Guide méthodologique d'analyse de risques à des fins d'homologation

ou de

définition des objectifs de sécurité

GESTION DES RISQUES

Version du 02 mars 2017

24 rue du Gabian
98000 MONACO
Tél. : (+377) 98 98 24 93
amsn@gouv.mc

Préambule

Ce document est un guide très simplifié de la méthode Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) réalisée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) française.

Le corps du texte définit la méthode, l'annexe 1 fournit les définitions des termes utilisés, l'annexe 2 propose un exemple de la démarche, enfin l'annexe 3 fournit une base de connaissance pour aider à l'analyse des risques cyber.

EBIOS[1] fait aujourd'hui figure de référence en France, dans les pays francophones et à l'international.

Pour appliquer une méthode plus complète il est conseillé de se rapporter au document original de l'ANSSI que l'on peut trouver :

https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

[1] EBIOS est une marque déposée par le Secrétariat Général de la Défense et de la Sécurité Nationale.

Table des matières

Introduction

Objectif du document

L’objectif principal du présent document est de fournir une méthodologie pour l’évaluation et la gestion des risques informatiques.

Domaine d'application

Cette méthodologie peut s'appliquer au secteur public et au secteur privé, à tous types d’organismes, à des systèmes d’information en cours d'élaboration et à des systèmes d’information existants.

Références réglementaires

Ce guide doit permettre de mettre en œuvre les règles préconisées dans :

- La Politique de Sécurité des Systèmes d’Information de l’État (PSSI-E), Arrêté Ministériel n° 2017-056 du 01 février 2017, notamment pour l’homologation de sécurité des systèmes d’information ;
- L’Arrêté Ministériel n°2016-723 du 12 décembre 2016, portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, qui prévoit la démarche d’homologation ;
- L’Arrêté Ministériel d’application de l’article 27 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique, concernant les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs d'importance vitale.

1 Gérer durablement les risques sur le patrimoine informationnel

La sécurité de l'information a pour but de protéger le patrimoine informationnel de l'organisme, indispensable à son bon fonctionnement et à l'atteinte des objectifs.

1.1 La difficulté : appréhender la complexité

Les systèmes d'information :

- peuvent être confrontés à des problèmes variés ;
- sont en évolution constante ;
- sont parfois liés les uns aux autres.

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

2 Description de la méthode

La méthode repose sur l'identification du patrimoine de l'organisme étudié, des vulnérabilités propres aux différents composants du patrimoine, des menaces existantes et de leurs impacts potentiels. À chaque menace correspond deux indicateurs que sont la gravité pour l'organisme et la vraisemblance (probabilité d'occurrence). Le croisement de ces deux indicateurs permet la classification du risque. Ces étapes franchies, la méthode permet de déterminer les mesures de sécurité à prendre.

2.1 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, ...).

2.2 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.

Chacun de ces facteurs doit donc être étudié, de la manière la plus large possible. Les facteurs importants pourront alors être mis en évidence, et cela permettra de comprendre comment ils peuvent se combiner, d'estimer, d'évaluer et de 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.

On 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.

2.3 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.

2.4 La validation du traitement des risques

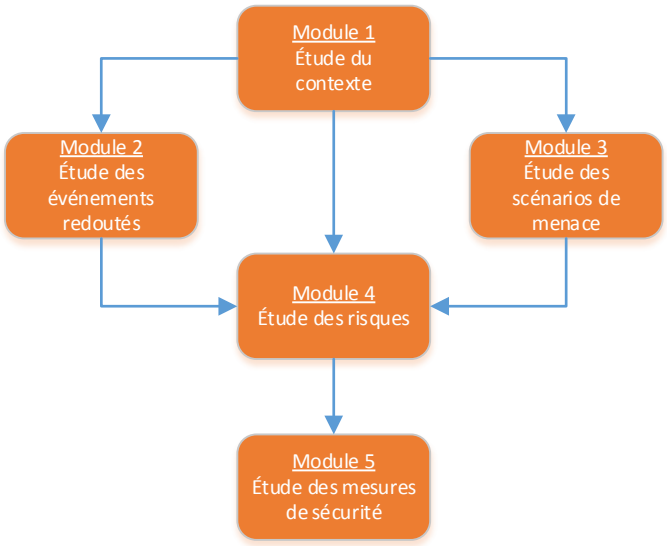
La manière dont les risques ont été gérés et les risques résiduels subsistants à l'issue du traitement doivent être validés, formellement, par une autorité responsable du périmètre de l'étude. Cette validation, généralement appelée homologation de sécurité, se fait sur la base d'un dossier dont les éléments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

2.5 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.

2.6 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.

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[2] 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.

[2] Un bien essentiel est une fonction (exemple : gérer une ressource) ou une donnée (exemple : résultats d'analyse) permettant de décrire un processus métier. Le bien essentiel repose sur un ou plusieurs biens supports qui représentent, quant à eux, les composants (organisationnels, techniques, humains, etc.) permettant de réaliser le processus.

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.

2.7 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), la méthode est un véritable outil de négociation et d'arbitrage.

Un outil de sensibilisation

Cette méthode 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.

Une méthode rapide

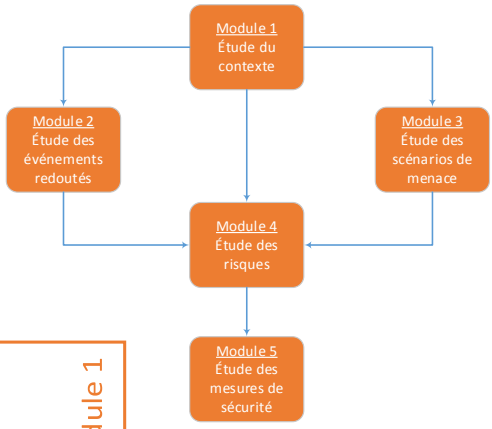
La durée de réalisation de l’étude est optimisée car elle permet d'obtenir les éléments nécessaires et suffisants selon le résultat attendu.

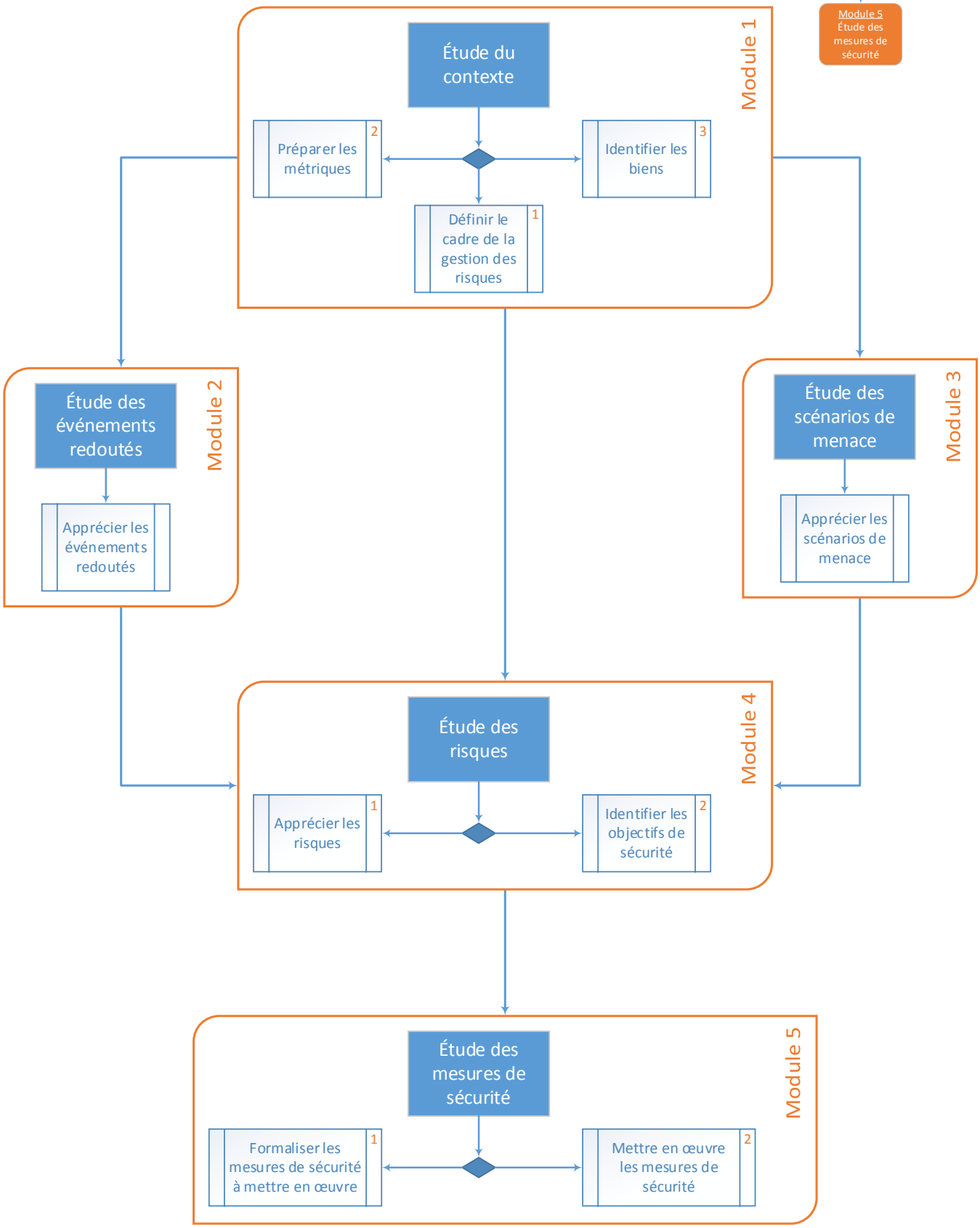
Une approche exhaustive

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

3 Description de la démarche

Ce chapitre présente les cinq modules de la méthode :

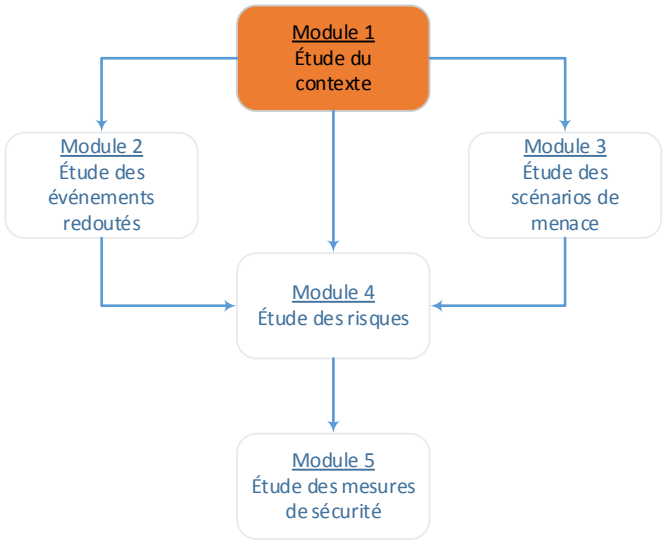




Chaque activité des cinq modules est décrite sous la forme d'une fiche.

3.1 Module 1 - Étude du contexte

Ce module a pour objectif de collecter les éléments nécessaires à la « gestion des risques », afin que celle-ci 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.

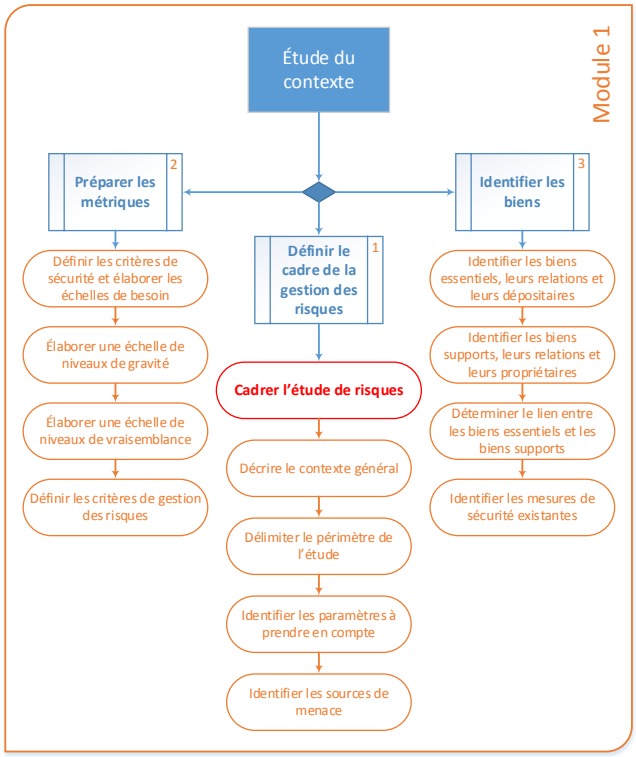
Activité 1.1 - Définir le cadre de la gestion des risques

Action 1.1.1. Cadrer l'étude de risques

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 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 si elle n'existe pas encore ;
- 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 expression des objectifs de sécurité à destination d'une commission d'homologation ou pour une passation de marché ;
- 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).

Conseils :

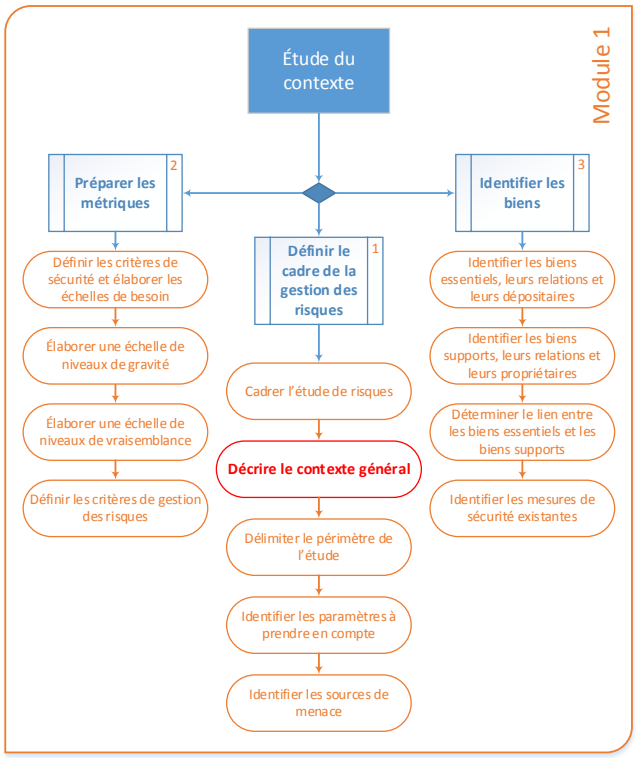
- Formuler un objectif explicite et en lien avec les objectifs de l'organisme.
- Identifier clairement le(s) livrable(s) attendu(s) et les personnes à qui il(s) est (sont) destiné(s).
- S'interroger sur l'utilité de chaque activité de la méthode et sur la manière de la réaliser (quelles actions ? quelles parties prenantes ?, ...) pour satisfaire l'objectif de l'étude et/ou pour élaborer le(s) livrable(s).

Action 1.1.2. Décrire le contexte général

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.

On peut ainsi utilement collecter les informations suivantes (qui ne sont ni obligatoires, ni exhaustives) :

- sur le contexte externe :
  - l'environnement social et culturel, politique, financier, réglementaire, légal, 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 ou humain.



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 :

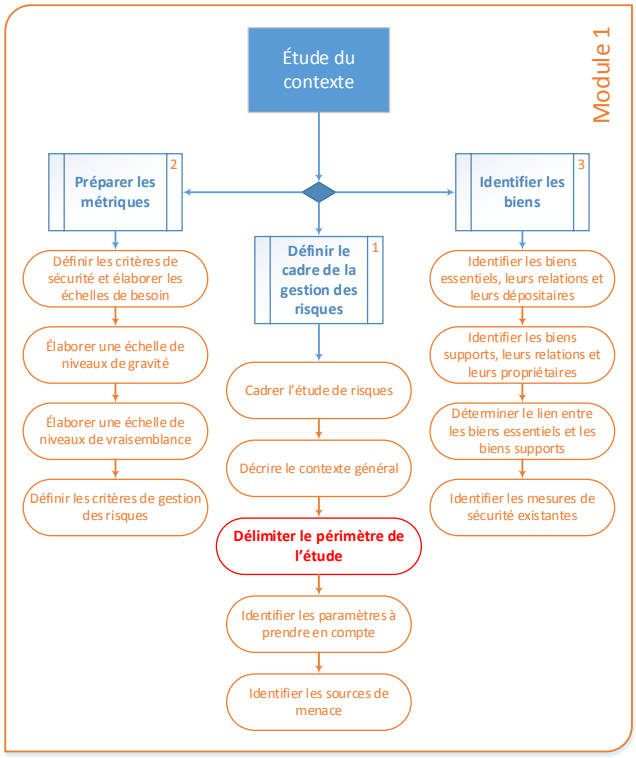
- Cette action peut être préparée à l'aide de documents publics (présentation des activités, bilan annuel, ...), stratégiques (schéma directeur, orientations, ...), d'organisation.
- Il est essentiel que l'organisme détermine ce qui est un risque pour lui. Par exemple, une réduction de l'utilité attendue (perte de revenus, perte de clientèle, diminution de la productivité, atteinte à l'image, ...) 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.

Action 1.1.3. Délimiter le périmètre de l'étude

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 ;
- la fonction ou l'objectif du SI ;
- la contribution aux processus métiers du SI ;
- les enjeux concernés dans le contexte global ;
- les processus concernés ;
- les interfaces avec les autres processus ou SI ;
- les parties prenantes ;
- les éventuels éléments à écarter de la réflexion (types de biens supports, menaces, ...).



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

Le découpage du périmètre en sous-périmètres peut être envisagé pour simplifier l'application de la démarche et faciliter la suite de l'étude.

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 peuvent être les suivants :

- au vu de l'architecture matérielle : faire autant de sous-périmètres qu'il y a de machines (ou ensemble de machines) autonomes ;
- décomposition par les fonctions ou les informations essentielles ;
- autonomie de responsabilité : (ensemble d'utilisateurs ou mise en œuvre technique) ;
- 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, ...) ;
- isolement de "sous-périmètres communs" : (serveurs communs, réseaux communs, personnels ou sous-zones communes par exemple).

Une fois le périmètre délimité, il convient de définir :

- les participants à l'étude, pour adapter les métriques et généraliser les résultats ;
- les critères de sélection des participants.

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, à quoi il sert et les enjeux pour l'organisme.
- Il n'est pas nécessaire de décrire la composition du périmètre de l'étude de manière détaillée (cela sera revu 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

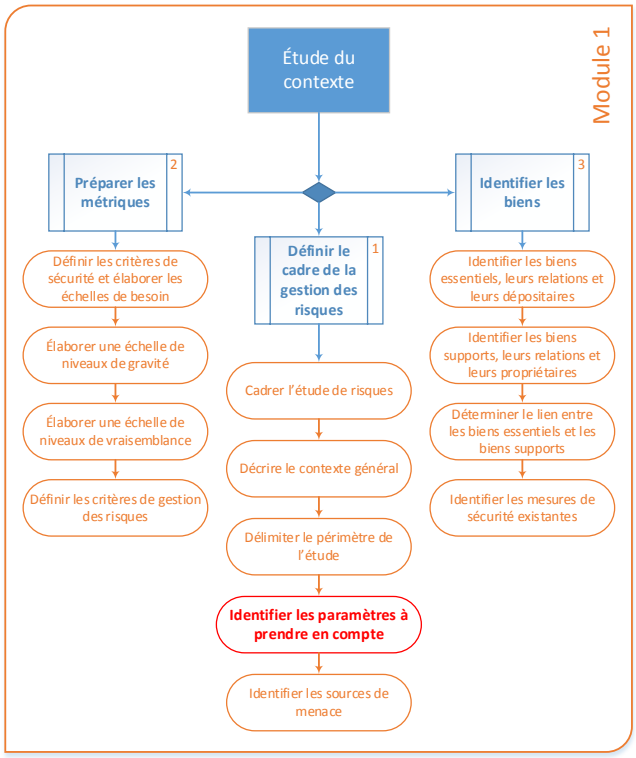
parties prenantes.

- La population participant 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.

Action 1.1.4. Identifier les paramètres à prendre en compte

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



On ne retiendra que les éléments 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 sont, notamment :

- la PSSI-E (E pour l'État);
- les schémas directeurs ;
- les plans de continuité (des activités, des applications, ...), de secours ou de reprise;
- les résultats d'audits relatifs à la sécurité de l'information, ...

Les contraintes qui pèsent sur l'organisme pourront être identifiées.

Il peut s'agir, par exemple, des :

- contraintes d'ordre politique : elles peuvent concerner les services exécutifs de l'État, les établissements publics ou en règle générale tout organisme devant appliquer les décisions gouvernementales ;
- contraintes d'ordre stratégique : des contraintes peuvent résulter d'évolutions prévues ou possibles des structures ou des orientations de l'organisme ;
- 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, ou inversement la concentration sur le territoire national ;
- contraintes conjoncturelles : le fonctionnement de l'organisme peut être profondément modifié par des situations particulières telles que des grèves, des crises nationales ou internationales ;
- contraintes structurelles : la structure de l'organisme peut induire, du fait de sa nature, une politique de sécurité qui lui est spécifique et une organisation de la sécurité adaptée à ces structures ;
- contraintes fonctionnelles : il s'agit des contraintes directement issues des missions générales ou spécifiques de l'organisme (personnel, qualification, formation, sensibilisation à la sécurité, motivation, disponibilité, ...)
- contraintes d'ordre calendaire ;
- contraintes relatives aux méthodes de l'organisme ;
- contraintes d'ordre culturel (habitudes, éducation, expérience professionnelle ou extra-professionnelle, opinions, philosophie, croyances, sentiments, statut social, ...) ;
- contraintes d'ordre budgétaire (les mesures de sécurité préconisées ont un coût qui peut, dans certains

cas, être très important).

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

- contraintes d'antériorité : tous les projets d'applications ne peuvent pas être développés simultanément. Certains sont dépendants de réalisations préalables ;
- contraintes techniques (règles d'accès aux fichiers, architecture, logiciels applicatifs, matériels, réseaux, infrastructures immobilières ;
- 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 (géographique ou économique) ;
- contraintes de temps (temps nécessaire à la mise en place de mesures de sécurité doit être mis en rapport avec l'évolutivité du Système d'Information) ;
- contraintes relatives aux méthodes (savoir-faire, habitudes) ;
- contraintes organisationnelles ('exploitation, maintenance, exigences d'actions de diagnostic, gestion des ressources humaines, gestion administrative, gestion des développements, gestion des relations externes, ...).

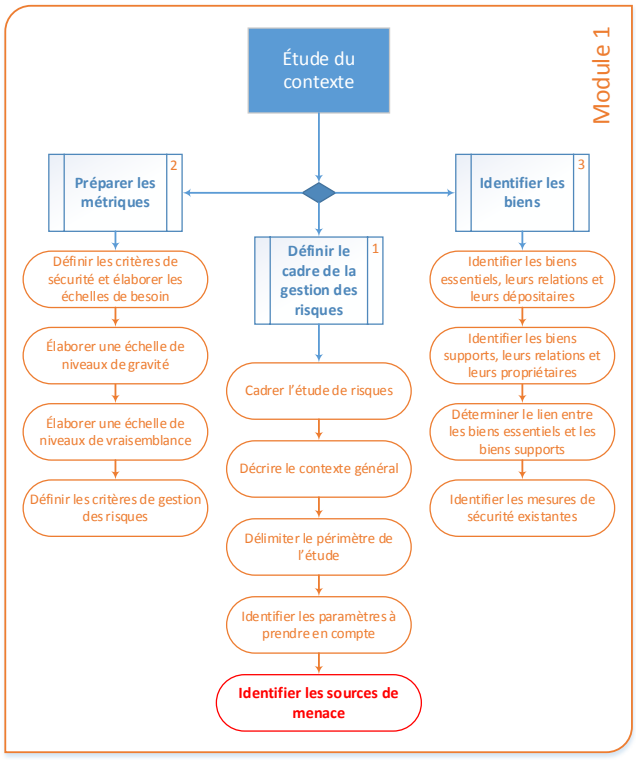
Conseils :

- 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.

Action 1.1.5. Identifier les sources de menaces

Les sources de menaces peuvent être identifiées à partir de la base de connaissance fournit en annexe 3.

Cette action consiste à déterminer les sources de menaces pertinentes vis-à-vis du 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.



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 ?

Il convient tout d'abord de choisir une typologie de sources de menaces. Les bases de connaissances de la méthode proposent en annexe une liste générique que l'on peut directement utiliser ou ajuster.

Bien que, potentiellement, n'importe quelle source de menace puisse être considérée, il convient 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, etc.

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.
- 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, ...) 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.

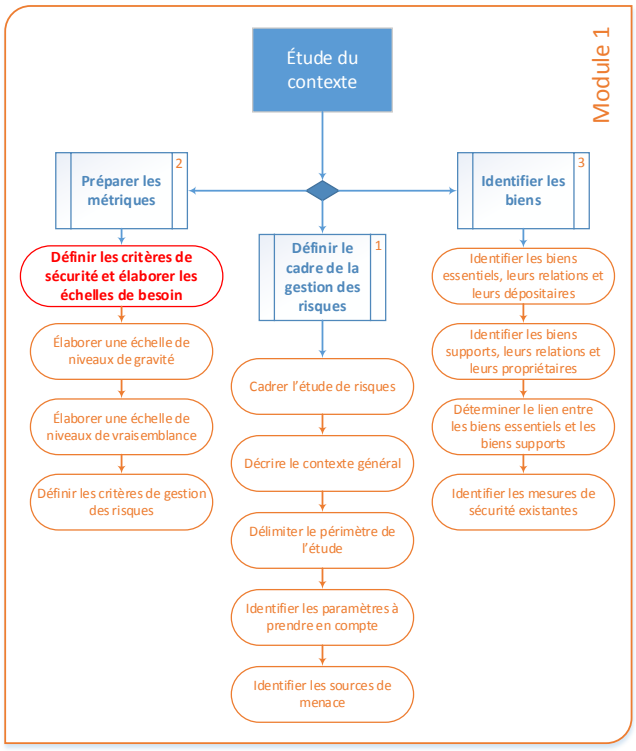
Activité 1.2 - Préparer les métriques

Cette activité fait partie de l'établissement du contexte. Elle a pour but de fixer l'ensemble des paramètres et des échelles qui serviront à gérer les risques. Elle peut être commune à plusieurs études.

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

Cette action consiste :

1. à choisir les critères de sécurité qui seront étudiés ;
2. à produire une définition pour chacun d'eux ;
3. 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 :

- la <u>disponibilité :</u> 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'<u>intégrité :</u> 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 <u>confidentialité :</u> elle reflète le besoin que des biens essentiels ne soient pas compromis ni divulgués.

Les besoins sont parfois exprimés selon d'autres "critères de sécurité", tels que la preuve, l'imputabilité, l'auditabilité, la fiabilité, la traçabilité, ... 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.

Une échelle de besoins est généralement basée sur le classement par ordre de grandeur, et est composée de plusieurs niveaux permettant de classer l'ensemble des biens essentiels étudiés.

Il doit être facile de déterminer le niveau nécessaire pour chaque bien essentiel. Les différents niveaux (par exemple : primordial, essentiel, important, souhaitable, accessoire, sans importance, ...) devraient ainsi être très explicites, non ambigus, et avec des limites claires. On notera 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*).

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

Critères de sécurité	Définitions adoptées
Disponibilité	Propriété d'accessibilité au moment voulu des biens essentiels par les personnes autorisées.
Intégrité	Propriété d'exactitude et de complétude des biens essentiels.
Confidentialité	Propriété des biens essentiels de n'être accessibles qu'aux personnes autorisées.

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

Niveaux de l'échelle de disponibilité	Description détaillée de l'échelle
Plus de 72 heures	Le bien essentiel peut être indisponible plus de 72 heures.
Entre 24 et 72 heures	Le bien essentiel doit être disponible dans les 72 heures.
Entre 4 et 24 heures	Le bien essentiel doit être disponible dans les 24 heures.
Moins de 4 heures	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 d'intégrité	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 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 de confidentialité	Description détaillée de l'échelle
Public	Le bien essentiel est public.
Diffusion Restreinte[3]	Le bien essentiel doit éviter d'être divulguer dans le domaine public.
Confidentiel Sécurité Nationale	Le bien essentiel ne doit être accessible qu'aux personnes habilités à ce niveau et ayant besoin d'en connaître.
Secret de Sécurité Nationale	Le bien essentiel ne doit être accessible qu'aux personnes habilités à ce niveau et ayant besoin d'en connaitre.

[3] Les mentions particulières « confidentiel personnel » et « confidentiel médical » entrent dans ce niveau de protection

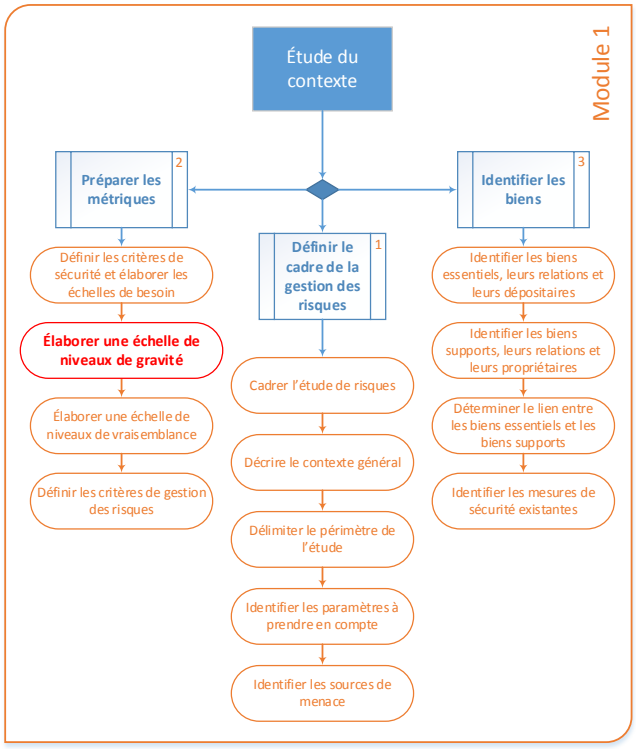
Action 1.2.2. Élaborer une échelle de niveaux de gravité

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 basée sur un classement 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.



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.

L'échelle suivante peut être utilisée pour estimer la gravité des évènements redoutés et des risques :

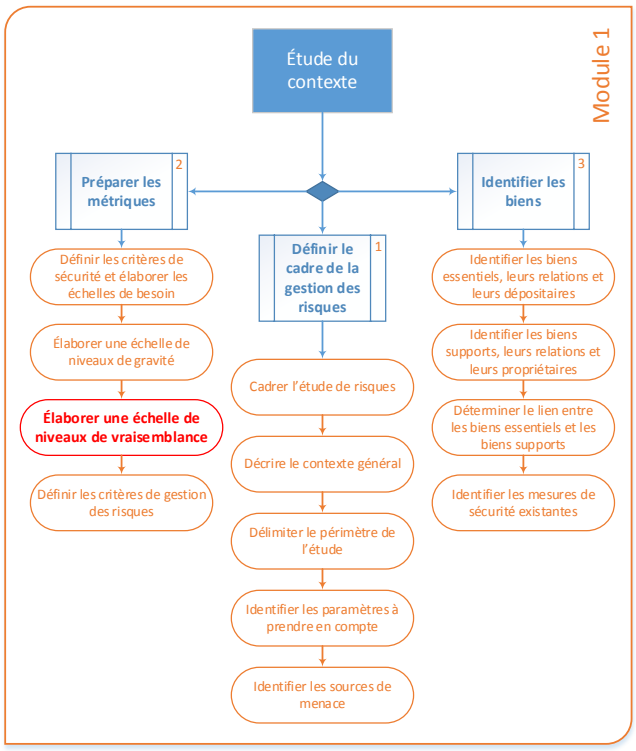
Niveaux de l'échelle des risques	Description détaillée de l'échelle
1. Négligeable	Surmontera les impacts sans aucune difficulté.
2. Limitée	Surmontera les impacts malgré quelques difficultés.
3. Importante	Surmontera les impacts avec de sérieuses difficultés.
4. Critique	Ne surmontera pas les impacts, sa survie est menacée.

Action 1.2.3. Élaborer une échelle de niveaux de vraisemblance

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 basée sur un classement 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.

L'échelle suivante peut être 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 un jour prochainement.

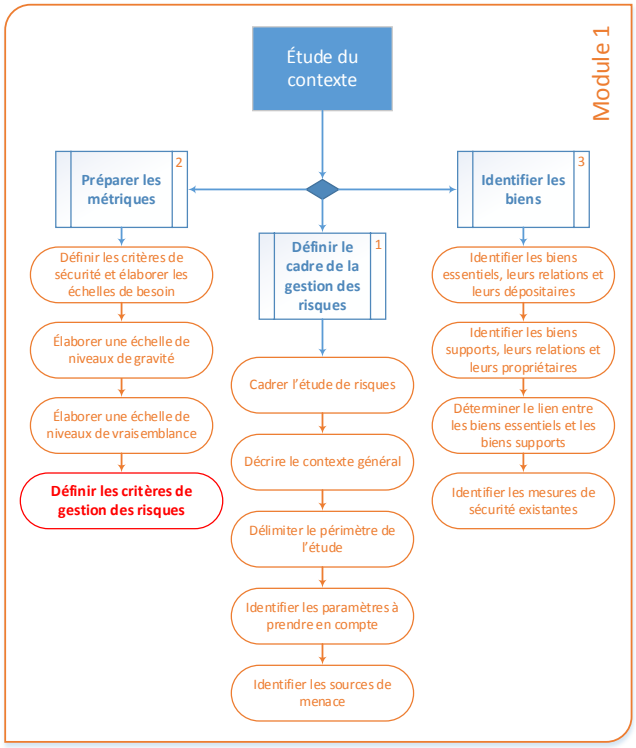
Action 1.2.4. Définir les critères de gestion des risques

Cette action consiste à formaliser les règles choisies pour faire des choix tout au long de l'étude.

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 tiennent ainsi compte de la nature des causes et des conséquences qui peuvent survenir, du niveau à partir duquel les risques deviennent acceptables ou tolérables, de la prise en compte ou non des combinaisons de plusieurs risques, ...

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.

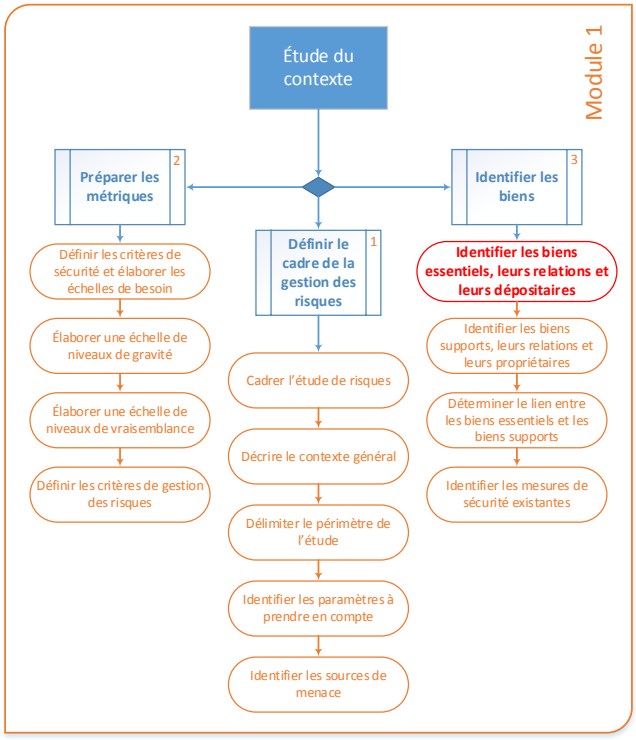
Activité 1.3 - Identifier les biens

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.

Action 1.3.1. Identifier les biens essentiels, leurs relations et leurs dépositaires (voir annexe)

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 n°1.165 du 23 décembre 1993, modifiée relative à la protection des informations nominatives ;
- 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 de sécurité nationale définies dans l'article 18 de la loi n°1.430 du 13 juillet 2016 portant diverses mesures relatives à la sécurité nationale et pour lesquelles le niveau d'exigence de sécurité n'est pas négociable ;
- les informations classifiées d'autres natures, ...

Selon leur finalité, certaines études pourront se limiter aux éléments vitaux du périmètre de l'étude.

Le niveau de détail des biens essentiels doit être cohérent avec le périmètre et l'objectif de l'étude.

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 :

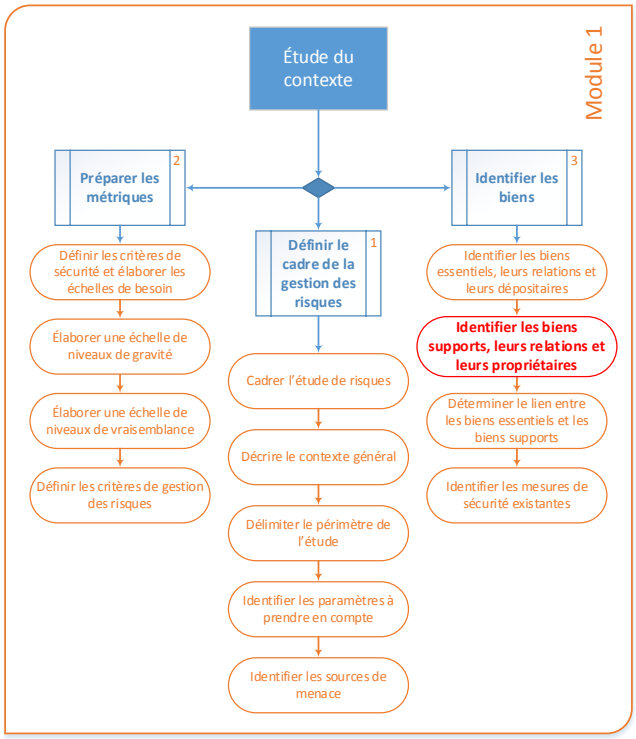
- Comme leur nom l'indique, il s'agit de recenser les biens réellement "essentiels" et non de réaliser un recensement exhaustif. Dix ou quinze biens essentiels (et c'est déjà beaucoup), suffisamment représentatifs, permettent ainsi de réduire le travail de la suite de l'étude à un volume nécessaire et 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.
- La sélection devrait être effectuée par un groupe de travail hétérogène et représentatif du périmètre de l'étude (responsables, informaticiens etutilisateurs).
- Des schémas simples peuvent être suffisants et sont souvent très utiles à la compréhension de toutes les parties prenantes.

Action 1.3.2. Identifier les biens supports, leurs relations et leurs propriétaires (voir annexe)

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 varier selon les objectifs de l'étude.

À cet effet, les bases de connaissances de la méthode, fournies en annexe, 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 souhaita table 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.

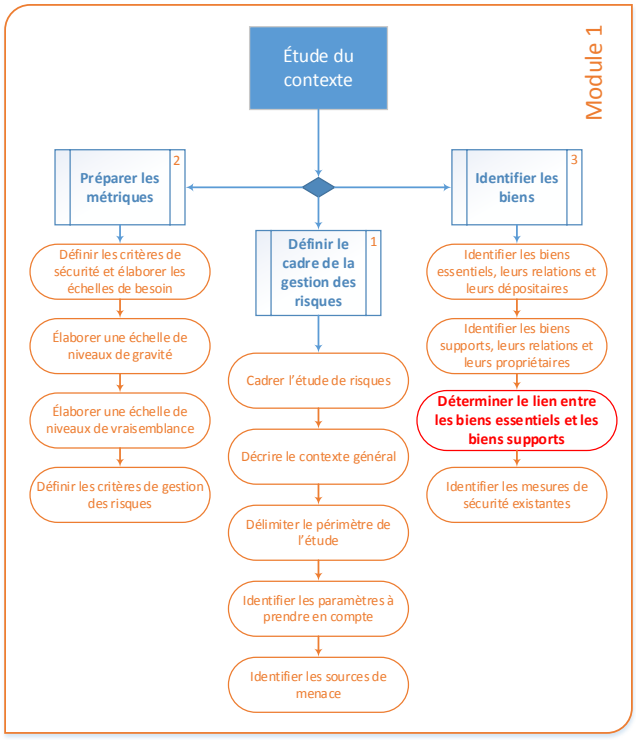
Conseils :

- 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.

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

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.



Conseil :

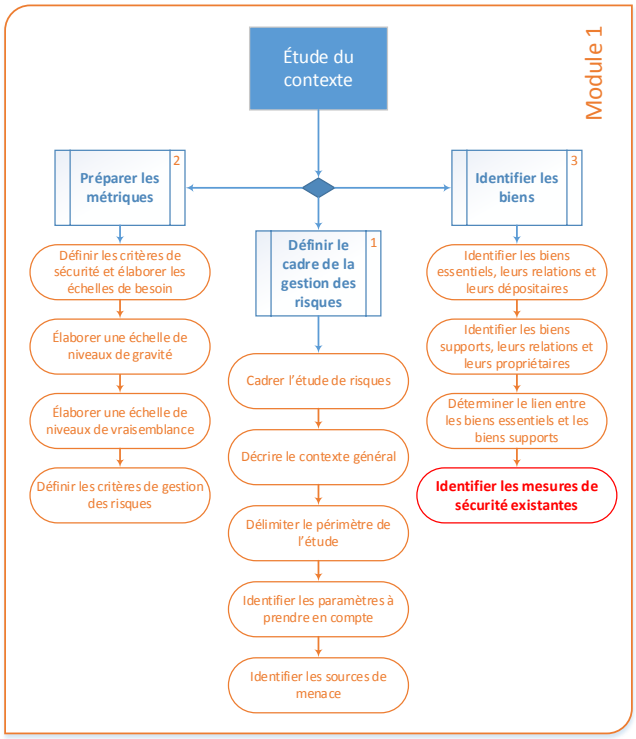
- Un simple tableau croisé entre les biens essentiels et les biens supports permet de représenter le lien entre les deux.

Action 1.3.4. Identifier les mesures de sécurité existantes

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.



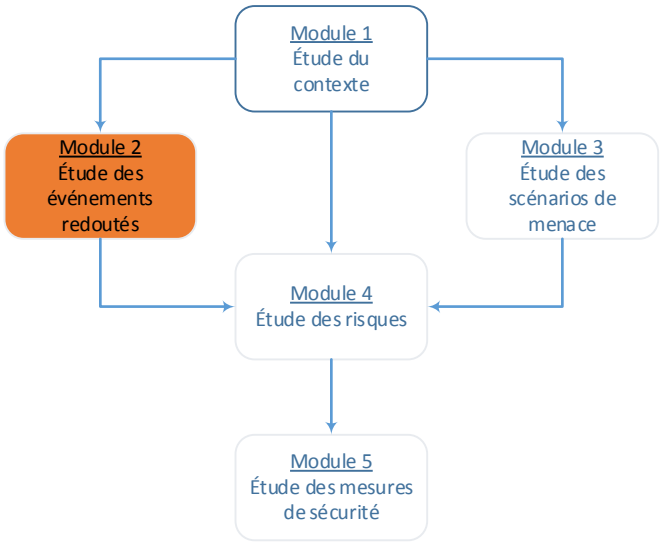
Conseils :

- 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).

3.2 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

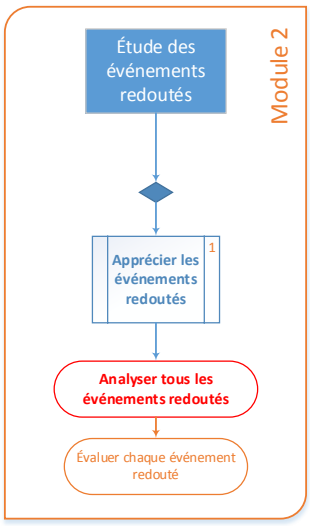
Activité 2.1 - Apprécier les événements redoutés

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.

Action 2.1.1. Analyser tous les évènements redoutés

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, il est recommandé de créer un groupe de travail hétérogène et représentatif du périmètre de l'étude (responsable du périmètre de l'étude, dépositaires des biens essentiels, experts métiers, ...).



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.

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 devront 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.

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.

Les bases de connaissances en annexe proposent une liste générique que l'on peut directement utiliser ou dans laquelle on peut sélectionner des types d'impacts.

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.

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.

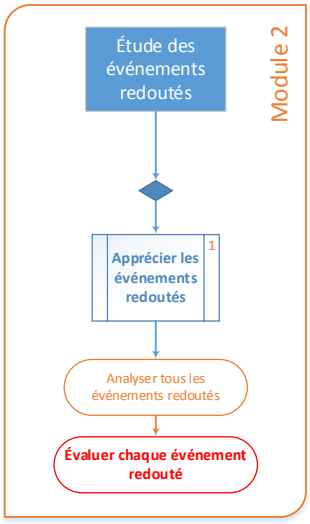
Action 2.1.2. Évaluer chaque évènement redouté

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 sa 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.

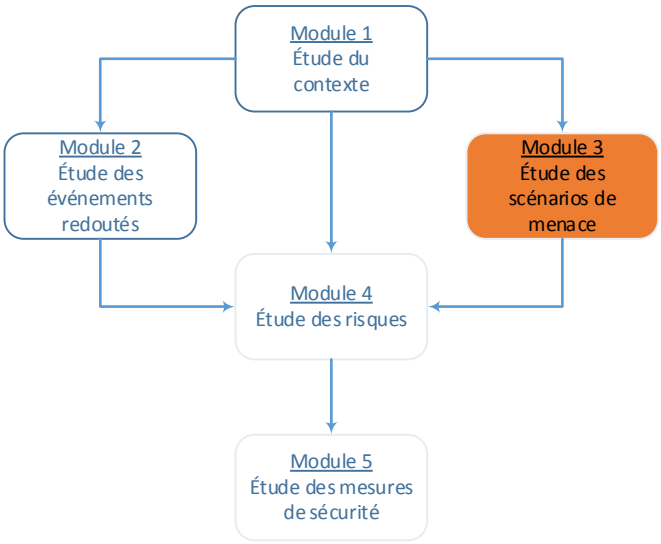


Conseils :

- 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.

3.3 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 :

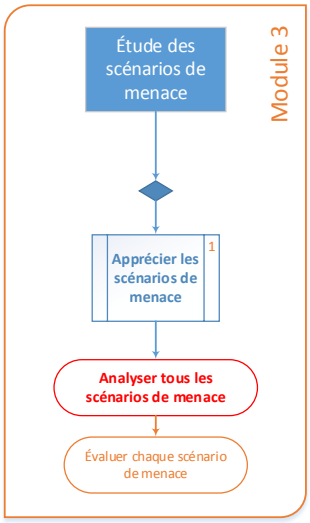
Activité 3.1 - Apprécier les scénarios de menaces

Activité 3.1 - Apprécier les scénarios de menaces

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.

Action 3.1.1. Analyser tous les scénarios de menaces

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 en annexe 3 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.

Pour chaque bien support et chaque menace sélectionnés, on détermine les vulnérabilités qui peuvent être exploitées pour que la menace se réalise. **Les bases de connaissances en annexe 3 proposent une typologie de vulnérabilités que l'on peut directement utiliser ou que l'on peut ajuster**.

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.

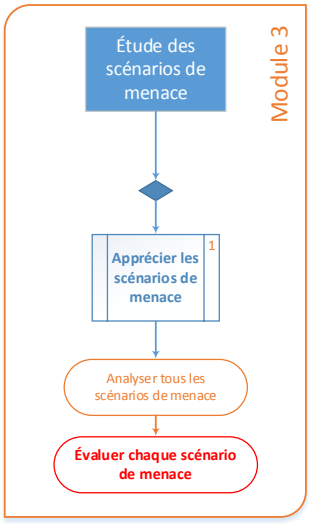
Action 3.1.2. Évaluer chaque scénario de menace

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.

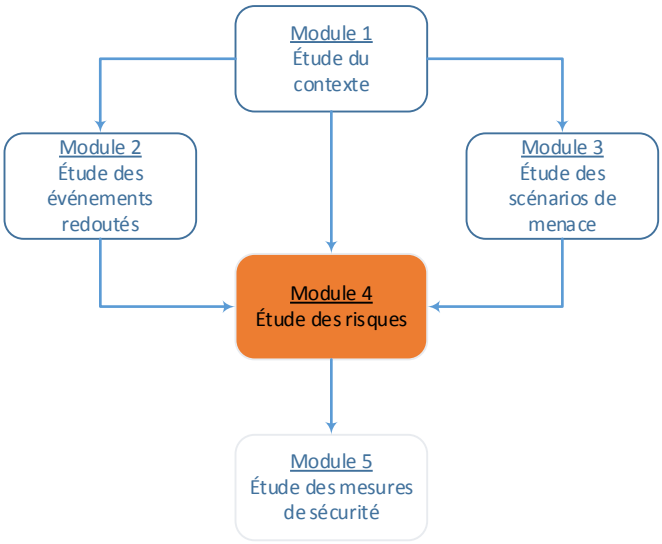


Conseils :

- 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, 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.

3.4 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.

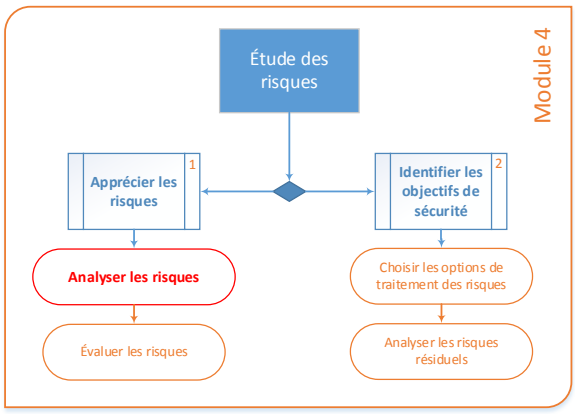
Activité 4.1 - Apprécier les risques

Action 4.1.1. Analyser les risques

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 que 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

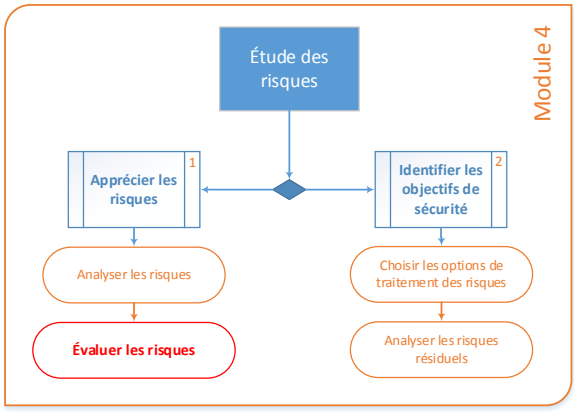
maximale des scénarios de menaces liés à un même événement redouté.

- 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. La mise en œuvre et la qualité de cette mise en œuvre pourront être vérifiées à l'occasion d'un audit spécifique.

Action 4.1.2. Évaluer les risques

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 :

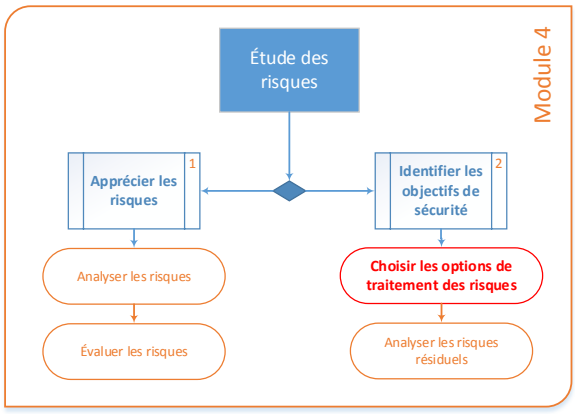
- La représentation sous une forme graphique (vraisemblance en abscisses et gravité en ordonnées) permet de visualiser le positionnement des risques les uns par rapport aux autres.
- Il peut s'avérer utile d'écarter des risques, quand leur nombre est important, afin d'obtenir des résultats rapidement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

Activité 4.2 - Identifier les objectifs de sécurité

Action 4.2.1. Choisir les options de traitement des risques

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 ou 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.

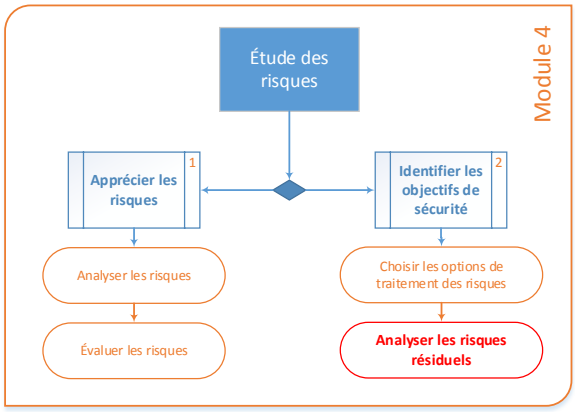
Conseils :

- 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.

Action 4.2.2. Analyser les risques résiduels

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.

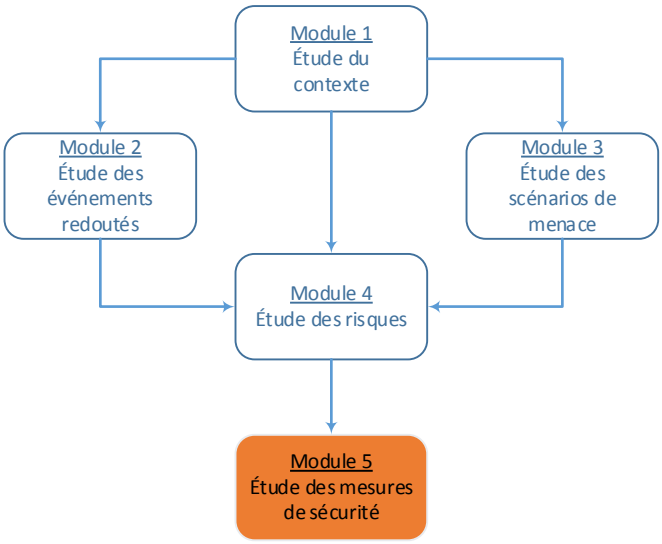
Pour chaque risque, il peut être utile de déterminer la gravité et la vraisemblance attendues une fois les objectifs de sécurité satisfaits. Ces niveaux constituent ainsi le niveau de risque acceptable.

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.

3.5 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 sécurité

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

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.

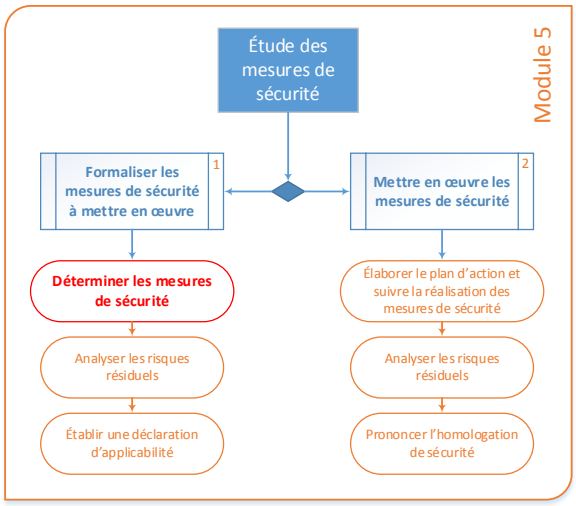
Action 5.1.1. Déterminer les mesures de sécurité

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 bases de connaissances en annexe proposent une liste générique que l'on peut directement utiliser ou que l'on peut ajuster.

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.

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 ;
- une ligne protectrice, destinée à bloquer, contenir et détecter l'apparition des incidents et des sinistres ;
- une ligne récupératrice, destinée à minimiser les conséquences des incidents et des sinistres et revenir à l'état initial.

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 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.

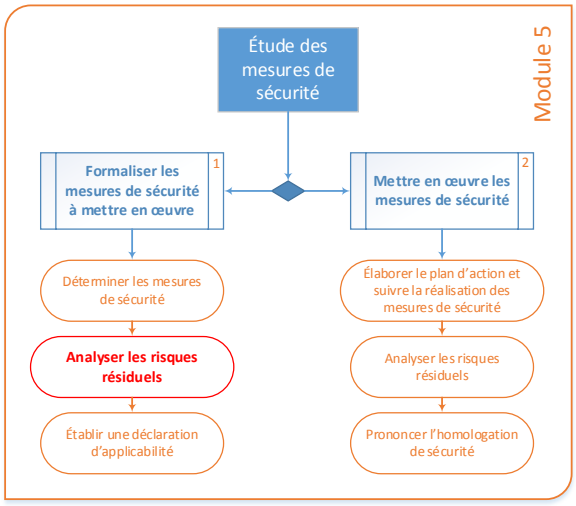
Conseils :

- Les mesures de sécurité devraient être claires, simples etmesurables.
- La manière dont les mesures de sécurité sont rédigées doit être adaptée à ceux à qui elles sont destinées.
- Il est important 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).

Action 5.1.2. Analyser les risques résiduels

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.

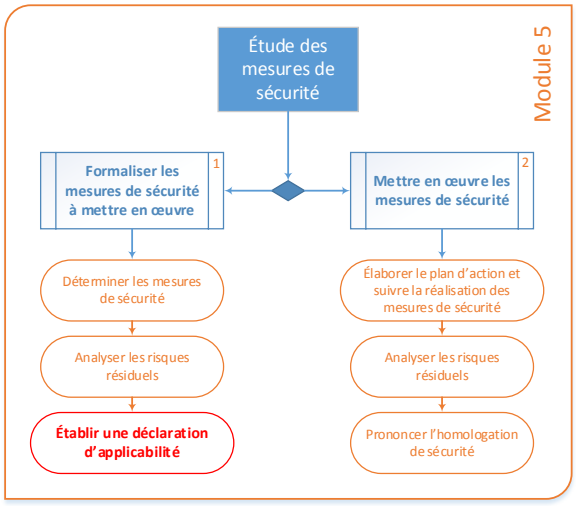
Conseils :

- 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.

Action 5.1.3. Établir une déclaration d'applicabilité

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.
- Il peut être utile de capitaliser les mesures de sécurité créées à partir des références applicables en complétant les bases de connaissances.

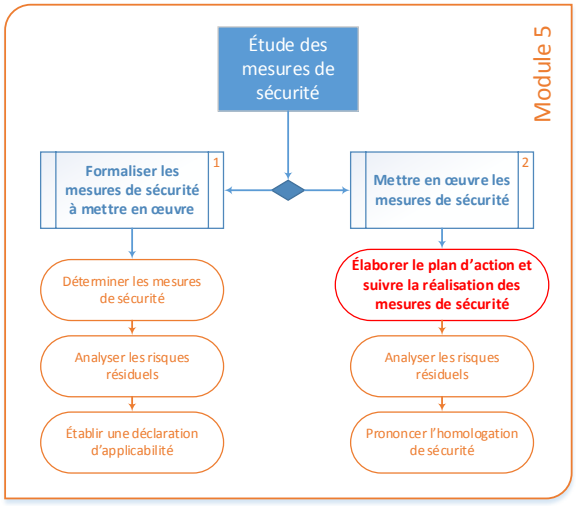
Activité 5.2 - Mettre en œuvre les mesures de sécurité

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.

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

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 « SMART » :

  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) ;

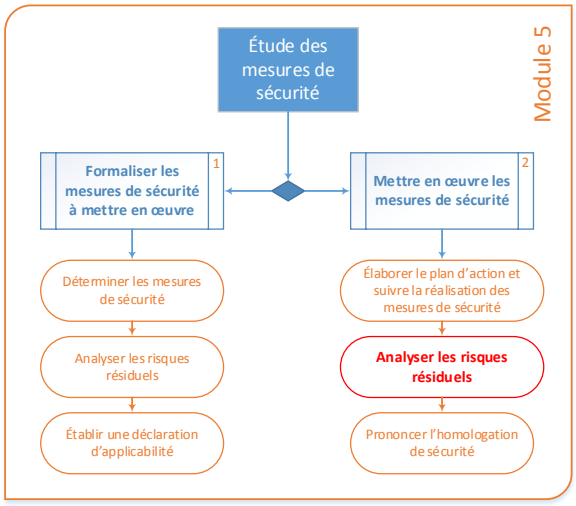
  T - liée au temps (avec une date buttoir, un délai, une période définie).

Action 5.2.2. Analyser les risques résiduels

Cette action consiste à identifier et à estimer les risques résiduels qui subsistent 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.

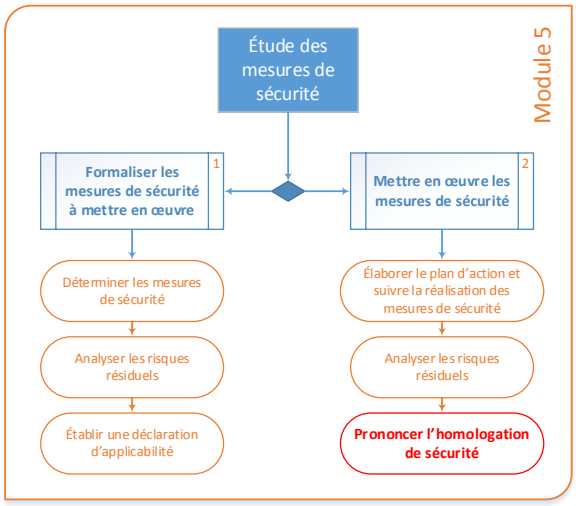
Action 5.2.3. Prononcer l'homologation de sécurité

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 doit 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/ou 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 ou plus 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.

4 Annexe 1 - Définitions/glossaire

Appréciation des risques	Sous-processus de la gestion des risques visant à identifier, analyser et à évaluer les risques
Besoin de sécurité	Définition précise et non ambiguë du niveau d'exigences opérationnelles relatives à un bien essentiel pour un critère de sécurité donné (disponibilité, confidentialité, intégrité, ...)
Bien	Toute ressource qui a de la valeur pour l'organisme et qui est nécessaire à la réalisation de ses objectifs. On distingue les biens essentiels et les biens supports
Bien essentiel	Information ou processus jugé comme important pour l'organisme. On appréciera ses besoins de sécurité mais pas ses vulnérabilités
Bien support	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
Confidentialité	Propriété des biens essentiels de n'être accessibles qu'aux personnes autorisés
Critère de sécurité	Caractéristique d'un bien essentiel permettant d'apprécier ses différents besoins de sécurité
Disponibilité	Propriété d'accessibilité au moment voulu des biens essentiels par les personnes autorisées
Établissement du contexte	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
Événement redouté	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
Gestion des risques	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
Gravité	Estimation de la hauteur des effets d'un événement redouté ou d'un risque. Elle représente ses conséquences
Homologation de sécurité	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
Impact	Conséquence directe ou indirecte de l'insatisfaction des besoins de sécurité sur l'organisme et/ou sur son environnement
Information	Tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement
Intégrité	Propriété d'exactitude et de complétude des biens essentiels

Menace	Moyen type utilisé par une source de menace
Mesure de sécurité	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	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	service exécutif de l'État, établissement public, Opérateur d'Importance Vitale, toutes autres structures de droit public ou privé
Partie prenante	Personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité
Prise de risques	Choix de traitement consistant à accepter les conséquences de la réalisation de tout ou partie de risques, sans appliquer de mesure de sécurité
Processus de l'organisme	Ensemble organisé d'activités qui utilisent des ressources pour transformer des entrées en sorties.
Processus informationnel	Ensemble organisé de traitements qui utilisent des biens supports pour transformer des informations d'entrées en informations de sorties
Réduction de risques	Choix de traitement consistant à appliquer des mesures de sécurité destinées à réduire les risques.
Refus de risques	Choix de traitement consistant à éviter les situations à risque.
Risque résiduel	Risque subsistant après le traitement du risque
Scénario de menace	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
Sécurité de l'information	Satisfaction des besoins de sécurité des biens essentiels
Source de menace	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
Système d'information	Ensemble des moyens humains et matériels ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire l'information
Transfert de risques	Choix de traitement consistant à partager les pertes consécutives à la réalisation de risques.
Vraisemblance	Estimation de la possibilité qu'un scénario de menace ou un risque, se produise. Elle représente sa force d'occurrence.
Vulnérabilité	Caractéristique d'un bien support qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information

5 Annexe 2 - Exemple d’application des actions décrites

6 Annexe 3 - Bases de connaissance