne doit être accessible qu'au personnel (interne) impliquées.*
Privé	*Le bien essentiel ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître.*

Action 1.2.2. Élaborer une échelle de niveaux de gravité

Description

Cette action consiste à créer une échelle décrivant tous les niveaux possibles des impacts. Tout comme les échelles de besoins, une échelle de niveaux d'impacts est généralement ordinale (les objets sont classés par ordre de grandeur, les nombres indiquent des rangs et non des quantités) et composée de plusieurs niveaux permettant de classer l'ensemble des risques. Chaque niveau reflète l'estimation de la hauteur des conséquences cumulées d'un sinistre.

Il doit être facile de déterminer le niveau nécessaire pour chaque risque. Les différents niveaux devraient ainsi être très explicites, non ambigus, et avec des limites claires.

Le principal enjeu concernant une échelle de niveaux d'impacts réside dans le fait qu'elle soit comprise et utilisable par les personnes qui vont juger de l'importance des conséquences de la réalisation des sinistres. Son élaboration peut utilement être réalisée en collaboration avec les personnes qui vont estimer ces niveaux. Ainsi, chaque valeur aura une réelle signification pour elles et les valeurs seront cohérentes.

Conseils

- Bien que les échelles de niveaux d'impacts puissent être relativement subjectives, il convient surtout de s'assurer que les parties prenantes sauront discriminer clairement les différents niveaux.
- S'assurer que les niveaux et leurs descriptions sont bien compris par les parties prenantes et les ajuster si besoin.
- Une échelle par niveaux permettra de mettre en évidence les progrès réalisés par la mise en place de mesures de sécurité, alors qu'une échelle ordinale permettra de positionner de manière bien distincte tous les risques dans une cartographie. Il est également possible d'utiliser les deux types d'échelles simultanément.

Exemple

L'échelle suivante sera utilisée pour estimer la gravité des événements redoutés et des risques :

Niveaux de l'échelle	***Description détaillée de l'échelle***
1. Négligeable	*@RCHIMED surmontera les impacts sans aucune difficulté.*
2. Limitée	*@RCHIMED surmontera les impacts malgré quelques difficultés.*
3. Importante	*@RCHIMED surmontera les impacts avec de sérieuses difficultés.*
4. Critique	*@RCHIMED ne surmontera pas les impacts (sa survie est menacée).*

Action 1.2.3. Élaborer une échelle de niveaux de vraisemblance

Description

Cette action consiste à créer une échelle décrivant tous les niveaux possibles de vraisemblance des scénarios de menaces. Tout comme les échelles de besoins et de niveaux d'impacts, une échelle de niveaux de vraisemblance est généralement ordinale (les objets sont classés par ordre de grandeur, les nombres indiquent des rangs et non des quantités) et composée de plusieurs niveaux permettant de classer l'ensemble des risques analysés. Chaque niveau reflète l'estimation de la possibilité de réalisation d'un sinistre.

Il doit être facile de déterminer le niveau nécessaire pour chaque risque. Les différents niveaux devraient ainsi être très explicites, non ambigus, et avec des limites claires.

Le principal enjeu concernant une échelle de niveaux de vraisemblance réside dans le fait qu'elle soit comprise et utilisable par les personnes qui vont juger de la possibilité qu'un sinistre ait lieu. Son élaboration peut utilement être réalisée en collaboration avec les personnes qui vont estimer ces niveaux. Ainsi, chaque valeur aura une réelle signification pour elles et les valeurs seront cohérentes.

Conseils

- Bien que les échelles de niveaux de vraisemblance puissent être relativement subjectives, il convient surtout de s'assurer que les parties prenantes sauront discriminer clairement les différents niveaux.
- S'assurer que les niveaux et leurs descriptions sont bien compris par les parties prenantes et les ajuster si besoin.
- Une échelle par niveaux permettra de mettre en évidence les progrès réalisés par la mise en place de mesures de sécurité, alors qu'une échelle ordinale permettra de positionner de manière bien distincte tous les risques dans une cartographie. Il est également possible d'utiliser les deux types d'échelles simultanément.

Exemple

L'échelle suivante sera utilisée pour estimer la vraisemblance des scénarios de menaces et des risques :

Niveaux de l'échelle	***Description détaillée de l'échelle***
1. Minime	*Cela ne devrait pas se (re)produire.*
2. Significative	*Cela pourrait se (re)produire.*
3. Forte	*Cela devrait se (re)produire un jour ou l'autre.*
4. Maximale	*Cela va certainement se (re)produire prochainement.*

Action 1.2.4. Définir les critères de gestion des risques

Description

Cette action consiste à formaliser les règles choisies pour faire des choix tout au long d'une étude. Toute action de l'étude qui nécessite une décision peut faire l'objet d'un critère de gestion de risques.

Les critères de gestion des risques permettent notamment d'estimer et d'évaluer les risques et de prendre des décisions concernant leur appréciation et leur traitement. Ils reflètent les valeurs, les objectifs et les ressources de l'organisme. Ils peuvent être imposés ou résulter d'obligations légales et réglementaires, ou d'autres exigences auxquelles l'organisme répond. Ils tiennent ainsi compte de la nature des causes et des conséquences qui peuvent survenir, de la façon dont elles vont être mesurées, des méthodes d'estimation, des échelles choisies, des avis des parties prenantes, du niveau à partir duquel les risques deviennent acceptables ou tolérables, de la prise en compte ou non des combinaisons de plusieurs risques…

Il convient que les critères de gestion des risques soient cohérents avec la politique de gestion des risques de l'organisme, définis au préalablement à l'étude, ce qui contribue à la transparence et à la rigueur de l'approche, et facilite l'adhésion des parties prenantes, et revus régulièrement.

On peut ainsi définir la manière dont :

- les événements redoutés sont estimés et évalués ;
- les scénarios de menaces sont estimés et évalués ;
- les risques sont estimés et évalués ;
- les risques sont traités et validés (notamment les choix de traitement et les risques résiduels)…

Conseils

- Minimiser les automatismes, qui déresponsabilisent les parties prenantes et peuvent de plus apporter une scientificité illusoire.
- Lors d'une première utilisation de la méthode et s'il n'existe pas déjà de critères de gestion des risques, il est possible de les formaliser au fur et à mesure du déroulement de l'étude.

Exemple

Les critères de gestion des risques retenus sont les suivants :

Action	***Critère de gestion des risques (règle choisie pour réaliser l'action)***
Estimation des événements redoutés (module 2)	❑ *Les événements redoutés sont estimés en termes de gravité à l'aide de l'échelle définie à cet effet.*
Évaluation des événements redoutés (module 2)	❑ *Les événements redoutés sont classés par ordre décroissant de vraisemblance.*
Estimation des risques (module 4)	❑ *La gravité d'un risque est égale à celle de l'événement redouté considéré.* ❑ *La vraisemblance d'un risque est égale à la vraisemblance maximale de tous les scénarios de menaces liés à l'événement redouté considéré.*
Évaluation des risques (module 4)	❑ *Les risques dont la gravité est critique, et ceux dont la gravité est importante et la vraisemblance forte ou maximale, sont jugés comme intolérables.* ❑ *Les risques dont la gravité est importante et la vraisemblance significative, et ceux dont la gravité est limitée et la vraisemblance forte ou maximale, sont jugés comme significatifs.* ❑ *Les autres risques sont jugés comme négligeables.*
…	❑ *…*

Activité 1.3 – Identifier les biens

Objectif

Cette activité fait partie de l'établissement du contexte. Elle a pour but d'identifier les biens au sein du périmètre de l'étude et ainsi de mettre en évidence les éléments nécessaires aux autres activités.

Avantages

- Permet de comprendre le fonctionnement du périmètre de l'étude
- Permet de prendre en compte les mesures de sécurité existantes (que celles-ci soient formalisées ou non) pour valoriser le travail déjà effectué et ne pas le remettre en cause

Données d'entrée

- Données concernant le contexte du périmètre de l'étude (documents concernant le système d'information, synthèses d'entretiens avec des responsables de l'organisme…).

Actions préconisées et rôle des parties prenantes

Actions : \ Parties prenantes :	Responsable	RSSI	*Risk manager*	Autorité	Dépositaire	Propriétaire
Action 1.3.1. Identifier les biens essentiels, leurs relations et leurs dépositaires	A	C	I		R	
Action 1.3.2. Identifier les biens supports, leurs relations et leurs propriétaires	A	C				R
Action 1.3.3. Déterminer le lien entre les biens essentiels et les biens supports	A	C				R
Action 1.3.4. Identifier les mesures de sécurité existantes	A	C				R

Données produites

- Biens essentiels
- Biens supports
- Tableau croisé biens essentiels / biens supports
- Mesures de sécurité existantes

Communication et concertation

- Les données sont obtenues sur la base d'étude de l'existant, d'entretiens individuels ou d'échanges entre les parties prenantes
- Elles peuvent être intégrées à la politique de sécurité de l'information

Surveillance et revue

- La méthode de collecte et d'enregistrement des données est clairement précisée
- Toutes les données produites sont comprises et acceptées par les parties prenantes

Propositions pour mettre en œuvre les actions préconisées

Action 1.3.1. Identifier les biens essentiels, leurs relations et leurs dépositaires

Description

Cette action consiste à recenser, au sein du patrimoine informationnel du périmètre de l'étude, celui qui peut être jugé comme essentiel.

Les biens essentiels représentent le patrimoine informationnel, ou les "biens immatériels", que l'on souhaite protéger, c'est-à-dire ceux pour lesquels le non respect de la disponibilité, de l'intégrité, de la confidentialité, voire d'autres critères de sécurité, mettrait en cause la responsabilité du dépositaire, ou causerait un préjudice à eux-mêmes ou à des tiers. Par exemple :

- les informations on fonctions vitales pour l'exercice de la mission ou du métier de l'organisme ;
- les traitements secrets ou procédés technologiques de haut niveau ;
- les informations personnelles, notamment les informations nominatives au sens de la loi française informatique et libertés ;
- les informations stratégiques nécessaires pour atteindre les objectifs correspondants aux orientations stratégiques ;
- les informations coûteuses, dont la collecte, le stockage, le traitement ou la transmission nécessitent un délai important et/ou un coût d'acquisition élevé ;
- les informations relevant du secret défense définies dans l'[IGI 1300] et pour lesquelles le niveau d'exigence de sécurité n'est pas négociable ;
- les informations classifiées d'autres natures…

Selon leur finalité, certaines études ne mériteront pas une analyse exhaustive de l'ensemble des biens informationnels composant le périmètre de l'étude. Dans ce contexte, ils seront limités aux éléments vitaux du périmètre de l'étude. Ceux qui n'auront pas été retenues à l'issue de cette activité ne feront l'objet dans la suite de l'étude d'aucun besoin de sécurité. Cependant, ils hériteront souvent des mesures de sécurité prises pour protéger les autres biens informationnels.

Le niveau de détail des biens essentiels doit être cohérent avec le périmètre et l'objectif de l'étude. Ainsi, l'étude d'un organisme entier traitera de ses principaux processus ou domaines d'activités, alors que l'étude d'un système informatique en développement nécessitera de recenser les principaux flux d'information concernés, voire chaque champ d'une base de données.

Par ailleurs, il est important de bien comprendre les relations fonctionnelles entre les biens essentiels. Il est donc souhaitable de les décrire, par exemple sous la forme de modèles de flux.

Enfin, chaque bien essentiel doit être "rattaché" à un dépositaire nommément ou fonctionnellement identifié. C'est ce dépositaire qui est censé être responsable de ses biens essentiels, des risques pesant sur ceux-ci et qui sera le plus légitime pour exprimer leurs besoins de sécurité.

Conseils

- Comme leur nom l'indique, il s'agit de recenser les biens réellement "essentiels" et non de réaliser un recensement exhaustif. Dix ou quinze biens essentiels, suffisamment représentatifs, permettent ainsi de réduire le travail de la suite de l'étude à un volume nécessaire et suffisant.
- Il est possible de partir d'un recensement relativement exhaustif pour ensuite sélectionner un sous-ensemble de biens essentiels.
- Un bien essentiel, dont les besoins de sécurité varieront dans le temps peut être utilement scindé en plusieurs biens essentiels (ex : une réponse à un appel d'offres, avant ou après, de répondre à l'appel d'offres, pourra être décomposé en deux biens essentiels distincts)
- La sélection devrait être effectuée par un groupe de travail hétérogène et représentatif du périmètre de l'étude (responsables, informaticiens et utilisateurs).
- Des schémas simples sont très utiles à la compréhension de toutes les parties prenantes.

Exemple

Dans le cadre du sujet d'étude, le cabinet @RCHIMED a retenu les processus suivants en tant que biens essentiels :

Processus essentiels	***Informations essentielles concernées***	***Dépositaires***
Établir les devis (estimation du coût global d'un projet, négociations avec les clients…)	✓ *Cahier des charges* ✓ *Catalogues techniques* ✓ *Contrat (demande de réalisation)* ✓ *Devis*	*Service commercial*
Créer des plans et calculer les structures	✓ *Dossier technique d'un projet* ✓ *Paramètres techniques (pour les calculs de structure)* ✓ *Plan technique* ✓ *Résultat de calcul de structure*	*Bureau d'études*
Créer des visualisations	✓ *Dossier technique d'un projet* ✓ *Visualisation 3D*	*Bureau d'études*
Gérer le contenu du site Internet	✓ *Informations société (contacts, présentation…)* ✓ *Exemple de devis* ✓ *Exemple de visualisation 3D* ✓ *Page Web*	*Directeur adjoint*

Action 1.3.2. Identifier les biens supports, leurs relations et leurs propriétaires

Description

Cette action consiste à prendre connaissance des composants du système d'information, qu'il s'agisse de biens techniques ou non techniques, supports aux biens essentiels précédemment identifiés. On note que ces biens supports possèdent des vulnérabilités que des sources de menaces pourront exploiter, portant ainsi atteinte aux biens essentiels.

L'identification des biens supports ne peut se faire que lorsque ceux-ci sont connus. Ainsi, lors des phases préliminaires du cycle de vie d'un projet, il n'est pas possible de les recenser, puisqu'ils ne sont pas encore spécifiés. En revanche, cela devient progressivement possible à mesure que l'on affine les spécifications et la connaissance concrète du périmètre de l'étude.
Le niveau de détail des biens supports peut également varier selon les objectifs de l'étude. Ainsi, une étude rapide destinée à donner les grandes orientations en matière de sécurité de l'information sera très peu détaillée pour cette action (un réseau, un site, une organisation…), alors qu'une étude précise et exhaustive destinée à démontrer relativement formellement que tous les risques ont été gérés sur un système critique nécessitera un niveau de détail beaucoup plus important (telle version de tel système d'exploitation, tel type de personnel, telle pièce dans les bâtiments…).
À cet effet, les bases de connaissances de la méthode proposent une liste générique que l'on peut directement utiliser ou que l'on peut ajuster.

En outre, il est important de bien comprendre les relations entre les biens supports. Il est donc souhaitable de les décrire, par exemple en précisant les inclusions, les interconnexions… Ceci permettra d'étudier les possibles phénomènes de propagation d'incident ou de sinistre.

Une fois les biens supports identifiés, il convient de "rattacher" un propriétaire pour chacun d'eux, nommément ou fonctionnellement identifié. En effet, la personne qui en a la responsabilité sera sans doute la plus à même d'analyser ses vulnérabilités et celle qui sera garante de l'application de mesures de sécurité.

Conseils

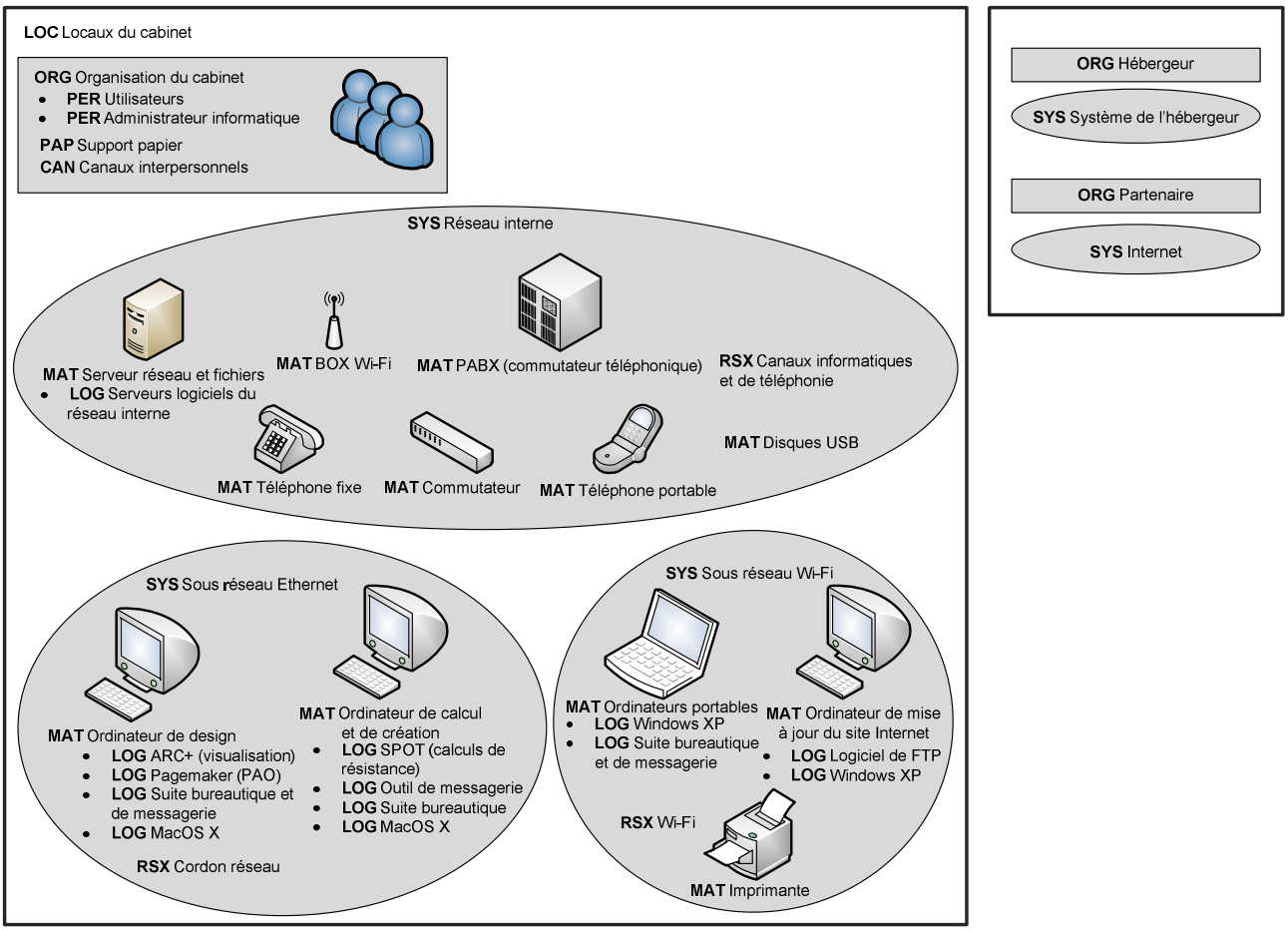
- Commencer par recenser les grands types de biens supports et n'affiner le niveau de détail qu'en cas de besoin, ou bien les affiner mais ne retenir pour la suite de l'étude qu'un nombre raisonnable de biens supports.
- Il peut être parfois utile de décrire les biens supports afin d'éliminer les ambiguïtés ou d'expliciter la différence par rapport aux autres biens supports.
- Recenser les biens supports à partir des biens essentiels permet de ne considérer que les biens supports réellement dans le périmètre du périmètre de l'étude.
- Des schémas simples sont très utiles à la compréhension de toutes les parties prenantes.

Exemple

Sans les détailler dans un premier temps, @RCHIMED a retenu les biens supports suivants :

- *en interne :*
  - *SYS – Réseau interne,*
  - *SYS – Sous réseau Ethernet,*
  - *SYS – Sous réseau Wifi,*
  - *ORG – Organisation du cabinet,*
  - *LOC – Locaux du cabinet ;*
- *en interface :*
  - *SYS – Système de l'hébergeur (Internet et par courrier électronique),*
  - *ORG – Hébergeur (par courrier papier),*
  - *SYS – Internet (pour des accès distants et le courrier électronique),*
  - *ORG – Partenaire (cotraitants bâtiment, clients…).*

Le schéma suivant décompose ces biens supports et les positionne les uns par rapport aux autres :



Action 1.3.3. Déterminer le lien entre les biens essentiels et les biens supports

Description

Cette action consiste à déterminer le lien entre les biens essentiels et les biens supports. Ceci permettra de révéler la criticité de ces derniers, ainsi que les risques véritables pesant sur le périmètre de l'étude.

Pour ce faire, il suffit de se demander sur quels biens supports, parmi ceux identifiés dans l'action précédente, repose chaque bien essentiel. On s'interroge ainsi sur les biens supports qui vont stocker ou traiter les biens essentiels, à un moment ou un autre de leur cycle de vie.

Conseils

- Un simple tableau croisé entre les biens essentiels et les biens supports permet de représenter le lien entre les deux.

Exemple

Le tableau suivant présente les biens supports et leurs liens avec les biens essentiels :

Biens essentiels / ***Biens supports***	***Établir les devis***	***Créer des plans et calculer les structures***	***Créer des visualisations***	***Gérer le contenu du site Internet***
Biens supports communs à @RCHIMED				
SYS – Réseau interne	X	X	X	X
MAT – Serveur réseau et fichiers	X	X	X	X
LOG – Serveurs logiciels du réseau interne		X	X	
MAT – Disque USB	X	X	X	
MAT – BOX Wifi	X	X	X	X
MAT – Commutateur	X	X	X	X
MAT – PABX (commutateur téléphonique)	X	X	X	X
MAT – Téléphone fixe	X	X	X	X
MAT – Téléphone portable	X	X	X	X
RSX – Canaux informatiques et de téléphonie	X	X	X	X
ORG – Organisation du cabinet	X	X	X	X
PER – Utilisateur	X	X	X	
PER – Administrateur informatique	X	X	X	X
PAP – Support papier	X	X	X	
CAN – Canaux interpersonnels	X	X	X	X
LOC – Locaux du cabinet	X	X	X	X
Biens supports spécifiques au bureau d'études				
SYS – Sous réseau Ethernet		X	X	
MAT – Ordinateur de design		X	X	
LOG – MacOS X		X	X	
LOG – ARC+ (visualisation)			X	
LOG – Pagemaker (PAO)		X	X	
LOG – Suite bureautique et de messagerie		X	X	
MAT – Ordinateur de calcul et de création		X		
…	…	…	…	…

Action 1.3.4. Identifier les mesures de sécurité existantes

Description

Cette action consiste à recenser l'ensemble des mesures de sécurité existantes sur les biens supports ou d'ores et déjà prévues.

Pour chaque bien support identifié, il convient de s'interroger sur l'existence de mesures de sécurité. Ces mesures peuvent être techniques ou non techniques (produit de sécurité logique ou physique, configuration particulière, mesures organisationnelles ou humaines, règles, procédures…).

Chaque mesure de sécurité peut utilement être catégorisée selon la ligne de défense (préventive, protectrice ou récupératrice) à laquelle elle appartient. Cela facilitera ultérieurement la détermination des mesures de sécurité en appliquant une défense en profondeur.

Conseils

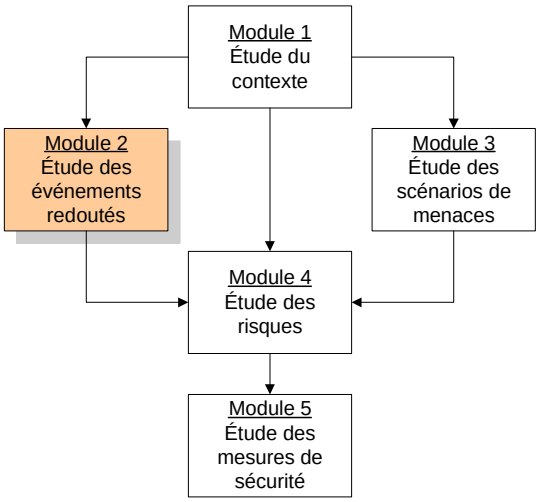
- Cette action s'enrichit généralement au fur et à mesure de l'avancement de l'étude.
- L'identification de mesures de sécurité existantes permet souvent de mettre en évidence des biens supports que l'on n'avait pas précédemment identifiés.
- Il est souvent plus facile de relever les mesures existantes telles qu'elles sont exprimées par les parties prenantes et d'investiguer ensuite pour les préciser et les catégoriser (ligne de défense et bien support).

Exemple

@RCHIMED a recensé les mesures de sécurité existantes suivantes :

Mesure de sécurité	***Bien support sur lequel elle repose***	***Thème ISO 27002***	***Prévention***	***Protection***	***Récupération***
Accord sur le niveau de service de l'hébergeur	*ORG – Organisation du cabinet*	*6.2. Tiers*	*X*		*X*
Activation d'une alarme anti-intrusion durant les heures de fermeture	*LOC – Locaux du cabinet*	*9.1. Zones sécurisées*	*X*		
Consignes de fermeture à clef des locaux	*LOC – Locaux du cabinet*	*9.1. Zones sécurisées*		*X*	
Dispositifs de lutte contre l'incendie	*LOC – Locaux du cabinet*	*9.1. Zones sécurisées*		*X*	
Climatisation	*LOC – Locaux du cabinet*	*9.2. Sécurité du matériel*	*X*		
Contrat de maintenance informatique (intervention sous 4h)	*ORG – Organisation du cabinet*	*9.2. Sécurité du matériel*	*X*		*X*
Alimentation secourue	*MAT – Serveur réseau et fichiers*	*9.2. Sécurité du matériel*		*X*	
Installation d'un antivirus sous Windows XP	*LOG – Windows XP*	*10.4. Protection contre les codes malveillant et mobile*		*X*	
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	*MAT – Disque USB*	*10.5. Sauvegarde*			*X*
Activation du WPA2	*MAT – Commutateur*	*10.6. Gestion de la sécurité des réseaux*	*X*		
Accès restreint en entrée (messagerie, services WEB…)	*MAT – Commutateur*	*10.6. Gestion de la sécurité des réseaux*	*X*		
Contrôle d'accès par mot de passe sous Windows XP	*LOG – Windows XP*	*11.5. Contrôle d'accès au système d'exploitation*	*X*		
Assurance multirisque professionnelle et sur les matériels informatiques	*ORG – Organisation du cabinet*	*14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité*			*X*
…	*…*	*…*	*…*	*…*	*…*

Module 2 – Étude des événements redoutés



Ce module a pour objectif d'identifier de manière systématique les scénarios génériques que l'on souhaite éviter concernant le périmètre de l'étude : les événements redoutés. Les réflexions sont menées à un niveau davantage fonctionnel que technique (sur des biens essentiels et non sur des biens supports).

Il permet tout d'abord de faire émerger tous les événements redoutés en identifiant et combinant chacune de leurs composantes : on estime ainsi la valeur de ce que l'on souhaite protéger (les besoins de sécurité des biens essentiels), on met en évidence les sources de menaces auxquelles on est confronté et les conséquences (impacts) des sinistres. Il est alors possible d'estimer le niveau de chaque événement redouté (sa gravité et sa vraisemblance).

Il permet également de recenser les éventuelles mesures de sécurité existantes et d'estimer leur effet en ré-estimant la gravité des événements redoutés, une fois les mesures de sécurité appliquées.

À l'issue de ce module, les événements redoutés sont identifiés, explicités et positionnés les uns par rapport aux autres, en termes de gravité et de vraisemblance.

Le module comprend une activité :

- Activité 2.1 – Apprécier les événements redoutés

Activité 2.1 – Apprécier les événements redoutés

Objectif

Cette activité fait partie de l'appréciation des risques. Elle a pour but de faire émerger et de caractériser les événements liés à la sécurité de l'information que l'organisme redoute, sans étudier la manière dont ceux-ci peuvent arriver. Elle permet également de fournir les éléments nécessaires au choix de traitement des risques afférents et à la définition des priorités de traitement.

Avantages

- Permet aux parties prenantes de comparer objectivement l'importance des biens essentiels et de prendre conscience des véritables enjeux de sécurité
- Permet d'étudier un périmètre sans détailler les biens supports et les scénarios envisageables
- Permet de hiérarchiser les événements redoutés, voire d'en écarter de la suite de l'étude

Données d'entrée

- Critères de sécurité
- Biens essentiels
- Échelles de mesures
- Typologie d'impacts
- Sources de menaces
- Critères de gestion des risques

Actions préconisées et rôle des parties prenantes

Actions : \ Parties prenantes :	Responsable	RSSI	*Risk manager*	Autorité	Dépositaire	Propriétaire
Action 2.1.1. Analyser tous les événements redoutés	A	C			R	
Action 2.1.2. Évaluer chaque événement redouté	R	C	I	A	C	

Données produites

- Événements redoutés

Communication et concertation

- Les données sont obtenues sur la base d'échanges entre les parties prenantes
- Les besoins peuvent être exprimés par plusieurs personnes qui ne donneront pas forcément les mêmes réponses ; il convient alors de confronter les arguments, de les collecter et d'obtenir un consensus qui peut nécessiter la décision d'une autorité
- Les événements redoutés peuvent être présentés sous la forme d'exemples d'événements redoutés hiérarchisés, d'arbres d'impacts ou de fiches détaillées (bien essentiel, critère de sécurité, besoins de sécurité, sources de menaces, impacts, gravité)

Surveillance et revue

- Les événements redoutés sont comparables les uns aux autres
- Des processus sont mis en place pour vérifier qu'on a bien considéré toutes les informations nécessaires (par rapport à l'état de l'art, aux organismes dans le même secteur d'activités…)
- Les résultats sont justifiés (sources externes, littérature, études, normes, cadres opérationnels, pratiques exemplaires, bases de connaissances…)
- Les résultats reflètent l'expérience des participants ou le contexte avec crédibilité
- Des descriptions riches et respectant la réalité sont illustrées clairement et avec verve
- Les critères de gestion sont utilisés de façon cohérente avec les limites des échelles utilisées
- Des échelles de mesures identiques sont utilisées
- Lorsque des résultats sont convertis, les choix sont justifiés et validés
- L'analyse des données recueillies et des résultats ne dénature pas le sens de l'information
- L'interprétation des personnes réalisant l'étude s'accorde avec les données recueillies
- Les résultats obtenus à l'aide des critères de gestion des risques sont discutés

Propositions pour mettre en œuvre les actions préconisées

Action 2.1.1. Analyser tous les événements redoutés

Description

Cette action consiste à identifier et à estimer les événements redoutés pour chaque critère de sécurité et chaque bien essentiel identifié. On va ainsi faire émerger les besoins de sécurité des biens essentiels, les impacts encourus au cas où ils ne seraient pas respectés et les sources de menaces susceptibles d'en être à l'origine, et leur attribuer un niveau de gravité.

Pour mener à bien cette activité, un groupe de travail hétérogène et représentatif du périmètre de l'étude (responsable du périmètre de l'étude, dépositaires des biens essentiels, experts métiers…) est constitué.

Pour chaque critère de sécurité de chaque bien essentiel, le but est de définir le besoin de sécurité, les impacts occasionnés par son non-respect et les sources de menaces susceptibles d'en être à l'origine. Ces événements redoutés sont obtenus en questionnant les parties prenantes sur ce qu'elles craignent et en approfondissant la réflexion jusqu'à ce que tous les éléments aient été formulés.

Bien que l'on puisse réaliser cette action de manière séquentielle (expression des besoins de sécurité, puis identification des impacts, et enfin identification des sources de menaces), la réflexion est généralement menée globalement. En effet, il semble plus naturel de s'interroger sur tous les éléments constitutifs d'un même événement redouté (besoins de sécurité, impacts et sources de menaces) pour ensuite développer chaque autre événement redouté, et par ailleurs, les parties prenantes ne répondent pas forcément aux questions dans un ordre séquentiel, du fait de l'interprétation qu'elles peuvent faire des différents concepts (besoin, impact, source, événement redouté).

D'une manière générale, il est recommandé :

- d'exprimer les besoins de sécurité de chaque bien essentiel en choisissant la valeur limite acceptable de chaque échelle de besoins définie ;
- d'identifier, pour chaque besoin de sécurité exprimé et pour chaque type d'impact (d'après une typologie), des exemples d'impacts survenant par le non-respect du besoin de sécurité ;
- d'identifier, pour chaque besoin de sécurité exprimé et pour chaque type de sources de menace (d'après une typologie), des exemples de sources de menaces susceptibles d'être à l'origine du non respect du besoin de sécurité.

Concernant les besoins de sécurité, les parties prenantes devraient être invitées à choisir un niveau sur chaque échelle de besoins pour chaque bien essentiel.
Pour ce faire, on peut par exemple leur demander à partir de quel niveau :

- le bien essentiel n'est plus conforme à la qualité attendue, ou
- elles ne peuvent plus exercer leur métier dans de bonnes conditions.

Il s'agit de besoins exprimés au regard des processus métiers. Ils sont indépendants des risques encourus et des moyens de sécurité mis en œuvre. Ils représentent donc une valeur intrinsèque de la sensibilité des biens essentiels.
Si un bien essentiel a des besoins qui varient dans le temps, il est recommandé d'étudier séparément ses différents états comme s'il s'agissait d'autant de biens essentiels.
Quand les parties prenantes sont interrogées séparément, une synthèse devrait être établie pour harmoniser les différents points de vue. Cette opération devrait être effectuée par des personnes disposant d'une vision globale des biens essentiels. Un consensus peut alors être obtenu par expression des argumentaires de chacun, suivie d'un arbitrage. Dans le cas où des divergences trop importantes apparaîtraient, il peut être nécessaire de demander aux parties prenantes de justifier davantage leurs valeurs, voire de les reconsidérer.

Concernant les impacts, les parties prenantes devraient expliquer les conséquences possibles du non-respect de chaque besoin de sécurité exprimé.

On peut y parvenir en leur demandant :

- ce qui peut concrètement arriver si le besoin de sécurité n'est pas respecté, ou
- ce qui est définitivement perdu ou plus rattrapable si la limite est dépassée.

Pour ce faire, il convient d'identifier les types d'impacts pertinents dans le contexte du sujet étudié. Les bases de connaissances de la méthode proposent une liste générique que l'on peut directement utiliser ou dans laquelle on peut sélectionner des types d'impacts. Ces impacts sont proposés à titre indicatif, le groupe de travail peut proposer les plus significatifs pour l'organisme et les adapter précisément à l'organisme. Les résultats précédents pourront être utilisés pour le choix de ces types d'impacts. On retiendra la remise en cause des missions, du métier ou des valeurs de l'organisme, comme des impacts significatifs. Afin de rendre les impacts plus objectifs, il est utile de fournir des exemples explicites en termes de conséquences envisageables.
Les types d'impacts ainsi définis permettent de pousser les parties prenantes à envisager des conséquences de différentes natures, auxquelles elles n'auraient peut-être pas songé.
Si les impacts identifiés sont finalement jugés comme acceptables, cela peut signifier que le besoin de sécurité exprimé a été surestimé. Il convient dès lors de reprendre le questionnement avec un niveau inférieur de l'échelle de besoins correspondante.
Il est également possible de constituer des arbres pour représenter enchaînements d'impacts :

- pour chaque besoin de sécurité exprimé et pour chaque type d'impact, rechercher les impacts directs en se posant la question suivante : que se passerait-il dans le domaine de ce type d'impact si le besoin de sécurité n'était pas respecté ?
- rechercher les éventuels impacts induits en se posant la question suivante pour chaque impact direct : que se passerait-il si cet impact arrivait ? puis rechercher les éventuels impacts induits, conséquences de chaque impact induit, et ainsi de suite…
- arrêter l'inventaire quand les mêmes impacts reviennent plusieurs fois et que ceux-ci correspondent à des critères, croyances ou éléments de cultures fort(e)s ;
- si possible, vérifier sur le terrain ou sur la base d'expériences vécues la réalité et le poids relatif de chaque impact identifié.

Concernant les sources de menaces, les parties prenantes doivent sélectionner, parmi celles qui ont été retenues, celles qui peuvent être à l'origine de chaque événement redouté et les illustrer par des exemples concrets.

Pour estimer la gravité des événements redoutés au cas où ceux-ci se réaliseraient, il convient d'attribuer un niveau de gravité à chaque événement redouté en utilisant l'échelle de gravité définie. L'estimation est faite au regard :

- de la valeur du bien essentiel considéré,
- de la hauteur et du nombre des impacts identifiés.

Elle ne doit pas tenir compte des éventuelles mesures de sécurité existantes.

Il convient finalement d'examiner les résultats obtenus afin de mettre en évidence et de résoudre les éventuelles incohérences entre leurs besoins de sécurité, leurs impacts, leurs sources de menaces et leurs niveaux de gravité. À l'issue, chaque événement redouté peut être comparé aux autres. Les valeurs doivent être cohérentes les unes par rapport aux autres.
Il est ainsi possible d'ajuster les résultats obtenus en vérifiant :

- la corrélation éventuelle entre les différents événements redoutés (des biens essentiels peuvent avoir des dépendances les uns par rapports aux autres) ;
- l'importance relative des besoins de sécurité entre les différents événements redoutés ;
- le niveau de détail des libellés des exemples (qui devraient être harmonisés).

Cette action ne doit pas être négligée car elle permet d'accroître la cohérence de l'étude, sa qualité et son réalisme, la facilité de validation, la compréhension et l'adhésion des parties prenantes.

Conseils

- Le point de vue des parties prenantes devrait être justifié par des commentaires.
- Les illustrations concrètes (impacts et sources de menaces) sont préférées aux généralités.
- Il peut être utile de formuler les événements redoutés sous la forme de scénarios narratifs. Cette forme peut être mieux comprise et acceptée de la part des parties prenantes.
- Considérer tous les types d'impacts des bases de connaissances pour pousser les parties prenantes à envisager des impacts auxquels ils n'auraient peut-être pas songé.
- S'assurer que les termes sont bien compris par les parties prenantes et les ajuster si besoin.
- Pour que la traçabilité des choix effectués soit la plus claire possible, il est possible de transformer les événements redoutés non retenus en hypothèses.
- Faire estimer la gravité par les parties prenantes, leur présenter l'ensemble des résultats

collectés et les ajuster de façon à refléter leur point de vue.

- Cette action peut utilement permettre de revoir ou d'enrichir les besoins de sécurité, les sources de menaces et les impacts.

Exemple

Chaque ligne du tableau suivant représente un événement redouté par le cabinet @RCHIMED (bien essentiel, critère de sécurité, besoin de sécurité selon les échelles de besoin, sources de menaces et impacts). La gravité de chaque évènement redouté est estimée (cf. échelle de gravité) sans tenir compte des mesures de sécurité existantes.

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Établir les devis				
Indisponibilité de devis	*24-72h*	✓ *Employé peu sérieux* ✓ *Incendie des locaux* ✓ *Panne électrique*	✓ *Impossibilité de signer un contrat* ✓ *Perte d'un marché* ✓ *Perte de crédibilité*	*2. Limitée*
Altération de devis	*Intègre*	✓ *Employé peu sérieux*	✓ *Impossibilité de signer un contrat* ✓ *Perte d'un marché* ✓ *Impossibilité de remplir les obligations légales* ✓ *Perte de crédibilité*	*3. Importante*
Compromission de devis	*Limité*	✓ *Employé peu sérieux* ✓ *Concurrent*	✓ *Perte d'un marché* ✓ *Action en justice à l'encontre du cabinet* ✓ *Perte de crédibilité*	*3. Importante*
Créer des plans et calculer les structures				
Indisponibilité de plans ou de calculs de structures	*24-72h*	✓ *Employé peu sérieux* ✓ *Virus non ciblé* ✓ *Personnel de nettoyage (soudoyé)* ✓ *Personnels de maintenance* ✓ *Panne électrique*	✓ *Perte de crédibilité*	*2. Limitée*
Altération de plans ou de calculs de structures	*Intègre*	✓ *Employé peu sérieux* ✓ *Concurrent*	✓ *Impossibilité de remplir les obligations légales* ✓ *Perte de crédibilité* ✓ *Action en justice à l'encontre du cabinet* ✓ *Perte de notoriété* ✓ *Mise en danger (bâtiment qui s'écroule)*	*4. Critique*
Compromission de plans ou calculs de structures	*Limité*	✓ *Employé peu sérieux* ✓ *Personnel de nettoyage (soudoyé)* ✓ *Personnels de maintenance*	✓ *Perte d'un marché* ✓ *Perte de crédibilité* ✓ *Perte de notoriété* ✓ *Impossibilité de remplir les obligations légales (si contractuel)*	*3. Importante*
Créer des visualisations				
Indisponibilité de visualisations	*24-72h*	✓ *Employé peu sérieux* ✓ *Virus non ciblé* ✓ *Incendie des locaux* ✓ *Panne électrique*	✓ *Bouche à oreille négatif* ✓ *Perte de crédibilité* ✓ *Perte de notoriété*	*2. Limitée*
Altération de visualisations	*Détectable*	✓ *Employé peu sérieux*	✓ *Bouche à oreille négatif* ✓ *Perte de crédibilité* ✓ *Perte de notoriété*	*2. Limitée*
Compromission de visualisations	*Public*	-	-	*1. Négligeable*
Gérer le contenu du site Internet				
Indisponibilité du site Internet	*24-72h*	✓ *Employé peu sérieux* ✓ *Virus non ciblé* ✓ *Concurrent* ✓ *Script-kiddies* ✓ *Panne électrique* ✓ *Hébergeur*	✓ *Perte de crédibilité* ✓ *Perte de notoriété* ✓ *Bouche à oreille négatif*	*2. Limitée*
Altération du contenu du site Internet	*Maîtrisé*	✓ *Employé peu sérieux* ✓ *Virus non ciblé* ✓ *Concurrent* ✓ *Script-kiddies* ✓ *Hébergeur*	✓ *Perte de crédibilité* ✓ *Perte de notoriété* ✓ *Bouche à oreille négatif* ✓ *Perte d'un marché ou de clientèle*	*3. Importante*
Compromission du contenu du site Internet	*Public*	-	-	*1. Négligeable*

Action 2.1.2. Évaluer chaque événement redouté

Description

Cette action consiste à juger de l'importance des événements redoutés en les hiérarchisant selon les critères de gestion des risques retenus.

Il convient essentiellement de fournir les éléments nécessaires pour décider de développer ou non l'étude concernant chaque événement redouté, de traiter ou non les risques afférents et de prioriser la mise en œuvre de leur traitement.

Pour ce faire, on peut positionner chaque événement redouté dans un tableau selon leur gravité. Dans ce cas, on utilise généralement un libellé court et explicite, reflétant l'atteinte d'un critère de sécurité d'un bien essentiel, pour chaque événement redouté.

Certains événements redoutés peuvent être écartés de la suite de l'étude si les critères de gestion des risques retenus le prévoient (par exemple, si la gravité est très faible). Il est important d'expliquer pourquoi ils ne sont pas retenus, car ils ne seront pas étudiés dans la suite de l'étude et constituent ainsi des événements redoutés non traités. Cette opération doit donc être dûment justifiée.

Conseils

- La représentation par gravité permet de visualiser le positionnement des événements redoutés les uns par rapport aux autres.
- Certains événements redoutés peuvent éventuellement être écartés de la suite de l'étude si les critères de gestion des risques retenus le prévoient (par exemple, si le niveau des besoins de sécurité ou la gravité est très faible). Qu'ils soient jugés improbables, jugés sans conséquence, traités par ailleurs, ultérieurement ou volontairement écartés, il est important d'expliquer pourquoi ils ne sont pas retenus, car ils ne seront pas étudiés dans la suite de l'étude bien qu'ils puissent être à l'origine de risques pour l'organisme. Cette opération doit donc être dûment justifiée.

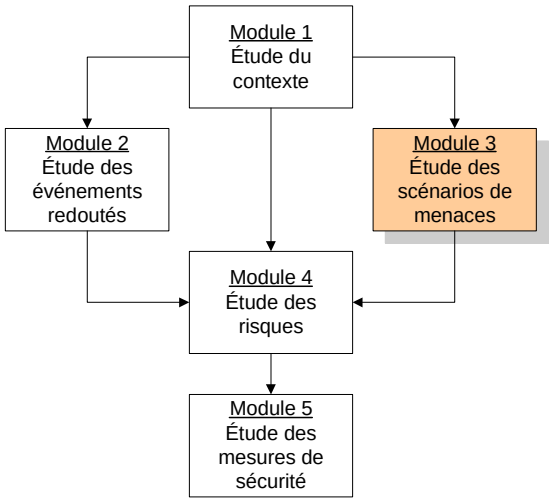
Exemple

L'importance relative des événements redoutés précédemment analysés (identifiés et estimés) est évaluée à l'aide du tableau suivant (cf. critères de gestion des risques) :

Gravité	***Événements redoutés***
4. Critique	✓ *Altération de plans ou de calculs de structures*
3. Importante	✓ *Altération de devis* ✓ *Compromission de plans ou calculs de structures* ✓ *Compromission de devis* ✓ *Altération du contenu du site Internet*
2. Limitée	✓ *Indisponibilité de devis* ✓ *Indisponibilité de visualisations* ✓ *Altération de visualisations* ✓ *Indisponibilité de plans ou de calculs de structures* ✓ *Indisponibilité du site Internet*
1. Négligeable	✓ *Compromission de visualisations* ✓ *Compromission du contenu du site Internet*

Module 3 – Étude des scénarios de menaces

Ce module a pour objectif d'identifier de manière systématique les modes opératoires génériques qui peuvent porter atteinte à la sécurité des informations du périmètre de l'étude : les scénarios de menaces. Les réflexions sont menées à un niveau davantage technique que fonctionnel (sur des biens supports et non plus des biens essentiels).



Il permet tout d'abord de faire émerger tous les scénarios de menaces en identifiant et combinant chacune de leurs composantes : on met ainsi en évidence les différentes menaces qui pèsent sur le périmètre de l'étude, les failles exploitables pour qu'elles se réalisent (les vulnérabilités des biens supports), et les sources de menaces susceptibles de les utiliser. Il est ainsi possible d'estimer le niveau de chaque scénario de menace (sa vraisemblance).

Il permet également de recenser les éventuelles mesures de sécurité existantes et d'estimer leur effet en ré-estimant la vraisemblance des scénarios de menaces, une fois les mesures de sécurité appliquées.

À l'issue de ce module, les scénarios de menaces sont identifiés, explicités et positionnés les uns par rapport aux autres en termes de vraisemblance.

Le module comprend une activité :

- Activité 3.1 – Apprécier les scénarios de menaces

Activité 3.1 – Apprécier les scénarios de menaces

Objectif

Cette activité fait partie de l'appréciation des risques. Elle a pour but d'identifier les différentes possibilités d'actions sur les biens supports, afin de disposer d'une liste complète de scénarios de menaces. Elle permet également de fournir les éléments nécessaires au choix de traitement des risques afférents et à la définition des priorités de traitement.

Avantages

- Permet aux parties prenantes de réaliser la diversité des menaces et de comparer objectivement la faisabilité des modes opératoires
- Permet de garantir une exhaustivité de la réflexion sur les menaces et les vulnérabilités
- Permet de s'adapter aux connaissances dont on dispose sur le périmètre de l'étude
- Permet de hiérarchiser les scénarios de menaces, voire d'en écarter de la suite de l'étude

Données d'entrée

- Critères de sécurité
- Biens supports
- Échelles de mesures
- Typologie de menaces et des vulnérabilités
- Sources de menaces
- Critères de gestion des risques

Actions préconisées et rôle des parties prenantes

Actions : \ Parties prenantes :	Responsable	RSSI	*Risk manager*	Autorité	Dépositaire	Propriétaire
Action 3.1.1. Analyser tous les scénarios de menaces	A	C				R
Action 3.1.2. Évaluer chaque scénario de menace	A	C	I			C

Données produites

- Scénarios de menaces

Communication et concertation

- Les données sont obtenues sur la base d'échanges entre les parties prenantes
- Les scénarios de menaces peuvent être présentés sous la forme d'exemples de scénarios hiérarchisés, d'arbres de menaces ou de fiches détaillées (bien support, critère de sécurité, sources de menaces, vraisemblance, menaces, vulnérabilités et pré-requis)

Surveillance et revue

- Les scénarios de menaces sont comparables les uns aux autres
- Des processus sont mis en place pour vérifier qu'on a bien considéré toutes les informations nécessaires (par rapport à l'état de l'art, aux organismes dans le même secteur d'activités dans la même région, le même pays, le même continent ou à l'internationale)
- Les résultats sont justifiés de manière explicite et, si possible, basés sur des éléments factuels (données historiques, fréquence des sinistres, non-pertinence…)
- Les résultats reflètent l'expérience des participants ou le contexte avec crédibilité
- Des descriptions riches et respectant la réalité sont illustrées clairement et avec verve
- Des échelles de mesures identiques et comparables sont utilisées pour tous les scénarios
- Les critères de gestion sont utilisés de façon cohérente en considérant les limites des échelles
- La conversion de résultats (ex. : en valeurs numériques) est justifiée et validée
- L'analyse des données recueillies et des résultats ne dénature pas le sens de l'information
- L'interprétation des personnes réalisant l'étude s'accorde avec les données recueillies
- Les résultats obtenus à l'aide des critères de gestion des risques sont discutés

Propositions pour mettre en œuvre les actions préconisées

Action 3.1.1. Analyser tous les scénarios de menaces

Description

Cette action consiste à identifier les scénarios de menaces pour chaque critère de sécurité et chaque bien support identifié et à les estimer en termes de vraisemblance.

Les scénarios de menaces sont obtenus en questionnant les parties prenantes sur ce qu'elles savent et en approfondissant la réflexion jusqu'à ce que tous les éléments aient été formulés.

D'une manière générale, il est recommandé d'identifier ensemble tous les éléments qui composent les scénarios de menaces :

- les menaces qui pourraient se concrétiser ;
- les vulnérabilités exploitables sur les biens supports ;
- les sources de menaces susceptibles d'en être à l'origine.

Pour mener à bien cette action, il convient tout d'abord de choisir une typologie de menaces. À cet effet, les bases de connaissances de la méthode proposent une liste générique que l'on peut directement utiliser ou que l'on peut ajuster. Cette typologie doit aider les parties prenantes à envisager des événements auxquels elles n'auraient peut-être pas songé, et ce, dans leur contexte particulier.
Au sein des menaces retenues, on ne sélectionne que celles qui touchent le critère de sécurité et le bien support considérés. On peut également écarter les menaces que l'on estime inapplicables ou que l'on ne souhaite pas étudier. Cela signifie que des risques ne seront pas appréciés. Il convient donc de justifier cette opération.
Il est également possible de constituer des arbres pour représenter enchaînements de menaces :

- pour chaque critère de sécurité et pour chaque bien support, rechercher les menaces directes en se posant la question suivante : que peut-il se passer sur ce bien support pour que ce critère de sécurité soit touché ?
- rechercher les menaces qui devraient être réalisées pour que les menaces se réalisent en se posant la question suivante pour chaque menace directe : quelles sont les menaces qui requises au préalable pour que cette menace puisse se réaliser ? puis rechercher les éventuelles menaces requises pour que chaque menace requise se réalise, et ainsi de suite…
- arrêter l'inventaire quand les mêmes menaces reviennent plusieurs fois et que celles-ci convergent vers des sources de menaces ;
- si possible, vérifier sur le terrain ou sur la base d'expériences vécues la réalité et le poids relatif de chaque menace identifiée.

Pour chaque bien support et chaque menace sélectionnée, on détermine les vulnérabilités qui peuvent être exploitées pour que la menace se réalise. Les bases de connaissances de la méthode proposent une typologie de vulnérabilités que l'on peut directement utiliser ou que l'on peut ajuster. Le nombre et le niveau de détail des vulnérabilités dépendent de l'objectif de l'étude et des livrables attendus.

Les sources de menaces doivent être sélectionnées parmi celles retenues. Il convient de ne retenir que celles qui peuvent être à l'origine des différents scénarios de menaces et de les illustrer par des exemples concrets.

Pour estimer la vraisemblance des scénarios de menaces, il convient d'attribuer un niveau à chaque scénario de menace en utilisant l'échelle de vraisemblance définie. L'estimation est essentiellement faite au regard :

- de l'existence plus ou moins avérée et de la facilité d'exploitation des vulnérabilités identifiées,
- de l'exposition aux menaces considérées,
- de l'exposition et du potentiel des sources de menaces identifiées.

Elle ne doit pas tenir compte des éventuelles mesures de sécurité existantes.

Il convient finalement d'examiner les scénarios de menaces dans leur ensemble afin de mettre en évidence et de résoudre les éventuelles incohérences entre leurs menaces, leurs biens supports et leurs vulnérabilités, leurs sources de menaces et leurs niveaux de vraisemblance. À l'issue, chaque scénario de menace peut être comparé aux autres : les valeurs doivent être cohérentes les unes par rapport aux autres.
Il est ainsi possible d'ajuster les résultats obtenus en vérifiant :

- la corrélation éventuelle entre les différents scénarios de menaces (des biens supports peuvent avoir des dépendances les uns par rapports aux autres) ;
- le niveau de détail des libellés des exemples (qui devraient être harmonisés).

Cette action ne doit pas être négligée car elle permet d'accroître la cohérence de l'étude, sa qualité et son réalisme, la facilité de validation, la compréhension et l'adhésion des parties prenantes.

Conseils

- Le point de vue des parties prenantes devrait être justifié par des commentaires.
- Les illustrations concrètes (menaces, vulnérabilités et sources de menaces) sont préférées aux généralités.
- Il peut être utile de formuler les scénarios de menaces sous la forme de scénarios narratifs. Cette forme peut être mieux comprise et acceptée de la part des parties prenantes.
- S'assurer que les termes sont bien compris par les parties prenantes et les ajuster si besoin.
- Pour que la traçabilité des choix effectués soit la plus claire possible, il est possible de transformer les scénarios de menaces non retenus en hypothèses.
- Faire estimer la vraisemblance par les parties prenantes, leur présenter l'ensemble des résultats collectés et les ajuster de façon à refléter leur point de vue.
- Cette action peut utilement permettre de revoir ou d'enrichir les menaces, les vulnérabilités et les sources de menaces.

Exemple

Les pages suivantes présentent les scénarios de menaces potentiellement réalisables dans le cadre du sujet de l'étude.

Les sources de menaces susceptibles d'en être à l'origine sont identifiées et la vraisemblance de chaque scénario de menace est estimée (cf. échelle de vraisemblance).

Le détail des scénarios de menaces (menaces, vulnérabilités et pré-requis) est décrit dans les bases de connaissances de la méthode EBIOS.

Scénarios de menaces	***Sources de menaces***	***Vraisemblance***
SYS – Réseau interne		
Menaces sur le réseau interne causant une indisponibilité	✓ *Employé peu sérieux* ✓ *Maintenance informatique* ✓ *Script-kiddies* ✓ *Virus non ciblé* ✓ *Incendie des locaux* ✓ *Panne électrique* ✓ *Phénomène naturel (foudre, usure…)*	*3. Forte*
Menaces sur le réseau interne causant une altération	✓ *Employé peu sérieux* ✓ *Maintenance informatique* ✓ *Script-kiddies* ✓ *Virus non ciblé*	*2. Significative*
Menaces sur le réseau interne causant une compromission	✓ *Employé peu sérieux* ✓ *Maintenance informatique* ✓ *Script-kiddies*	*2. Significative*
SYS – Sous réseau Ethernet		
Menaces sur le sous réseau Ethernet causant une indisponibilité	✓ *Employé peu sérieux* ✓ *Maintenance informatique* ✓ *Script-kiddies* ✓ *Virus non ciblé* ✓ *Incendie des locaux* ✓ *Panne électrique* ✓ *Phénomène naturel (foudre, usure…)*	*3. Forte*
Menaces sur le sous réseau Ethernet causant une altération	✓ *Employé peu sérieux* ✓ *Maintenance informatique* ✓ *Script-kiddies* ✓ *Virus non ciblé*	*2. Significative*
Menaces sur le sous réseau Ethernet causant une compromission	✓ *Employé peu sérieux* ✓ *Maintenance informatique*	*2. Significative*

Scénarios de menaces	Sources de menaces	Vraisemblance
	✓ Script-kiddies	
SYS – Sous réseau Wifi		
Menaces sur le sous réseau Wifi causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ Script-kiddies ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur le sous réseau Wifi causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ Script-kiddies ✓ Virus non ciblé	3. Forte
Menaces sur le sous réseau Wifi causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ Script-kiddies	3. Forte
ORG – Organisation du cabinet		
Menaces sur l'organisation d'@RCHIMED causant une indisponibilité	✓ Employé peu sérieux ✓ Personnel de nettoyage ✓ Maladie	2. Significative
Menaces sur l'organisation d'@RCHIMED causant une altération	✓ Employé peu sérieux ✓ Personnel de nettoyage	1. Minime
Menaces sur l'organisation d'@RCHIMED causant une compromission	✓ Concurrent (en visite incognito) ✓ Employé peu sérieux ✓ Cotraitant ✓ Client ✓ Maintenance informatique ✓ Personnel de nettoyage	4. Maximale
SYS – Système de l'hébergeur		
Menaces sur le système de l'hébergeur causant une indisponibilité	✓ Hébergeur ✓ Script-kiddies ✓ Virus non ciblé ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	4. Maximale
Menaces sur le système de l'hébergeur causant une altération	✓ Hébergeur ✓ Script-kiddies ✓ Virus non ciblé	3. Forte
Menaces sur le système de l'hébergeur causant une compromission	✓ Concurrent ✓ Client ✓ Partenaire	4. Maximale
ORG – Hébergeur		
Menaces sur l'hébergeur causant une indisponibilité	✓ Hébergeur	2. Significative
Menaces sur l'hébergeur causant une altération	✓ Hébergeur	2. Significative
Menaces sur l'hébergeur causant une compromission	✓ Hébergeur	1. Minime
SYS – Internet		
Menaces sur Internet causant une indisponibilité	✓ Fournisseur d'accès Internet	2. Significative
Menaces sur Internet causant une altération	✓ Script-kiddies	1. Minime
Menaces sur Internet causant une compromission	✓ Script-kiddies ✓ Concurrent	2. Significative
ORG – Partenaire		
Menaces sur un partenaire causant une indisponibilité	✓ Partenaire	3. Forte
Menaces sur un partenaire causant une altération	✓ Partenaire	1. Minime
Menaces sur un partenaire causant une compromission	✓ Partenaire	4. Maximale

Action 3.1.2. Évaluer chaque scénario de menace

Description

Cette action consiste à juger de l'importance des scénarios de menaces en les hiérarchisant selon les critères de gestion des risques retenus.

Il convient essentiellement de fournir les éléments nécessaires pour décider de traiter ou non les risques afférents et de prioriser la mise en œuvre de leur traitement.

Pour ce faire, on peut positionner chaque scénario de menace dans un tableau trié selon leur vraisemblance. Dans ce cas, on utilise généralement un libellé court et explicite, reflétant l'atteinte d'un critère de sécurité par un bien support, pour chaque scénario de menace.

Certains scénarios de menaces peuvent être écartés de la suite de l'étude si les critères de gestion des risques retenus le prévoient (par exemple, si la vraisemblance est très faible). Il est important d'expliquer pourquoi ils ne sont pas retenus, car ils ne seront pas étudiés dans la suite de l'étude et constituent ainsi des scénarios de menaces non traités. Cette opération doit donc être dûment justifiée.

Conseils

- La représentation par vraisemblance permet de visualiser le positionnement des scénarios de menaces les uns par rapport aux autres.
- Certains scénarios de menaces peuvent éventuellement être écartés de la suite de l'étude si les critères de gestion des risques retenus le prévoient (par exemple, si le niveau des besoins de sécurité est très faible). Qu'ils soient jugés improbables, jugés sans conséquence, traités par ailleurs, ultérieurement ou volontairement écartés, il est important d'expliquer pourquoi ils ne sont pas retenus, car ils ne seront pas étudiés dans la suite de l'étude bien qu'ils puissent être à l'origine de risques pour l'organisme. Cette opération doit donc être dûment justifiée.

Exemple

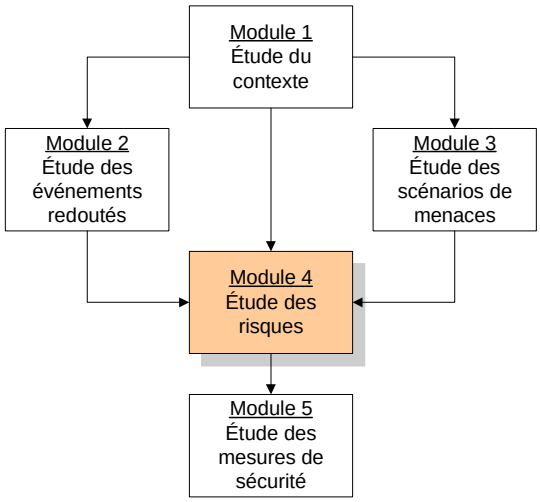
L'importance relative des scénarios de menaces précédemment analysés (identifiés et estimés) est évaluée de la façon suivante (cf. critères de gestion des risques) :

Vraisemblance	***Scénarios de menaces***
4. Maximale	✓ *Menaces sur l'organisation d'@RCHIMED causant une compromission* ✓ *Menaces sur le système de l'hébergeur causant une indisponibilité* ✓ *Menaces sur le système de l'hébergeur causant une compromission* ✓ *Menaces sur un partenaire causant une compromission*
3. Forte	✓ *Menaces sur le réseau interne causant une indisponibilité* ✓ *Menaces sur le sous réseau Ethernet causant une indisponibilité* ✓ *Menaces sur le sous réseau Wifi causant une indisponibilité* ✓ *Menaces sur le sous réseau Wifi causant une altération* ✓ *Menaces sur le sous réseau Wifi causant une compromission* ✓ *Menaces sur le système de l'hébergeur causant une altération* ✓ *Menaces sur un partenaire causant une indisponibilité*
2. Significative	✓ *Menaces sur le réseau interne causant une altération* ✓ *Menaces sur le réseau interne causant une compromission* ✓ *Menaces sur le sous réseau Ethernet causant une altération* ✓ *Menaces sur le sous réseau Ethernet causant une compromission* ✓ *Menaces sur l'organisation d'@RCHIMED causant une indisponibilité* ✓ *Menaces sur l'hébergeur causant une indisponibilité* ✓ *Menaces sur l'hébergeur causant une altération* ✓ *Menaces sur Internet causant une indisponibilité* ✓ *Menaces sur Internet causant une compromission*

Vraisemblance	***Scénarios de menaces***
1. Minime	✓ *Menaces sur l'organisation d'@RCHIMED causant une altération* ✓ *Menaces sur l'hébergeur causant une compromission* ✓ *Menaces sur Internet causant une altération* ✓ *Menaces sur un partenaire causant une altération*

Module 4 – Étude des risques

Ce module a pour objectif de mettre en évidence de manière systématique les risques pesant sur le périmètre de l'étude, puis de choisir la manière de les traiter en tenant compte des spécificités du contexte. Les réflexions sont menées à un niveau davantage fonctionnel que technique.



En corrélant les événements redoutés avec les scénarios de menaces susceptibles de les engendrer, ce module permet d'identifier les seuls scénarios réellement pertinents vis-à-vis du périmètre de l'étude. Il permet en outre de les qualifier explicitement en vue de les hiérarchiser et de choisir les options de traitement adéquates.

À l'issue de ce module, les risques sont appréciés et évalués, et les choix de traitement effectués.

Le module comprend les activités suivantes :

- Activité 4.1 – Apprécier les risques
- Activité 4.2 – Identifier les objectifs de sécurité

Activité 4.1 – Apprécier les risques

Objectif

Cette activité fait partie de l'appréciation des risques. Elle a pour but de mettre en évidence et de caractériser les risques réels pesant sur le périmètre de l'étude.

Avantages

- Permet de construire des scénarios de manière simple et exhaustive
- Permet de justifier de l'utilité des mesures de sécurité existantes
- Permet d'éviter de traiter des scénarios qui ne constituent pas des risques
- Permet de fournir les données nécessaires à l'évaluation des risques
- Permet de forcer les parties prenantes à s'interroger objectivement sur le niveau des risques

Données d'entrée

- Événements redoutés
- Scénarios de menaces
- Tableau croisé biens essentiels / biens supports
- Critères de gestion des risques
- Mesures de sécurité existantes

Actions préconisées et rôle des parties prenantes

Actions : \ Parties prenantes :	Responsable	RSSI	*Risk manager*	Autorité	Dépositaire	Propriétaire
Action 4.1.1. Analyser les risques	R	C			C	C
Action 4.1.2. Évaluer les risques	R	C	I	A	I	I

Données produites

- Risques

Communication et concertation

- Les données sont obtenues sur la base d'échanges entre les parties prenantes
- Les résultats peuvent faire l'objet d'une cartographie des risques

Surveillance et revue

- Des processus sont mis en place pour assurer vérifier qu'on a bien considéré toutes les informations nécessaires (par rapport à l'état de l'art, aux autres organismes dans le même secteur d'activités…)
- Il convient d'examiner les risques dans leur ensemble afin de mettre en évidence et de résoudre les éventuelles incohérences entre leurs composantes. À l'issue, chaque risque peut être comparé aux autres : la manière de les présenter doit donc être harmonisée et les valeurs doivent être cohérentes les unes par rapport aux autres.

Propositions pour mettre en œuvre les actions préconisées

Action 4.1.1. Analyser les risques

Description

Cette action consiste à mettre en évidence l'ensemble des risques qui pèsent réellement sur le périmètre de l'étude et à déterminer leur gravité et leur vraisemblance, une première fois sans tenir compte des mesures de sécurité existantes, et une seconde fois en les prenant en compte. On fait ainsi le lien entre les événements redoutés et les scénarios de menaces, c'est-à-dire entre ce que l'organisme craint et ce à quoi il est exposé.

Pour identifier les risques, il convient pour chaque événement redouté de retenir les scénarios de menaces qui :

- concernent les biens supports liés au bien essentiel considéré ;
- touchent le même critère de sécurité ;
- sont à l'initiative des mêmes sources de menaces (on ne gardera que celles en commun).

Chaque combinaison constitue un risque. Néanmoins, il est souhaitable de regrouper les risques afin leur liste ne soit pas trop longue. On considère ainsi généralement qu'un risque est composé d'un événement redouté et de tous les scénarios de menaces concernés.

Pour chaque risque, il convient ensuite de déterminer parmi les mesures de sécurité existantes identifiées, celles qui doivent avoir pour effet de :

- protéger les besoins de sécurité des biens essentiels identifiés (ces mesures de sécurité sont essentiellement des mesures de prévention et de récupération) ;
- réduire chaque impact identifié (prévision et préparation, prévention, confinement, lutte, récupération, restauration, compensation…) ;
- contrer chaque source de menaces identifiée (prévision et préparation, dissuasion, détection, confinement…) ;
- se protéger contre les menaces (essentiellement des mesures de détection et de protection) ;
- réduire les vulnérabilités des biens supports identifiés (essentiellement des mesures de prévention et de protection).

Enfin, pour estimer le niveau de chaque risque identifié en termes de gravité et de vraisemblance, on exploite les données produites dans les modules précédents.
Une première estimation, dite "brute", est réalisée sans tenir compte des mesures de sécurité existantes. Pour ce faire, la gravité et la vraisemblance de chaque risque sont estimées en fonction des critères de gestion des risques retenus. À défaut, sa gravité est égale à celle de l'événement redouté considéré et sa vraisemblance est égale à la valeur maximale des scénarios de menace concernés. Elles peuvent ensuite être ajustées, notamment la vraisemblance, qui jusqu'à présent, ne tenait pas compte des besoins de sécurité de l'élément essentiel et des sources de menaces en commun.
Une seconde estimation, dite "nette", est réalisée pour la gravité et la vraisemblance de chaque risque en tenant compte de l'effet des mesures de sécurité existantes, s'il en existe.

Conseils

- Il est généralement utile, à des fins de communication, d'illustrer les risques par des exemples représentatifs et explicites pour les parties prenantes.
- Le regroupement de risques, dans le but de réduire leur nombre, peut être réalisé par événement redouté, par impact, par scénario de menace, ou encore par menace.
- L'ajustement de la vraisemblance des risques est généralement effectué en fonction de la vraisemblance maximale des scénarios de menaces liés à un même événement redouté.
- Il n'est pas nécessaire de vérifier la bonne application des mesures de sécurité existantes. En effet, l'important est ici d'identifier ce qui a déjà été pensé pour ne pas le perdre. Le fait que ce soit mis en œuvre et la qualité de cette mise en œuvre pourront être vérifiés à l'occasion d'un audit spécifique.

Exemple

@RCHIMED a établi la liste des risques à partir des événements redoutés et des scénarios de menaces précédemment appréciés.
Les mesures de sécurité existantes ayant un effet sur chaque risque ont également été identifiées.
La gravité et la vraisemblance ont finalement été estimées, sans, puis avec, les mesures de sécurité (les niveaux rayés correspondent aux valeurs avant application de ces mesures).

Risque lié à l'indisponibilité d'un devis au-delà de 72h

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Indisponibilité de devis	24-72h	✓ Employé peu sérieux ✓ Incendie des locaux ✓ Panne électrique	✓ Impossibilité de signer un contrat ✓ Perte d'un marché ✓ Perte de crédibilité	2. Limitée

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le réseau interne causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ Script-kiddies ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur le sous réseau Wifi causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ Script-kiddies ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur l'organisation d'@RCHIMED causant une indisponibilité	✓ Employé peu sérieux ✓ Personnel de nettoyage ✓ Maladie	2. Significative
Menaces sur Internet causant une indisponibilité	✓ Fournisseur d'accès Internet	2. Significative
Menaces sur un partenaire causant une indisponibilité	✓ Partenaire	3. Forte

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	Récupération
Activation du WPA2	MAT – Commutateur	X		
Assurance multirisque professionnelle et sur les matériels informatiques	ORG – Organisation du cabinet			X
Climatisation	LOC – Locaux du cabinet	X		
Contrat de maintenance informatique (intervention sous 4h)	ORG – Organisation du cabinet	X		X
Contrôle d'accès par mot de passe	LOG – Windows XP	X		
Dispositifs de lutte contre l'incendie	LOC – Locaux du cabinet		X	
Installation d'un antivirus	LOG – Windows XP		X	
Alimentation secourue	MAT – Serveur réseau et fichiers		X	
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	X		
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	MAT – Disque USB			X

Niveau de risque				
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre
[…]

Risque lié à la compromission d'un devis au-delà du personnel et des partenaires
[…]

Action 4.1.2. Évaluer les risques

Description

Cette action consiste à juger de l'importance des risques en les hiérarchisant selon les critères de gestion des risques retenus.

Certains risques peuvent être écartés de la suite de l'étude si les critères de gestion des risques définis le prévoient (par exemple, si la gravité et/ou la vraisemblance est très faible). Il est important d'expliquer pourquoi ils ne sont pas retenus, car ils ne seront pas étudiés dans la suite de l'étude et constituent ainsi des risques non traités. Cette opération doit donc être dûment justifiée.

Conseils

- La représentation sous une forme graphique (vraisemblance en abscisses et gravité en ordonnées) permet de visualiser le positionnement des risques les uns par rapport aux autres.
- Il peut s'avérer utile d'écarter des risques quand leur nombre est important afin d'obtenir des résultats rapidement en se concentrant sur l'essentiel. On pourra les étudier dans un second temps. Néanmoins, il reste préférable d'éviter cette opération.

Exemple

Les risques précédemment analysés (identifiés et estimés) peuvent être évalués à l'aide du tableau suivant (les risques rayés correspondent à ceux réduits par des mesures de sécurité existantes) :

Gravité					
	4. Critique		*Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres*		
	3. Importante		*Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver*	*Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre* ~~*Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver*~~	*Risque lié à la compromission d'un devis au-delà du personnel et des partenaires* *Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires*
	2. Limitée		*Risque lié à l'indisponibilité d'un devis au-delà de 72h* *Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h* *Risque lié à l'indisponibilité de visualisations au-delà de 72h* *Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h*	~~*Risque lié à l'indisponibilité d'un devis au-delà de 72h*~~ ~~*Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h*~~ ~~*Risque lié à l'indisponibilité de visualisations au-delà de 72h*~~ *Risque lié à l'altération de visualisations sans pouvoir la détecter*	~~*Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h*~~
	1. Négligeable				*Risque lié à la compromission de visualisations, jugées comme publiques* *Risque lié à la compromission du contenu du site Internet public*
		1. Minime	***2. Significative***	***3. Forte***	***4. Maximale***
		Vraisemblance			

Risques négligeables	*Risques significatifs*	*Risques intolérables*

Activité 4.2 – Identifier les objectifs de sécurité

Objectif

Cette activité fait partie du traitement des risques. Elle a pour but de choisir la manière dont chaque risque devra être traité au regard de son évaluation.

Avantages

- Permet de choisir entre différentes options orientant le traitement des risques
- Permet aux parties prenantes de s'exprimer sans préjuger des moyens à mettre en œuvre
- Permet de constituer un cahier des charges cohérent avec l'ensemble des informations recueillies tout au long de l'étude

Données d'entrée

- Risques
- Paramètres à prendre en compte

Actions préconisées et rôle des parties prenantes

Actions : \ Parties prenantes :	Responsable	RSSI	*Risk manager*	Autorité	Dépositaire	Propriétaire
Action 4.2.1. Choisir les options de traitement des risques	R	C		A		
Action 4.2.2. Analyser les risques résiduels						

Données produites

- Objectifs de sécurité identifiés
- Risques résiduels identifiés

Communication et concertation

- Les données sont obtenues sur la base d'échanges entre les parties prenantes
- Les objectifs de sécurité peuvent faire l'objet :
  - d'une fiche d'expression rationnelle des objectifs de sécurité (FEROS), au sens du [Guide 150] ;
  - d'un cahier des charges "ouvert", c'est-à-dire laissant toute liberté pour déterminer des mesures de sécurité pour traiter les risques…

Surveillance et revue

- Des processus sont mis en place pour vérifier qu'on a bien considéré toutes les informations nécessaires (par rapport à l'état de l'art, aux organismes dans le même secteur d'activités…)

Propositions pour mettre en œuvre les actions préconisées

Action 4.2.1. Choisir les options de traitement des risques

Description

Cette action consiste à identifier les objectifs de sécurité, c'est-à-dire à choisir la manière dont on va devoir traiter les risques afin que le niveau de risque résiduel devienne acceptable.

Cette action doit être réalisée en fonction des critères de gestion des risques retenus.

Il convient ainsi, pour tout ou partie de chaque risque de choisir parmi les options suivantes :

- l'éviter (ou le refuser) : changer le contexte de telle sorte qu'on n'y soit plus exposé ;
- le réduire : prendre des mesures de sécurité pour diminuer l'impact et/ou la vraisemblance ;
- le prendre (ou le maintenir), voire l'augmenter : assumer les conséquences sans prendre de mesure de sécurité supplémentaire ;
- le transférer (ou le partager) : partager les pertes occasionnées par un sinistre ou faire assumer la responsabilité à un(des) tiers.

On note que l'on peut choisir plusieurs options pour chaque risque (ex. : un risque peut être partiellement réduit par la mise en œuvre de mesures de sécurité, partiellement transféré par le recours à une assurance et partiellement pris pour ce qui subsiste).

Le choix des options de traitement doit être fait au regard :

- des éléments constitutifs du risque (bien essentiel, bien support, critère de sécurité touché, impacts, menaces…) : ils permettent de juger de la faisabilité de leur traitement ;
- des critères de gestion des risques retenus : ils peuvent orienter le choix (évitement, réduction, prise ou transfert) selon la gravité et la vraisemblance (par exemple, il peut être décidé que les risques dont la gravité et la vraisemblance sont très faibles doivent être pris, les plus importants évités, et les autres réduits ou transférés) ;
- des paramètres à prendre en compte : ils peuvent avoir une influence sur les choix de traitement, notamment les contraintes et les hypothèses.

Conseils

- Il peut s'avérer utile l'illustrer ou d'orienter les choix de traitement en indiquant des exemples de mesures de sécurité pour chaque objectif de sécurité.
- Cette action fait généralement l'objet de modifications lorsque les négociations du module suivant poussent à réviser les choix de traitement.

Exemple

@RCHIMED souhaite essentiellement réduire les risques jugés comme prioritaires et significatifs, et prendre les risques jugés comme non prioritaires.

Le tableau suivant présente les objectifs de sécurité identifiés (les croix correspondent aux premiers choix, les croix entre parenthèses correspondent aux autres possibilités acceptées) :

Risque	Évitement	Réduction	Prise	Transfert
Risque lié à l'indisponibilité d'un devis au-delà de 72h		(X)	X	
Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	(X)	X	X	(X)
Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	(X)	X	X	(X)
Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h		(X)	X	
Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	(X)	X	X	(X)
Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	(X)	X	X	(X)
Risque lié à l'indisponibilité de visualisations au-delà de 72h		(X)	X	
Risque lié à l'altération de visualisations sans pouvoir la détecter		X	(X)	(X)
Risque lié à la compromission de visualisations, jugées comme publiques		(X)	X	
Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h		(X)	X	
Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver		X	(X)	(X)
Risque lié à la compromission du contenu du site Internet public		(X)	X	

Action 4.2.2. Analyser les risques résiduels

Description

Cette action consiste à identifier et à estimer les risques résiduels qui subsisteront quand chaque objectif de sécurité sera atteint, et à vérifier que l'on sera prêt à les accepter en toute connaissance de cause.

Cette action doit être réalisée en fonction des critères de gestion des risques retenus.

D'une manière générale, les risques résiduels sont mis en évidence selon le choix de traitement :

- un risque évité ne génère aucun risque résiduel s'il est complètement évité ; sinon, les risques résiduels correspondent à ce qui n'est pas évité ;
- un risque réduit mène à des risques résiduels s'il n'est pas totalement réduit ;
- un risque pris constitue un risque résiduel à part entière ;
- un risque transféré n'induit aucun risque résiduel s'il est totalement transféré ; sinon, les risques résiduels correspondent à ce qui n'est pas transféré.

La gravité et la vraisemblance des risques résiduels doivent finalement être estimées.

Pour chaque risque, il peut être utile de déterminer la gravité et la vraisemblance attendues une fois les objectifs de sécurité satisfaits. Ces niveaux constituent ainsi le niveau de risque acceptable.

Conseils

- Il est préférable de mettre systématiquement des risques résiduels en évidence. Ceci montre qu'une réflexion a été menée et tend à démontrer par leur énoncé que ces risques résiduels peuvent être acceptés.
- Il est possible que cette action ne mette en évidence aucun risque résiduel, notamment dans le cas où l'on prévoirait de réduire tous les risques. Le module suivant permettra de mettre en évidence des risques résiduels si la réduction des risques n'est pas complète.
- L'estimation des risques résiduels ne doit pas être négligée. En effet, c'est sur cette base que l'on pourra juger de leur acceptation.

Exemple

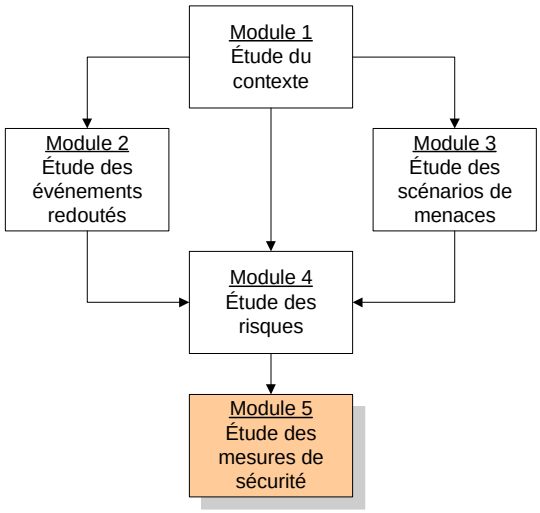
À l'issue de l'identification des objectifs de sécurité, @RCHIMED a mis en évidence les risques résiduels suivants :

Risques résiduels	***Gravité***	***Vraisemblance***
Risque lié à l'indisponibilité d'un devis au-delà de 72h	*2. Limitée*	*2. Significative*
Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h	*2. Limitée*	*2. Significative*
Risque lié à l'indisponibilité de visualisations au-delà de 72h	*2. Limitée*	*2. Significative*
Risque lié à la compromission de visualisations, jugées comme publiques	*1. Négligeable*	*4. Maximale*
Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h	*2. Limitée*	*2. Significative*
Risque lié à la compromission du contenu du site Internet public	*1. Négligeable*	*4. Maximale*

On note que ces risques résiduels pourront être réduits ultérieurement, quand les autres risques seront devenus acceptables.

Module 5 – Étude des mesures de sécurité

Ce module a pour objectif de déterminer les moyens de traiter les risques et de suivre leur mise en œuvre, en cohérence avec le contexte de l'étude. Les réflexions sont préférentiellement menées de manière conjointe entre les niveaux fonctionnels et techniques.



Il permet de trouver un consensus sur les mesures de sécurité destinées à traiter les risques, conformément aux objectifs précédemment identifiés, d'en démontrer la bonne couverture, et enfin, d'effectuer la planification, la mise en œuvre et la validation du traitement.

À l'issue de ce module, les mesures de sécurité sont déterminées et les points clés validés formellement. Le suivi de la mise en œuvre peut également être réalisé.

Le module comprend les activités suivantes :

- Activité 5.1 – Formaliser les mesures de sécurité à mettre en œuvre
- Activité 5.2 – Mettre en œuvre les mesures de sécurit

Activité 5.1 – Formaliser les mesures de sécurité à mettre en œuvre

Objectif

Cette activité fait partie du traitement des risques. Elle a pour but de déterminer les mesures de sécurité adéquates pour atteindre les objectifs de sécurité identifiés, d'identifier les risques résiduels et de valider "formellement" les choix effectués.

Avantages

- Permet d'exploiter les référentiels de mesures existants et/ou d'en élaborer des spécifiques
- Permet de s'adapter à l'objectif de la gestion des risques et aux livrables attendus
- Permet de mesurer l'efficacité des mesures de sécurité (rapport coût / effet)
- Permet aux parties prenantes de décider objectivement de la poursuite des actions
- Favorise l'implication et la responsabilisation des parties prenantes

Données d'entrée

- Objectifs de sécurité identifiés
- Paramètres à prendre en compte
- Meilleures pratiques (ex. : mesures de sécurité de l'[ISO 27002])

Actions préconisées et rôle des parties prenantes

Actions : \ Parties prenantes :	Responsable	RSSI	*Risk manager*	Autorité	Dépositaire	Propriétaire
Action 5.1.1. Déterminer les mesures de sécurité	R	C				C
Action 5.1.2. Analyser les risques résiduels	R	C	I	A	I	C
Action 5.1.3. Établir une déclaration d'applicabilité	R	C	I	A	I	C

Données produites

- Mesures de sécurité spécifiées
- Risques résiduels complétés
- Déclaration d'applicabilité

Communication et concertation

- Les résultats sont négociés au regard des objectifs de sécurité
- Les résultats de cette activité peuvent faire l'objet :
  - d'une déclaration d'applicabilité au sens de l'[ISO 27001] ;
  - d'une politique ou d'un règlement de sécurité de l'information ;
  - d'un profil de protection au sens de l'[ISO 15408] ;
  - d'une cible de sécurité au sens de l'[IGI 1300] ou de l'[ISO 15408] ;
  - d'un cahier des charges "fermé", c'est-à-dire spécifiant les mesures de sécurité destinées à traiter les risques…
- Trier les mesures de sécurité selon l'objectif de l'étude et les livrables attendus

Surveillance et revue

- Des processus sont mis en place pour vérifier qu'on a bien considéré toutes les informations nécessaires (par rapport à l'état de l'art, aux organismes dans le même secteur d'activités…)
- Les résultats précédents orientent les choix des mesures de sécurité (capacité de relier les mesures de sécurité aux objectifs de sécurité et aux paramètres à prendre en compte dans le traitement des risques)
- Les résultats revêtent une signification précise pour l'organisation (ils sont explicites pour les personnes auxquelles ils sont destinés)
- Les conclusions de l'étude couvrent l'ensemble des questions posées au départ
- Les résultats de l'analyse des données recueillies reflètent l'expérience des participants ou le contexte avec crédibilité
- Les résultats correspondent à ce que les participants voulaient dire et non simplement à ce qui a été exprimé (perspective émique)

- L’étude reflète le fait qu'elle soit répétable et récursive
- Les décisions et interprétations méthodologiques, de même que les positions particulières des personnes réalisant l'étude, sont considérées
- Des descriptions riches et respectant la réalité sont illustrées clairement et avec verve
- Des méthodes d’organisation, de présentation et d’analyse des données créative sont incorporées à l’étude
- La démarche et ses résultats sont cohérents et s'inscrivent dans le contexte particulier de l'étude (congruence)
- L’étude a été faite en tenant compte de la nature humaine et du contexte socioculturel de l'organisation étudiée

Propositions pour mettre en œuvre les actions préconisées

Action 5.1.1. Déterminer les mesures de sécurité

Description

Cette action consiste à déterminer les moyens d'atteindre les objectifs de sécurité. Il s'agit donc ici de définir les mesures de sécurité qui vont permettre d'éviter, de réduire ou de transférer tout ou partie des risques (la prise de risque ne requiert pas de mesures de sécurité), en tenant compte des contraintes identifiées, notamment budgétaires et techniques.

Les mesures de sécurité peuvent être sélectionnées et utilisées telles quelles dans des référentiels de mesures (normes, méthodes, bases de connaissances, catalogues de sécurité…), adaptées d'après des référentiels, ou créées de toute pièce. À cette fin, les bases de connaissances de la méthode proposent une liste générique que l'on peut directement utiliser ou que l'on peut ajuster.

Le contenu et le niveau de détail des mesures de sécurité doivent être cohérents avec le but de l'étude et des livrables attendus. Il peut s'agir d'exigences plus ou moins détaillées, de principes, de règles, de consignes, de procédures, de points de contrôle, de choix de produits, etc…

Par ailleurs, dès lors qu'une mesure de sécurité est spécifiée, il convient d'identifier :

- la ligne de défense (préventive, protectrice ou récupératrice) à laquelle elle appartient, afin de faciliter la détermination des mesures de sécurité en appliquant une défense en profondeur ;
- le bien support qui la porte, afin de faciliter l'optimisation des mesures de sécurité, son propriétaire étant a priori responsable de l'application de la mesure de sécurité.

Pour qu'un risque soit évité, il convient de changer un élément du contexte afin de ne plus y être exposé. Cela peut se traduire par des mesures de sécurité telles que le changement de localisation géographique, le fait de ne pas commencer ou poursuivre l'activité porteuse du risque, la séparation d'informations ayant des besoins de sécurité bien différents sur des biens supports isolés…

Pour qu'un risque soit transféré, il convient de partager les pertes avec un tiers. Les mesures de sécurité peuvent ainsi consister à souscrire à une assurance, financer le risque, utiliser des produits, des services ou des individus certifiés, contractualiser des clauses de transfert de responsabilité…

Pour qu'un risque soit réduit à un niveau acceptable, il convient de diminuer sa gravité et/ou sa vraisemblance en agissant sur ses composantes (sources de menaces, menaces, vulnérabilités, impacts…). Il est ainsi souvent nécessaire de mettre en œuvre plusieurs mesures de sécurité, et si possible, en appliquant les principes de défense en profondeur[3].

[3] Les principes de la défense en profondeur sont les suivants :

- la globalité : la défense englobe toutes les dimensions des systèmes d'information (aspects techniques, organisationnels, humains ou autres) ;
- la coordination : les moyens mis en place agissent à l'aide d'une capacité d'alerte et de diffusion et à la suite de corrélations d'incidents ;
- le dynamisme : l'organisme considère plusieurs niveaux de risques, planifie ses actions selon ces niveaux et dispose d'une capacité de réaction ;
- la suffisance : chaque mesure de sécurité bénéficie d'une protection propre, d'un moyen de détection, et de procédures de réaction ;
- la complétude : les biens essentiels sont protégés de manière proportionnée au niveau des risques, par au minimum trois lignes de défense et des retours d'expériences sont formalisés ;
- la démonstration : le dispositif de défense est justifié par la démonstration de couverture, et il existe une stratégie d'homologation qui adhère au cycle de vie du système d'information.

Afin de mettre en place une défense en profondeur, la démarche consiste dans un premier temps à établir au moins trois lignes de défense (selon la gravité des risques et la capacité des sources de menaces) pour chaque risque :

- une ligne préventive, destinée à éviter l'apparition des incidents et des sinistres à l'aide de mesures de sécurité qui agissent sur :
  - les sources de menaces (dissuasion, déception…),
  - les besoins de sécurité des biens essentiels (anticipation, prévention…),
  - les vulnérabilités des biens supports (réduction des failles, préparation…) ;
- une ligne protectrice, destinée à bloquer, contenir et détecter l'apparition des incidents et des sinistres à l'aide de mesures de sécurité qui agissent sur :
  - les besoins de sécurité des biens essentiels (confinement…),
  - les sources de menaces (lutte…),
  - les menaces (détection, protection, réaction défensive…),
  - les vulnérabilités des biens supports (résistance, résilience…) ;
- une ligne récupératrice, destinée à minimiser les conséquences des incidents et des sinistres et revenir à l'état initial, à l'aide de mesures de sécurité qui agissent sur :
  - les besoins de sécurité des biens essentiels (récupération, restauration…),
  - les sources de menaces (réaction offensive…),
  - les impacts (compensation…).

Chaque ligne de défense peut ensuite être renforcée en déterminant plusieurs mesures de sécurité sur un ou plusieurs bien support (un matériel, un logiciel, des locaux, une organisation…).
Un ensemble de mesures de soutien (alerte, diffusion, corrélation d'événements, protection des mesures de sécurité, réaction…) devrait compléter le dispositif de défense en profondeur.

On note que les éventuelles mesures de sécurité existantes doivent être considérées, mais peuvent aussi être remises en question par des mesures de sécurité plus appropriées.

Il convient enfin d'améliorer le dispositif global de sécurité, bien support par bien support. Le but est ici de faire le bilan pour gagner en pertinence, en économie et en efficacité.
La liste des mesures de sécurité portées par chaque bien support doit tout d'abord être établie.
Ensuite, l'applicabilité et la cohérence des mesures de sécurité portées par chaque bien support doivent être étudiées. Il est ainsi possible de vérifier que les mesures de sécurité sont compatibles entre elles, de factoriser certaines mesures de sécurité, de vérifier que la formulation va être comprise par le propriétaire du bien support, qu'il va être capable de la mettre en œuvre… Le cas échéant, les mesures de sécurité peuvent être adaptées en conséquence.

On estime finalement l'impact de la mise en œuvre de chaque mesure de sécurité en termes de coût financier ou de charge de personnel (étude, réalisation, application, maintien en situation opérationnelle…), mais aussi en termes de conséquences sur les habitudes et la culture des personnes et sur les processus métiers du fait du changement induit.

Conseils

- Les mesures de sécurité devraient être claires, simples et mesurables.
- La manière dont les mesures de sécurité sont rédigées doit être adaptée à ceux à qui elles sont destinées.
- Dans le cadre de la mise en place d'un système de management de la sécurité de l'information selon l'[ISO 27001], il convient de sélectionner en premier lieu les mesures de sécurité de son annexe A (ou de l'[ISO 27002]).
- Il est important dans lors de cette action de considérer les contraintes, notamment budgétaires ou techniques, et de privilégier la performance et le confort pour ceux qui vont devoir appliquer les mesures de sécurité (rapport entre sécurité et acceptation psychologique).

Exemple

Le tableau suivant présente la liste des mesures de sécurité destinées à réduire ou transférer les risques prioritaires (elles traitent également les autres risques) :

Mesure de sécurité	R1	R2	R3	R4	R5	R6	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
Chiffrement des fichiers liés aux plans et calculs de structures à l'aide de certificats électroniques				X			LOG – MacOS X	7.1. Responsabilités relatives aux biens		X	
Désactivation des composants inutiles sur le serveur	X	X	X	X	X	X	LOG – Serveurs logiciels du réseau interne	10.1. Procédures et responsabilités liées à l'exploitation	X		
Mise à jour régulière de l'antivirus des serveurs et de sa base de signatures	X		X		X	X	LOG – Windows XP	10.4. Protection contre les codes malveillant et mobile		X	
Accès restreint en entrée (messagerie, services WEB…)	X	X	X	X	X	X	MAT – Commutateur	10.6. Gestion de la sécurité des réseaux	X		
Rangement des supports amovibles dans un meuble fermant à clef		X		X			MAT – Disque USB	10.7. Manipulation des supports	X		
Utilisation d'antivols pour les ordinateurs portables		X		X			MAT – Ordinateurs portables	9.2. Sécurité du matériel	X		X
Utilisation de films empêchant l'espionnage de l'écran des ordinateurs portables		X		X			MAT – Ordinateurs portables	9.2. Sécurité du matériel	X		X
Accompagnement systématique des visiteurs dans les locaux		X		X			ORG – Organisation du cabinet	6.2. Tiers	X	X	
Inventaire des biens sensibles	X	X	X	X	X	X	ORG – Organisation du cabinet	7.1. Responsabilités relatives aux biens	X	X	X
Accord sur le niveau de service de l'hébergeur						X	ORG – Organisation du cabinet	10.2. Gestion de la prestation de service par un tiers	X		X
Contrôle annuel de l'application des mesures de sécurité	X	X	X	X	X	X	ORG – Organisation du cabinet	15.3. Prises en compte de l'audit du système d'information	X		
Assurance multirisque professionnelle et sur les matériels informatiques		X					ORG – Organisation du cabinet	14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité			X
Destruction des documents sensibles lors de leur mise au rebut		X		X			PAP – Support papier	10.7. Manipulation des supports	X		
Sensibilisation régulière des personnels aux risques encourus	X	X	X	X	X	X	PER – Utilisateur	8.2. Pendant la durée du contrat	X		
Retrait des droits d'accès en fin de contrat	X	X	X	X	X	X	PER – Administrateur	8.3. Fin ou modification de contrat	X		
Utilisation de mots de passe de qualité pour chaque compte utilisateur	X	X	X	X	X		PER – Utilisateur	11.3. Responsabilités utilisateurs	X		
…	…	…	…	…	…	…	…	…	…	…	…

Ces mesures de sécurité ont été déterminées dans l'objectif de couvrir différents éléments des risques à traiter (vulnérabilités, menaces, sources de menaces, besoins de sécurité ou impacts), d'aborder la plupart des thèmes de l'ISO 27002, de couvrir les différentes lignes de défense (prévention, protection et récupération), et ont été optimisées bien support par bien support.

Action 5.1.2. Analyser les risques résiduels

Description

Cette action consiste à identifier et à estimer les risques résiduels qui subsisteront quand chaque mesure de sécurité sera mise en œuvre. Cela permet de vérifier que l'on sera prêt à les accepter en toute connaissance de cause.

Pour chaque objectif de sécurité, il convient de :

- réaliser un argumentaire justificatif, qui devrait démontrer que :
  - la combinaison des mesures de sécurité traite le risque conformément à l'objectif de sécurité identifié,
  - l'ensemble des mesures de sécurité constitue un tout cohérent et dont les éléments se soutiennent mutuellement,
  - le niveau de résistance des mesures de sécurité choisi est cohérent avec les sources de menaces retenues ;
- compléter la liste des risques résiduels au regard des mesures de sécurité identifiées, et les estimer en termes de gravité et de vraisemblance ;
- estimer l'effet des mesures de sécurité sur la gravité et la vraisemblance du risque concerné en les ré-estimant.

Conseils

- Il peut être utile de réaliser un tableau croisé entre les objectifs de sécurité et les mesures de sécurité pour vérifier la couverture et qu'il n'existe pas de mesure de sécurité inutile.
- L'analyse des risques résiduels ne doit pas être négligée. En effet, c'est sur cette base que l'on pourra juger de leur acceptation.

Exemple

Si les mesures de sécurité précédemment identifiées sont mises en œuvre, alors le niveau des risques jugés comme intolérables ou significatifs peut être ré-estimé comme suit :

Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre

Niveau de risque				
Gravité	*1. Négligeable*	*2. Limitée*	***3. Importante***	*4. Critique*
Vraisemblance	***1. Minime***	~~*2. Significative*~~	~~*3. Forte*~~	*4. Maximale*

Risque lié à la compromission d'un devis au-delà du personnel et des partenaires

Niveau de risque				
Gravité	*1. Négligeable*	***2. Limitée***	~~*3. Importante*~~	*4. Critique*
Vraisemblance	*1. Minime*	***2. Significative***	~~*3. Forte*~~	~~*4. Maximale*~~

Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres

Niveau de risque				
Gravité	*1. Négligeable*	*2. Limitée*	***3. Importante***	~~*4. Critique*~~
Vraisemblance	***1. Minime***	~~*2. Significative*~~	*3. Forte*	*4. Maximale*

Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires

Niveau de risque				
Gravité	*1. Négligeable*	***2. Limitée***	~~*3. Importante*~~	*4. Critique*
Vraisemblance	*1. Minime*	***2. Significative***	~~*3. Forte*~~	~~*4. Maximale*~~

[…]

Action 5.1.3. Établir une déclaration d'applicabilité

Description

Cette action consiste à expliquer comment les paramètres à prendre en compte (références applicables, contraintes et hypothèses) ont été pris en compte au sein de l'étude et de justifier le fait de ne pas en avoir tenu compte, le cas échéant.

Elle permet ainsi de ne rien oublier de ce qu'il a été décidé de considérer lors de l'étude, et donc de rappeler, si ce n'est pas déjà fait, qu'il est nécessaire de tenir compte des paramètres identifiés dans l'établissement du contexte dans l'appréciation et dans le traitement des risques, et notamment dans la détermination des mesures de sécurité.

Certains paramètres à prendre en compte, notamment les références applicables, peuvent faire l'objet de mesures de sécurité complémentaires, dont il convient de vérifier la cohérence avec les autres mesures de sécurité. On note que le fait de ne pas prendre en compte des références réglementaires applicables engendre des risques de nature juridique qu'il convient de mettre en évidence.

Certains paramètres à prendre en compte peuvent également requérir de modifier des mesures de sécurité.

Cette action peut ainsi servir à démontrer l'applicabilité détaillée de meilleures pratiques en expliquant le positionnement face à chacune d'elles.
Pour chacune des meilleures pratiques, il suffit de déterminer, parmi les mesures de sécurité précédemment identifiées, celles qui lui correspondent.
Ainsi, les meilleures pratiques couvertes par au moins une mesure de sécurité peuvent être jugées comme utiles pour le périmètre de l'étude. Les mesures de sécurité liées à ces meilleures pratiques expliquent comment celles-ci sont appliquées, et ce, de manière nécessaire et suffisante.
A contrario, les meilleures pratiques qui ne sont couvertes par aucune mesure de sécurité peuvent être jugées comme inutiles pour le périmètre de l'étude. En effet, elles ne servent à traiter aucun risque ni à couvrir aucun paramètre à prendre en compte.

Conseils

- Ne pas négliger cette action, en termes d'importance ou de charges. En effet, la prise en compte des références applicables nécessite d'une part de vérifier que le contenu de ces références n'est pas en contradiction avec les mesures de sécurité, et d'autre part de créer des mesures de sécurité correspondant à ce contenu (créer des mesures de sécurité correspondant aux clauses de l'[ISO 27001]).
- Il peut être utile de capitaliser les mesures de sécurité créées à partir des références applicables en complétant les bases de connaissances.
- Le résultat de cette action peut directement constituer une déclaration d'applicabilité selon l'[ISO 27001].

Exemple

La prise en compte de chaque contrainte identifiée est explicitée comme suit :

Paramètre à prendre en compte	***Explication / Justification***
Le personnel est utilisateur de l'informatique, mais pas spécialiste	***Pris en compte*** *Les mesures de sécurité applicables par le personnel ne demandent pas une grande expertise*
Le personnel de nettoyage intervient de 7h à 8h	***Non pris en compte*** *Les horaires doivent correspondrent à ceux du personnel*
Aucun déménagement n'est planifié	***Pris en compte*** *Les mesures de sécurité formalisées ne demandent pas de déménagement*
…	…

Activité 5.2 – Mettre en œuvre les mesures de sécurité

Objectif

Cette activité fait partie du traitement des risques. Elle a pour but d'élaborer et de suivre la réalisation du plan de traitement des risques par les mesures de sécurité afin de pouvoir prononcer l'homologation de sécurité.

Avantages

- Améliore la légitimité et la visibilité des actions
- Favorise la réalisation et l'application des mesures de sécurité spécifiées

Données d'entrée

- Mesures de sécurité spécifiées
- Objectifs de sécurité identifiés

Actions préconisées et rôle des parties prenantes

Actions : \ Parties prenantes :	Responsable	RSSI	*Risk manager*	Autorité	Dépositaire	Propriétaire
Action 5.2.1. Élaborer le plan d'action et suivre la réalisation des mesures de sécurité	R	C				C
Action 5.2.2. Analyser les risques résiduels	R	C				
Action 5.2.3. Prononcer l'homologation de sécurité	R	C	I	A		

Données produites

- Plan d'action
- Mesures de sécurité mises en œuvre
- Risques résiduels mis à jour
- Décision d'homologation de sécurité

Communication et concertation

- Les données sont obtenues sur la base de réunions
- Elles peuvent faire l'objet d'un plan d'action ou d'un plan de traitement des risques
- Le contenu du dossier servant à l'homologation de sécurité doit être adapté à l'autorité et/ou à la commission d'homologation

Surveillance et revue

- L'interprétation des personnes réalisant l'étude s'accorde avec les données recueillies

Propositions pour mettre en œuvre les actions préconisées

Action 5.2.1. Élaborer le plan d'action et suivre la réalisation des mesures de sécurité

Description

Cette action consiste à identifier parmi les mesures de sécurité formalisées celles qui ne seraient pas déjà appliquées et à planifier concrètement les actions nécessaires à leur mise en œuvre.

Pour chaque mesure de sécurité précédemment formalisée, il convient d'indiquer, par exemple sous la forme d'un tableau :

- son libellé ;
- sa priorité (qui peut être déterminée par les critères de gestion de risques, par exemple en fonction de la gravité et de la vraisemblance des risques concernés) ;
- le responsable de la mise en œuvre (une personne ou une fonction) ;
- si besoin, le détail des actions à mener (notamment si plusieurs étapes sont nécessaires) ;
- l'échéance prévisionnelle ;
- le coût prévisionnel de mise en œuvre (notamment l'achat de produits et la charge estimée) ;
- l'état d'avancement (non démarré / en cours / terminé / contrôlé…) ;
- les moyens de contrôler la mise en œuvre (indicateur opérationnel, éléments de preuve…) ;
- les éventuels risques, résiduels ou induits, mis en évidence au fur et à mesure de l'avancement du plan d'action.

Conseils

- Il peut être utile de préciser si les mesures de sécurité doivent être appliquées avant ou après l'homologation. Celles qui servent à traiter des risques jugés comme bloquants devraient généralement être appliquées avant et celles qui servent à traiter des risques jugés comme majeurs, indirects et mineurs peuvent être appliquées après.
- D'une manière générale, chaque action du plan d'action devrait être :
  - S – spécifique (un acteur, un domaine à la fois) ;
  - M – mesurable (définition du moyen de contrôle) ;
  - A – atteignable (éventuellement en plusieurs étapes, avec les ressources nécessaires) ;
  - R – réaliste (en fonction des acteurs, de leurs capacités) ;
  - T – liée au temps (avec une date buttoir, un délai, une période définie).

Exemple

Le plan d'action d'@RCHIMED, trié par terme, avancement et coût financier, est établi comme suit :

Mesure de sécurité	*Responsable*	*Difficulté*	*Coût financier*	*Terme*	*Avancement*
Mesures du trimestre					
Activation d'une alarme anti-intrusion durant les heures de fermeture	*Directeur*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Consignes de fermeture à clef des locaux	*Directeur*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Dispositifs de lutte contre l'incendie	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Climatisation	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Contrôle d'accès par mot de passe sous MacOS X	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Contrôle d'accès par mot de passe sous Windows XP	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Accès restreint en entrée (messagerie, services WEB…)	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Activation du WPA2	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Sauvegarde hebdomadaire sur des disques USB stockés dans un meuble fermant à clef	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Installation d'un antivirus sous MacOS X	*Directeur adjoint*	*1. Faible*	*2. Moins de 1000€*	*1. Trimestre*	*3. Terminé*
Installation d'un antivirus sous Windows XP	*Directeur adjoint*	*1. Faible*	*2. Moins de 1000€*	*1. Trimestre*	*3. Terminé*

Mesure de sécurité	Responsable	Difficulté	Coût financier	Terme	Avancement
Alimentation secourue	Directeur adjoint	1. Faible	2. Moins de 1000€	1. Trimestre	3. Terminé
Contrat de maintenance informatique (intervention sous 4h)	Directeur adjoint	1. Faible	2. Moins de 1000€	1. Trimestre	3. Terminé
Accord sur le niveau de service de l'hébergeur	Directeur adjoint	1. Faible	2. Moins de 1000€	1. Trimestre	3. Terminé
Assurance multirisque professionnelle et sur les matériels informatiques	Directeur	1. Faible	3. Plus de 1000€	1. Trimestre	3. Terminé
Élaboration d'une politique de sécurité de l'information	Directeur adjoint	2. Moyenne	1. Nul	1. Trimestre	2. En cours
Rangement systématique des documents liés aux plans et calculs de structures dans un meuble fermé à clef	Bureau d'études	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Chiffrement des fichiers liés aux plans et calculs de structures à l'aide de certificats électroniques	Bureau d'études	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Création d'empreintes des fichiers liés aux plans et aux calculs de structure	Bureau d'études	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Création d'empreintes des fichiers liés aux visualisations	Bureau d'études	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
…	…	…	…	…	…
Installation d'un antivirus sur les serveurs	Directeur adjoint	1. Faible	2. Moins de 1000€	1. Trimestre	1. Non démarré
Utilisation d'antivols pour les ordinateurs portables	Service commercial	1. Faible	2. Moins de 1000€	1. Trimestre	1. Non démarré
Utilisation de films empêchant l'espionnage de l'écran des ordinateurs portables	Service commercial	1. Faible	2. Moins de 1000€	1. Trimestre	1. Non démarré
Destruction des documents sensibles lors de leur mise au rebut	Tous	1. Faible	2. Moins de 1000€	1. Trimestre	1. Non démarré
Pose de barreaux aux fenêtres	Directeur adjoint	1. Faible	3. Plus de 1000€	1. Trimestre	1. Non démarré
Mesures de l'année					
Établissement de la liste des exigences réglementaires	Directeur adjoint	1. Faible	1. Nul	2. Année	1. Non démarré
Test trimestriel des fichiers sauvegardés	Directeur adjoint	2. Moyenne	1. Nul	2. Année	1. Non démarré
Vérification des empreintes des fichiers liés aux devis de manière régulière	Directeur adjoint	2. Moyenne	1. Nul	2. Année	1. Non démarré
…	…	…	…	…	…
Marquage du besoin de confidentialité des documents électroniques liés aux devis	Service commercial	2. Moyenne	1. Nul	2. Année	1. Non démarré
Marquage du besoin de confidentialité des documents papiers liés aux devis	Service commercial	2. Moyenne	1. Nul	2. Année	1. Non démarré
Extension de l'assurance aux risques d'altération d'informations	Directeur	2. Moyenne	2. Moins de 1000€	2. Année	1. Non démarré
Extension de l'assurance aux risques de vol d'informations	Directeur	2. Moyenne	2. Moins de 1000€	2. Année	1. Non démarré
Utilisation de scellés sur les ordinateurs afin de pouvoir constater leur ouverture non désirée	Directeur adjoint	1. Faible	2. Moins de 1000€	2. Année	1. Non démarré
Formation des personnels aux outils métiers et aux mesures de sécurité	Directeur adjoint	2. Moyenne	3. Plus de 1000€	2. Année	1. Non démarré
Mesures dans les trois ans					
Gestion des vulnérabilités sur les serveurs	Directeur adjoint	3. Élevée	1. Nul	3. 3 ans	1. Non démarré
Gestion des vulnérabilités sur Windows XP	Directeur adjoint	3. Élevée	1. Nul	3. 3 ans	1. Non démarré
Gestion des vulnérabilités sur MacOS X	Directeur adjoint	3. Élevée	1. Nul	3. 3 ans	1. Non démarré
Établissement d'un accord d'échange d'informations avec les clients et les partenaires	Directeur adjoint et partenaires	2. Moyenne	1. Nul	3. 3 ans	1. Non démarré
Mise en place d'un système RAID logiciel	Directeur adjoint	3. Élevée	3. Plus de 1000€	3. 3 ans	1. Non démarré

Action 5.2.2. Analyser les risques résiduels

Description

Cette action consiste à identifier et à estimer les risques résiduels qui subsiste réellement une fois les mesures de sécurité mises en œuvre. Cela permet de vérifier que l'on sera prêt à les accepter en toute connaissance de cause.

Pour chaque objectif de sécurité, il convient de compléter la démonstration de couverture et donc de :

- revoir l'argumentaire justificatif, qui devrait démontrer que :
  - la combinaison des mesures de sécurité mises en œuvre traite le risque conformément à l'objectif de sécurité identifié,
  - l'ensemble des mesures de sécurité mises en œuvre constitue un tout cohérent et dont les éléments se soutiennent mutuellement,
  - le niveau de résistance des mesures de sécurité mises en œuvre est cohérent avec les sources de menaces retenues ;
- compléter la liste des risques résiduels au regard des mesures de sécurité mises en œuvre, et les estimer en termes de gravité et de vraisemblance ;
- estimer l'effet des mesures de sécurité mises en œuvre sur la gravité et la vraisemblance du risque concerné en les ré-estimant.

Conseils

- Il peut être utile de réaliser un tableau croisé entre les objectifs de sécurité et les mesures de sécurité mises en œuvre pour vérifier la couverture et qu'il n'existe pas de mesure de sécurité inutile.
- L'analyse des risques résiduels ne doit pas être négligée. En effet, c'est sur cette base que l'on pourra juger de leur acceptation.

Exemple

Un ensemble de risques subsiste après la mise en œuvre des mesures de sécurité formalisées :

Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre

Niveau de risque				
Gravité	*1. Négligeable*	*2. Limitée*	***3. Importante***	*4. Critique*
Vraisemblance	***1. Minime***	~~*2. Significative*~~	~~*3. Forte*~~	*4. Maximale*

Risque lié à la compromission d'un devis au-delà du personnel et des partenaires

Niveau de risque				
Gravité	*1. Négligeable*	***2. Limitée***	~~*3. Importante*~~	*4. Critique*
Vraisemblance	*1. Minime*	***2. Significative***	~~*3. Forte*~~	~~*4. Maximale*~~

Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres

Niveau de risque				
Gravité	*1. Négligeable*	*2. Limitée*	***3. Importante***	~~*4. Critique*~~
Vraisemblance	***1. Minime***	~~*2. Significative*~~	*3. Forte*	*4. Maximale*

Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires

Niveau de risque				
Gravité	*1. Négligeable*	***2. Limitée***	~~*3. Importante*~~	*4. Critique*
Vraisemblance	*1. Minime*	***2. Significative***	~~*3. Forte*~~	~~*4. Maximale*~~

[…]

Action 5.2.3. Prononcer l'homologation de sécurité

Description

Cette action consiste à faire valider les conclusions de l'étude de manière formelle.

La décision d'homologation est l'engagement par lequel l'autorité atteste que le projet a bien pris en compte les contraintes opérationnelles établies au départ, que le système et les informations sont protégés conformément aux objectifs de sécurité, et que le système d'information est apte à entrer en service avec des risques résiduels acceptés et maîtrisés.

Cette décision est théoriquement prise préalablement à l'emploi du système d'information considéré.

L'autorité peut s'appuyer sur une commission d'homologation qui lui fournira les éléments d'information et la synthèse nécessaires à sa décision. Si la responsabilité du système d'information n'est pas incarnée par une seule autorité, l'homologation peut être collégiale ou confiée à une autorité parmi les autorités concernées.

L'autorité peut prononcer :

- une homologation provisoire, assortie de réserves et d'un délai de mise en conformité ;
- un refus d'homologation au vu des résultats d'audit et des risques résiduels encourus jugés inacceptables ;
- une homologation complète, assortie le cas échéant de conditions, pour une durée déterminée (fréquemment entre 3 et 5 ans).

L'homologation peut être assortie de conditions, qui sont alors mentionnées dans la décision d'homologation. L'autorité peut modifier les conditions dont l'homologation est assortie ou retirer l'homologation lorsqu'elle estime que les risques encourus ne sont pas acceptables au regard du besoin de protection du système et des informations. Toute évolution du système ayant une répercussion sur la sécurité devrait donner lieu à une nouvelle homologation de sécurité.

Conseils

- Afin d'assurer une intégration de la SSI tout au long du projet, la commission d'homologation doit être créée dès l'étude d'opportunité.
- La commission d'homologation doit valider les différentes étapes de l'étude des risques, aux jalons clés du programme, sur la base de livrables adaptés.
- La commission d'homologation peut se prononcer sur la base d'un plan d'action visant à réduire les risques résiduels, à satisfaire des objectifs de sécurité et à mettre en œuvre les mesures de sécurité.
- Les différentes étapes de l'étude des risques doivent être raffinées tout au long du projet.

Exemple

Le Directeur d'@RCHIMED a prononcé l'homologation de sécurité du cabinet au vu de l'étude réalisée (délimitation du périmètre, appréciation des risques, élaboration du plan d'action, mise en évidence des risques résiduels…) et des livrables élaborés (note de cadrage, note de stratégie, politique de sécurité de l'information).

Cette homologation de sécurité est valable un an et pourra être renouvelée tous les ans.

La mise en œuvre du plan d'action devra être démontrée, ainsi que l'amélioration continue de l'étude de sécurité.

Annexe A – Démonstration de la couverture des normes

EBIOS satisfait les exigences de l'[ISO 27001]

La méthode EBIOS permet de réaliser l'ensemble de la phase de planification (première phase du système de management de la sécurité de l'information – *information security management system* – ISMS) de l'[ISO 27001] et peut servir de support à la mise en œuvre des autres phases.

Elle permet notamment de satisfaire l'ensemble des exigences relatives à la gestion des risques de l'[ISO 27001]. Le tableau suivant en illustre la correspondance :

Exigences de l'[ISO 27001] relatives à la gestion des risques	**Activités d'EBIOS permettant de les satisfaire**
4.2.1 Établissement de l'ISMS L'organisme doit effectuer les tâches suivantes : a) définir le domaine d'application et les limites de l'ISMS en termes des caractéristiques de l'activité, de l'organisme, de son emplacement, de ses biens, de sa technologie, ainsi que des détails et de la justification de toutes exclusions du domaine d'application	Activité 1.1 – Définir le cadre de la gestion des risques Activité 1.3 – Identifier les biens
b) définir une politique pour l'ISMS en termes des caractéristiques de l'activité, de l'organisme, de son emplacement, de ses biens, et de sa technologie, qui : 1) inclut un cadre pour fixer les objectifs et indiquer une orientation générale et des principes d'action concernant la sécurité de l'information ; 2) tient compte des exigences liées à l'activité et des exigences légales ou réglementaires, ainsi que des obligations de sécurité contractuelles ; 3) s'aligne sur le contexte de management du risque stratégique auquel est exposé l'organisme, dans lequel se dérouleront l'établissement et la mise à jour de l'ISMS ; 4) établit les critères d'évaluation future du risque (voir 4.2.1c))	Activité 1.1 – Définir le cadre de la gestion des risques Activité 1.2 – Préparer les métriques
c) définir l'approche d'appréciation du risque de l'organisme : 1) Identifier une méthodologie d'appréciation du risque adaptée à l'ISMS, ainsi qu'à la sécurité de l'information identifiée de l'organisme et aux exigences légales et réglementaires. 2) Développer des critères d'acceptation des risques et identifier les niveaux de risque acceptables. (voir 5.1f)). La méthodologie d'appréciation du risque choisie doit assurer que les appréciations du risque produisent des résultats comparables et reproductibles.	Activité 1.1 – Définir le cadre de la gestion des risques Activité 1.2 – Préparer les métriques
d) identifier les risques. 1) Identifier les biens relevant du domaine d'application de l'ISMS, ainsi que leurs propriétaires. 2) Identifier les menaces auxquelles sont confrontés ces biens. 3) Identifier les vulnérabilités qui pourraient être exploitées par les menaces. 4) Identifier les impacts que les pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les biens.	Activité 1.3 – Identifier les biens Activité 2.1 – Apprécier les événements redoutés Activité 3.1 – Apprécier les scénarios de menaces

Exigences de l'[ISO 27001] relatives à la gestion des risques	Activités d'EBIOS permettant de les satisfaire
e) analyser et évaluer les risques. 1) Évaluer l'impact sur l'activité de l'organisme qui pourrait découler d'une défaillance de la sécurité, en tenant compte des conséquences d'une perte de confidentialité, intégrité ou disponibilité des biens. 2) Évaluer la probabilité réaliste d'une défaillance de sécurité de cette nature au vu des menaces et des vulnérabilités prédominantes, des impacts associés à ces biens et des mesures actuellement mises en œuvre. 3) Estimer les niveaux de risques. 4) Déterminer si le risque est acceptable ou doit faire l'objet d'un traitement en utilisant les critères d'acceptation du risque établis en 4.2.1c)2).	Activité 2.1 – Apprécier les événements redoutés Activité 4.1 – Apprécier les risques
f) identifier et évaluer les options de traitement des risques. Les actions envisageables incluent : 1) l'application de mesures appropriées ; 2) l'acceptation des risques en connaissance de cause et avec objectivité, dans la mesure où ils sont acceptables au regard des politiques de l'organisme et des critères d'acceptation du risque (voir 4.2.1c)2)) ; 3) l'annulation des risques ; et 4) le transfert des risques liés à l'activité associés, à des tiers, par exemple assureurs, fournisseurs.	Activité 4.2 – Identifier les objectifs de sécurité
g) sélectionner les objectifs des mesures et les mesures proprement dites pour le traitement des risques. Les objectifs des mesures et les mesures proprement dites doivent être sélectionnés et mis en œuvre pour répondre aux exigences identifiées par le processus d'appréciation du risque et de traitement du risque. Cette sélection doit tenir compte des critères d'acceptation des risques (voir 4.2.1c)) ainsi que des exigences légales, réglementaires et contractuelles. Les objectifs des mesures et les mesures proprement dites définis à l'annexe A doivent être sélectionnés comme partie intégrante de ce processus, dans la mesure où ils peuvent satisfaire à ces exigences. Les objectifs des mesures et les mesures proprement dites énumérés à l'annexe A ne sont pas exhaustifs et des objectifs des mesures et des mesures proprement dites additionnels peuvent également être sélectionnés.	Activité 5.1 – Formaliser les mesures de sécurité à mettre en œuvre
h) obtenir l'approbation par la direction des risques résiduels proposés	Activité 5.2 – Mettre en œuvre les mesures de sécurit
i) obtenir l'autorisation de la direction pour mettre en œuvre et exploiter l'ISMS	Activité 5.1 – Formaliser les mesures de sécurité à mettre en œuvre
j) préparer une déclaration d'applicabilité (*Statement of Applicability – SoA*). Une SoA doit être élaborée et comprendre les informations suivantes : 1) les objectifs des mesures et les mesures proprement dites, sélectionnés en 4.2.1g) et les raisons pour lesquelles ils ont été sélectionnés ; 2) les objectifs des mesures et les mesures proprement dites actuellement mis en œuvre (voir 4.2.12)) ; et 3) l'exclusion des objectifs des mesures et des mesures proprement dites spécifiés à l'annexe A et la justification de leur exclusion.	Activité 5.1 – Formaliser les mesures de sécurité à mettre en œuvre

Exigences de l'[ISO 27001] relatives à la gestion des risques	Activités d'EBIOS permettant de les satisfaire
4.2.2 Mise en œuvre et fonctionnement de l'ISMS L'organisme doit effectuer les tâches suivantes : a) élaborer un plan de traitement du risque qui identifie les actions à engager, les ressources, les responsabilités et les priorités appropriées pour le management des risques liés à la sécurité de l'information (voir l'article 5) ; b) mettre en œuvre le plan de traitement du risque afin d'atteindre les objectifs des mesures identifiés, ce plan prévoyant le mode de financement et l'affectation de rôles et de responsabilités ; c) mettre en œuvre les mesures sélectionnées en 4.2.1g) afin de répondre aux objectifs des mesures ; […]	Activité 5.2 – Mettre en œuvre les mesures de sécurit
4.2.3 Surveillance et réexamen de l'ISMS […] d) réexaminer les appréciations du risque à intervalles planifiés et réexaminer le niveau de risque résiduel et le niveau de risque acceptable identifié, compte tenu des changements apportés : 1) à l'organisme ; 2) à la technologie ; 3) aux objectifs métiers et aux processus de l'organisme ; 4) aux menaces identifiées ; 5) à l'efficacité des mesures mises en œuvre ; et 6) aux événements extérieurs, tels que les modifications apportées au milieu de la législation ou de la réglementation, les obligations contractuelles modifiées et les changements du climat social ; […]	Toutes les activités
4.3 Exigences relatives à la documentation	Les données produites par les activités d'EBIOS permettent d'élaborer la plupart des documents exigés

EBIOS décline parfaitement l'[ISO 27005]

La méthode EBIOS permet de mettre en œuvre l'[ISO 27005] (cadre pour les méthodes de gestion des risques de sécurité de l'information). Le tableau suivant en illustre la correspondance :

Chapitres de l'[ISO 27005]	Activités d'EBIOS correspondantes
Foreword	Avant-propos
Introduction	Introduction
1. Scope	Domaine d'application
2. Normative references	Références réglementaires et normatives
3. Terms and definitions	Annexe B – Références – Définitions
4. Structure of this standard	Structure du document
5. Background	1. Gérer durablement les risques sur le patrimoine informationnel
6. Overview of the information security risk management process	2. EBIOS : la méthode de gestion des risques
7. Context establishment	Module 1 – Étude du contexte
7.1. General considerations	Module 1 – Étude du contexte
7.2. Basic Criteria	Activité 1.2 – Préparer les métriques
7.3. The scope and boundaries	Activité 1.3 – Identifier les biens
7.4. Organization for information security risk management	Activité 1.1 – Définir le cadre de la gestion des risques
8. Information security risk assessment	Module 2 – Étude des événements redoutés Module 3 – Étude des scénarios de menaces Module 4 – Étude des risques
8.1. General description of information security risk assessment	Module 2 – Étude des événements redoutés Module 3 – Étude des scénarios de menaces Module 4 – Étude des risques
8.2. Risk analysis	Module 2 – Étude des événements redoutés Module 3 – Étude des scénarios de menaces Module 4 – Étude des risques
8.3. Risk evaluation	Module 4 – Étude des risques
9. Information security risk treatment	Module 4 – Étude des risques Module 5 – Étude des mesures de sécurité
9.1. General description of information security risk treatment	Module 4 – Étude des risques Module 5 – Étude des mesures de sécurité
9.2. Risk reduction	Activité 4.2 – Identifier les objectifs de sécurité Module 5 – Étude des mesures de sécurité
9.3. Risk retention	Activité 4.2 – Identifier les objectifs de sécurité Module 5 – Étude des mesures de sécurité
9.4. Risk avoidance	Activité 4.2 – Identifier les objectifs de sécurité Module 5 – Étude des mesures de sécurité
9.5. Risk transfer	Activité 4.2 – Identifier les objectifs de sécurité Module 5 – Étude des mesures de sécurité
10. Information security risk acceptance	Activité 5.2 – Mettre en œuvre les mesures de sécurit
11. Information security risk communication	Toutes les activités (partie Communication et concertation)
12. Information security risk monitoring and review	Toutes les activités (partie Surveillance et revue)
12.1. Monitoring and review of risk factors	Toutes les activités (partie Surveillance et revue)
12.2. Risk management monitoring, reviewing and improving	Toutes les activités (partie Surveillance et revue)

EBIOS est décline parfaitement l'[ISO 31000]

La méthode EBIOS permet de mettre en œuvre la démarche type de gestion des risques (applicable à tous les types de risques) décrite dans l'[ISO 31000]. Le tableau suivant en illustre la correspondance :

Chapitres de l'[ISO 31000]	Activités d'EBIOS correspondantes
Avant-propos	Avant-propos
Introduction	Introduction Structure du document
1. Domaine d'application	Domaine d'application
2. Références normatives	Références réglementaires et normatives
3. Termes et définitions	Annexe B – Références – Définitions
4. Principes de management du risque	1. Gérer durablement les risques sur le patrimoine informationnel 2. EBIOS : la méthode de gestion des risques
5. Cadre organisationnel de management du risque	Activité 1.1 – Définir le cadre de la gestion des risques
5.1. Généralités	Activité 1.1 – Définir le cadre de la gestion des risques
5.2. Mandat et engagement	Activité 1.1 – Définir le cadre de la gestion des risques
5.3. Conception du cadre organisationnel de management du risque	Activité 1.1 – Définir le cadre de la gestion des risques
5.4. Mise en œuvre du management du risque	Activité 1.1 – Définir le cadre de la gestion des risques
5.5. Surveillance et revue du cadre organisationnel	Activité 1.1 – Définir le cadre de la gestion des risques
5.6. Amélioration continue du cadre organisationnel	Activité 1.1 – Définir le cadre de la gestion des risques
6. Processus de management du risque	3. Description de la démarche
6.1. Généralités	2.2. Une démarche itérative en cinq modules
6.2. Communication et consultation	Toutes les activités (partie Communication et concertation)
6.3. Établissement du contexte	Module 1 – Étude du contexte
6.4. Appréciation du risque	Module 2 – Étude des événements redoutés Module 3 – Étude des scénarios de menaces Module 4 – Étude des risques
6.5. Traitement du risque	Module 4 – Étude des risques Module 5 – Étude des mesures de sécurité
6.6. Surveillance et revue	Toutes les activités (partie Surveillance et revue)
6.7. Documentation du processus de management du risque	Toutes les activités (partie Données produites)

Annexe B – Références

Acronymes

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
FEROS	Fiche d'Expression Rationnelle des Objectifs de Sécurité
ISO	*International Organization for Standardization* (organisation internationale de normalisation)
PP	Profil de Protection

Définitions

Appréciation des risques
(*risk assessment*)

Sous-processus de la gestion des risques visant à identifier, analyser et à évaluer les risques.

(d'après [ISO Guide 73] – Appréciation du risque : *ensemble du processus d'identification des risques, d'analyse du risque et d'évaluation du risque*)

Besoin de sécurité
(*sensitivity*)

Définition précise et non ambiguë du niveau d'exigences opérationnelles relatives à un bien essentiel pour un critère de sécurité donné (disponibilité, confidentialité, intégrité…).

Exemples :

- *doit être disponible dans la journée ;*
- *ne doit être connu que du groupe projet ;*
- *peut ne pas être intègre dans la mesure où l'on peut le détecter et retrouver son intégrité ;*
- …

Bien
(*asset*)

Toute ressource qui a de la valeur pour l'organisme et qui est nécessaire à la réalisation de ses objectifs. On distingue notamment les biens essentiels et les biens supports.

(d'après [ISO 27001] : *tout élément représentant de la valeur pour l'organisme*)

Exemples :

- *liste de noms ;*
- *requête de certification ;*
- *gestion de la facturation ;*
- *algorithme de chiffrement ;*
- *micro-ordinateur portable ;*
- *Ethernet ;*
- *système d'exploitation ;*
- …

Bien essentiel
(*primary asset*)

Information ou processus jugé comme important pour l'organisme. On appréciera ses besoins de sécurité mais pas ses vulnérabilités.

Exemples :

- *une liste de noms ;*
- *passer une commande client ;*
- *gérer la facturation ;*
- *un algorithme de chiffrement ;*
- *…*

Bien support

(*supporting asset*)

Bien sur lequel reposent des biens essentiels. On distingue notamment les systèmes informatiques, les organisations et les locaux. On appréciera ses vulnérabilités mais pas ses besoins de sécurité.

Exemples :

- *société d'infogérance ;*
- *locaux de l'organisme ;*
- *administrateur système ;*
- *micro-ordinateur portable ;*
- *Ethernet ;*
- *système d'exploitation ;*
- *portail de téléprocédure ;*
- *…*

Communication et concertation

(*communication and consultation*)

Processus itératifs et continus mis en oeuvre par un organisme afin de fournir, partager ou obtenir des informations et d'engager un dialogue avec les parties prenantes et autres parties, concernant la gestion des risques.

(d'après [ISO Guide 73] : *processus itératifs et continus mis en oeuvre par un organisme afin de fournir, partager ou obtenir des informations et d'engager un dialogue avec les parties prenantes et autres parties, concernant le management du risque*)

Confidentialité

(*confidentiality*)

Propriété des biens essentiels de n'être accessibles qu'aux personnes autorisés.

(d'après [IGI 1300] : *caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou processus autorisés*)

Critère de sécurité

(*security criteria*)

Caractéristique d'un bien essentiel permettant d'apprécier ses différents besoins de sécurité.

Exemples :

- *disponibilité,*
- *intégrité,*
- *confidentialité,*
- *…*

Disponibilité

(*availability*)

Propriété d'accessibilité au moment voulu des biens essentiels par les personnes autorisées.

(d'après [IGI 1300] : *propriété d'une information ou d'un traitement d'être, à la demande, utilisable par une personne ou un système*)

Établissement du contexte

(*context establishment*)

Définition des paramètres externes et internes à prendre en compte lors de la gestion des risques et définition du périmètre de l'étude ainsi que des critères de gestion des risques.

(d'après [ISO Guide 73] : *définition des paramètres externes et internes à prendre en compte lors du management du risque et définition du domaine d'application ainsi que des critères de risque pour la politique de management du risque*)

Événement redouté

(*feared event*)

Scénario générique représentant une situation crainte par l'organisme. Il s'exprime par la combinaison des sources de menaces susceptibles d'en être à l'origine, d'un bien essentiel, d'un critère de sécurité, du besoin de sécurité concerné et des impacts potentiels.

Exemples :

- *une personne mal intentionnée (un journaliste, un concurrent…) parvient à obtenir le budget prévisionnel de l'organisme, jugé confidentiel, et publie l'information dans les médias*
- *…*

Gestion des risques

(*risk management*)

Processus itératif de pilotage, visant à maintenir les risques à un niveau acceptable pour l'organisme. La gestion des risques inclut typiquement l'appréciation, le traitement, la validation du traitement et la communication relative aux risques.

(d'après [ISO Guide 73] – Processus de management du risque : *application systématique de politiques, procédures et pratiques de management aux activités de communication, de concertation, d'établissement du contexte, ainsi qu'aux activités d'identification, d'analyse, d'évaluation, de traitement, de surveillance et de revue des risques*)

Gravité

(*consequences*)

Estimation de la hauteur des effets d'un événement redouté ou d'un risque. Elle représente ses conséquences.

(d'après [ISO Guide 73] – Conséquence : *effet d'un événement affectant les objectifs*)

Exemples :

- *négligeable : l'organisme surmontera les impacts sans aucune difficulté,*
- *limitée : l'organisme surmontera les impacts malgré quelques difficultés,*
- *importante : l'organisme surmontera les impacts avec de sérieuses difficultés,*
- *critique : l'organisme ne surmontera pas les impacts (sa survie est menacée),*
- *…*

Homologation de sécurité

(*security accreditation*)

Déclaration, par une autorité dite d'homologation, que le périmètre de l'étude est apte à traiter des biens au niveau des besoins de sécurité exprimé, conformément aux objectifs de sécurité visés, et qu'elle accepte les risques résiduels induits.

(d'après [IGI 1300] : *déclaration par l'autorité d'homologation, au vu du dossier d'homologation, que le système d'information considéré est apte à traiter des informations d'un niveau de classification donné conformément aux objectifs de sécurité visés, et que les risques de sécurité résiduels induits sont acceptés et maîtrisés. L'homologation de sécurité reste valide tant que le SI opère dans les conditions approuvées par l'autorité d'homologation*)

Impact
(*impact*)

Conséquence directe ou indirecte de l'insatisfaction des besoins de sécurité sur l'organisme et/ou sur son environnement.

Exemples de types d'impacts :

- *sur les missions,*
- *sur la sécurité des personnes,*
- *financiers,*
- *juridiques,*
- *sur l'image,*
- *sur l'environnement,*
- *…*

Information
(*information*)

Tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement. [IGI 1300]

Exemples :

- *un message ;*
- *une liste de noms ;*
- *une requête de certification ;*
- *liste de révocation ;*
- *…*

Intégrité
(*integrity*)

Propriété d'exactitude et de complétude des biens essentiels.

(d'après [IGI 1300] : *propriété assurant qu'une information ou un traitement n'a pas été modifié ou détruit de façon non autorisée*)

Menace
(*threat*)

Moyen type utilisé par une source de menace.

Exemples :

- *vol de supports ou de documents ;*
- *piégeage du logiciel ;*
- *atteinte à la disponibilité du personnel ;*
- *écoute passive ;*
- *crue ;*
- …

Mesure de sécurité
(*control*)

Moyen de traiter un risque de sécurité de l'information. La nature et le niveau de détail de la description d'une mesure de sécurité peuvent être très variables.

Objectif de sécurité
(*security objective*)

Expression de la décision de traiter un risque selon des modalités prescrites. On distingue notamment la réduction, le transfert (partage des pertes), le refus (changements structurels pour éviter une situation à risque) et la prise de risque.

Organisme
(*organisation*)

Ensemble d'installations et de personnes avec des responsabilités, pouvoirs et relations. [ISO 9000]

Exemples :

- *entreprise,*
- *département ministériel,*
- *…*

Partie prenante
(*stakeholder*)

Personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité. [ISO Guide 73]

Prise de risques (*risk retention*)	Choix de traitement consistant à accepter les conséquences de la réalisation de tout ou partie de risques, sans appliquer de mesure de sécurité. (d'après [ISO Guide 73] – Prise de risque : *acceptation de l'avantage potentiel d'un gain ou de la charge potentielle d'une perte découlant d'un risque particulier*)
Processus de l'organisme (*business process*)	Ensemble organisé d'activités qui utilisent des ressources pour transformer des entrées en sorties. [ISO 9000]
Processus informationnel (*information process*)	Ensemble organisé de traitements qui utilisent des biens supports pour transformer des informations d'entrées en informations de sorties (d'après [ISO 9000]).
Réduction de risques (*risk reduction*)	Choix de traitement consistant à appliquer des mesures de sécurité destinées à réduire les risques. *Exemples :* - *élaborer une politique de sécurité de l'information,* - *mettre en œuvre un antivirus qui devra régulièrement être mis à jour,* - *sensibiliser les personnels aux risques,* - *…*
Refus de risques (*risk avoidance*)	Choix de traitement consistant à éviter les situations à risque. (d'après [ISO Guide 73] – Refus du risque : *décision argumentée de ne pas s'engager dans une activité, ou de s'en retirer, afin de ne pas être exposé à un risque particulier*) *Exemples :* - *changement de lieu d'implantation des locaux,* - *réduction des ambitions d'un projet,* - *arrêt d'un service,* - *…*
Risque résiduel (*residual risk*)	Risque subsistant après le traitement du risque. [ISO Guide 73]
Risque de sécurité de l'information (*information security risk*)	Scénario, avec un niveau donné, combinant un événement redouté et un ou plusieurs scénarios de menaces. Son niveau correspond à l'estimation de sa gravité et de sa vraisemblance. (d'après [ISO Guide 73] : *effet de l'incertitude sur l'atteinte des objectifs. […] NOTE 3 – Un risque est souvent caractérisé en référence à des événements et des conséquences potentiels ou à une combinaison des deux. NOTE 4 – Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement et de sa vraisemblance*)

Scénario de menace

(*vector*)

Scénario, avec un niveau donné, décrivant des modes opératoires. Il combine les sources de menaces susceptibles d'en être à l'origine, un bien support, un critère de sécurité, des menaces et les vulnérabilités exploitables pour qu'elles se réalisent.

Son niveau correspond à l'estimation de sa vraisemblance.

Exemples :

- *vol de supports ou de documents du fait de la facilité de pénétrer dans les locaux,*
- *piégeage du logiciel du fait de la naïveté des utilisateurs,*
- *inondation due au fait que les bâtiments sont inondables*
- *…*

Sécurité de l'information

(*information security*)

Satisfaction des besoins de sécurité des biens essentiels.

Source de menace

(*threat source*)

Chose ou personne à l'origine de menaces. Elle peut être caractérisée par son type (humain ou environnemental), par sa cause (accidentelle ou délibérée) et selon le cas par ses ressources disponibles, son expertise, sa motivation…

(d'après [ISO Guide 73] – Source de risque : *tout élément qui, seul ou combiné à d'autres, présente un potentiel intrinsèque d'engendrer un risque*)

Exemples :

- *ancien membre du personnel ayant peu de compétences techniques et de temps mais susceptible d'avoir une forte motivation,*
- *pirate avec de fortes compétences techniques, bien équipé et une forte motivation liée à l'argent qu'il peut gagner,*
- *climat très fortement pluvieux pendant trois mois par an,*
- *virus,*
- *utilisateurs,*
- *…*

Surveillance et revue

(*risk monitoring and review*)

Sous-processus de la gestion des risques visant à surveiller (de manière continue) et à revoir (de manière régulière) les risques de sécurité de l'information et leur gestion.

(d'après [ISO Guide 73] – Surveillance : *vérification, supervision, observation critique ou détermination de l'état afin d'identifier continûment des changements par rapport au niveau de performance exigé ou attendu* ; Revue : *activité entreprise afin de déterminer l'adaptation, l'adéquation et l'efficacité de l'objet étudié pour atteindre les objectifs établis*)

Système d'information

(*information system*)

Ensemble des moyens humains et matériels ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire l'information. [IGI 1300]

Traitement des risques

(*risk treatment*)

Sous-processus de la gestion des risques permettant de choisir et de mettre en œuvre des mesures de sécurité visant à modifier les risques de sécurité de l'information.

(d'après [ISO Guide 73] – Traitement du risque : *processus destiné à modifier un risque*)

Transfert de risques

(*risk transfer*)

Choix de traitement consistant à partager les pertes consécutives à la réalisation de risques.

(d'après [ISO Guide 73] – Partage du risque : *forme de traitement du risque impliquant la répartition consentie du risque avec d'autres parties*)

Exemples :

- *recours à une assurance,*
- *emploi de produits certifiés,*
- *…*

Validation du traitement des risques

(*risk acceptance*)

Sous-processus de la gestion des risques visant à décider d'accepter la manière dont les risques ont été traités ainsi que les risques résiduels à l'issue du traitement des risques.

(d'après [ISO Guide 73] – Acceptation du risque : *décision argumentée en faveur de la prise d'un risque particulier*)

Vraisemblance

(*likelihood*)

Estimation de la possibilité qu'un scénario de menace ou un risque, se produise. Elle représente sa force d'occurrence.

(d'après [ISO Guide 73] : *possibilité que quelque chose se produise*)

Exemples :

- *minime : cela ne devrait pas se (re)produire,*
- *forte : cela pourrait se (re)produire,*
- *significative : cela devrait se (re)produire un jour ou l'autre,*
- *maximale : cela va certainement se (re)produire prochainement,*
- *…*

Vulnérabilité

(*vulnerability*)

Caractéristique d'un bien support qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information.

(d'après [ISO Guide 73] : *propriétés intrinsèques de quelque chose entraînant une sensibilité à une source de risque pouvant induire une conséquence*)

Exemples :

- *crédulité du personnel,*
- *facilité de pénétrer sur un site,*
- *possibilité de créer ou modifier des commandes systèmes,*
- *…*

Références bibliographiques

[Guide 150] *Fiche d'Expression Rationnelle des Objectifs de Sécurité des systèmes d'information (FEROS)*, Secrétariat général de la défense nationale – SGDN (1991).

[IGI 1300] *Instruction générale interministérielle sur la protection du secret de la défense nationale*, Secrétariat général de la défense nationale – SGDN (2003).

[ISO 15408] *Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information*, International Organization for Standardization – ISO (2005).

[ISO 27001] *Information technology – Security Techniques – Information security management systems – Requirements*, International Organization for Standardization – ISO (2005).

[ISO 27002] *Information technology – Code of practice for information security management*, International Organization for Standardization – ISO (2005).

[ISO 27005] *Information technology – Security Techniques – Information security risk management*, International Organization for Standardization – ISO (2008).

[ISO 31000] *Management du risque – Principes et lignes directrices de mise en oeuvre*, International Organization for Standardization – ISO (2008).

[ISO 9000] *Systèmes de management de la qualité – Principes essentiels et vocabulaire* – International Organization for Standardization – ISO (2000).

[ISO Guide 73] *Management du risque – Vocabulaire* – International Organization for Standardization – ISO (2009).

[RGS] *Référentiel général de sécurité* – SGDN (2009).