Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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 2
DÉMARCHE

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

Table des illustrations

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 seconde section de la méthode. Il présente la démarche méthodologique sous la forme de fiches descriptives.

Chaque étape fait l'objet d'une description, d'un schéma situant l'étape dans la démarche EBIOS complète et d'un synoptique décrivant les activités de l'étape.

Chaque activité est décrite selon le formalisme suivant.

DESCRIPTION
Résumé de la démarche méthodologique et schéma permettant de situer l'activité au sein de l'étape.

PRÉALABLES
Autres activités devant être réalisées au préalable de l'activité.

DONNÉES EN ENTRÉE
Données nécessaires à la mise en œuvre de l'activité.

ACTIONS
Actions à réaliser pour mener à bien l'activité.

DONNÉES EN SORTIE
Données produites par les actions de l'activité.

CONSEILS PRATIQUES
Commentaires et conseils pour la mise en œuvre de l'activité.

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

Présentation de la démarche

La méthode formalise une démarche d'appréciation et de traitement des risques dans le domaine de la sécurité des systèmes d'information.

Elle s'applique pour les systèmes à concevoir et les systèmes existants, sur le périmètre global du système d'information ou sur un périmètre particulier de celui-ci.

Elle est découpée en cinq étapes représentées dans la figure suivante :

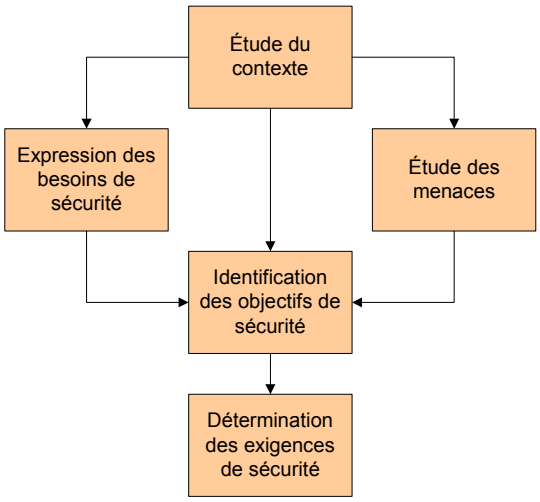
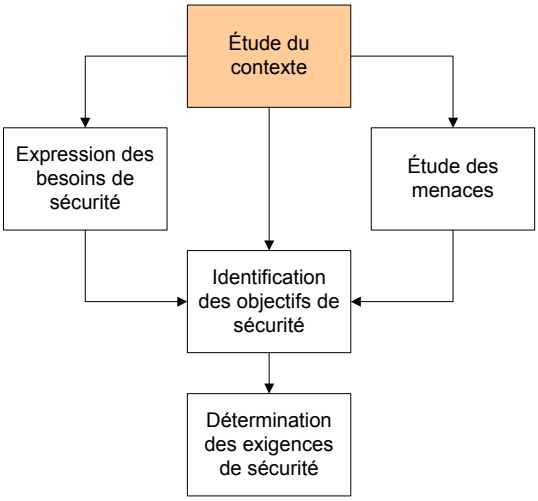


Figure 1 – Démarche EBIOS globale

- À l'issue de la première étape, l'environnement, le but et le fonctionnement du système-cible sont parfaitement connus, les éléments essentiels et les entités sur lesquelles ils reposent sont identifiés.
- La seconde étape contribue à l'appréciation des risques (estimation des risques et définition des critères de risques). Elle permet de formaliser les impacts et de valuer les besoins de sécurité des éléments essentiels en termes de disponibilité, d'intégrité, de confidentialité…
- La troisième étape s'inscrit aussi dans le cadre de l'appréciation des risques (analyse des risques). Elle consiste à recenser et décrire les menaces pesant sur le système. Pour ce faire, on étudie les méthodes d'attaque et les éléments menaçants susceptibles de les utiliser, les vulnérabilités exploitables des entités et leurs opportunités.
- La quatrième étape contribue à l'évaluation et au traitement des risques. Elle permet de formaliser les risques réels pesant sur le système en confrontant les menaces (événements négatifs) aux besoins de sécurité (conséquences). Ils sont couverts par des objectifs de sécurité, en cohérence avec les hypothèses, règles de sécurité, références réglementaires, mode d'exploitation et contraintes identifiés, qui constituent le cahier des charges de sécurité.
- La cinquième et dernière étape s'inscrit dans le cadre du traitement des risques. Elle explique comment déterminer les exigences fonctionnelles permettant de réaliser les objectifs de sécurité et les exigences d'assurance permettant d'augmenter la confiance envers leur réalisation.

Étape 1 – Étude du contexte

Cette étape essentielle a pour objectif d'identifier globalement le système-cible et de le situer dans son environnement pour déterminer précisément la cible de l'étude de sécurité.



Elle permet notamment de préciser pour le système les enjeux, le contexte de son utilisation, les missions ou services qu'il doit rendre et les moyens utilisés. Elle permet également de réunir toutes les informations nécessaires à la planification de l'étude.

À l'issue de cette étape, le champ d'investigation de l'étude est clairement délimité, les hypothèses, les obligations et les contraintes sont recensées et les sujets à traiter sont connus.

L'étape se divise en trois activités :

- Étude de l'organisme
- Étude du système-cible
- Détermination de la cible de l'étude de sécurité

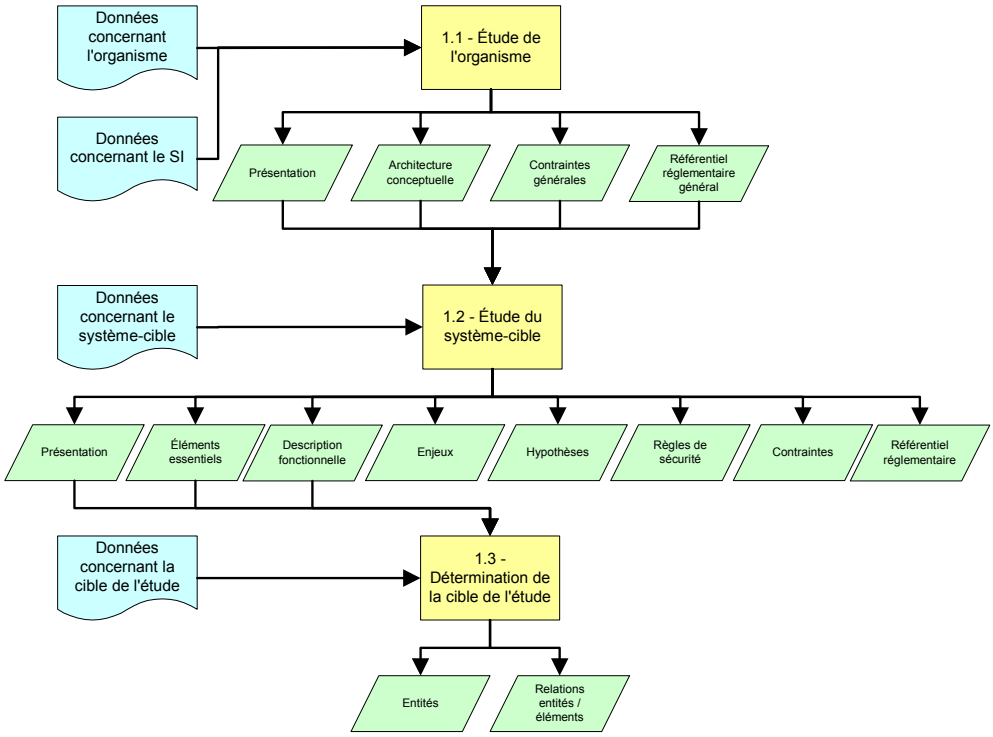
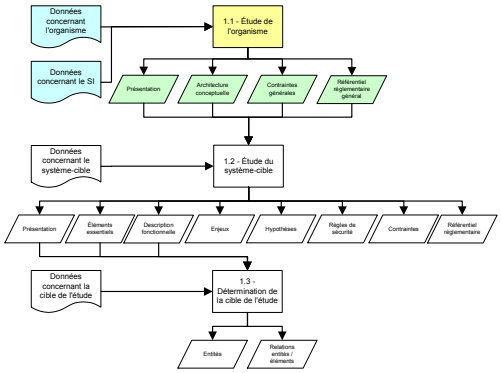


Figure 2 – Synoptique détaillé de l'étude du contexte

Activité 1.1 – Étude de l'organisme



DESCRIPTION

Cette activité consiste à définir le cadre de l'étude. Des informations générales sur l'organisme concerné par le projet de sécurité doivent donc être réunies dans le but de mieux apprécier sa nature, son organisation et les contraintes qui pèsent sur celui-ci. Il est aussi nécessaire d'obtenir une vision globale du système d'information de l'organisme. Ces éléments permettront dans les activités suivantes de préciser les enjeux du système-cible pour cet organisme et de veiller à la cohérence des objectifs et des exigences de sécurité avec ses missions.

PRÉALABLES

Sans objet

DONNÉES EN ENTRÉE

- Données concernant l'organisme et son système d'information (documents stratégiques, documents concernant les missions, les attributions et l'organisation, documents concernant le système d'information, synthèses d'entretiens avec les responsables de l'organisme).

ACTIONS

- Présenter l'organisme.
- Lister les contraintes pesant sur l'organisme.
- Lister les références réglementaires applicables à l'organisme.
- Faire une description fonctionnelle du SI global.

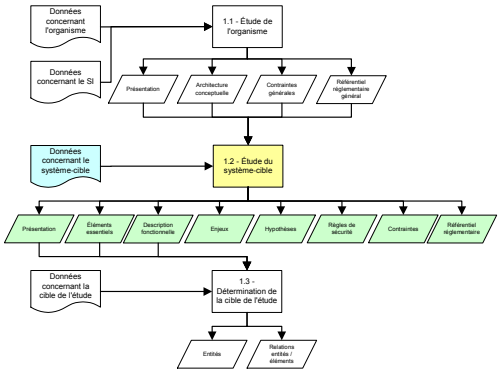
DONNÉES EN SORTIE

- Présentation de l'organisme.
- Liste des contraintes générales pesant sur l'organisme.
- Liste des références réglementaires générales applicables à l'organisme.
- Architecture conceptuelle du système d'information.

CONSEILS PRATIQUES

- Cette première activité est essentielle pour la suite de l'étude, elle permet d'appréhender au mieux le contexte de l'étude.
- Un groupe de travail (ou comité de pilotage) doit être constitué, les personnes à rencontrer doivent être identifiées et des entretiens doivent être planifiés.
- Un premier entretien doit permettre de vérifier la nature du problème initialement posé et si le problème est du ressort de l'équipe constituée. Le maximum d'informations doit pouvoir être obtenu lors de cet entretien.
- Il conviendra de juger de l'opportunité d'aborder tel ou tel thème proposé, en fonction de l'étendue du projet, des premiers éléments recueillis avant l'entretien, des responsabilités de son interlocuteur…
- L'étude de l'organisme doit impliquer la partie décisionnelle de celui-ci au plus haut niveau hiérarchique.
- Les informations sont obtenues auprès des responsables opérationnels impliqués par l'étude.
- Des questionnaires permettent de préparer les entretiens qui guideront les personnes interrogées dans le but de formaliser les réponses.

Activité 1.2 – Étude du système-cible



DESCRIPTION

Cette activité a pour but de préciser le contexte d'utilisation du système à concevoir ou existant. Pour cela, il est nécessaire de préciser le sous-ensemble du système d'information de l'organisme constituant le système-cible de l'étude et ses enjeux. Le système-cible est alors décrit et sont recensées les hypothèses, les règles de sécurité et ses contraintes.

PRÉALABLES

- Activité 1.1.

DONNÉES EN ENTRÉE

- Données concernant le système-cible.
- Présentation de l'organisme.
- Liste des contraintes générales pesant sur l'organisme.
- Liste des références réglementaires générales applicables à l'organisme.
- Architecture conceptuelle du système d'information.

ACTIONS

- Présenter le système-cible.
- Lister les enjeux.
- Lister les éléments essentiels.
- Faire une description fonctionnelle du système-cible.
- Lister les hypothèses.
- Lister les règles de sécurité.
- Lister les contraintes pesant sur le système-cible.
- Lister les références réglementaires spécifiques au système-cible.

DONNÉES EN SORTIE

- Présentation du système-cible.
- Liste des éléments essentiels.
- Description fonctionnelle du système-cible.
- Liste des enjeux du système-cible.
- Liste des hypothèses.
- Liste des règles de sécurité.
- Liste des contraintes spécifiques au système-cible.
- Liste des références réglementaires spécifiques au système-cible.

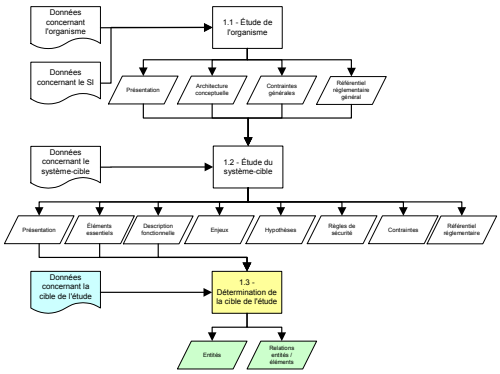
CONSEILS PRATIQUES

- Le nombre et la granularité des éléments essentiels dépendra du but de l'étude et de la nature du système-cible. En effet, l'étude d'un système d'information global visant à obtenir une vision générale des risques ne requerra pas la même finesse que l'étude d'un système précis devant être homologué formellement.
- L'absence de spécifications du système peut remettre en cause la poursuite de l'étude de sécurité. En effet, il est peu utile de chercher à sécuriser un système mal connu. En revanche, il est envisageable de poursuivre une étude rapide, globale, qui devra ensuite être affinée à mesure que les spécifications s'enrichissent.
- Le découpage en sous-systèmes peut être envisagé dans le cas de systèmes complexes. Dans ce cas, il conviendra de mener plusieurs études en parallèle.

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

DESCRIPTION

Cette activité a pour but la détermination précise des entités sur lesquelles reposent les éléments essentiels du système-cible (fonctions et informations). L'activité consiste à recenser et décrire les différentes entités, qu'elles soient de type matériel, logiciel, réseau, personnel, site ou organisation. Il s'agit aussi de répertorier les éléments essentiels qui reposent sur chacune de ces entités.



PRÉALABLES

- Activité 1.2.

DONNÉES EN ENTRÉE

- Données concernant la cible de l'étude de sécurité.
- Présentation du système-cible.
- Liste des éléments essentiels.
- Description fonctionnelle du système-cible.

ACTIONS

- Lister et décrire les entités du système.
- Croiser les éléments essentiels et les entités.

DONNÉES EN SORTIE

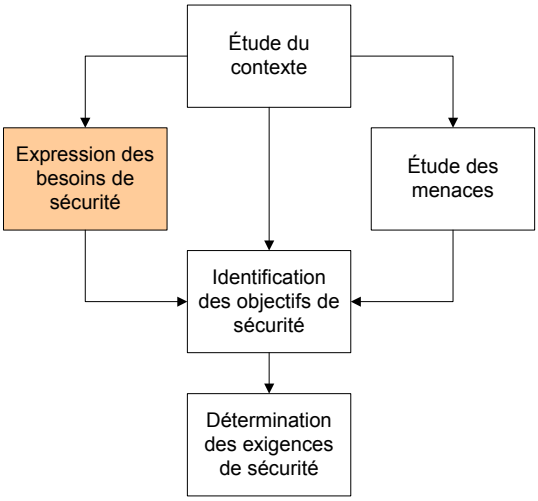
- Liste des entités.
- Tableaux entités / éléments.

CONSEILS PRATIQUES

- Il est conseillé d'utiliser les types et sous-types d'entités décrits dans le guide "Outillage pour l'appréciation des risques SSI" pour lister et décrire les entités du système.
- Il est important de ne pas oublier d'identifier une entité de type organisation (tout comme une entité de type site) dans le cas où le système-cible repose sur une seule organisation (un seul site). En effet, certaines entités sont souvent uniques pour beaucoup de systèmes-cibles, mais il faut tout de même les répertorier car elles possèdent des vulnérabilités qu'il faudra prendre en compte dans la suite de l'étude. On se retrouve généralement avec au moins une entité de chaque type.
- Il est possible d'ajouter à la description fonctionnelle les entités sur lesquelles le système-cible repose en les superposant aux schémas. Ceci permet de mieux visualiser et appréhender le système.

Étape 2 – Expression des besoins de sécurité

Cette étape contribue à l'estimation des risques et à la définition des critères de risques. Elle permet aux utilisateurs du système d'exprimer leurs besoins en matière de sécurité pour les fonctions et informations qu'ils manipulent.



L'expression des besoins de sécurité résulte des exigences opérationnelles du système, indépendamment de toute solution technique.

Elle repose sur l'élaboration et l'utilisation d'une échelle de besoins et la mise en évidence des impacts inacceptables pour l'organisme.

L'expression des besoins permet aussi de définir le mode d'exploitation du système, c'est-à-dire la manière générale dont sont gérés les utilisateurs du système.

L'étape se divise en deux activités :

- Réalisation des fiches de besoins
- Synthèse des besoins de sécurité

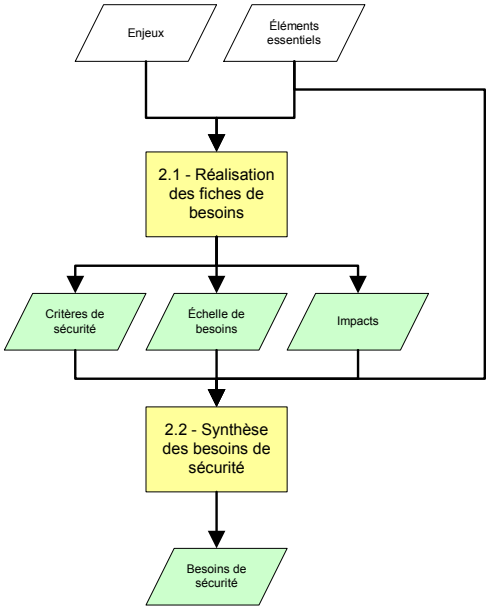
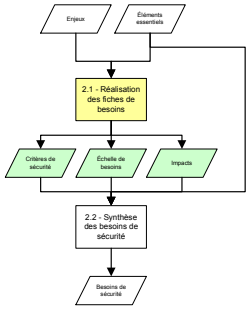


Figure 3 – Synoptique détaillé de l'expression des besoins de sécurité

Activité 2.1 – Réalisation des fiches de besoins

DESCRIPTION



Cette activité a pour but de créer les tableaux nécessaires à l'expression des besoins de sécurité par les utilisateurs. Ils permettront aux utilisateurs d'exprimer les besoins de sécurité des éléments qu'ils manipulent habituellement dans le cadre de leur activité, d'une manière objective et cohérente. Il s'agit d'une activité contribuant à l'estimation des risques et à la définition des critères de risques dans le processus de gestion des risques.

PRÉALABLES

- Activité 1.2.

DONNÉES EN ENTRÉE

- Liste des enjeux du système-cible.
- Liste des éléments essentiels.

ACTIONS

- Choisir les critères de sécurité à prendre en compte
- Déterminer l'échelle de besoins.
- Déterminer les impacts pertinents.

DONNÉES EN SORTIE

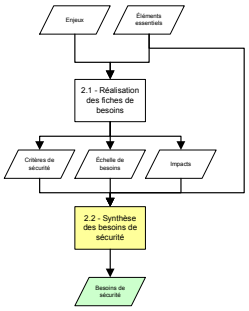
- Liste de critères de sécurité.
- Échelle de besoins.
- Liste d'impacts.

CONSEILS PRATIQUES

- L'échelle de besoins est l'un des instruments de discussion les plus importants de l'étude. Elle doit être déterminée par le groupe de travail et servira non seulement aux discussions au sujet des besoins de sécurité mais aussi aux discussions concernant les objectifs de sécurité.
- L'échelle de besoins doit être objective et cohérente. Elle comprendra des pondérations et des valeurs de référence et s'appuiera sur la liste des critères de sécurité à considérer et une liste d'impacts avec des exemples représentatifs.
- Pour les impacts, une représentation sous la forme d'un arbre de causes permet de mieux présenter l'idée au groupe de travail.
- Afin de déterminer leurs besoins de sécurité, une fiche sera réalisée pour chaque élément essentiel et par personne interrogée. La création d'une fiche par fonction ou sous-fonction est justifiée dans la mesure où les besoins de sécurité d'une fonction ne sont pas directement déduits des informations qu'elle traite. Exemples :
  - Une fonction peut être confidentielle, non pas du fait qu'elle manipule des informations confidentielles mais uniquement par la nature du traitement qu'elle effectue.
  - L'accès à un service peut ne pas demander une forte disponibilité, par contre, le fonctionnement de ce service peut nécessiter la disponibilité maximale des informations qu'il utilise.

Activité 2.2 – Synthèse des besoins de sécurité

DESCRIPTION



Cette activité a pour but d'affecter aux éléments essentiels leurs besoins de sécurité qui résultent de la synthèse des valeurs attribuées par les utilisateurs. À l'issue de cette activité, il sera possible de disposer d'une vision objective et cohérente des besoins de sécurité du système-cible. Il s'agit d'une activité contribuant à l'évaluation des risques dans le processus de gestion des risques.

PRÉALABLES

- Activité 2.1.

DONNÉES EN ENTRÉE

- Liste des éléments essentiels.
- Liste de critères de sécurité.
- Échelle de besoins.
- Liste d'impacts.

ACTIONS

- Attribuer un besoin de sécurité par critère de sécurité (disponibilité, intégrité, confidentialité…) à chaque élément essentiel.

DONNÉES EN SORTIE

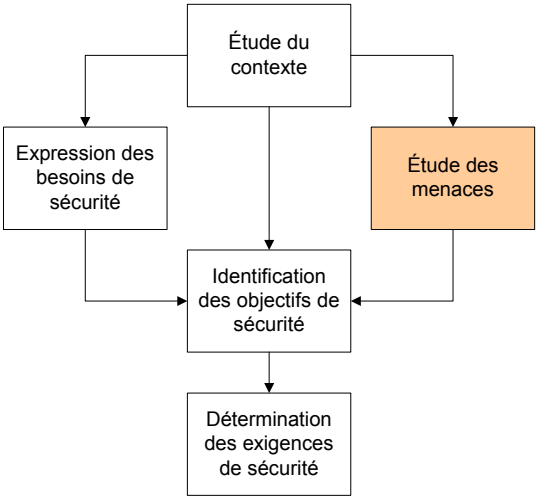
- Fiche de synthèse des besoins de sécurité.

CONSEILS PRATIQUES

- L'attribution de besoins de sécurité aux éléments essentiels représente la limite acceptable pour l'organisme.
- L'estimation des besoins de sécurité représente la vision du système que peut avoir un utilisateur, il est important que celui-ci justifie les valeurs extrêmes de son point de vue pour ensuite effectuer une synthèse cohérente au niveau de l'organisme.
- Dans la mesure du possible, les besoins de sécurité doivent tous être justifiés.
- Les utilisateurs retenus pour l'appréciation des besoins de sécurité doivent être représentatifs en regard de l'utilisation du système. Ils doivent donc s'exprimer sur des éléments qu'ils utilisent habituellement.
- Il est possible d'ajouter à la description fonctionnelle les besoins de sécurité de chacun des éléments essentiels en les superposant aux schémas. Ceci permet de mieux appréhender les éventuelles dépendances entre les valeurs de besoins de sécurité. En effet, les besoins de sécurité des fonctions et des informations sont parfois liés, ainsi que les fonctions entre elles et les informations entre elles. Ils peuvent se propager dès lors que les éléments sont liés.

Étape 3 – Étude des menaces

Cette étape contribue à l'appréciation des risques. Elle a pour objectif la détermination des menaces pesant sur le système.



Ces menaces sont formalisées en identifiant leurs composants : les méthodes d'attaque auxquelles l'organisme est exposé, les éléments menaçants qui peuvent les employer, les vulnérabilités exploitables sur les entités du système et leur niveau.

Les menaces mises en évidence au travers de cette étape sont spécifiques au système. Leur caractérisation est indépendante des besoins de sécurité, des informations traitées et des fonctions supportées par le système.

L'étude des menaces comporte trois activités :

- Étude des origines des menaces
- Étude des vulnérabilités
- Formalisation des menaces

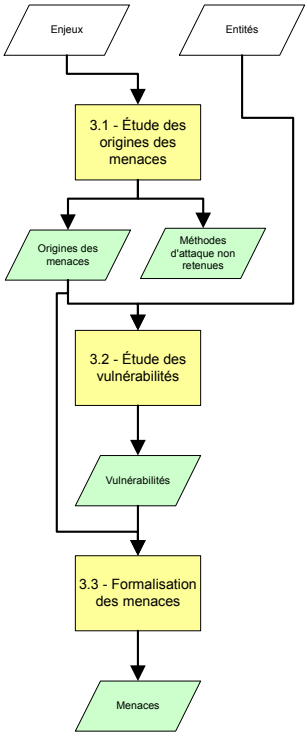
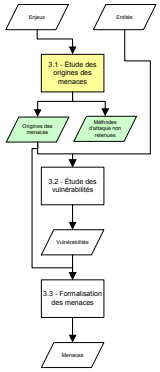


Figure 4 – Synoptique détaillé de l'étude des menaces

Activité 3.1 – Étude des origines des menaces



DESCRIPTION

Cette activité a pour but de sélectionner les méthodes d'attaque qui sont pertinentes pour le système-cible. Chacune des méthodes d'attaque est caractérisée par les critères de sécurité qu'elle peut affecter (disponibilité, intégrité, confidentialité…). Elle est associée à des éléments menaçants. Ces éléments menaçants sont caractérisés par leur type (naturel, humain ou environnemental) et leurs causes possibles (accidentelle, délibérée). Cette caractérisation peut être synthétisée sous la forme d'un potentiel d'attaque. Si les méthodes d'attaque composent des risques réels pour le système-cible, le niveau des mesures de sécurité devra être cohérent avec ce potentiel d'attaque. Cette activité correspond à l'identification des sources dans le processus de gestion des risques.

PRÉALABLES

- Activité 1.2.

DONNÉES EN ENTRÉE

- Liste des enjeux du système-cible.

ACTIONS

- Lister les méthodes d'attaque pertinentes.
- Caractériser les méthodes d'attaque par les critères de sécurité qu'elles peuvent affecter.
- Caractériser, pour chaque méthode d'attaque retenue, les éléments menaçants associés par leur type (naturel, humain ou environnemental) et leur cause (accidentelle ou délibérée).
- Ajouter une valeur représentant le potentiel d'attaque de l'élément menaçant.
- Mettre en évidence les méthodes d'attaque non retenues avec des justifications.

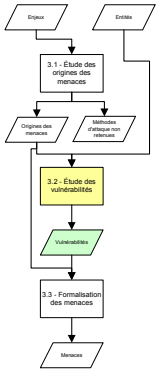
DONNÉES EN SORTIE

- Liste des origines des menaces (méthodes d'attaque et éléments menaçants).
- Liste des méthodes d'attaque non retenues et justifications.

CONSEILS PRATIQUES

- Il est conseillé d'utiliser les méthodes d'attaque et éléments menaçants génériques décrits dans le guide "Outillage pour l'appréciation des risques SSI" pour lister et caractériser les méthodes d'attaque pertinentes et éléments menaçants.
- Les méthodes d'attaque sont recensées par un expert sécurité auprès du responsable du système concerné ou des missions considérées.
- Les justifications permettant de les retenir ou de les rejeter doivent être clairement exprimées.
- La caractérisation des éléments menaçants devrait aussi être exprimée sous la forme d'une valeur qui représente le potentiel d'attaque ; elle facilitera la détermination de la résistance des mécanismes pour les objectifs et exigences de sécurité.

Activité 3.2 – Étude des vulnérabilités



DESCRIPTION

Cette activité a pour objet la détermination des vulnérabilités spécifiques du système-cible et éventuellement la caractérisation de celles-ci en terme de niveau. Ces vulnérabilités intrinsèques du système-cible proviennent des caractéristiques des entités qui le composent. Ces vulnérabilités étant exploitées pour affecter la sécurité du système, les objectifs de sécurité consisteront donc essentiellement à les diminuer. Cette activité contribue à l'estimation des risques dans le processus de gestion des risques.

PRÉALABLES

- Activités 1.3 et 3.1.

DONNÉES EN ENTRÉE

- Liste des entités.
- Liste des origines des menaces (méthodes d'attaque et éléments menaçants).

ACTIONS

- Identifier les vulnérabilités des entités selon les méthodes d'attaque.
- Estimer éventuellement le niveau des vulnérabilités.

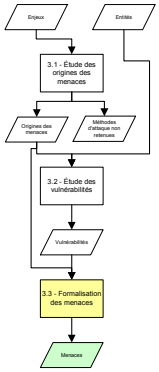
DONNÉES EN SORTIE

- Liste des vulnérabilités retenues et de leur niveau.

CONSEILS PRATIQUES

- Il est conseillé d'utiliser les vulnérabilités génériques décrites dans le guide "Outillage pour l'appréciation des risques SSI" pour identifier les vulnérabilités des entités selon les méthodes d'attaque.
- L'étude des vulnérabilités s'effectue avec les mêmes responsables sollicités lors de l'étude des origines des menaces.
- Il faut noter que si la liste des méthodes d'attaque proposée peut prétendre à l'exhaustivité, du fait de son caractère générique, celle des vulnérabilités est par nature variable et doit être personnalisée.

Activité 3.3 – Formalisation des menaces



DESCRIPTION

Cette activité a pour but de déterminer les menaces pouvant affecter le système-cible. Elles résultent de l'association des méthodes d'attaque (utilisées par des éléments menaçants identifiés) aux vulnérabilités retenues (reposant sur des entités identifiées). À l'issue de cette activité, il sera possible de disposer d'une vision objective et exhaustive des menaces réelles pesant sur le système-cible. Cette activité contribue à l'estimation des risques dans le processus de gestion des risques.

PRÉALABLES

- Activités 3.1 et 3.2.

DONNÉES EN ENTRÉE

- Liste des origines des menaces (méthodes d'attaque et éléments menaçants).
- Liste des vulnérabilités retenues et de leur niveau.

ACTIONS

- Formuler explicitement les menaces.
- Hiérarchiser éventuellement les menaces selon leur opportunité.

DONNÉES EN SORTIE

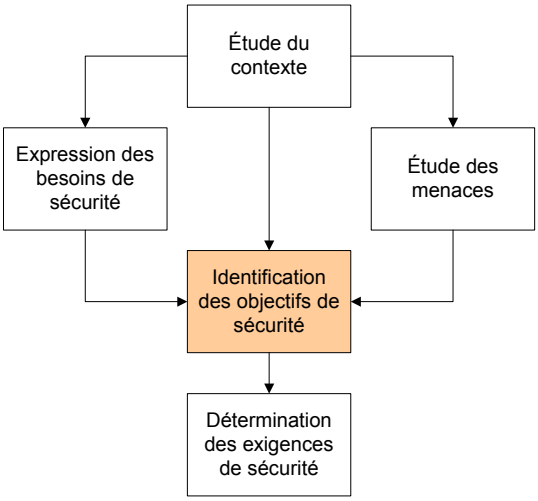
- Liste des menaces retenues.

CONSEILS PRATIQUES

- La formalisation des menaces doit être la plus précise possible et mettre en évidence la méthode d'attaque, l'élément menaçant, la ou les vulnérabilités exploitées ainsi que les entités concernées.
- Les menaces peuvent être caractérisées par leur opportunité. Celle-ci est déterminée selon le niveau des vulnérabilités exploitées par les éléments menaçants.

Étape 4 – Identification des objectifs de sécurité

Cette étape a pour but d'évaluer et de traiter les risques pesant sur le système.



La confrontation des menaces aux besoins de sécurité permet de mettre en évidence les risques à couvrir par des objectifs de sécurité. Ces objectifs de sécurité constituent le cahier des charges de sécurité du système-cible et de son environnement. Ils doivent être cohérents avec l'ensemble des hypothèses, des contraintes, des références réglementaires et des règles de sécurité identifiées au cours de l'étude.

Le niveau des objectifs de sécurité et le niveau d'assurance doivent aussi être déterminés lors de cette étape.

L'étape comporte trois activités :

- Confrontation des menaces aux besoins
- Formalisation des objectifs de sécurité
- Détermination des niveaux de sécurité

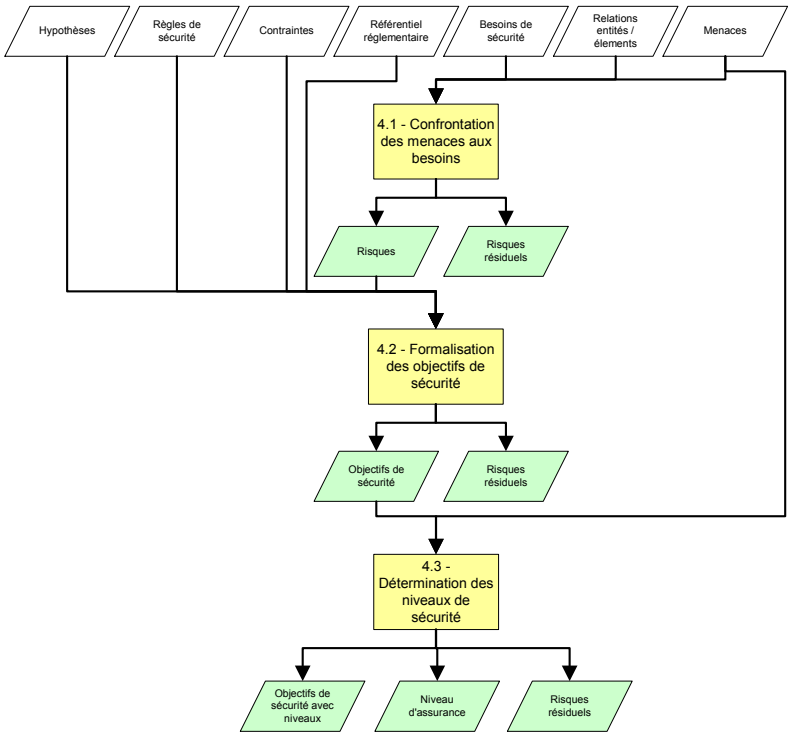
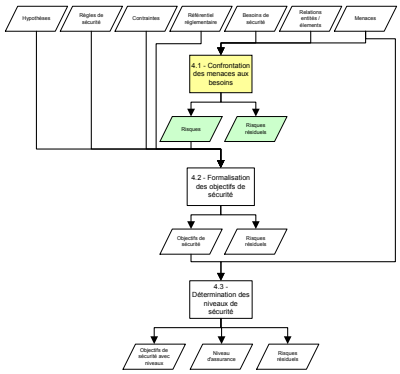


Figure 5 – Synoptique détaillé de l'identification des objectifs de sécurité

Activité 4.1 – Confrontation des menaces aux besoins



DESCRIPTION

Cette activité a pour but de déterminer les risques réels pesant sur le système-cible. La confrontation des menaces aux besoins de sécurité permet de retenir et hiérarchiser les risques qui sont véritablement susceptibles de porter atteinte aux éléments essentiels. L'ensemble de ces risques devra être évalué, la plupart d'entre eux devant être couverts par des objectifs de sécurité. Cette activité contribue à l'évaluation des risques dans le processus de gestion des risques.

PRÉALABLES

- Activités 1.3, 2.2 et 3.3.

DONNÉES EN ENTRÉE

- Tableaux entités / éléments.
- Fiche de synthèse des besoins de sécurité.
- Liste des menaces retenues.

ACTIONS

- Déterminer les risques en confrontant menaces et besoins de sécurité.
- Formuler explicitement les risques.
- Hiérarchiser les risques selon l'impact sur les éléments essentiels et l'opportunité des menaces.
- Mettre en évidence les risques non retenus (risques résiduels) avec des justifications.

DONNÉES EN SORTIE

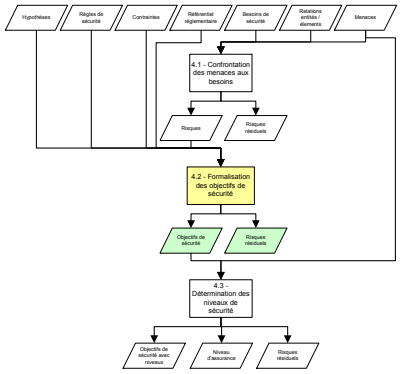
- Liste hiérarchisée des risques.
- Liste des risques résiduels (défauts de couverture des risques) et justifications.

CONSEILS PRATIQUES

- Plus la formulation d'un risque est précise, plus il sera facile au lecteur d'appréhender le risque et aux personnes réalisant l'étude d'identifier des objectifs de sécurité précis et concrets. Le risque a en effet un caractère spécifique au système-cible. Ainsi, le libellé d'un risque peut comprendre l'élément menaçant, les vulnérabilités exploitées, les entités sur lesquelles elles reposent, les éléments essentiels qui peuvent être affectés et les conséquences possibles en termes de besoins de sécurité et d'impacts.
- Ce n'est pas aux personnes réalisant l'étude de hiérarchiser les risques, mais aux utilisateurs et responsables du système. Il sera néanmoins possible de faciliter cette tâche à l'aide de l'étude. Par exemple, les valeurs maximales des besoins de sécurité qui peuvent être touchés par les risques et l'opportunité des menaces permettent de juger de l'importance des risques.
- Le classement des risques permet la détermination des priorités dans le choix et la mise en œuvre des contre-mesures.

Activité 4.2 – Formalisation des objectifs de sécurité

DESCRIPTION



Cette activité a pour but de déterminer les objectifs de sécurité permettant de couvrir les risques, conformément à la détermination des niveaux de sécurité. La complétude de la couverture de l'ensemble des risques par les objectifs de sécurité, en prenant en compte les hypothèses, règles de sécurité et contraintes, devra être démontrée. Cette activité contribue au traitement des risques dans le processus de gestion des risques.

PRÉALABLES

- Activités 1.1, 1.2, 2.4 et 4.1.

DONNÉES EN ENTRÉE

- Liste des hypothèses.
- Liste des règles de sécurité.
- Liste des contraintes.
- Liste des références réglementaires.
- Choix du mode d'exploitation de sécurité.
- Liste hiérarchisée des risques.

ACTIONS

- Lister les objectifs de sécurité.
- Justifier la complétude de la couverture, en vérifiant la compatibilité avec les contraintes pesant sur l'organisme et le système-cible :
  - des risques,
  - des hypothèses (et les enjeux),
  - des règles de sécurité (et les références réglementaires),
- Classer éventuellement les objectifs de sécurité en deux catégories :
  - objectifs de sécurité portant sur le système-cible,
  - objectifs de sécurité portant sur l'environnement du système-cible.
- Mettre en évidence les défauts de couvertures (risques résiduels) avec des justifications.

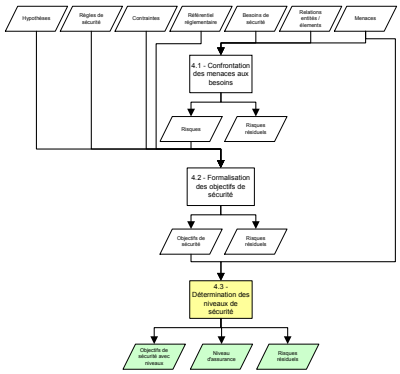
DONNÉES EN SORTIE

- Liste des objectifs de sécurité.
- Liste des risques résiduels (défaut de couverture par les objectifs de sécurité) et justifications.

CONSEILS PRATIQUES

- 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 objectifs de sécurité pourront constituer un cahier des charges de sécurité ouvert en terme de solutions de sécurité permettant de couvrir les risques.

Activité 4.3 – Détermination des niveaux de sécurité



DESCRIPTION

Cette activité a pour but de déterminer le niveau de résistance adéquat pour les objectifs de sécurité. Elle permet également de choisir le niveau des exigences de sécurité d'assurance. Cette activité contribue au traitement des risques dans le processus de gestion des risques.

PRÉALABLES

- Activités 3.3 et 4.2.

DONNÉES EN ENTRÉE

- Liste des objectifs de sécurité.
- Liste des menaces retenues.

ACTIONS

- Déterminer le niveau de résistance adéquat pour chaque objectif de sécurité.
- Choisir le niveau des exigences d'assurance.

DONNÉES EN SORTIE

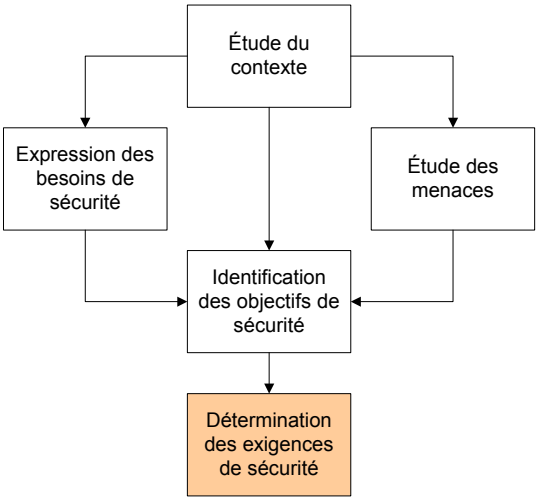
- Liste des objectifs de sécurité avec le niveau de résistance.
- Liste des risques résiduels (défaut de couverture du niveau de résistance par les objectifs de sécurité) et justifications.
- Choix du niveau des exigences d'assurance.

CONSEILS PRATIQUES

- Le potentiel d'attaque des éléments menaçants permet de déterminer le niveau de résistance adéquat des objectifs de sécurité. Ce niveau dépend de plusieurs facteurs dont le potentiel d'attaque, les contraintes, les besoins de sécurité et l'opportunité de la menace.

Étape 5 – Détermination des exigences de sécurité

Le but de cette étape est de déterminer comment réaliser les objectifs de sécurité, c'est-à-dire comment traiter les risques portant sur le système.



Pour cela, seront déterminées :

- les exigences de sécurité fonctionnelles qui décrivent le comportement de sécurité attendu et sont destinées à satisfaire aux objectifs de sécurité tels qu'ils ont été formulés dans l'étape précédente,
- les exigences de sécurité d'assurance qui constituent le fondement de la confiance dans le fait que le produit ou le système satisfait à ses objectifs de sécurité.

Ces exigences sont établies à partir, notamment, de composants fonctionnels et d'assurance proposés par l'[ISO 15408] (Critères Communs).

La couverture des objectifs de sécurité par les exigences fonctionnelles et d'assurance doit être justifiée sous forme d'argumentaire, indiquant la nécessité et la suffisance de ces dernières.

Cette étape comprend deux activités principales :

- Détermination des exigences de sécurité fonctionnelles
- Détermination des exigences de sécurité d'assurance

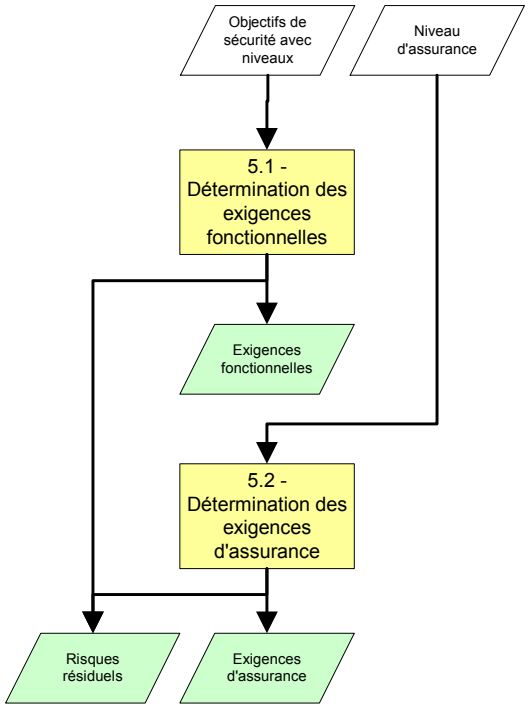
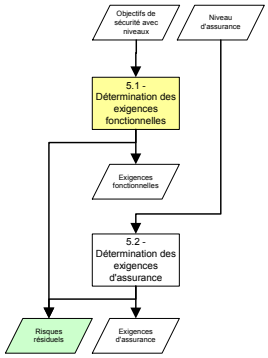


Figure 6 – Synoptique détaillé de la détermination des exigences de sécurité

Activité 5.1 – Détermination des exigences de sécurité fonctionnelles



DESCRIPTION

Cette activité a pour but de déterminer les exigences de sécurité fonctionnelles permettant de couvrir les objectifs de sécurité identifiés pour le système-cible. Elle permet de décider de la manière dont chaque risque identifié devra être traité. Les risques pourront être refusés, optimisés, transférés ou pris et le risque résiduel devra être clairement identifié et accepté. Cette activité contribue au traitement des risques dans le processus de gestion des risques.

PRÉALABLES

- Activité 4.3.

DONNÉES EN ENTRÉE

- Liste des objectifs de sécurité avec le niveau de résistance.

ACTIONS

- Lister les exigences de sécurité fonctionnelles.
- Justifier la complétude de la couverture des objectifs de sécurité.
- Mettre en évidence les éventuels défauts de couverture (risques résiduels) avec des justifications.
- Classer les exigences de sécurité fonctionnelles en deux catégories :
  - exigences de sécurité fonctionnelles portant sur le système-cible,
  - exigences de sécurité fonctionnelles portant sur l'environnement du système-cible.
- Justifier éventuellement la couverture des dépendances des exigences de sécurité fonctionnelles.

DONNÉES EN SORTIE

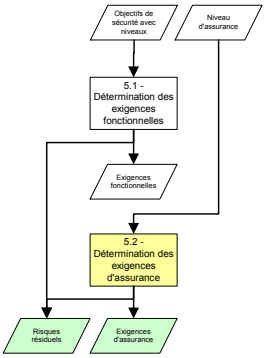
- Liste des exigences de sécurité fonctionnelles justifiées.
- Liste des risques résiduels (défaut de couverture par les exigences de sécurité fonctionnelles) et justifications.

CONSEILS PRATIQUES

- 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 destinées à satisfaire les objectifs de sécurité couvrant les vulnérabilités.
- Les exigences de sécurité fonctionnelles peuvent être sélectionnées parmi les composants fonctionnels de la base de connaissances ou rédigées de toute pièce. Chacun des objectifs de sécurité devra être couvert par au moins une exigence de sécurité et la complète couverture doit être dûment justifiée. Les exigences sont ensuite raffinées, dans la mesure du possible, et les dépendances entre composants doivent être étudiées et justifiées.
- Selon le niveau d'expertise sur le système, les composants peuvent être laissés non-raffinés en précisant toutefois qu'ils seront raffinés par le maître d'œuvre dans le cadre de sa réponse.

Activité 5.2 – Détermination des exigences de sécurité d'assurance

DESCRIPTION



Cette activité a pour but l'expression complète des exigences de sécurité d'assurance de la cible de l'étude de sécurité. Elles sont sélectionnées selon le niveau d'assurance choisi lors de la détermination des niveaux de sécurité. Elles constituent le fondement de la confiance dans le fait qu'un système-cible satisfait à ses objectifs de sécurité. Cette activité contribue au traitement des risques dans le processus de gestion des risques.

PRÉALABLES

- Activité 4.3.

DONNÉES EN ENTRÉE

- Choix du niveau des exigences d'assurance.

ACTIONS

- Lister les exigences de sécurité d'assurance.
- Classer éventuellement les exigences de sécurité d'assurance en deux catégories :
  - 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 de sécurité d'assurance.

DONNÉES EN SORTIE

- Liste des exigences de sécurité d'assurance justifiées.
- Liste des risques résiduels (défaut de couverture par les exigences de sécurité d'assurance) et justifications.

CONSEILS PRATIQUES

- Les exigences de sécurité d'assurance peuvent être sélectionnées parmi les composants fonctionnels de la base de connaissances ou rédigées de toute pièce.

Annexe – Donnés produites

- Présentation de l'organisme.
- Liste des contraintes générales pesant sur l'organisme.
- Liste des références réglementaires générales applicables à l'organisme.
- Architecture conceptuelle du système d'information.
- Présentation du système-cible.
- Liste des éléments essentiels.
- Description fonctionnelle du système-cible.
- Liste des enjeux du système-cible.
- Liste des hypothèses.
- Liste des règles de sécurité.
- Liste des contraintes spécifiques au système-cible.
- Liste des références réglementaires spécifiques au système-cible.
- Liste des entités.
- Tableaux entités / éléments.
- Liste de critères de sécurité.
- Échelle de besoins.
- Liste d'impacts.
- Fiche de synthèse des besoins de sécurité.
- Choix du mode d'exploitation de sécurité.
- Liste des origines des menaces (méthodes d'attaque et éléments menaçants).
- Liste des méthodes d'attaque non retenues et justifications.
- Liste des vulnérabilités retenues et de leur niveau.
- Liste des menaces retenues.
- Liste hiérarchisée des risques.
- Liste des risques résiduels (défauts de couverture des risques) et justifications.
- Liste des objectifs de sécurité.
- Liste des risques résiduels (défaut de couverture par les objectifs de sécurité) et justifications.
- Liste des objectifs de sécurité avec le niveau de résistance.
- Liste des risques résiduels (défaut de couverture du niveau de résistance par les objectifs de sécurité) et justifications.
- Choix du niveau des exigences d'assurance.
- Liste des exigences de sécurité fonctionnelles justifiées.
- Liste des risques résiduels (défaut de couverture par les exigences de sécurité fonctionnelles) et justifications.
- Liste des exigences de sécurité d'assurance justifiées.
- Liste des risques résiduels (défaut de couverture par les exigences de sécurité d'assurance) et justifications.

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