PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS®

SECTION 3
TECHNIQUES

Version 2 – 5 février 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)
en collaboration avec le Club EBIOS

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante
(voir formulaire de recueil de commentaires en fin de guide) :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

ebios.dcssi@sgdn.pm.gouv.fr

Historique des modifications

Version	Objet de la modification	Statut
02/1997 (1.1)	Publication du guide d'expression des besoins et d'identification des objectifs de sécurité (EBIOS).	Validé
23/01/2004	Révision globale : - Explications et mise en cohérence avec les normes internationales de sécurité et de gestion des risques - Mise en évidence du référentiel réglementaire par rapport à l'ensemble des contraintes à prendre en compte - Intégration des concepts d'hypothèse et de règles de sécurité (ISO/IEC 15408) - Transfert de la sélection des éléments essentiels dans l'Étude du système-cible - Amélioration de l'élaboration de l'échelle de besoins est améliorée : les valeurs représentant les limites acceptables pour l'organisme par rapport à des impacts personnalisés - Intégration de la détermination des besoins par élément dans l'activité suivante - Intégration de la détermination du mode d'exploitation dans les hypothèses - Adaptation des concepts à l'ISO/IEC 15408 : on étudie l'origine des menaces, c'est-à-dire les méthodes d'attaque et les éléments menaçants, ainsi que leur caractérisation, qui peut inclure un type (naturel, humain, environnemental) une cause (accidentelle, délibérée, en affinant en exposition, ressources disponibles, expertise, motivation), un potentiel d'attaque - Mise en évidence des méthodes d'attaque non retenues - Formalisation des menaces, au sens ISO/IEC 15408 (élément menaçant, attaque et bien sous la forme des entités), avant la confrontation aux besoins de sécurité - Modification de la confrontation des menaces aux besoins, qui permet d'identifier les risques - Mise en évidence des risques non retenus - Intégration de la détermination des objectifs de sécurité minimums dans les activités Formalisation des objectifs de sécurité et Détermination des exigences fonctionnelles - Modification de la détermination des objectifs de sécurité, qui prend en compte les hypothèses, règles de politique de sécurité, contraintes, référentiel réglementaire et risques - Ajout de la détermination des niveaux de sécurité, qui permet de déterminer le niveau des objectifs de sécurité (notamment en fonction des potentiels d'attaque) et de choisir un niveau d'assurance - Ajout de la détermination des exigences de sécurité fonctionnelles, qui permet de déterminer les exigences fonctionnelles couvrant les objectifs de sécurité et de présenter cette couverture - Ajout de la détermination des exigences de sécurité d'assurance, qui permet de déterminer les éventuelles exigences d'assurance Améliorations de forme, ajustements et corrections mineures (grammaire, orthographe, formulations, présentations, cohérence…)	Version de travail
05/02/2004	Publication de la version 2 du guide EBIOS	Validé

Table des matières

Introduction

La méthode EBIOS[1] est composée de cinq sections complémentaires.

- Section 1 – Introduction
  Cette section présente le contexte, l'intérêt et le positionnement de la démarche EBIOS. Elle contient aussi une bibliographie, un glossaire et des acronymes.

- Section 2 – Démarche
  Cette section expose le déroulement des activités de la méthode.

- Section 3 – Techniques
  Cette section propose des moyens de réaliser les activités de la méthode. Il conviendra d'adapter ces techniques aux besoins et pratiques de l'organisme.

- Section 4 – Outillage pour l'appréciation des risques SSI
  Cette section constitue la première partie des bases de connaissances de la méthode EBIOS (types d'entités, méthodes d'attaques, vulnérabilités).

- Section 5 – Outillage pour le traitement des risques SSI
  Cette section constitue la seconde partie des bases de connaissances de la méthode EBIOS (objectifs de sécurité, exigences de sécurité, tableaux de détermination des objectifs et exigences de sécurité fonctionnelles).

Le présent document constitue la troisième section de la méthode. Il détaille les activités de la méthode et propose des solutions pour les mettre en œuvre.

Les techniques présentées dans cette section ne sont que des propositions. Il appartient à chacun de choisir les plus appropriées à son contexte, c'est-à-dire à la culture et aux usages de son organisme, ainsi qu'aux outils qu'il préfère utiliser. Des ajustements quant au niveau de détail pourront aussi être opérés.

[1] EBIOS est une marque déposée du Secrétariat général de la défense nationale en France.

Étape 1 – Étude du contexte

Activité 1.1 – Étude de l'organisme

Présenter l'organisme

La présentation de l'organisme permet de rappeler les éléments caractéristiques qui définissent l'identité d'un organisme. Il s'agit de la vocation, du métier, des missions, des valeurs propres et des axes stratégiques de cet organisme. Ils doivent être identifiés ainsi que ceux qui contribuent à leur élaboration (ex : sous-traitance).

La difficulté de cette activité réside dans la compréhension de l'organisation véritable de l'organisme. La structure réelle permet de comprendre le rôle et l'importance donnée à chaque division dans l'atteinte des objectifs de l'organisme.
Par exemple, le rattachement du responsable sécurité à la direction générale plutôt qu'à la direction informatique peut être significatif de l'implication de la direction dans la sécurité des systèmes d'information.

La vocation principale (ce que l'organisme veut faire)

La vocation principale d'un organisme peut se définir comme ce qui constitue sa raison d'être (son domaine d'activité, son segment de marché…). La vocation peut être, par exemple, le service public ou l'industrie.

Le métier (ce que l'organisme sait faire)

Le métier de l'organisme, caractérisé par l'ensemble des techniques ou du savoir-faire des employés, permet l'accomplissement des missions. Il est propre au domaine d'activité de l'organisme et souvent il en définit la culture.

Les missions (ce que l'organisme doit faire)

La vocation se réalise par l'accomplissement des missions. Il s'agit de préciser les services fournis et/ou les produits fabriqués en précisant qui en sont les destinataires finaux.

Les valeurs propres (ce que l'organisme fait bien)

Il s'agit des grands principes ou d'une éthique bien définie qui sont attachés à la façon d'exercer un métier. Cela peut concerner le personnel, les rapports avec les intervenants extérieurs (clientèle...), la qualité des produits fournis ou des prestations de service.
À titre d'exemple, un organisme peut avoir le service public pour vocation, le transport comme métier et assurer des missions de ramassage scolaire. Ses valeurs étant la ponctualité du service et la sécurité dans son exécution.

Structure de l'organisme

La structure de l'organisme peut être de différents types :

- la structure divisionnelle : chaque division constituée est placée sous l'autorité d'un directeur de division responsable des décisions stratégiques, administratives et opérationnelles pour son unité ;
- la structure fonctionnelle : l'autorité fonctionnelle s'exerce sur les procédures, sur la nature du travail et parfois sur les décisions ou la planification (ex : la production, l'informatique, les ressources humaines, le marketing…).

Remarques :

- une division au sein de l'organisme à structure divisionnelle peut être organisée en structure fonctionnelle et inversement ;
- on dira qu'un organisme a une structure matricielle si l'ensemble de l'organisation est fondé sur les deux types de structure ;

- quelle que soit la structure de l'organisme, on peut distinguer les niveaux suivants :
  - le niveau décisionnel (définition des orientations stratégiques) ;
  - le niveau de pilotage (coordination et gestion) ;
  - le niveau opérationnel (production et activités de soutien).

Organigramme

Il s'agit d'obtenir la représentation, à l'aide d'un schéma, de la structure de l'organisme. Cette représentation doit mettre en évidence les liaisons de subordination et de délégation d'autorité, mais aussi tenir compte des autres dépendances. En effet, même si elles ne sont porteuses d'aucune autorité formelle, il existe des liaisons permettant la circulation d'informations.
Par exemple, le correspondant informatique qui est un utilisateur dépendant de son chef de service peut également recevoir des recommandations, de la direction informatique.

Les axes stratégiques (ce que l'organisme veut mieux faire)

Il s'agit de formaliser les lignes directrices de l'organisme qui déterminent son évolution afin de mieux saisir les enjeux qui y sont liés, ainsi que les grandes évolutions prévues.

Lister les contraintes pesant sur l'organisme

Il s'agit de prendre en compte l'ensemble des contraintes qui pèsent sur l'organisme et qui pourront déterminer des orientations en matière de sécurité. Elles peuvent être d'origine interne à l'organisme, dans ce cas celui-ci peut éventuellement les aménager, ou extérieures à l'organisme et donc en règle générale incontournables. Les contraintes de ressources (budget, personnels) et d'urgence sont les plus importantes.

L'organisme se fixe des objectifs à atteindre (touchant au métier, à son comportement…) qui engageront son avenir à plus ou moins long terme. Il définit ainsi ce qu'il veut devenir, et les moyens qu'il conviendra de mettre en place. Pour préciser ces grands axes, l'organisme tient compte de l'évolution des techniques et des savoir-faire, des souhaits exprimés par les utilisateurs, les clients… Cette finalité peut s'exprimer sous la forme de politiques de fonctionnement ou de développement. Il s'agit par exemple de la réduction des coûts de fonctionnement, de l'amélioration de la qualité de service…

Ces politiques ont vraisemblablement un volet consacré au système d'information (SI) qui doit, pour ce qui le concerne, contribuer à les appliquer. Par conséquent, la prise en compte des caractéristiques liées à l'identité ou à la mission et à la stratégie de l'organisme est fondamentale pour l'analyse du problème car l'atteinte d'un élément du SI (en terme de sécurité) pourrait constituer une remise en cause de ces objectifs stratégiques. De plus, il est essentiel que les propositions de mesures de sécurité restent en cohérence avec les règles, les usages et les moyens en vigueur dans l'organisme.

Les paragraphes suivants présentent une liste non exhaustive de types de contraintes.

Les contraintes d'ordre politique

Elles peuvent concerner les administrations de l'État, les établissements publics ou en règle générale tout organisme devant appliquer les décisions gouvernementales. D'une manière générale, il s'agit de décisions d'orientation stratégique ou opérationnelle, émanant d'une Direction ou d'une instance décisionnelle et qui doivent être appliquées.
Par exemple le principe de dématérialisation des factures ou des documents administratifs induit des problèmes de sécurité.

Les contraintes d'ordre stratégique

Des contraintes peuvent résulter d'évolutions prévues ou possibles des structures ou des orientations de l'organisme. Elles s'expriment dans les schémas directeurs d'organisation stratégiques ou opérationnels.
Par exemple les coopérations internationales sur la mise en commun d'informations sensibles peuvent nécessiter des accords au niveau des échanges sécurisés.

Les contraintes territoriales

La structure et/ou la vocation de l'organisme peut induire des contraintes particulières telles que la dispersion des sites sur l'ensemble du territoire national ou à l'étranger.
Par exemple les agences de la poste, les ambassades, les banques, les différentes filiales d'un grand groupe industriel...

Les contraintes conjoncturelles

Le fonctionnement de l'organisme peut être profondément modifié par des situations particulières telles que des grèves, des crises nationales ou internationales.
Par exemple la continuité de certains services doit pouvoir être assurée même en période de crise grave.

Les contraintes structurelles

La structure de l'organisme peut induire, du fait de sa nature (divisionnelle, fonctionnelle ou autre), une politique de sécurité qui lui est spécifique et une organisation de la sécurité adaptée à ces structures.
Par exemple une structure internationale doit pouvoir concilier des exigences de sécurité propres à chaque nation.

Les contraintes fonctionnelles

Il s'agit des contraintes directement issues des missions générales ou spécifiques de l'organisme.
Par exemple un organisme peut avoir une mission de permanence qui exigera une disponibilité maximale de ses moyens.

Les contraintes relatives au personnel

Les contraintes relatives au personnel sont de natures très diverses et liées aux caractéristiques suivantes : niveau de responsabilité, recrutement, qualification, formation, sensibilisation à la sécurité, motivation, disponibilité…
Par exemple, il peut être nécessaire que l'ensemble du personnel d'un organisme de la défense soit habilité pour des confidentialités supérieures.

Les contraintes d'ordre calendaire

Elles peuvent résulter de réorganisations de services, de la mise en place de nouvelles politiques nationales ou internationales qui vont imposer des échéances à date fixe.
Par exemple, la création d'une direction de la sécurité.

Les contraintes relatives aux méthodes

Compte tenu des savoir-faire internes à l'organisme, certaines méthodes (au niveau de la planification du projet, des spécifications, du développement…) seront imposées.
La contrainte peut être, par exemple, de devoir associer la politique de sécurité aux actions relatives à la qualité, en vigueur dans l'organisme.

Les contraintes d'ordre culturel

Dans certains organismes les habitudes de travail ou le métier principal ont fait naître une "culture", propre à cet organisme, qui peut constituer une incompatibilité avec les mesures de sécurité. Cette culture constitue le cadre de référence général des personnes de l'organisme et peut concerner de nombreux paramètres tels que les caractères, l'éducation, l'instruction, l'expérience professionnelle ou extra-professionnelle, les opinions, la philosophie, les croyances, les sentiments, le statut social…

Les contraintes d'ordre budgétaire

Les mesures de sécurité préconisées ont un coût qui peut, dans certains cas, être très important. Si les investissements dans le domaine de la sécurité ne peuvent s'appuyer sur des critères de rentabilité, une justification économique est généralement exigée par les services financiers de l'organisation.
Par exemple dans le secteur privé et pour certains organismes publics, le coût total des mesures de sécurité ne doit pas être supérieur aux conséquences des risques redoutés. La direction doit donc apprécier et prendre des risques calculés si elle veut éviter un coût prohibitif pour la sécurité.

Lister les références réglementaires applicables à l'organisme

La prise en compte des lois, règles ou règlements, peut modifier l'environnement, les habitudes de travail, l'accomplissement des missions ou avoir une influence sur l'organisation interne.
Par exemple le fonctionnement d'administrations de l'État est régi par des codes spécifiques (code des douanes, code des marchés publics...).

Il convient par conséquent de recenser les références réglementaires applicables à l'organisme, qu'il s'agisse de lois, de décrets, de codes spécifiques au domaine de l'organisme ou de règlements internes ou externes. Cela concerne aussi les contrats ou conventions et d'une manière générale les obligations à caractère juridique.

Faire une description fonctionnelle du SI global

Il s'agit d'identifier les domaines fonctionnels qui contribuent à l'atteinte des objectifs stratégiques et leurs interactions. On s'efforce à ce niveau de représenter les interactions existantes et/ou futures des domaines fonctionnels avec le domaine auquel le système-cible appartient.
Cette démarche suppose que le besoin ait été exprimé clairement de façon fonctionnelle.
Cette activité ayant pour but de formaliser l'architecture conceptuelle du SI, afin que l'on puisse par la suite délimiter et caractériser le système-cible, il est parfois possible d'obtenir les études ayant permis d'établir le SI (modèles conceptuels de communication et de traitements d'après [MERISE] par exemple).

Un découpage en domaines fonctionnels permet d'avoir une vue générale d'ensemble du fonctionnement du SI et des éventuelles relations avec des acteurs externes. Cette répartition permettra de mieux situer le système-cible dans le SI et de mieux appréhender les enjeux qui lui sont associés.

En règle générale, tout système d'information peut être partitionné en :
- fonctions opérationnelles ou d'appui opérationnel ;
- fonctions de support ;
- fonctions de contrôle et de suivi des activités.

Les fonctions opérationnelles relèvent des missions de l'organisme.
Les fonctions de support relèvent de la gestion des moyens nécessaires à la réalisation des fonctions opérationnelles.
Quant aux fonctions de contrôle et de suivi des activités, elles concernent le management.

L'évolution d'une fonction de type opérationnel peut avoir des incidences fortes sur les autres fonctions, a contrario la modification d'une fonction de support ou de contrôle n'a généralement pas d'impact direct sur les fonctions opérationnelles.

Activité 1.2 – Étude du système-cible

Le système d'information (SI) contribue, en partie, à la réalisation des objectifs stratégiques de l'organisme. Une compréhension suffisamment claire du SI et de son fonctionnement est nécessaire pour extraire tous les éléments utiles à l'élaboration des besoins de sécurité du système-cible. Pour cela, il convient de replacer le système-cible dans le SI de l'organisme.

Présenter le système-cible

Le système-cible doit faire l'objet d'une description synthétique qui met clairement en évidence son périmètre, ses relations avec les autres domaines ou acteurs externes et ses finalités au sein du système d'information global.

Lister les enjeux

À ce stade de la réflexion, les objectifs stratégiques sont censés être connus (cf. schéma directeur informatique, étude d'opportunité…), les besoins fonctionnels ciblés et définis, les contraintes informationnelles et organisationnelles du système-cible répertoriées. Il convient dès lors d'analyser les enjeux et le contexte dans lequel se situe le système-cible.

Cette analyse permet d'identifier le poids stratégique du système-cible pour l'organisme et d'évaluer le niveau d'importance des fonctions dans le système-cible. Elle consiste à mettre en évidence l'impact de la réalisation ou de l'exploitation du système, les attentes des utilisateurs ou de leur hiérarchie, l'apport attendu… Les enjeux peuvent être, par exemple, d'ordre technique, financier ou politique.

Lister les éléments essentiels

Pour décrire plus précisément le système-cible, l'opération suivante consiste à identifier les éléments essentiels. Cette sélection est effectuée par un groupe de travail hétérogène et représentatif du SI (responsables, informaticiens et utilisateurs).
Les éléments essentiels sont généralement les fonctions et informations au cœur de l'activité du système-cible. Il est aussi possible de considérer d'autres éléments essentiels tels que les processus de l'organisme. Cette seconde approche sera plus appropriée dans le cadre d'élaboration d'une politique de sécurité des systèmes d'information, d'un schéma directeur de sécurité des systèmes d'information ou d'un plan de continuité. Les éléments essentiels constituent le patrimoine informationnel ou les "biens immatériels" que l'on souhaite protéger. Selon leur finalité, certaines études ne mériteront pas une analyse exhaustive de l'ensemble des éléments composant le système cible. Dans ce contexte, le périmètre de l'étude pourra être limité aux éléments vitaux du système cible.
La sélection des éléments essentiels s'effectue auprès d'un responsable utilisateur du système (existant ou futur). Il indique, après une première analyse, ceux qui présentent un caractère de sensibilité. Les éléments essentiels sont généralement des fonctions ou informations pour lesquelles le non respect de la disponibilité, de l'intégrité, de la confidentialité, voire d'autres critères de sécurité, mettrait en cause la responsabilité du propriétaire ou du dépositaire, ou causerait un préjudice à eux-mêmes ou à des tiers.

Les fonctions (ou sous-fonctions) essentielles sont principalement :

- les fonctions dont la perte ou la dégradation rend la réalisation de la mission du système impossible ;
- les fonctions qui contiennent des traitements secrets ou des procédés technologiques de haut niveau ;
- des fonctions dont la modification peut affecter fortement la réalisation de la mission du système.

Le caractère de sensibilité des informations à retenir peut provenir des cas suivants :

- les informations relevant du secret défense définies dans l'[IGI 900] et pour lesquelles le niveau d'exigence de sécurité n'est pas négociable ;
- les informations sensibles non classifiées de défense telles que définies dans la [Rec 901] et pour lesquelles le niveau d'exigence est négociable en fonction des considérations environnementales propres à l'organisme.

Plus généralement les informations essentielles comprennent principalement :

- les informations classifiées qu'elles relèvent ou non du secret de défense ;
- les informations vitales pour l'exercice de la mission ou du métier de l'organisme ;
- les informations personnelles, notamment les informations nominatives au sens de la loi française informatique et libertés ;
- les informations stratégiques nécessaires pour atteindre les objectifs correspondants aux orientations stratégiques ;
- les informations coûteuses, dont la collecte, le stockage, le traitement ou la transmission nécessitent un délai important et/ou un coût d'acquisition élevé.

Les fonctions et informations qui n'auront pas été retenues à l'issue de cette activité ne feront l'objet dans la suite de l'étude d'aucun besoin de sécurité. Cela signifie que leur compromission éventuelle n'a pas de conséquence dans le bon déroulement de la mission remplie par le système.
Cependant, souvent ces fonctions et informations hériteront des mesures prises pour protéger les fonctions et informations retenues.

Les fiches d'expression des besoins de sécurité vont permettre aux utilisateurs d'exprimer leur appréciation de la sensibilité pour les fonctions et informations essentielles.

Faire une description fonctionnelle du système-cible

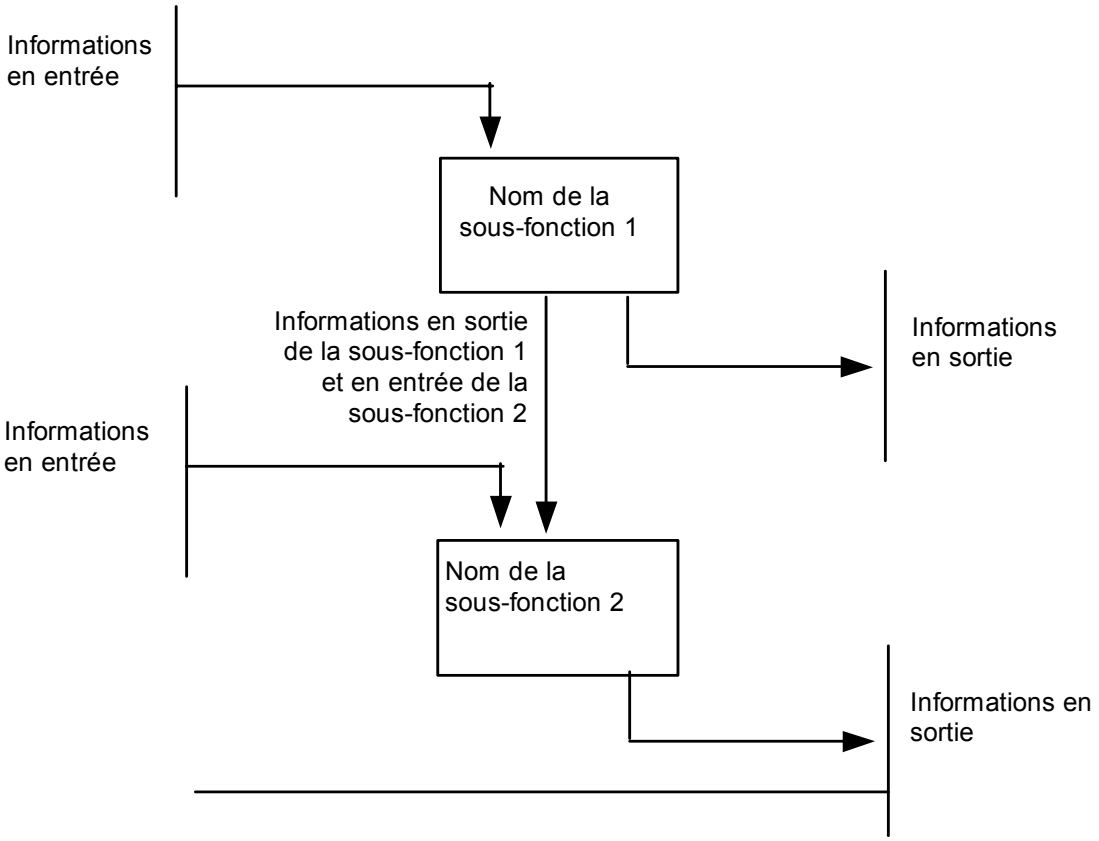
À ce niveau les finalités du système-cible sont clairement exprimées et sa place est établie par rapport à l'existant, il convient dès lors de préciser pour chaque fonction essentielle identifiée :

- les informations en entrée et en sortie (résultats attendus) ;
- les traitements à réaliser (en indiquant aussi les interfaces permettant au système-cible d'échanger des informations avec les autres SI).

Une fonction pourra être décomposée en sous-fonctions, la sous-fonction étant un ensemble cohérent de traitements (agrégat de tâches élémentaires) et d'informations.

Pour un système à concevoir, on utilise pour réaliser la modélisation du système-cible la méthode générale de conception retenue (Exemples : MERISE, SADT, UML…).

Pour un système existant ou dans le cas d'absence de modélisation lors de sa conception, il est proposé d'utiliser la représentation suivante : les fonctions sont représentées par un diagramme, selon une approche descendante, faisant apparaître la relation entre les sous-fonctions, et des informations en entrée et sortie des fonctions (voir l'exemple à la page suivante).



exemple : Représentation d'une fonction gestion des ressources humaines

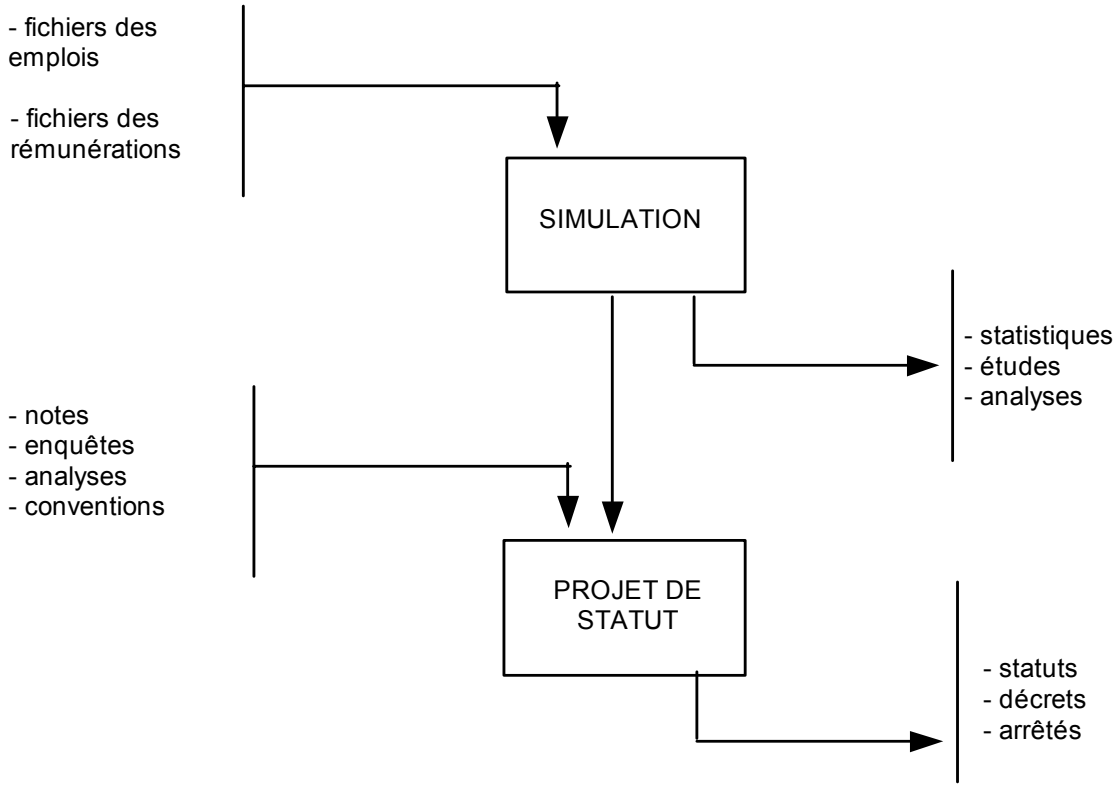


Figure 1 – Représentation des fonctions et informations

Découpage du système en sous-systèmes

Le découpage du système en sous-systèmes peut être envisagé pour faciliter la suite de l'étude.

L'objectif principal de la décomposition en sous-systèmes est de simplifier l'application de la méthode EBIOS. Ainsi, le responsable de l'étude peut choisir de décomposer le système en plusieurs sous-systèmes. Il déterminera ainsi, soit plusieurs systèmes-cible, plus simples à étudier séparément, soit un seul système-cible sur lequel portera précisément l'étude.

La décomposition en sous-systèmes reste de l'appréciation du responsable de l'étude. L'étude de plusieurs sous-systèmes est généralement plus simple que l'étude globale d'un système multiforme, mais le nombre de sous-systèmes doit rester faible (moins de cinq) car chacun fera l'objet d'une étude séparée.

La décomposition en sous-systèmes facilite :

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

Il n'y a pas de méthode à proprement parler permettant de décomposer un système en sous-systèmes, mais un ensemble de critères à examiner. Les principaux critères de décomposition applicables sont les suivants :

- Critère n°1 : au vu de l'architecture matérielle

  Faire autant de sous-systèmes qu'il y a de machines (ou ensemble de machines) autonomes. Si, dans le cas général, les différentes machines sont reliées les unes aux autres, la décomposition dépend du niveau d'interopérabilité des différentes parties (machines ou ensembles de machines) du système.

  Exemple : niveau croissant d'interopérabilité
  - Machines physiquement séparées. Transferts par bandes ou disquettes.
  - Machines reliées par une liaison dédiée aux transferts de fichiers.
  - Ensemble de machines autonomes coopérant via un réseau local.
  - Ensemble de machines reliées par un réseau local, munies du même système d'exploitation et administrées de façon centralisée.

- Critère n°2 : Décomposition par les fonctions ou les informations essentielles.

  Il peut être possible de décomposer un même sous-système physique au vu des fonctions réalisées par telle ou telle machine ou partie du système ou selon la façon dont sont traitées les informations les plus sensibles.

- Critère n° 3 : Autonomie de responsabilité

  Un ensemble d'entités formant un tout du point de vue de la responsabilité de mise en œuvre (ensemble d'utilisateurs ou mise en œuvre technique), pourra être utilisé comme un sous-système à étudier séparément. Il pourra s'agir d'une partie de système placée sous la responsabilité d'un service dûment identifié sur un organigramme de l'organisme. Ce critère peut également s'appliquer lorsqu'il existe plusieurs documentations séparées.

- Critère n° 4 : Implantation dans des sous-zones distinctes

  Si les constituants (matériels, supports, personnels) sont implantés dans des sous-zones différentes (bâtiments, sous-zones réservées, sous-sols...), chaque sous-zone est susceptible de constituer un sous-système (à condition que le niveau d'interopérabilité avec l'extérieur soit suffisamment faible).

- Critère n°5 : Isolement de "sous-systèmes communs"

  Les quatre premiers critères ayant été appliqués, certains ensembles d'entités ou des constituants peuvent se trouver à l'intersection de plusieurs sous-systèmes (serveurs communs, réseaux communs, personnels ou sous-zones communes par exemple). Ils sont susceptibles de former des sous-systèmes qu'il est possible d'étudier séparément. Les résultats de ces études étant par la suite reportés sur les sous-systèmes englobant. Il s'agit en quelque sorte d'une factorisation du travail.

Lister les hypothèses

Il s'agit de formaliser les hypothèses relatives au système-cible. Les hypothèses sont le plus souvent imposées par l'organisme responsable de l'étude, pour des raisons de politique interne ou externe de l'organisme, financières ou de calendrier.
Les hypothèses peuvent aussi constituer un risque accepté a priori sur un environnement donné.
Dans le cas de la rédaction d'un profil de protection ou d'une cible de sécurité, qui doivent démontrer la parfaite complétude des menaces par les objectifs de sécurité, il peut s'agir de vulnérabilités qui ne peuvent être couvertes par un objectif de sécurité dans les étapes suivantes. Dans ce même cas, il peut s'agir de la prise en compte formalisée de contraintes identifiées, alors que les autres ne constitueront que des aides à la compréhension du contexte.

Il est proposé d'adopter la nomenclature suivante pour les hypothèses : H.xx (H pour hypothèse et xx étant le nom de l'hypothèse).

Le cas particulier du choix du mode d'exploitation de sécurité

La détermination du mode d'exploitation de sécurité du système consiste à indiquer comment le système permet aux utilisateurs de catégories différentes de traiter, transmettre ou conserver des informations de sensibilités différentes. Elle permet de prendre connaissance de la problématique sécuritaire générale car le mode d'exploitation de sécurité définit le contexte de gestion de l'information d'un système d'information.

De manière générale, le mode d'exploitation de sécurité du système appartient à l'une des catégories suivantes :

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

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

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

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

Lister les règles de sécurité

La sécurité des systèmes d'information peut avoir fait l'objet d'un référentiel d'études et de documents ; bien qu'une analyse détaillée ne soit pas utile à ce stade, des renseignements peuvent être recherchés : priorités, résultats, consignes…
L'objectif est de recenser les principales règles et mesures de sécurité, formalisées ou non. Le recueil pourra se faire à partir des documents suivants :

- politique de sécurité du système d'information ;
- plans de continuité des applications ;
- consignes de sécurité des développements ;
- résultats d'audits sécurité ;
- projets de sécurité…

Il est proposé d'adopter la nomenclature suivante pour les règles de sécurité : P.xx (P pour politique et xx étant le nom de la règle de sécurité).

Lister les contraintes pesant sur le système-cible

L'identification des contraintes permet de recenser celles qui ont un impact sur le système-cible et de déterminer celles sur lesquelles il est toutefois possible d'agir. Elles complètent et amendent les contraintes de l'organisme déterminées précédemment. Les paragraphes suivants présentent une liste non exhaustive de types de contraintes qui peuvent être envisagées.

Contraintes d'antériorité

Tous les projets d'applications ne peuvent pas être développés simultanément. Certains sont dépendants de réalisations préalables. Un système peut faire l'objet d'une décomposition en sous-systèmes ; un système n'est pas forcément conditionné par la totalité des sous-systèmes (par extension à des fonctions d'un système) d'un autre système.

Contraintes techniques

En général les contraintes techniques, d'ordre physique, peuvent provenir des matériels et des logiciels installés, des locaux ou des sites abritant le SI :

- les fichiers (exigences en matière d'organisation, de gestion de supports, de gestion des règles d'accès…) ;
- l'architecture générale (exigences en matière de topologie, qu'elle soit centralisée, répartie, distribuée, ou de type client-serveur, d'architecture physique…) ;
- les logiciels applicatifs (exigences en matière de conception des logiciels spécifiques, de standards du marché…) ;
- les progiciels (exigences de standards, de niveau d'évaluation, qualité, conformité aux normes, sécurité…) ;
- les matériels (exigences en matière de standards, qualité, conformité aux normes…) ;
- les réseaux de communication (exigences en matière de couverture, de standards, de capacité, de fiabilité…) ;
- les infrastructures immobilières (exigences en matière de génie civil, construction des bâtiments, courants forts, courants faibles…).

Contraintes financières

La mise en place de mesures de sécurité est souvent limitée par le budget que l'organisme peut y consacrer, néanmoins la contrainte financière est à prendre en compte en dernier lieu (la part du budget allouée à la sécurité pouvant être négociée en fonction de l'étude de sécurité).

Contraintes d'environnement

Les contraintes d'environnement proviennent de l'environnement géographique ou économique dans lequel le SI est implanté : pays, climat, risques naturels, situation géographique, conjoncture économique…

Contraintes de temps

Le temps nécessaire à la mise en place de mesures de sécurité doit être mis en rapport avec l'évolutivité du SI ; en effet, si le temps d'implémentation est très long, la parade peut ne pas être en rapport avec les risques qui auront évolués. Le temps est déterminant dans le choix des solutions et des priorités.

Contraintes relatives aux méthodes

Compte tenu des savoir-faire et des habitudes dans l'organisme, certaines méthodes (au niveau de la planification du projet, des spécifications et du développement…) seront imposées.
Sur la base des éléments relevés, un ensemble d'hypothèses organisationnelles en sera déduit et répertorié.

Contraintes organisationnelles

Voici quelques pistes de réflexion :

- l'exploitation (exigences en matière de délais, de fourniture de résultats, de services, exigences de surveillance, de suivi, de plans de secours, fonctionnement en mode dégradé…) ;
- la maintenance (exigences d'actions de diagnostic d'incidents, de prévention, de correction rapide…) ;
- la gestion des ressources humaines (exigences en matière de formation des opérationnels et des utilisateurs, de qualification pour l'occupation des postes tels qu'administrateur système ou administrateur de données…) ;
- la gestion administrative (exigences en matière de responsabilités des acteurs…) ;
- la gestion des développements (exigences en matière d'outils de développement, AGL, de plans de recette, d'organisation à mettre en place…) ;
- la gestion des relations externes (exigences en matière d'organisation des relations tierces, en matière de contrats…).

Lister les références réglementaires spécifiques au système-cible

La prise en compte des lois, règles ou règlements peut limiter le choix de solutions matérielles ou procédures et modifier l'environnement ou les habitudes de travail.

Il convient par conséquent de recenser l'ensemble des références réglementaires applicables au système-cible.

Activité 1.3 – Détermination de la cible de l'étude de sécurité

Lister et décrire les entités du système

Le système-cible se compose d'un assemblage d'entités techniques et non techniques qu'il convient d'identifier et de décrire. Ces entités possèdent des vulnérabilités que des méthodes d'attaque pourront exploiter, portant ainsi atteinte aux éléments essentiels, immatériels, du système-cible (fonctions et informations). Ce sont donc ces entités qu'il faudra sécuriser. Celles-ci peuvent être de différents types.

Les types d'entités sont présentés dans les paragraphes suivants (il est conseillé d'utiliser les types et sous-types d'entités du guide "Outillage pour l'appréciation des risques SSI" pour lister et décrire les entités du système).

Les matériels

Le type matériel est constitué de l'ensemble des éléments physiques d'un système informatique, qu'il s'agisse de supports actifs de traitement de données ou de supports passifs de données.

Les logiciels

Le type logiciel est constitué de l'ensemble des programmes participant au fonctionnement d'un ensemble de traitements de l'information.

Les réseaux

Le type réseau est constitué de l'ensemble des dispositifs de télécommunication permettant l'interconnexion de plusieurs ordinateurs ou composants d'un système d'information physiquement éloignés.

Les personnels

Le type personnel est constitué de l'ensemble des groupes d'individus en relation avec le système d'information.

Les sites

Le type site est constitué de l'ensemble des lieux contenant tout ou une partie du système et les moyens physiques nécessaires à son fonctionnement.

Les organisations

Le type organisation décrit le cadre organisationnel, constitué de l'ensemble des structures de personnels affectés à une tâche et des procédures régissant ces structures.

Les systèmes (optionnel)

Le type système est constitué de l'ensemble des installations spécifiques liées aux technologies de l'information, avec un objectif particulier et un environnement opérationnel. Il est composé de diverses entités appartenant aux autres types décrits ci-avant. Ce type est utile dans le cas d'une analyse macroscopique.

Afin d'apporter une meilleure compréhension de ce type d'entité, prenons l'exemple de la mise en réseau de terminaux embarqués permettant la consultation de bases de données de véhicules dans le cadre d'opérations de surveillance.

Types de matériels :

- *terminal embarqué dans véhicule terrestre, de type micro-ordinateur portable compatible PC exploitant une mini base de données ;*
- *système serveur central avec frontaux de communications à architecture modulaire exploitant une base de données nationale.*

Types de logiciels :
- *système d'exploitation du serveur central : grandes capacités de traitement transactionnel ;*
- *système de gestion de base de données relationnelle fonctionnant en mode coopératif à deux niveaux installée sur le serveur national.*

Types de réseaux :
- *réseau national à commutation de paquets X25 (contrainte existante) ;*
- *réseau radio à couverture nationale entre terminaux embarqués et le réseau national X25.*

Types de personnels :
- *personnels de développement et maintenance des applications : personnels internes et assistance externe ;*
- *personnels d'exploitation du centre informatique habilités et spécialisés travaillant sur plateau technique ;*
- *utilisateurs des terminaux embarqués : personnels habilités.*

Types de sites :
- *centre informatique protégé par enceinte et système de vidéosurveillance dans zone géographique non classée dans sites à risques majeurs ;*
- *véhicules automobiles légers répartis sur tout le territoire national.*

Types d'organisations :
- *développement et maintenance en régie ;*
- *procédures de mises à jour des bases locales et centrale faites depuis des brigades spécialisées en postes fixes connectées directement sur le réseau national.*

Les types d'entités peuvent être décomposés en sous-types d'entités dont la description est affinée.

Croiser les éléments essentiels et les entités

Cette tâche permet de mettre en évidence :
- les liens entre les fonctions essentielles et les entités qui contribuent à la réalisation de ces fonctions pour le système-cible,
- les liens entre les informations essentielles et les entités qui concourent au traitement de ces informations pour le système-cible.

Ces liens seront utilisés dans la confrontation des menaces aux besoins. Ils sont représentés par une matrice où figurent les éléments essentiels et les entités sélectionnées. Le lien élément essentiel / entité est matérialisé dans le tableau par une ou plusieurs croix au croisement de l'élément essentiel et des entités concernées par cet élément essentiel.

Exemple de matrice de Éléments essentiels / entités :

Entités / ***Éléments essentiels***	***MATERIELS***				***LOGICIELS***				***RESEAUX***				***PERSONNELS***					***SITES***			***ORGA.***		
	M1	***M2***	***M3***	***M4***	***L1***	***L2***	***L3***	***L4***	***R1***	***R2***	***R3***	***R4***	***P1***	***P2***	***P3***	***P4***	***P5***	***S1***	***S2***	***S4***	***O1***	***O2***	***O3***
Fonction 1	+					+	+	+					+	+	+	+			+			+	+
…	+					+	+	+					+	+	+	+	+	+	+		+		+
Fonction N	+	+			+	+		+	+			+		+	+	+	+	+	+			+	+
Information 1	+		+		+	+		+		+		+		+	+	+	+	+	+			+	+
…	+			+	+	+		+			+	+		+	+	+	+	+	+			+	+
…	+					+	+	+					+	+	+	+			+	+	+	+	+
Information N	+					+	+	+					+	+	+	+	+	+	+	+			+

Étape 2 – Expression des besoins de sécurité

Activité 2.1 – Réalisation des fiches de besoins

Choisir les critères de sécurité à prendre en compte

Les besoins de sécurité associés à des fonctions et informations s'expriment selon des critères de sécurité[2]. Trois critères de sécurité sont incontournables :

- disponibilité (D) : propriété d'accessibilité au moment voulu des éléments essentiels par les utilisateurs autorisés.
  - Pour une fonction : garantie de la continuité des services de traitement ; absence de problèmes liés à des temps de réponse au sens large.
  - Pour une information : garantie de la disponibilité prévue pour l'accès aux données (délais et horaires) ; il n'y a pas de perte totale de l'information ; tant qu'il existe une version archivée de l'information, l'information est considérée comme disponible ; pour étudier la disponibilité d'une information, on suppose l'existence d'une version archivée, et on évalue la disponibilité qui correspond à la fonction d'archivage de cette information.
- intégrité (I) : propriété d'exactitude et de complétude des éléments essentiels.
  - Pour une fonction : assurance de conformité de l'algorithme ou de la mise en œuvre des traitements automatisés ou non par rapport aux spécifications ; absence de résultats incorrects ou incomplets de la fonction.
  - Pour une information : garantie d'exactitude et d'exhaustivité des données vis-à-vis d'erreurs de manipulation ou d'usages non autorisés ; non-altération de l'information.
- confidentialité (C) : propriété des éléments essentiels de n'être accessibles qu'aux utilisateurs autorisés.
  - Pour une fonction : protection des algorithmes décrivant les règles de gestion et les résultats dont la divulgation à un tiers non autorisé porterait préjudice ; absence de divulgation d'un traitement ou mécanisme à caractère confidentiel.
  - Pour une information : protection des données dont l'accès ou l'usage par des tiers non autorisés porterait préjudice ; absence de divulgation de données à caractère confidentiel.

Les besoins peuvent être également exprimés en termes de Preuve (imputabilité), de Contrôle (auditabilité), d'Anonymat ou tout autre critère de sécurité dont l'atteinte pour une fonction ou une information peut mettre en péril les enjeux du système :

- preuve, contrôle : garantie de ne pas pouvoir réfuter l'émission ou la réception d'une information, avec possibilité de pouvoir auditer les résultats fournis (exemple : un virement de fonds et la vérification du journal comptable à partir des informations d'entrée).
- anonymat : disposition par laquelle toute personne créant une information (un vote par exemple) et / ou effectuant une action (un appel téléphonique par exemple) qui fait l'objet d'un traitement informatique, ne puisse pas être identifiée.
- fiabilité : propriété de cohérence entre un comportement attendu et un résultat.
- …

Déterminer l'échelle de besoins

Les besoins de sécurité devront s'exprimer pour chaque critère de sécurité sélectionné. Une graduation des besoins de sécurité doit être élaborée sous la forme de niveaux de besoins. Pour cela, une définition doit être formulée pour chaque niveau de besoins de chaque critère de sécurité.
L'échelle présente généralement des niveaux entre 0 (aucune atteinte) et 4 (atteinte très importante).
Il est néanmoins envisageable de définir une échelle comprenant un nombre de niveaux différent.
Il est préférable que le nombre de niveaux soit le même pour chaque critère de sécurité.
Dans la mesure du possible, les valeurs de références doivent être explicites et comprendre un ensemble de valeurs bornées.

Ce travail est généralement réalisé dans un tableau à double entrée, avec les critères de sécurité en colonnes et les niveaux en lignes, les définitions devant être indiquées à chaque intersection.

[2] partiellement d'après le livre blanc sur la sécurité des systèmes d'information dans les établissements de crédit

Le tableau ci-dessous présente un exemple d'échelle pour les critères de sécurité disponibilité, d'intégrité et confidentialité, et une échelle à 5 niveaux.

Besoins de sécurité	***Disponibilité***	***Intégrité***	***Confidentialité***
0	*Aucun besoin de disponibilité*	*Aucun besoin d'intégrité*	*Public*
1	*Long terme (à préciser)*	*[valeur non utilisée]*	*Restreint*
2	*Moyen terme (à préciser)*	*Besoin moyen d'intégrité*	*Confidentiel (partenaires)*
3	*Court terme (à préciser)*	*[valeur non utilisée]*	*Confidentiel (interne)*
4	*Très court terme (à préciser)*	*Parfaitement intègre*	*Secret*

Cette échelle doit être adaptée au contexte de l'étude avec la participation des personnes qui vont déterminer les besoins. Ainsi, chaque valeur aura une réelle signification pour eux et les valeurs seront cohérentes.

Déterminer les impacts pertinents

Les conséquences de la réalisation d'un sinistre peuvent être appréciées selon différents points de vue. Les impacts significatifs pour l'organisme doivent être identifiés par le responsable utilisateur. Ils permettront d'envisager différents domaines pouvant être impactés et d'apporter des éléments de justification des besoins de sécurité.

Ces impacts peuvent être choisis parmi ceux proposés ci-dessous, bien que la liste ne soit pas exhaustive et qu'il soit nécessaire de l'adapter au contexte étudié :

- interruption de service :
  - incapacité à fournir le service ;
- perte d'image de marque :
  - perte de crédibilité de l'informatique en interne,
  - perte de notoriété ;
- perturbation du fonctionnement interne :
  - gêne pour l'organisme lui-même,
  - charges internes supplémentaires ;
- perturbation de fonctionnement de tiers :
  - gêne pour les tiers avec lesquels l'organisme est en relation,
  - préjudices divers ;
- infraction aux lois, aux règlements :
  - impossibilité de remplir les obligations légales ;
- infraction contractuelle :
  - impossibilité de remplir les obligations contractuelles ;
- atteinte à la sécurité du personnel, des usagers :
  - danger pour les personnels et / ou les usagers de l'organisme ;
- atteinte à la vie privée des usagers ;
- pertes financières ;
- frais financiers de secours et de remise à niveau :
  - en personnels,
  - en matériels,
  - en études, expertises ;
- perte de biens, de fonds, de valeurs ;
- perte de clientèles, perte de fournisseurs ;
- poursuites judiciaires et pénalités ;
- perte d'un avantage concurrentiel ;
- perte d'avance technologique, technique ;
- perte d'efficacité, de confiance ;
- perte de réputation technique ;
- affaiblissement de la capacité de négociation ;
- crise sociale (grèves) ;
- crise gouvernementale ;

- limogeage personnel ;
- dommages matériels ;
- ...

Ces impacts sont proposés à titre indicatif, le groupe de travail doit proposer les plus significatifs pour l'organisme et les adapter précisément à l'organisme. Les résultats des activités précédentes, notamment ceux liés à l'étude de l'organisme, aux enjeux, et au contexte du système pourront être utilisés pour le choix de ces impacts. On retiendra la remise en cause des missions, du métier ou des valeurs de l'organisme, comme des impacts significatifs. Afin de rendre les impacts plus objectifs, il convient de fournir des exemples explicites de chacun d'eux en termes de conséquences envisageables.

Une fois les critères de sécurité et les impacts déterminés, il est possible de réaliser les fiches d'expression des besoins de sécurité pour chaque élément essentiel.

Fiche d'expression des besoins de sécurité :

Nom de l'élément essentiel	***Impact 1***	***…***	***Impact n***	***Besoins de sécurité***	***Commentaires***
Critère de sécurité 1	*B11*	*…*	*B1n*	*f(B11…B1n)*	
…	*…*	*…*	*…*	*…*	
Critère de sécurité n	*Bn1*	*…*	*Bnn*	*f(Bn1…Bnn)*	

La synthèse du besoin de sécurité pour chaque élément essentiel et chaque critère de sécurité (colonne "Besoins de sécurité") sera déterminée en fonction de l'ensemble des valeurs exprimées selon les impacts.

Ces fiches peuvent être enrichies de sinistres pour chaque critère de sécurité, afin de faciliter l'expression des besoins de sécurité en envisageant différents points de vue.

Voici quelques exemples de sinistres relatifs aux principaux critères de sécurité (la situation et le contexte devraient conduire à lister des sinistres spécifiques pour chaque critère sélectionné) :

- pour la disponibilité :
  - dégradation des performances,
  - interruption de courte durée,
  - interruption de longue durée,
  - inaccessibilité,
  - perte totale (destruction) ;
- pour l'intégrité :
  - modification accidentelle,
  - modification délibérée,
  - résultats incorrects,
  - résultats incomplets ;
- pour la confidentialité :
  - divulgation interne,
  - divulgation externe.

Fiche d'expression des besoins de sécurité enrichie :

Nom de l'élément sensible	***Sinistres***	***Impact 1***	***…***	***Impact n***	***Besoins de sécurité***	***Commentaires***
Critère de sécurité 1	*Sinistre 1*	*B111*	*…*	*B11n*	*f(B111…B1nn)*	
Critère de sécurité 1	*…*	*…*	*…*	*…*		
Critère de sécurité 1	*Sinistre n*	*B1n1*	*…*	*B1nn*		
…	*…*	*…*	*…*	*…*	*…*	
Critère de sécurité n	*Sinistre 1*	*Bn11*	*…*	*Bn1n*	*f(Bn11…Bnnn)*	
Critère de sécurité n	*…*	*...*	*…*	*...*		
Critère de sécurité n	*Sinistre n*	*Bnn1*	*…*	*Bnnn*		

Dans ce cas, la synthèse du besoin de sécurité pour chaque élément essentiel et chaque critère de sécurité (colonne "Besoins de sécurité") sera déterminée en fonction de l'ensemble des valeurs exprimées selon les impacts et les sinistres.

Activité 2.2 – Synthèse des besoins de sécurité

Attribuer un besoin de sécurité par critère de sécurité à chaque élément essentiel

Pour mener à bien son étude, un groupe de travail hétérogène et représentatif du SI (responsables, informaticiens et utilisateurs) doit être constitué. Celui-ci va pouvoir débattre des besoins de sécurité exprimés et des justifications.

Recueil des besoins de sécurité

Le recueil des besoins de sécurité est réalisé au moyen des fiches d'expression des besoins de sécurité et de l'échelle de besoins remises aux utilisateurs concernés. Les valeurs renseignées reflètent le point de vue des utilisateurs vis-à-vis de leur besoin de sécurité. Ce point de vue pourra être justifié par un commentaire (notamment pour des valeurs extrêmes). Une synthèse au niveau de la fiche doit être effectuée afin d'obtenir un vecteur de besoins de sécurité pour chaque élément essentiel.

Ce sont les utilisateurs eux-mêmes qui devront effectuer cette évaluation en exprimant les valeurs acceptables, un dépassement étant inacceptable. Ils affecteront une note à chaque intersection ligne-colonne des fiches d'expression des besoins afin d'obtenir un vecteur disponibilité – intégrité – confidentialité… Cependant, les utilisateurs du système ne sont pas forcément des experts en sécurité des SI, ni sensibilisés à la SSI. Le groupe de travail ou les personnes qui réaliseront les interviews auprès de cette population ont donc un rôle important à jouer en s'assurant de la bonne compréhension de l'échelle de besoins et en s'assurant de l'homogénéité des résultats obtenus.

Les besoins de sécurité sont indépendants des risques encourus et des moyens de sécurité mis en œuvre. Ils représentent donc une valeur intrinsèque de la sensibilité des informations, des fonctions ou des sous-fonctions. Par exemple, dans le domaine de la défense, attribuer une valeur de confidentialité à des documents consiste à les classifier (secret défense, confidentiel défense...).

Si un élément essentiel a des besoins qui varient dans le temps, il convient d'étudier séparément ses différents états comme s'il s'agissait d'autant d'éléments essentiels.

Il est souhaitable de renseigner l'ensemble des fiches d'expression des besoins de sécurité si l'on veut obtenir des risques dont la formulation est précise quant à leur impact.

Synthèse des besoins de sécurité

Le groupe de travail renseigne les résultats obtenus auprès des utilisateurs sur la fiche de synthèse des besoins de sécurité et détermine la valeur considérée comme la synthèse. Cette synthèse, harmonisant les différents points de vue, est ensuite validée. Le validateur doit avoir une vision globale des éléments essentiels (par exemple par le responsable utilisateur, ou plus généralement le propriétaire des éléments essentiels). Un consensus peut être obtenu par expression des argumentaires de chacun et arbitrage. En dernier recours, on peut considérer que la synthèse du besoin de sécurité, selon les critères de sécurité d'un élément essentiel est le maximum des valeurs attribuées par les utilisateurs dans chacune des fiches.

Dans le cas où des divergences trop importantes apparaîtraient, il peut être nécessaire de demander aux utilisateurs de reconsidérer leurs valeurs ou de les expliciter davantage. La synthèse doit, dans tous les cas, être justifiée par rapport aux éléments importants de l'organisme mis en évidence lors de l'étude du contexte.

Exemple de fiche de synthèse des besoins de sécurité :

Liste des éléments essentiels	***Synthèse des besoins de sécurité***		
	Confidentialité	***Intégrité***	***Disponibilité***
Fonction 1	*0*	*3*	*3*
Fonction 2	*1*	*3*	*2*
…	*…*	*…*	*…*
Fonction n	*0*	*4*	*2*
Information 1	*2*	*1*	*1*

…	…	…	…
Information n	*4*	*3*	*0*

Étape 3 – Étude des menaces

Activité 3.1 – Étude des origines des menaces

Lister les méthodes d'attaque pertinentes

La sélection des méthodes d'attaque consiste, en s'appuyant sur la liste de méthodes d'attaques et éléments menaçants génériques proposée dans le guide "Outillage pour l'appréciation des risques SSI", à retenir celles que l'on considère comme pertinentes, par rapport au contexte, aux missions et aux entités qui composent le système-cible. Elle s'effectue avec le groupe de travail à partir d'une liste de méthodes d'attaque relatives à des thèmes. Ces thèmes sont :

- sinistres physiques
- événements naturels
- perte de services essentiels
- perturbations dues aux rayonnements
- compromission des informations
- défaillances techniques
- actions illicites
- compromission des fonctions

Ce classement permet de sélectionner plus facilement les méthodes d'attaque concernées. Certains thèmes (sinistres physiques, événements naturels, perte de services essentiels) peuvent être écartés à condition de le justifier. Par exemple, il se peut que des études antérieures aient déjà traité le sujet.

Une méthode d'attaque doit être retenue si son accomplissement est réaliste et si on peut supposer qu'elle aura un impact.

Il est recommandé de justifier la non-sélection d'une méthode d'attaque ou d'un thème, afin de garder une trace des choix effectués. Pour que la traçabilité des choix effectués soit la plus claire possible, il est possible de transformer toutes les méthodes d'attaque non retenues en hypothèses (sachant que plusieurs méthodes d'attaques non retenues peuvent être regroupées dans une seule hypothèse).

Les méthodes d'attaque proposées dans les bases de connaissances sont dites génériques, parce qu'elles définissent une catégorie dans laquelle peuvent entrer des méthodes d'attaque décrites dans un degré de granularité beaucoup plus fin. La liste proposée peut donc prétendre à l'exhaustivité dans la mesure où il est toujours possible de faire entrer une méthode d'attaque précise dans une catégorie proposée. Cependant, cette liste peut être adaptée au contexte de l'organisme et de celui d'utilisation du système-cible.

Des méthodes d'attaque peuvent être également obtenues à partir d'études de sécurité effectuées sur les systèmes voisins ou issues de documents de portée générale (politique de sécurité, charte de sécurité).

Caractériser les méthodes d'attaque par les critères de sécurité qu'elles peuvent affecter

Chaque méthode d'attaque peut affecter au moins un critère de sécurité (disponibilité, intégrité, confidentialité…).
Il convient donc de caractériser toutes les méthodes d'attaque retenues par les critères de sécurité qu'elles peuvent toucher. Cette caractérisation consiste à déterminer les impacts directs sur les critères de sécurité, et non toutes les possibilités induites.
Exemple : l'incendie affecte en premier lieu le critère de disponibilité, bien qu'il puisse aussi affecter l'intégrité et la confidentialité par voie de conséquence ; on caractérisera donc généralement l'incendie par une atteinte à la disponibilité.
La caractérisation de chaque méthode d'attaque par les critères de sécurité (identiques à ceux qui ont permis l'expression de besoins de sécurité) permettra lors d'une étape suivante de pouvoir confronter aisément les besoins de sécurité aux menaces afin de déterminer les risques réels.

Caractériser les éléments menaçants associés par leur type et leurs causes

Les méthodes d'attaque sont employées par des éléments menaçants qu'il convient de caractériser pour chaque méthode d'attaque. Doivent être décrits :

- le type d'élément menaçant (naturel, humain ou environnemental, c'est-à-dire externe au système-cible),
- les causes de chaque élément menaçant (accidentelle ou délibérée) ; elles peuvent être affinées en précisant l'exposition et les ressources disponibles dans le cas d'une cause accidentelle et en précisant l'expertise, les ressources disponibles et la motivation dans le cas d'une cause délibérée.

Il est conseillé d'utiliser la partie relative aux méthodes d'attaque et éléments menaçants génériques du guide "Outillage pour l'appréciation des risques SSI" pour caractériser les éléments menaçants.

La typologie des menaces proposée dans l'[IGI 900] et la [Rec 901] peut également être appliquée. L'origine ludique, avide, stratégique ou terroriste peut donc être précisée.

Ajouter une valeur représentant le potentiel d'attaque de l'élément menaçant

La caractérisation des éléments menaçants peut être synthétisée par une valeur unique pour chaque méthode d'attaque retenue : il s'agit du potentiel d'attaque, généralement égale à l'une des valeurs suivantes :

- 1 (accidentel et aléatoire),
- 2 (opportunités ou ressources limitées),
- 3 (haut degré d'expertise, d'opportunité et de ressources).

Ce potentiel d'attaque permettra de déterminer un niveau de résistance adéquat pour les objectifs de sécurité.

Le tableau suivant présente un exemple de sélection et de caractérisation de méthodes d'attaque :

		Éléments menaçants						***Critères de sécurité touchés***		
		Type			***Cause***					
	Méthodes d'attaque	***Naturel***	***Humain***	***Environnemental***	***Accidentelle***	***Délibérée***	***Potentiel d'attaque***	***Disponibilité***	***Intégrité***	***Confidentialité***
1	*Incendie*	+	+	+	+	+	*2*	+	+	
13	*Perte des moyens de télécommunications*			+	+	+	*1*	+		
19	*Écoute passive*		+	+		+	*2*			+
20	*Vol de supports ou de documents*			+		+	*2*			+
21	*Vol de matériels*			+		+	*1*	+		+
23	*Divulgation*		+	+	+	+	*1*			+
26	*Piégeage du logiciel*			+		+	*1*	+	+	+
42	*Atteinte à la disponibilité du personnel*	+	+	+	+	+	*1*	+		

Mettre en évidence les méthodes d'attaque non retenues avec des justifications

Il convient de justifier dûment l'écartement de toute méthode d'attaque. Qu'elle soit jugée improbable, jugée sans conséquence, traitée par ailleurs ou volontairement écartée, il est important d'expliquer pourquoi elle n'est pas retenue, car elle ne sera pas étudiée dans la suite de l'étude bien qu'elle puisse être à l'origine de risques pour l'organisme.

Activité 3.2 – Étude des vulnérabilités

Identifier les vulnérabilités des entités selon les méthodes d'attaque

Pour chaque méthode d'attaque retenue, il convient de déterminer les vulnérabilités du système-cible qui en permettent la réalisation (il est conseillé d'utiliser les vulnérabilités génériques du guide "Outillage pour l'appréciation des risques SSI" pour identifier les vulnérabilités selon les types ou sous-types d'entités et les méthodes d'attaque).

Une vulnérabilité est une caractéristique du système qui pourrait être exploitée par un élément menaçant et permettre alors la réalisation d'une méthode d'attaque. Cette caractéristique, attachée aux entités du système, peut constituer une faiblesse ou une faille au regard de la sécurité.
Exemples :

- *pour une entité de type matériel, la capacité à émettre des rayonnements ou l'attrait du matériel (ordinateur portable) constitue une caractéristique ;*
- *pour une entité de type site, la facilité avec laquelle on peut y pénétrer constitue également une caractéristique.*

Ces caractéristiques deviennent des vulnérabilités si des méthodes d'attaque peuvent les exploiter :

- *l'utilisation d'ordinateurs portables est une vulnérabilité face à la méthode d'attaque vol de matériels ;*
- *la capacité à émettre des rayonnements est une vulnérabilité face à la méthode d'attaque interception de signaux parasites compromettants.*

Une méthode d'attaque peut exploiter plusieurs vulnérabilités pour se réaliser.
Exemple : La méthode d'attaque piégeage du matériel peut se réaliser si :

- *il est facile de pénétrer dans le site (vulnérabilité du type d'entités site) ;*
- *le matériel permet la pose d'éléments additionnels (vulnérabilité des types d'entités matériels et logiciels) ;*
- *il n'y a pas de plan de contrôle des matériels (entité de type organisation).*

Une liste de vulnérabilités génériques associées à chaque méthode d'attaque et à chaque sous-type d'entités est fournie dans les bases de connaissances. La sélection s'effectue à partir de cette liste mais peut s'appuyer sur des éléments particuliers au système. Il est important de noter que la liste proposée est une base de réflexion personnalisable qui devra être adaptée au contexte étudié. Cette liste est par nature continuellement évolutive.

Estimer éventuellement le niveau des vulnérabilités

Les vulnérabilités peuvent être caractérisées par leur niveau, représentant la possibilité de réalisation des méthodes d'attaque qui les exploitent.

Ce niveau s'apprécie en fonction de plusieurs critères :

- du contexte propre au système ;
- de l'état de l'art dans le domaine considéré.

Dans beaucoup de cas, il n'existe pas de données statistiques permettant d'élaborer des lois de comportement du système d'information. Seuls les risques naturels et technologiques disposent de chiffres qui rendent possible une évaluation à l'aide de techniques quantitatives, mais il faut souligner que ces analyses sont par nature subjectives.

Estimer le niveau des vulnérabilités a pour objectif de ne garder que les vulnérabilités pertinentes et les hiérarchiser. On peut se contenter de les sélectionner, mais l'estimation de cette valeur permet d'obtenir un degré de finesse supplémentaire.

Pour cela, il est possible d'utiliser l'échelle suivante :

0	*totalement improbable ou infaisable*
1	*faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré*
2	*moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique*
3	*fortement probable ou réalisable avec des moyens standards et/ou avec des connaissances de base*
4	*certain ou réalisable par tout public*

Dans le cas de méthodes d'attaque naturelles ou humaines, l'estimation du niveau des vulnérabilités est basée sur leur faisabilité effective observée. Dans le cas de la malveillance, l'estimation du niveau des vulnérabilités est plutôt basée sur la faisabilité en termes de moyens, de compétences et de connaissances nécessaires.

On obtient la liste des vulnérabilités estimées associées aux méthodes d'attaque retenues par types ou sous-types d'entité.

Le tableau suivant propose un exemple du résultat.

Méthodes d'attaque		*Vulnérabilités*	*Matériel et logiciel*	*Réseaux internes*	*Réseaux externes*	*Site*	*Personnel*	*Organisation*
1	*Incendie*	*Manque de cohérence des mesures incendie avec le système informatique*				*2*		
		Absence de consignes (alerte, prévention, formation…)						*2*
		Absence d'organisation sécurité incendie						*3*
13	*Perte des moyens de télécommunications*	*Défauts d'exploitation du réseau téléphonique interne*				*1*		
		Dysfonctionnement des réseaux externes (RTC)			*1*			
		Dysfonctionnement des réseaux externes (services réseaux)			*1*			
…	…	…	…	…	…	…	…	…

Activité 3.3 – Formalisation des menaces

Formuler explicitement les menaces

La formulation des menaces peut être plus ou moins riche. Il s'agit avant tout d'exprimer explicitement un scénario d'attaque, le niveau de détail pouvant varier selon la finalité de l'étude.

Dans le meilleur des cas, la formulation de la menace comporte :
- l'élément menaçant avec ses caractéristiques, notamment son potentiel d'attaque,
- la méthode d'attaque employée par l'élément menaçant et les critères de sécurité touchés,
- les vulnérabilités exploitées avec leur niveau,
- les entités qui présentent ces vulnérabilités.

Les menaces peuvent être caractérisées par une valeur d'opportunité déterminée selon le niveau des vulnérabilités exploitées.
Bien que les valeurs d'opportunité puissent être subjectives, leur intérêt réside dans le fait qu'elles soient relatives les une par rapport aux autres.
Si une menace comporte l'exploitation d'une seule vulnérabilité, l'opportunité de la menace est égale au niveau de la vulnérabilité.
Si une menace comporte l'exploitation de plusieurs vulnérabilités, il convient de déterminer l'opportunité de la menace d'après les niveaux respectifs des vulnérabilités :
- généralement en reconsidérant l'opportunité de la menace,
- soit en retenant le plus faible niveau des vulnérabilités dans le cas où la menace ne se réalise qu'en exploitant l'ensemble des vulnérabilités,
- soit en retenant le plus fort niveau des vulnérabilités dans le cas où la menace peut se réaliser en n'exploitant qu'une des vulnérabilités.

Exemple :

Menaces		*Méthode d'attaque*	*Potentiel d'attaque*	*D*	*I*	*C*	*Opportunité*
M.INCENDIE	*Aggravation des conséquences d'un incendie à cause du manque de cohérence des mesures incendie avec le système informatique (site du cabinet d'études), de l'absence de consignes ou d'organisation sécurité incendie (organisation du cabinet d'études)*	*1*	*2*	*+*			*2*
M.TELECOM	*Perte des moyens de télécommunications à cause d'un dysfonctionnement des réseaux externes (Internet)*	*12*	*1*	*+*			*1*
M.VOL-DOC	*Vol de supports ou de documents par une personne en visite ou un personnel de nettoyage du fait de la facilité de pénétrer dans les locaux pendant les heures ouvrables (site du cabinet d'études)*	*19*	*2*			*+*	*3*
…	…	…	…	…	…	…	…

Hiérarchiser éventuellement les menaces selon leur opportunité

La liste des menaces résultante peut être triée par ordre décroissant d'opportunité des menaces. Cette liste est un outil de communication auquel il convient d'apporter une grande attention. Elle permet en effet d'exprimer le plus explicitement possible ce à quoi l'organisme est exposé. Les menaces dont l'opportunité est importante devraient donc apparaître en premier dans la liste afin de sensibiliser les acteurs efficacement.

Étape 4 – Identification des objectifs de sécurité

Activité 4.1 – Confrontation des menaces aux besoins

Déterminer les risques en confrontant menaces et besoins de sécurité

La détermination des risques auxquels l'organisme est confronté consiste à mettre en évidence la manière dont les éléments essentiels peuvent être touchés par les menaces, c'est-à-dire à déterminer comment ce à quoi l'organisme tient peut être affecté par ce à quoi il est exposé.

Cette association est réalisée en confrontant les menaces aux besoins. D'un côté, les besoins de sécurité des éléments essentiels ont été exprimés selon différents critères de sécurité (disponibilité, intégrité, confidentialité…). D'un autre côté, les menaces ont été caractérisées par les critères de sécurité qu'elles peuvent affecter (d'après la caractérisation des méthodes d'attaque et selon les mêmes critères de sécurité). Il est donc possible de confronter chaque élément essentiel avec chaque menace selon les critères de sécurité afin de déterminer les conséquences possibles de la réalisation des menaces.

Pour chaque élément essentiel, un tableau listant les méthodes d'attaque est réalisé. Les méthodes d'attaque retenues à ce stade de l'étude ne sont uniquement celles susceptibles d'exploiter des vulnérabilités de l'élément essentiel (on effectue cette vérification à l'aide des tableaux des relations entités / éléments établis lors de l'étude du contexte). Les besoins de sécurité de l'élément essentiel étudié et les critères de sécurité qui peuvent être affectés par chaque méthode d'attaque retenue sont alors reportés.

Les fiches peuvent être réalisées par méthode d'attaque ou affinées par menace, mais les renseignements utiles sont les critères de sécurité affectés par les méthodes d'attaque. Ils sont donc reportés à chaque menace correspondante. Il est possible de faire figurer les menaces à la place des méthodes d'attaque, mais ce sont les atteintes des méthodes d'attaque qui sont confrontées aux besoins, c'est pourquoi on factorise généralement cette opération avec les méthodes d'attaque.

On applique alors les règles suivantes pour chaque critère de sécurité :

- si un critère de sécurité ne peut pas être affecté, alors les besoins de sécurité concernés sont nuls ;
- si un critère de sécurité peut être affecté, alors les besoins de sécurité concernés sont égaux aux besoins de sécurité de l'élément considéré.

Exemple :

I.VISU (Visualisation)		*Besoins de sécurité:*			*D*	*I*	*C*
					2	*2*	*0*
Méthodes d'attaque		*Atteinte*			***Besoins de sécurité concernés***		
		D	*I*	*C*	***D***	***I***	***C***
1	*Incendie*	+	+		*2*	*2*	
13	*Perte des moyens de télécommunications*	+			*2*		
19	*Écoute passive*			+			
20	*Vol de supports ou de documents*			+			
21	*Vol de matériels*	+		+	*2*		
23	*Divulgation externe*			+			
26	*Piégeage du logiciel*	+	+	+	*2*	*2*	
42	*Atteinte à la disponibilité du personnel*	+			*2*		
…	…	…	…	…	…	…	…

Les valeurs résultantes représentent le risque pour l'organisme car elles intègrent la valeur du besoin.

Nous cherchons en fait à déterminer les risques d'atteinte des besoins de sécurité des éléments essentiels. Si une menace se concrétise, elle est en effet susceptible de porter atteinte à ces besoins et aux impacts majeurs identifiés et utilisés pour les établir.

L'ensemble des tableaux peut alors être synthétisé afin d'avoir une vision globale des risques. Cette synthèse peut être réalisée à l'aide des méthodes d'attaque ou des menaces. Par l'intermédiaire de cette synthèse, la réflexion est menée sur l'impact réel des menaces sur les éléments essentiels, et donc sur l'organisme.

Exemple de synthèse des risques en fonction des méthodes d'attaque :

Synthèse des risques				*Élément 1*			…			*Élément N*		
				D	*I*	*C*	*D*	*I*	*C*	*D*	*I*	*C*
				3	*2*	*0*	…	…	…	*0*	*1*	*0*
				Besoins de sécurité concernés								
Méthodes d'attaque	*D*	*I*	*C*	*D*	*I*	*C*	*D*	*I*	*C*	*D*	*I*	*C*
Écoute passive			*X*	*0*	*0*	*0*	…	…	…	*0*	*0*	*0*
Vol de matériels	*X*		*X*	*3*	*0*	*0*	…	…	…	*0*	*0*	*0*
…	…	…	…	…	…	…	…	…	…	…	…	…

Il est possible de déterminer les valeurs maximales des besoins de sécurité concernés par menace ou méthode d'attaque. Ceci constituera un élément de hiérarchisation des risques.

Formuler explicitement les risques

En utilisant le tableau de synthèse des risques, la formulation des menaces et éventuellement l'échelle de besoins, il convient de rédiger le libellé des risques le plus explicitement possible. La finesse de la formulation dépend de la granularité souhaitée.

Dans le meilleur des cas, la formulation d'un risque comporte :
- l'élément menaçant avec ses caractéristiques, notamment son potentiel d'attaque,
- la méthode d'attaque employée par l'élément menaçant,
- les vulnérabilités exploitées,
- les entités qui présentent ces vulnérabilités,
- l'opportunité de la menace,
- les principaux besoins de sécurité concernés,
- les impacts sur l'organisme (d'après l'échelle de besoins).

Exemple :

Risques		*Maximum des besoins de sécurité concernés*	*Opportunité de la menace*	*Potentiel d'attaque*
R.PIEGEAGE	*Un intrus piége le logiciel du fait de la modification des commandes système, de l'implantation de programmes pirates, de la modification d'un applicatif (matériels, logiciels et Internet) ou d'une action sur les logiciels des ressources du système (Internet), portant ainsi atteinte à la confidentialité d'informations sensibles (devis, dossier de contentieux…) et à l'intégrité d'éléments essentiels (calculer les structures, devis, plan technique, paramètres techniques, dossier de contentieux…)*	*4*	*3*	*1*
R.VOL-VISITEUR	*Du fait de la facilité de pénétrer dans les locaux (site du cabinet d'études), une personne en visite ou un personnel de nettoyage vole un matériel reconnu comme particulièrement attractifs (valeurs marchande, technologique de la plupart des matériels, logiciels et éléments de réseaux) portant ainsi atteinte à la disponibilité de plusieurs éléments essentiels et à la confidentialité d'informations sensibles (devis, dossier de contentieux…)*	*2*	*1*	*1*
…	…	…	…	…

Hiérarchiser les risques selon l'impact sur les éléments essentiels et l'opportunité des menaces

La liste des risques résultante peut être triée par ordre décroissant des valeurs maximales des besoins de sécurité concernés et par ordre décroissant d'opportunité des menaces concernées. Cette liste est un outil de communication auquel il convient d'apporter une grande attention. Elle permet en effet d'exprimer le plus explicitement possible les risques réels pesant sur l'organisme. Les risques pouvant affecter les besoins de sécurité les plus grands et dont l'opportunité des menaces est importante devraient donc apparaître en premier dans la liste afin de sensibiliser les acteurs efficacement. Ceci permettra de les traiter de manière prioritaire.

Un autre moyen pour hiérarchiser les risques tout en obtenant l'adhésion des participants est de leur faire hiérarchiser les risques. En effet, ce sont eux qui prendront la décision de considérer ou non chaque risque et de le traiter. Il est donc important qu'ils soient impliqués à ce niveau de l'étude.

Il est aussi possible de proposer une hiérarchisation des risques selon la première méthode et de la revoir avec la seconde méthode.

Mettre en évidence les risques non retenus avec des justifications

Le groupe de travail peut suggérer d'écarter les risques qui n'affectent que peu de besoins de sécurité et dont l'opportunité des menaces est faible. Il convient alors de mettre ces risques en évidence et de justifier dûment leur rejet car ils constituent des risques résiduels pour l'organisme.

Activité 4.2 – Formalisation des objectifs de sécurité

Lister les objectifs de sécurité

Les objectifs de sécurité doivent couvrir la totalité des risques qu'il a été décidé de couvrir, tout en prenant en compte les hypothèses, les règles de sécurité et les différents éléments du contexte (les contraintes et enjeux notamment). Ils doivent être cohérents avec l'objectif opérationnel ou l'objectif "produit" déclaré du système-cible et toute connaissance sur son environnement physique.

Les objectifs de sécurité consistent généralement en l'expression de la volonté de couvrir les risques par la maîtrise d'ouvrage, sans préciser les solutions pour y parvenir.
Ils constitueront ainsi un cahier des charges complet, ouvert (ne préjugeant pas des solutions à adopter) et parfaitement adapté à la problématique de l'organisme.

Les composantes du risque que les objectifs de sécurité peuvent traiter sont les suivantes :
- l'origine des menaces (éléments menaçants et méthodes d'attaque),
- les vulnérabilités exploitées (il est possible d'utiliser les objectifs de sécurité génériques et le tableau de détermination des objectifs et exigences de sécurité du guide "Outillage pour le traitement des risques SSI" pour lister les objectifs de sécurité couvrant les vulnérabilités),
- les conséquences (éléments essentiels touchés et impacts sur l'organisme).

Il est proposé d'adopter la nomenclature suivante pour les objectifs de sécurité : O.xx (O pour Objectif technique et xx étant le nom de l'objectif de sécurité).

Exemples :

O.INC-ORIGINE	*Des mesures doivent être prises pour éviter la naissance d'un incendie*
O.INC-CSQ	*Des mesures doivent être prises pour réduire l'effet d'un incendie sur les éléments essentiels et en termes de pertes financières*
O.INC-COHERENCE	*Le site du cabinet d'études doit disposer de mesures incendie cohérentes avec le système informatique*
O.INC-ORGA	*L'organisation du cabinet d'études doit comprendre des consignes et une organisation sécurité incendie*
O.TELECOM-ORIGINE	*Des mesures doivent être prises pour éviter les dysfonctionnements des réseaux externes*
O.TELECOM-CSQ	*Des mesures doivent être prises pour réduire l'effet des dysfonctionnements des réseaux externes sur les éléments essentiels et en termes de perturbation du fonctionnement interne*
O.TELECOM	*Les dysfonctionnements des réseaux externes ne doivent pas gêner l'utilisation de Internet par les utilisateurs du cabinet d'études*

Justifier la complétude de la couverture

Les objectifs de sécurité déterminés précédemment ont pour but de contrer ou minimiser les risques pesant sur le système-cible et de prendre en compte les hypothèses et règles de sécurité.
Les personnes réalisant l'étude vont maintenant devoir s'assurer qu'ils sont nécessaires et suffisants pour couvrir l'ensemble des risques, hypothèses et règles de sécurité identifiés.

Une première justification consiste à démontrer que les objectifs de sécurité :
- couvrent suffisamment tous les risques,
- couvrent les règles de sécurité (et les références réglementaires),
- sont pertinents vis-à-vis des hypothèses (et les enjeux du système-cible).

Il convient pour chaque objectif de sécurité de vérifier la compatibilité avec les contraintes pesant sur l'organisme et sur le système-cible.

La couverture peut être synthétisée par une valeur selon l'échelle suivante :

0	Aucune couverture
1	Couverture partielle
2	Couverture complète

Exemple :

Risques	*Objectifs de sécurité*	*Justification de la couverture*	*Couverture*	*Potentiel d'attaque*
R.PIEGEAGE	*O.SYS-COMMANDES* *O.SYS-ACTIONS*	*Les deux objectifs de sécurité couvrent l'ensemble des vulnérabilités exploitées dans le risque :* *- possibilité de modifier les commandes systèmes via Internet,* *- possibilité d'implanter des programmes pirates via Internet,* *- possibilité de modifier un applicatif via Internet,* *- possibilité d'agir sur les logiciels des ressources du système via Internet.*	*2*	*1*
R.VOL-VISITEUR	*O.LOCAUX* *O.VOL-PROTECTION* *O.PRISE-EN-CHARGE* *O.AUTH-DOC*	*Les deux premiers objectifs de sécurité couvrent les vulnérabilités exploitées dans le risque :* *- facilité de pénétrer dans le cabinet d'études,* *- matériel reconnu comme particulièrement attractifs (valeurs marchande et technologique).* *Le troisième objectif de sécurité améliore la réduction du risque en responsabilisant les utilisateurs.* *Le dernier objectif de sécurité offre une garantie d'authentification du rédacteur des documents.*	*2*	*1*
…	…	…	…	…

Une seconde justification consiste à démontrer que chaque objectif de sécurité répond au moins à un risque, une règle de sécurité (ou une référence réglementaire) ou une hypothèse (ou un enjeu du système-cible ou au mode d'exploitation de sécurité).

Exemple :

Objectifs de sécurité	*R.PIEGEAGE*	*R.VOL-VISITEUR*	*R.VOL-RIGUEUR*	*R.VOL-UTIL*	*R.VIRUS-VERIF*	*R.INCENDIE*	*R.VIRUS-MAIL*	*R.PABX*	*R.TELECOM*	*R.MALADIE*	*R.VOL-DOC*	*R.ECOUTE*	*R.PERTE-DOC*	*R.DIVULGATION*
O.INC-COHERENCE						+								
O.INC-ORGA						+								
O.TELECOM									+					
O.ECOUTE												+		
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Classer éventuellement les objectifs de sécurité en deux catégories

La détermination des objectifs de sécurité a pour but de traiter toutes les préoccupations relatives à la sécurité et de déclarer les aspects de sécurité qui sont :

- soit pris en compte directement par le système-cible (ce sont les objectifs de sécurité portant sur le système-cible),
- soit pris en compte par son environnement (ce sont les objectifs de sécurité portant sur l'environnement du système-cible).

Elle est basée sur une analyse des impacts induits sur le développement (crédibilité technique, calendaire…), la politique de sécurité (conformité avec les éléments de politique générale), les facteurs économiques (coûts induits par la prise en compte de mesures techniques ou organisationnelles) et les décisions d'accepter les risques (risques dont l'opportunité des menaces est négligeable ou encore risques pour lesquels des mesures externes, telle que la souscription à des polices d'assurance, peuvent être prises).

Mettre en évidence les défauts de couvertures avec des justifications

Le groupe de travail peut décider de ne pas couvrir parfaitement les risques, règles de sécurité ou hypothèses par les objectifs de sécurité. Il convient alors de le mettre en évidence et de justifier dûment l'incomplétude car ceci introduit des risques résiduels pour l'organisme.

Exemples :

- *Un membre du personnel divulgue des renseignements à un concurrent dans le cadre d'un marché du fait de la facilité d'échanger des informations par le biais des matériels, logiciels et réseaux du cabinet d'études, et porte ainsi atteinte à la confidentialité d'informations sensibles (devis, dossier de contentieux…).*
- *Un membre du personnel divulgue des renseignements à un concurrent dans le cadre d'un marché du fait de l'absence de procédures de contrôle de l'utilisation des outils de communication, et porte ainsi atteinte à la confidentialité d'informations sensibles (devis, dossier de contentieux…).*

Activité 4.3 – Détermination des niveaux de sécurité

Déterminer le niveau de résistance adéquat pour chaque objectif de sécurité

Le niveau de résistance[3] attendu des mesures de sécurité qui satisferont les objectifs de sécurité est essentiellement déterminé en fonction du potentiel d'attaque des éléments menaçants à l'origine des risques pesant sur l'organisme. En effet, le niveau de protection adéquat dépend du niveau de l'attaquant.

Néanmoins, il dépend aussi d'autres facteurs tels que les besoins de sécurité des éléments essentiels qui peuvent être touchés, l'opportunité des menaces, le contexte général…

Nous considérons trois niveaux de résistance, exprimant les efforts minimums supposés nécessaires pour mettre en défaut le comportement de sécurité attendu par attaque directe des mécanismes de sécurité sous-jacents :

1 - Niveau élémentaire	Un niveau de la résistance tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation fortuite de la sécurité du système par des attaquants possédant un potentiel d'attaque faible.
2 - Niveau moyen	Un niveau de la résistance tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation facile à mettre en œuvre ou une violation intentionnelle de la sécurité du système par des attaquants possédant un potentiel d'attaque modéré.
3 - Niveau élevé	Un niveau de la résistance tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation délibérément planifiée ou organisée de la sécurité du système par des attaquants possédant un potentiel d'attaque élevé.

Concernant les objectifs de sécurité couvrant des risques, le niveau requis dépend du potentiel d'attaque. Si un objectif de sécurité couvre plusieurs risques dont les potentiels d'attaque diffèrent, on retient le niveau le plus élevé. Il est nécessaire d'ajuster cette valeur en prenant en compte les besoins de sécurité des éléments essentiels qui peuvent être touchés, l'opportunité des menaces, le contexte général…
Concernant les objectifs de sécurité couvrant les règles de sécurité (ou les références réglementaires), leur niveau est choisi par l'organisme en fonction de l'importance qu'il accorde à celles-ci et des efforts qu'il compte mettre en œuvre pour les faire respecter.

Le niveau de résistance de chaque objectif de sécurité doit être justifié.

Choisir le niveau des exigences d'assurance

Il existe 7 niveaux d'assurance[4] prédéfinis (appelés EAL – *Evaluation Assurance Level*) :

EAL 1	Testé fonctionnellement
EAL 2	Testé structurellement
EAL 3	Testé et vérifié méthodiquement
EAL 4	Conçu, testé et revu méthodiquement

[3] Niveaux issus de la définition des niveaux de résistance des fonctions de l'ISO/IEC 15408.
[4] Le niveau d'assurance représente un paquet de composants d'assurance tirés de la Partie 3 de l'ISO/IEC 15408 qui représente un niveau de l'échelle d'assurance prédéfinie.

EAL 5	Conçu à l'aide de méthode semi-formelles et testé
EAL 6	Conception vérifiée à l'aide de méthodes semi-formelles et testé
EAL 7	Conception vérifiée à l'aide de méthodes formelles et testé

Ces niveaux sont composés de différents composants de rigueur croissante qui permettent d'évaluer la sécurité mise en œuvre.

Le niveau d'assurance EAL représente le niveau de confiance que l'on peut accorder à la mise en œuvre des objectifs de sécurité. Plus précisément, le niveau d'assurance porte sur la mise en œuvre des exigences fonctionnelles de sécurité, qui sont un raffinement des objectifs de sécurité. Plus il est élevé, plus l'organisme disposera de garanties sur celles-ci. Mais il est important de considérer le coût de la mise en œuvre des exigences d'assurance, ainsi que la faisabilité pour l'organisme ou ses fournisseurs.

Il n'existe pas de méthode simple pour déterminer le niveau d'assurance, qui reste davantage un choix financier ou marketing.

Le niveau d'assurance EAL choisi peut éventuellement être augmenté par d'autres composants d'assurance.

Il n'est pas nécessaire de s'appuyer sur un EAL. Il est aussi possible pour l'organisme de définir ses propres exigences d'assurance en choisissant des exigences parmi les composants existants ou même d'en définir de nouveaux.

Les exigences de sécurité d'assurance comprennent en général à la fois des exigences pour la présence de comportements souhaités et pour l'absence de comportements non-souhaités. Il est normalement possible de démontrer, par l'utilisation ou le test, qu'un comportement souhaité est bien présent.
Il n'est, par contre, pas toujours possible d'effectuer une démonstration concluante sur l'absence d'un comportement non-souhaité. C'est pourquoi, les tests et l'examen de la conception et de l'implémentation contribuent de façon significative à la réduction du risque qu'un tel comportement soit présent. Les éléments de l'argumentaire doivent donc étayer l'affirmation qu'un tel comportement non souhaité est absent.

Étape 5 – Détermination des exigences de sécurité

Activité 5.1 – Détermination des exigences de sécurité fonctionnelles

Lister les exigences de sécurité fonctionnelles

Les exigences de sécurité fonctionnelles représentent les moyens d'atteindre les objectifs de sécurité et donc de traiter les risques SSI afférents. Ils doivent être déterminés par ou avec la maîtrise d'œuvre (il est possible d'utiliser les exigences de sécurité fonctionnelles génériques et le tableau de détermination des objectifs et exigences de sécurité du guide "Outillage pour le traitement des risques SSI" pour lister les exigences de sécurité fonctionnelles susceptibles de satisfaire les objectifs de sécurité couvrant les vulnérabilités identifiées).

Pour réduire les risques SSI, le tableau suivant présente, à titre indicatif, les principaux types de mesures de sécurité spécifiées par les exigences de sécurité fonctionnelles en fonction des composantes des risques :

	Composantes principales du risque		
Principaux types de mesures	Vulnérabilités	Origine des menaces (méthodes d'attaque et éléments menaçants)	Conséquences (éléments essentiels et impacts)
Prévision et préparation	X	X	X
Dissuasion		X	
Protection	X		
Détection	X	X	
Confinement		X	X
"Lutte"	X		X
Récupération			X
Restauration			X
Compensation			X

Ce tableau constitue une aide à la détermination des exigences de sécurité fonctionnelles. En effet, il permet de ne pas oublier de considérer les différents types de mesures possibles.

Les exigences fonctionnelles de sécurité contribuent au traitement des risques SSI, qui peut non seulement consister à les réduire, mais aussi à les refuser, les transférer ou les prendre.
Le refus d'un risque sera représenté par des exigences fonctionnelles de sécurité portant sur une modification structurelle de la situation du système-cible de telle sorte qu'il ne soit plus exposé au risque.
Le transfert d'un risque sera représenté par des exigences fonctionnelles de sécurité spécifiques telles que le recours à des contrats d'assurance ou de sous-traitance.
La prise de risque sera représentée par l'absence d'exigence fonctionnelle de sécurité ou la satisfaction incomplète des objectifs de sécurité. Des risques résiduels seront donc identifiés.

Les exigences fonctionnelles sont imposées aux fonctions du système-cible qui supportent tout particulièrement la sécurité des technologies de l'information et qui déterminent le comportement voulu en terme de sécurité, ainsi qu'à l'environnement du système-cible.
Ces exigences fonctionnelles peuvent être issues de l'ISO/IEC 15408 (Critères Communs) ou créées de toute pièce. Il est fortement recommandé de ne créer de toute pièce une exigence fonctionnelle que s'il s'avère qu'elle traite d'un aspect fonctionnel n'existant pas dans les composants de l'ISO/IEC 15408.
La liste d'exigences de sécurité fonctionnelles issues des Critères Communs est composée de classes, familles et composants fonctionnels. Il peut exister des dépendances entre les composants. Ces dépendances apparaissent quand un composant n'est pas autosuffisant et dépend de la présence d'un autre composant. Il peut exister des dépendances entre composants fonctionnels et entre des composants fonctionnels et des composants d'assurance. Selon le niveau de connaissance

sur le système et le niveau d'expertise des acteurs du groupe de travail, les composants peuvent être laissés non-raffinés en précisant toutefois qu'ils seront raffinés par le maître d'œuvre.

L'ISO/IEC 15408 laisse la possibilité de recourir à des exigences fonctionnelles non contenues dans la liste fournie, pour représenter l'ensemble des exigences de sécurité des technologies de l'information. Les consignes suivantes doivent s'appliquer à l'incorporation de ces exigences fonctionnelles étendues :

- toutes les exigences de sécurité fonctionnelles doivent être formulées par référence à des composants d'exigences fonctionnelles. Dans le cas où aucun des composants d'exigences n'est facilement applicable à tout ou partie des exigences de sécurité, le groupe de travail peut formuler ces exigences de façon explicite sans référence à l'ISO/IEC 15408,
- toute exigence fonctionnelle étendue doit être exprimée clairement et sans ambiguïté pour que l'évaluation soit faisable ; le niveau de détail et le mode d'expression des composants fonctionnels existant dans l'ISO/IEC 15408 doivent être utilisés comme modèles,
- les résultats d'évaluation obtenus en utilisant les exigences fonctionnelles étendues doivent le mentionner par un avertissement,
- l'incorporation d'exigences fonctionnelles étendues doit se faire conformément aux classes APE ou ASE de la partie 3 de l'ISO/IEC 15408, quand cela est approprié.

Dans le meilleur des cas, la formulation d'une exigence de sécurité fonctionnelle doit être :

- S – spécifique (un acteur, un domaine à la fois),
- M – mesurable (définition du moyen de contrôle),
- A – atteignable (éventuellement en plusieurs étapes, en donnant les ressources nécessaires),
- R – réaliste (en fonction des acteurs, de leurs capacités),
- T – liée au temps (il y a une date buttoir, un délai, une période définie).

La détermination des exigences de sécurité fonctionnelles nécessite de prendre en compte tous les éléments du contexte, notamment les contraintes budgétaires et techniques.

Exemples :

EF.INC-DETECT	*Les locaux du cabinet d'architecture doivent être équipés d'un système de détection d'incendie muni d'une remontée d'alarme vers une supervision qui pourrait être externalisée. Ces mesures doivent être étudiées et mises en place par des experts du domaine. Elles doivent être testées au moins une fois par an.*
EF.FOURN-ACCES	*Le cabinet d'études doit être abonné chez au moins deux fournisseurs d'accès à Internet distincts.*
EF.MAINTENANCE	*Un contrat de maintenance doit garantir la disponibilité des moyens de communication internes et externes dans un délai conforme aux enjeux du métier du cabinet d'études (12 heures d'indisponibilité).*
EF.CHIFFREMENT	*Les échanges de courriers électroniques doivent être protégés en confidentialité par une solution de chiffrement disponible sur le marché. Les outils utilisant les clés de chiffrement doivent bénéficier d'une politique de gestion de ces clés.*
EF.LOCAUX	*Les personnes extérieures entrant dans la partie « métier » du cabinet d'études doivent être accompagnées.* *Les personnels de maintenance, de nettoyage ou toute autre personne extérieure au cabinet d'études ne doivent pas pénétrer dans les locaux en l'absence des membres du cabinet d'études.* *Les locaux doivent être protégés par des serrures de sécurité dont les clés ne sont détenues que par le Directeur et son adjoint.*
…	…

Justifier la complétude de la couverture des objectifs de sécurité

Une matrice de couverture doit être réalisée afin de s'assurer que tous les objectifs de sécurité portant sur le système-cible ou sur son environnement sont couverts par au moins une exigence de sécurité fonctionnelle. De même, chaque exigence de sécurité fonctionnelle doit couvrir au minimum l'un de ces objectifs de sécurité.

L'argumentaire relatif aux exigences de sécurité doit démontrer que l'ensemble des exigences de sécurité convient pour satisfaire aux objectifs de sécurité et qu'ils sont reliés à ces derniers. Il doit pouvoir être démontré :

- que la combinaison des composants individuels d'exigences fonctionnelles satisfait aux objectifs de sécurité déclarés,
- que l'ensemble des exigences de sécurité constitue un tout ayant une cohérence interne et dont les éléments se soutiennent mutuellement,
- que le niveau de résistance des fonctions choisi, de même que toute résistance de fonction explicite annoncée, est cohérent avec les objectifs de sécurité.

Ainsi, une première justification consiste à démontrer la couverture des objectifs de sécurité.

La couverture peut être synthétisée par une valeur selon l'échelle suivante :

0	Aucune couverture
1	Couverture partielle
2	Couverture complète

Exemple :

Objectifs de sécurité	*Niveaux de résistance*	*Exigences de sécurité fonctionnelles*	*Justification de la couverture*	*Couverture*
O.INC-COHERENCE	*2*	*EF.INC-LUTTE*	*La cohérence des mesures de sécurité incendie avec le système informatique est pleinement considérée par l'exigence de sécurité relative à lutte contre l'incendie.*	*2*
O.PABX	*1*	*EF.MAINTENANCE EF.REPRISE*	***Le dérangement occasionné par un défaut d'exploitation du réseau téléphonique interne (PABX en panne sur le site du cabinet d'études) est réduit par ces exigences de sécurité mais le sinistre peut avoir lieu.***	***1***
O.TELECOM	*1*	*EF.FOURN-ACCES EF.MISES-A-JOUR EF.REPRISE*	*Les dysfonctionnements des réseaux externes sont prévenus par la première exigence de sécurité. Les deux suivantes permettent de diminuer l'indisponibilité.*	*2*
O.ECOUTE	*2*	*EF.CHIFFREMENT*	*Le chiffrement satisfait l'objectif de protection en confidentialité. La rédaction d'une politique de gestion des clés permet d'atteindre le niveau de résistance requis.*	*2*
…	*…*	*…*	*…*	*…*

Une seconde justification consiste à démontrer chaque exigence de sécurité fonctionnelle couvre au moins un objectif de sécurité.

Exemple :

Exigences de sécurité	*O.INC-COHERENCE*	*O.INC-ORGA*	*O.PABX*	*O.TELECOM*	*O.ECOUTE*	*O.LOCAUX*	*O.PERS-SENSIB*	*O.VOL-PROTECTION*	*O.PRISE-EN-CHARGE*	*O.MANIPULATION*	*O.ORGA-SENSIB*	*O.MALICIEUX*	*O.SUPP-CONTRÔLE*	*O.SYS-COMMANDES*	*O.SYS-ACTIONS*	*O.MALADIE*	*O.PSSI*	*O.REGLEMENT*	*O.AUTH-DOC*
EF.INC-DETECT		+																	
EF.INC-LUTTE	+	+																	
EF.INC-CONSIGNES		+																	
EF.INC-ORGA		+																	
EF.MAINTENANCE			+																
EF.FOURN-ACCES				+															
EF.CHIFFREMENT					+														
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Mettre en évidence les éventuels défauts de couverture avec des justifications

L'obtention d'un consensus sur les moyens qui permettront de réaliser les objectifs de sécurité est nécessaire. Ce consensus ne peut être obtenu qu'en comparant les risques encourus au coût des mesures de sécurité correspondant aux exigences de sécurité fonctionnelles envisagées.
Il est raisonnable de considérer d'abord les risques les plus importants et les plus probables, puisque le fait de les traiter peut aboutir occasionnellement à en traiter des moins importants.

Le groupe de travail peut décider de ne pas couvrir parfaitement les objectifs de sécurité par les exigences de sécurité. Il convient alors de le mettre en évidence et de justifier dûment l'incomplétude car ceci introduit des risques résiduels pour l'organisme.

Exemples :

- *Perte des moyens de télécommunications à cause d'un défaut d'exploitation du réseau téléphonique interne (PABX en panne sur le site du cabinet d'études) ; un plan de reprise et une garantie de maintenance sous 12 heures réduisent l'indisponibilité de ces moyens.*
- *Un membre du personnel se fait manipuler, bien qu'il soit sensibilisé, et divulgue des renseignements à un concurrent dans le cadre d'un marché, portant ainsi atteinte à la confidentialité d'informations sensibles (devis, dossier de contentieux…).*
- *Un intrus piége le logiciel du fait d'une action sur les logiciels des ressources du système via Internet, malgré les droits restreints sur les machines connectées, l'usage de firewalls et la mise à jour régulière des logiciels ; ceci peut porter atteinte à la confidentialité d'informations sensibles (devis, dossier de contentieux…) et à l'intégrité d'éléments essentiels (calculer les structures, devis, plan technique, paramètres techniques, dossier de contentieux…).*

Classer les exigences de sécurité fonctionnelles en deux catégories

Les exigences de sécurité résultent du raffinement des objectifs de sécurité en un ensemble :

- d'exigences de sécurité pour le système-cible,
- d'exigences de sécurité pour l'environnement.

Si elles sont satisfaites, elles garantiront que la cible de l'étude de sécurité peut satisfaire à ses objectifs de sécurité.

Justifier éventuellement la couverture des dépendances des exigences de sécurité fonctionnelles

Toutes les dépendances entre exigences de sécurité doivent être satisfaites. Il existe en effet des exigences de sécurité qui impliquent l'existence d'autres exigences de sécurité pour des raisons de

cohérence. Les dépendances peuvent être satisfaites en incluant le composant fonctionnel concerné dans les exigences fonctionnelles de sécurité du système-cible ou en tant qu'exigence sur son environnement.
L'insatisfaction d'une dépendance doit être rigoureusement justifiée.

Activité 5.2 – Détermination des exigences de sécurité d'assurance

Lister les exigences de sécurité d'assurance

Les exigences de sécurité d'assurance de l'ISO/IEC 15408 sont imposées aux actions du développeur, aux éléments de preuve produits et aux actions de l'évaluateur (exemple : contraintes sur la rigueur du processus de développement et exigences pour rechercher et analyser l'impact des vulnérabilités de sécurité potentielles).

L'assurance que les objectifs de sécurité sont atteints au moyen de fonctions de sécurité sélectionnées provient des deux facteurs suivants :

- la confiance dans la conformité de l'implémentation des fonctions de sécurité, c'est-à-dire l'estimation qu'elles sont correctement implémentées,
- la confiance dans l'efficacité des fonctions de sécurité, c'est-à-dire l'estimation qu'elles satisfont effectivement aux objectifs de sécurité exprimés.

Les exigences de sécurité d'assurance peuvent être reformulées selon la finalité de l'étude afin de rendre leur libellé plus accessible aux acteurs impliqués dans l'étude.

Exemple d'un libellé brut :

ACM_CAP.1 *Numéros de version*

Objectifs :

Une référence unique est exigée pour garantir qu'il n'y a pas d'ambiguïté sur l'exemplaire de la TOE qui fait l'objet de l'évaluation. L'identification de la TOE par sa référence garantit que les utilisateurs de la TOE peuvent être à même de savoir quel exemplaire de la TOE ils utilisent.

Dépendances :

Pas de dépendances.

Tâches du développeur :

ACM_CAP.1.1D Le développeur doit fournir une référence pour la TOE.

Contenu et présentation des éléments de preuve :

ACM_CAP.1.1C La référence de la TOE doit être unique pour chaque version de la TOE.

ACM_CAP.1.2C La TOE doit être identifiée par sa référence.

Tâches de l'évaluateur :

ACM_CAP.1.1E L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.

Exemple du libellé reformulé :

EA.NUM-VERSION *Le cabinet d'études doit disposer d'une référence unique (ou équivalent, numéro de version par exemple) de chaque version des entités du système-cible. Cette référence les identifie.*

Classer éventuellement les exigences de sécurité d'assurance en deux catégories

Les exigences de sécurité d'assurance peuvent appartenir à l'une des catégories suivantes :

- exigences de sécurité d'assurance portant sur le système-cible,
- exigences de sécurité d'assurance portant sur l'environnement du système-cible.

Justifier éventuellement la couverture des dépendances des exigences d'assurance

Les exigences de sécurité d'assurance peuvent dépendre d'autres exigences qu'il convient de prendre en compte afin que l'ensemble soit cohérent.
La démonstration de la complétude de la couverture doit être faite.
L'insatisfaction d'une dépendance doit être rigoureusement justifiée.

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?
.....
.....

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution