



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

Gestion des risques  
de sécurité des systèmes d'information

---

**PRÉCIS DE RÉDACTION ET EXERCICES**

Version du 17 janvier 2006

Ce document a été réalisé par le bureau conseil de la DCSSI  
(SGDN / DCSSI / SDO / BCS)

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

[conseil.dcssi@sgdn.pm.gouv.fr](mailto:conseil.dcssi@sgdn.pm.gouv.fr)

# Historique des modifications

<b>Date</b>	<b>Objet de la modification</b>	<b>Auteur(s)</b>	<b>Statut</b>
17/01/2006	Création du document	SGDN	Validé

# Sommaire

<b>INTRODUCTION</b> .....	<b>5</b>
<b>1 RAPPELS SUR LE RISQUE ET LA GESTION DES RISQUES SSI</b> .....	<b>6</b>
<b>2 PROPOSITIONS DE RÉDACTION DES ÉLÉMENTS DE LA GESTION DES RISQUES SSI</b> .....	<b>7</b>
2.1 L'ÉTUDE DU CONTEXTE .....	8
2.1.1 <i>L'hypothèse</i> .....	8
2.1.2 <i>La règle de sécurité</i> .....	8
2.1.3 <i>L'élément essentiel</i> .....	9
2.1.4 <i>L'entité</i> .....	9
2.2 L'EXPRESSION DES BESOINS DE SÉCURITÉ .....	10
2.2.1 <i>L'impact</i> .....	10
2.2.2 <i>Le besoin de sécurité</i> .....	10
2.3 L'ÉTUDE DES MENACES .....	11
2.3.1 <i>La méthode d'attaque</i> .....	11
2.3.2 <i>L'élément menaçant</i> .....	11
2.3.3 <i>La menace</i> .....	13
2.4 L'IDENTIFICATION DES OBJECTIFS DE SÉCURITÉ .....	14
2.4.1 <i>Le risque</i> .....	14
2.4.2 <i>L'objectif de sécurité</i> .....	15
2.5 LA DÉTERMINATION DES EXIGENCES DE SÉCURITÉ .....	16
2.5.1 <i>L'exigence de sécurité fonctionnelle</i> .....	16
2.5.2 <i>Le risque résiduel</i> .....	17
2.5.3 <i>L'exigence de sécurité d'assurance</i> .....	18
<b>3 EXERCICES</b> .....	<b>19</b>
3.1 QUESTIONS À CHOIX MULTIPLES .....	19
3.2 RÉPONSES COMMENTÉES .....	21
<b>ACRONYMES</b> .....	<b>24</b>
<b>RÉFÉRENCES BIBLIOGRAPHIQUES</b> .....	<b>24</b>
<b>FORMULAIRE DE RECUEIL DE COMMENTAIRES</b> .....	<b>25</b>

## Introduction

La gestion des risques de sécurité des systèmes d'information (SSI) est au cœur de toutes les réflexions relatives à la SSI. Il s'agit en effet du processus le plus adapté pour estimer les enjeux de sécurité et mettre en place les mesures adéquates, et ce, de manière continue.

Les concepts mis en œuvre dans ce processus sont de mieux en mieux reconnus et partagés dans le domaine de la SSI, d'autant plus que la plupart de ces éléments reposent maintenant sur des normes internationales ([Guide ISO 73], [ISO 13335], [ISO 15408], [ISO 15446], [ISO 17799]...).

Par ailleurs, les principaux outils de gestion des risques SSI utilisent naturellement ces concepts. C'est le cas de la méthode [EBIOS].

Les objectifs de ce précis de gestion des risques SSI sont d'une part de fournir une aide à la compréhension de ces concepts dans un souci de cohérence et d'homogénéisation des formulations, et d'autre part de permettre de juger de la qualité des livrables associés (plans d'action, politiques SSI, cahiers des charges SSI tels que [FEROS] ou profils de protection...). Il vise ainsi à contribuer à l'amélioration de la culture SSI.

Ce précis n'explique pas comment déterminer les différentes composantes de la gestion des risques SSI (il convient pour cela de se reporter aux outils adéquats tel que la méthode [EBIOS]), mais uniquement comment les formuler.

Il s'adresse à toute personne désirant utiliser les concepts de gestion des risques SSI dans un but opérationnel (principalement les maîtrises d'ouvrage et les maîtrises d'œuvre).

La production de livrables liés à la gestion des risques SSI constituant un instrument de communication important pour la prise de décision, la négociation et la sensibilisation, il s'avère nécessaire de garder une certaine souplesse dans la formulation de ces éléments, tout en ayant bien conscience des impondérables à respecter. Il conviendra de toujours garder à l'esprit que la formulation de tel ou tel élément est vouée à être communiquée dans un but précis selon le livrable (validation, sensibilisation, détermination de solutions à mettre en œuvre...).

Avertissement : ce précis fournit une aide à la formulation des concepts de manière linéaire, ce qui n'exclut pas le "rebouclage" de certaines activités de la méthode.

La première partie de ce précis rappelle brièvement de quoi est constituée la gestion des risques SSI. La seconde partie propose des formulations pour les différents concepts manipulés, avec des exemples concrets permettant d'illustrer les variations possibles.

Enfin, la troisième partie présente des exercices sous la forme de questions à choix multiples, afin de vérifier la compréhension de ces concepts.

# 1 Rappels sur le risque et la gestion des risques SSI

Le **risque SSI** est une combinaison d'une menace et des pertes qu'elle peut engendrer. La menace SSI est définie à partir d'un élément menaçant, exploitant une méthode d'attaque afin d'atteindre un bien.

La **gestion des risques SSI** consiste à coordonner, de manière continue, les activités visant à diriger et piloter un organisme vis-à-vis des risques. Elle inclut l'appréciation, le traitement, l'acceptation et la communication relative aux risques SSI :

1. L'**appréciation des risques SSI** représente l'ensemble du processus d'analyse des risques (mise en évidence des composantes des risques) et d'évaluation du risque (estimation de leur importance).

Elle consiste tout d'abord à décrire au minimum l'organisme, le système d'information (SI), les biens à protéger, les enjeux liés au SI et les contraintes à prendre en compte.

Les besoins de sécurité des informations et fonctions doivent ensuite être exprimés au moins en termes de disponibilité, d'intégrité et de confidentialité. Cette expression des besoins doit être faite indépendamment des menaces.

Les menaces pesant sur le SI doivent être identifiées et évaluées en terme d'opportunité.

Les risques doivent enfin être déterminés en confrontant les menaces aux besoins de sécurité.

2. Le **traitement des risques SSI** représente le processus de sélection et de mise en œuvre des mesures visant un refus, une optimisation, un transfert ou une prise de risque.

Il consiste tout d'abord à identifier les objectifs de sécurité permettant de couvrir le risque tout en prenant en compte les caractéristiques du contexte. Ces objectifs représentent un cahier des charges ne préjugant pas des solutions à mettre en œuvre, mais exprimant la volonté et la manière de traiter les risques.

Le traitement des risques se poursuit par la détermination d'exigences de sécurité, techniques ou non, satisfaisant les objectifs de sécurité identifiés.

Des mesures techniques ou non techniques répondant aux exigences de sécurité déterminées peuvent enfin être mises en œuvre.

À l'issue, les risques ont été refusés (éviter la situation à risque) et/ou optimisés (réduits) et/ou transférés (vers des tiers) et/ou pris, et un ensemble de risques résiduels peut subsister.

3. L'**acceptation des risques SSI** représente la décision d'accepter les choix effectués lors du traitement des risques SSI.

Cette activité consiste en une homologation de sécurité.

4. La **communication relative aux risques SSI** représente l'échange ou le partage d'informations concernant les risques.

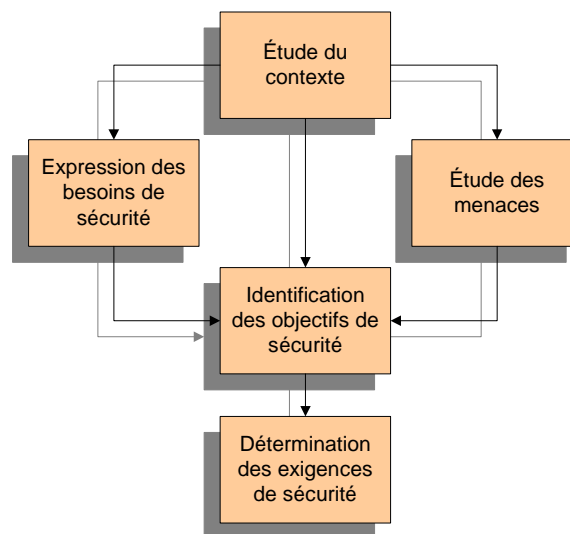
La gestion des risques SSI doit être considérée comme un processus continu et itératif.

## 2 Propositions de rédaction des éléments de la gestion des risques SSI

Les éléments importants de la gestion des risques SSI utiles dans le cadre des études de sécurité sont ici définis et des conseils de rédaction sont proposés afin d'homogénéiser les livrables dans lesquels ils figurent :

- ❑ fiches d'expression rationnelles des objectifs de sécurité [FEROS],
- ❑ profils de protection (PP – selon l'[ISO 15408]),
- ❑ cibles de sécurité,
- ❑ politiques de sécurité de systèmes d'information,
- ❑ ...

Les éléments sont décrits en suivant les étapes de la démarche générale de la méthode [EBIOS] :



Chaque élément est présenté de la façon suivante :

### Rappel de la définition

*Rappel de la définition utilisée dans la méthode EBIOS*

### Proposition de rédaction

**Les formulations proposées utilisent la syntaxe suivante :**

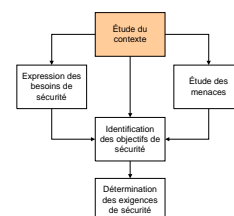
- **les accolades ( {...} ) encadrent une composante de la formulation complète,**
- **les signes d'addition ( + ) séparent les différentes composantes de la formulation complète,**
- **les parenthèses ( (...) ) encadrent une composante optionnelle de la formulation complète,**
- **les guillemets ( "... " ) encadrent un libellé qui peut être utilisé tel quel,**
- **les barres ( / ) indiquent un choix à effectuer entre plusieurs formulations.**

### Notes

*Informations complémentaires aidant à la compréhension et à la formulation*

### Exemples de formulations

- ❑ *Exemples concrets illustrant la formulation de chaque élément*



## 2.1 L'étude du contexte

### 2.1.1 L'hypothèse

**Rappel de la définition** Postulat, posé sur l'environnement opérationnel du système, permettant de procurer les fonctionnalités de sécurité attendues.

**Proposition de rédaction**

**{groupe nominal} + {verbe au présent} + {complément}**

**Exemples de formulations**

- ❑ Le système est placé dans une pièce conçue pour minimiser les émanations électromagnétiques.
- ❑ L'administrateur est placé dans une zone d'accès réservé.
- ❑ Les utilisateurs n'écrivent pas leurs mots de passe.
- ❑ Le réseau n'est pas connecté à un réseau dont la confiance n'aura pas été établie.
- ❑ Chacun au sein de la société connaît ses responsabilités en cas de diffusion illicite d'informations métiers ou de manipulation illégale de données nominatives.

### 2.1.2 La règle de sécurité

**Rappel de la définition** Règle, procédure, code de conduite ou ligne directrice de sécurité qu'une organisation impose pour son fonctionnement. [ISO 15408]

**Proposition de rédaction**

**{groupe nominal} + {"devoir" au présent} + {complément}**

**Exemples de formulations**

- ❑ Tous les produits utilisés par l'organisme doivent être conformes aux normes nationales pour la génération de mots de passe et la cryptologie.
- ❑ Tous les produits utilisés dans le domaine de l'organisme doivent être certifiés au niveau EAL4 augmenté du composant ADV\_IMP.2.
- ❑ Le contrôle d'accès doit s'effectuer par identifiant / mot de passe.
- ❑ Chaque ingénieur doit être responsable du fichier qu'il traite.
- ❑ Une alarme anti-intrusion doit être active durant les heures de fermeture (19h-7h).
- ❑ L'ensemble des règles de la politique de sécurité doit être appliqué.

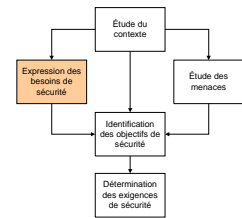
### 2.1.3 L'élément essentiel

<b>Rappel de la définition</b>	Information ou fonction ayant au moins un besoin de sécurité non nul.
<b>Proposition de rédaction</b>	Information : <b>{groupe nominal}</b> Fonction : <b>{verbe à l'infinitif} + {complément}</b>
<b>Notes</b>	Le niveau de détail des éléments essentiels dépend du niveau de détail des spécifications du SI et du livrable attendu de l'étude de sécurité. Dans certains cas, notamment dans celui de l'élaboration d'une politique de sécurité globale d'un organisme, un élément essentiel peut même être un domaine d'activité.
<b>Exemples de formulations</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Informations             <ul style="list-style-type: none"> <li><input type="checkbox"/> Données de la base de données du personnel</li> <li><input type="checkbox"/> Champ "Nom" de la base de données du personnel</li> <li><input type="checkbox"/> Requête de certification</li> </ul> </li> <li><input type="checkbox"/> Fonctions :             <ul style="list-style-type: none"> <li><input type="checkbox"/> Gérer la facturation</li> <li><input type="checkbox"/> Envoyer un courrier électronique</li> </ul> </li> </ul>

### 2.1.4 L'entité

<b>Rappel de la définition</b>	Il s'agit d'un bien qui peut être de type organisation, site, personnel, matériel, réseau, logiciel, système.
<b>Proposition de rédaction</b>	<b>{groupe nominal}</b>
<b>Notes</b>	<p>Le guide de la méthode [EBIOS] propose une typologie détaillée d'entités.</p> <p>Le niveau de détail des entités dépend du niveau de détail des spécifications du SI et du livrable attendu de l'étude de sécurité.</p>
<b>Exemples de formulations</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Organisation du cabinet d'études</li> <li><input type="checkbox"/> Locaux de Toulon</li> <li><input type="checkbox"/> Pièce 143 du bâtiment C</li> <li><input type="checkbox"/> Ingénieur du bureau d'étude</li> <li><input type="checkbox"/> Ordinateur portable</li> <li><input type="checkbox"/> Réseau Ethernet</li> <li><input type="checkbox"/> Système d'exploitation Linux</li> </ul>

## 2.2 L'expression des besoins de sécurité



### 2.2.1 L'impact

**Rappel de la définition** Conséquence sur l'organisme de la réalisation d'une menace.

**Proposition de rédaction**

{libellé}

**Notes**

Le guide de la méthode [EBIOS] propose des impacts génériques qu'il convient de choisir pertinemment et de personnaliser le plus possible.

**Exemples de formulations**

- Perte d'image de marque vis-à-vis de la clientèle
- Infraction aux lois et aux règlements donnant lieu à des poursuites judiciaires à l'encontre du Directeur
- Pertes financières

### 2.2.2 Le besoin de sécurité

**Rappel de la définition** Rappel de la définition précise et non ambiguë des niveaux correspondant aux critères de sécurité (disponibilité, confidentialité, intégrité...) qu'il convient d'assurer à un élément essentiel.

**Proposition de rédaction**

{libellé}

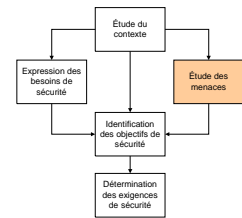
**Notes**

Il convient théoriquement qu'un besoin de sécurité corresponde à l'une des valeurs d'une échelle de besoins explicite, bornée et personnalisée.

**Exemples de formulations**

- Entre une heure et une demi-journée
- Besoin d'intégrité
- Aucun besoin de confidentialité
- Confidentiel défense (CD)

## 2.3 L'étude des menaces



### 2.3.1 La méthode d'attaque

**Rappel de la définition** Moyen type (action ou événement) pour un élément menaçant de réaliser une attaque.

**Proposition de rédaction**

{groupe nominal}

**Notes**

La méthode d'attaque peut être choisie parmi les 42 méthodes d'attaque proposées dans le guide de la méthode [EBIOS].

Le terme "attaque" (issu de l'[ISO 15408]) est employé au sens large : il peut autant s'agir d'événements de cause accidentelle que de cause délibérée.

**Exemples de formulations**

- Incendie
- Vol de support ou de document
- Écoute passive

### 2.3.2 L'élément menaçant

**Rappel de la définition**

Action humaine, élément naturel ou environnemental qui a des conséquences potentielles négatives sur le système. Elle peut être caractérisée par son type (naturel, humain, ou environnemental) et par sa cause (accidentelle ou délibérée). Dans le cas d'une cause accidentelle, elle est aussi caractérisée par une exposition et des ressources disponibles. Dans le cas d'une cause délibérée, elle est aussi caractérisée par une expertise, des ressources disponibles et une motivation.

**Proposition de rédaction**

{synthèse de la réflexion sur le type (humain, naturel ou environnemental), la cause (accidentelle ou délibérée), ainsi que sur l'exposition et les ressources disponibles dans le cas d'une cause accidentelle, ou sur l'expertise, les ressources disponibles et la motivation dans le cas d'une cause délibérée} + {"(potentiel d'attaque" + "faible" / "moyen" / "élevé" + ")"} }

**Notes**

La méthode [EBIOS] propose des éléments de réflexion pour décrire les éléments menaçants. Cette description reste libre.

On remarque que la terminologie employée évoque davantage les éléments menaçants de cause délibérée. Néanmoins, les mêmes termes sont également employés pour décrire les éléments menaçants de cause accidentelle.

**Exemples de formulations**

- ❑ Un pirate expérimenté et bien équipé, payé par un concurrent (potentiel d'attaque élevé)
- ❑ La forêt de pins entourant le site, aisément inflammable, en considérant les causes accidentelles et délibérées (potentiel d'attaque élevé)
- ❑ Le petit bois de feuillus à proximité du site, peu inflammable, en considérant les causes accidentelles et délibérées (potentiel d'attaque faible)
- ❑ Les utilisateurs autorisés pouvant omettre ou falsifier des données personnelles (potentiel d'attaque faible)
- ❑ Les personnes ou machines qui disposent de moyens d'investigation et d'action sur les réseaux supports du système d'information (potentiel d'attaque élevé)

### 2.3.3 La menace

#### Rappel de la définition

Attaque possible d'un élément menaçant sur des biens.

#### Proposition de rédaction

{élément(s) menaçant(s)} + {verbe d'action} + {méthode d'attaque} + {"en exploitant"} + {vulnérabilité(s)} + {"portant sur"} + {entité(s)} + {"(opportunité " + "faible" / "moyenne" / "élevée" + ")"}

#### Notes

La menace est généralement formulée comme un scénario quand il est nécessaire de la communiquer. Cette formulation devra être adaptée aux livrables à produire.

Il convient de garder une liberté de formulation par rapport à la proposition faite ci-dessus afin de la rendre "parlante".

Le simple rappel de tous les éléments constituant la menace peut être accepté (et sera même plus complet), sous forme de tableau par exemple (avec en colonnes le libellé de la méthode d'attaque, la description des éléments menaçants avec leur potentiel d'attaque, les vulnérabilités, les entités concernées et l'opportunité).

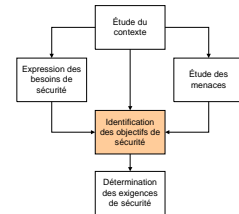
Dans le cas où l'on ne dispose pas des informations suffisantes sur toutes les composantes de la menace, il est possible de la formuler sans ces composantes.

La méthode EBIOS explique comment déterminer l'opportunité de la menace.

#### Exemples de formulations

- ❑ Une personne en visite ou un personnel de nettoyage (potentiel d'attaque faible) vole des supports ou des documents en profitant de la facilité de pénétrer dans les locaux du site du cabinet d'études pendant les heures ouvrables (opportunité élevée)
- ❑ Un pirate expérimenté et bien équipé, payé par un concurrent (potentiel d'attaque élevé), pratique une écoute passive en exploitant les media et supports (ex. : Ethernet, systèmes de communication sans fil) disposant des caractéristiques permettant l'écoute passive (opportunité faible)
- ❑ La forêt entourant complètement le site, aisément inflammable, surtout en été (potentiel d'attaque élevé), en considérant les causes accidentelles et délibérées, prend feu et provoque l'incendie des locaux du site du fait de l'absence de cloisonnement anti-feu (opportunité élevée)
- ❑ Le niveau de la Seine (potentiel d'attaque élevé) augmente et noie les bâtiments et les matériels au rez-de-chaussée du bâtiment (opportunité faible)

## 2.4 L'identification des objectifs de sécurité



### 2.4.1 Le risque

#### Rappel de la définition

Combinaison d'une menace et des pertes qu'elle peut engendrer, c'est-à-dire de l'opportunité de l'exploitation d'une ou plusieurs vulnérabilités d'une ou plusieurs entités par un élément menaçant employant une méthode d'attaque et de l'impact sur les éléments essentiels et sur l'organisme.

#### Proposition de rédaction

**{menace} + {"; ceci porte atteinte à "} + {synthèse des besoins de sécurité concernés} + {"; l'impact résultant est "} + {synthèse des impacts les plus concernés}**

#### Notes

Le risque est généralement formulé comme un scénario quand il est nécessaire de le communiquer. Cette formulation sera adaptée aux livrables à produire.

Il convient de garder une liberté de formulation par rapport à la proposition faite ci-dessus afin de la rendre "parlante".

Le simple rappel de tous les éléments constituant le risque peut suffire, sous forme de tableau par exemple (avec en colonnes tous les éléments de la menace plus les éléments essentiels concernés et les principaux impacts liés).

#### Exemples de formulations

- ❑ Une personne en visite ou un personnel de nettoyage (potentiel d'attaque faible) vole des supports ou des documents en profitant de la facilité de pénétrer dans les locaux du site du cabinet d'études pendant les heures ouvrables (opportunité élevée) ; ceci porte atteinte à la disponibilité de plusieurs éléments essentiels et à la confidentialité d'informations sensibles (devis, dossier de contentieux...) ; l'impact résultant est une perte notable d'image de marque
- ❑ Un pirate expérimenté et bien équipé, payé par un concurrent (potentiel d'attaque élevé), pratique une écoute passive en exploitant les media et supports (ex. : Ethernet, systèmes de communication sans fil) disposant des caractéristiques permettant l'écoute passive (opportunité faible) ; ceci porte atteinte à la confidentialité d'informations sensibles (devis, dossier de contentieux...) ; l'impact résultant est une perte de clientèle (réutilisation par le concurrent)
- ❑ La forêt entourant complètement le site, aisément inflammable, surtout en été (potentiel d'attaque élevé), en considérant les causes accidentelles et délibérées, prend feu et provoque l'incendie des locaux du site du fait de l'absence de cloisonnement anti-feu (opportunité élevée) ; ceci porte atteinte à la disponibilité de l'ensemble des éléments essentiels ; l'impact résultant est un arrêt d'activité
- ❑ Le niveau de la Seine (potentiel d'attaque élevé) augmente et noie les bâtiments et les matériels au rez-de-chaussée du bâtiment (opportunité faible) ; ceci porte atteinte à la disponibilité de la majorité des éléments essentiels ; l'impact résultant est une interruption de service

## 2.4.2 L'objectif de sécurité

**Rappel de la définition** Expression de l'intention de contrer des menaces ou des risques identifiés (selon le contexte) et/ou de satisfaire à des règles de sécurité et à des hypothèses ; un objectif peut porter sur le système-cible, sur son environnement de développement ou sur son environnement opérationnel.

**Proposition de rédaction**

**{ "Refuser" / "Optimiser" / "Transférer" / "Prendre" } + {"le risque suivant : "} + {risque} / {"Prendre en compte "} + {règle(s) de sécurité} / {"Garantir la conformité avec "} + {hypothèse(s)}**

**Notes** L'objectif de sécurité est formulé de manière adaptée aux livrables à produire. C'est généralement l'expression de la maîtrise d'ouvrage qui ne doit pas préciser comment traiter le risque.

Il convient d'indiquer le traitement souhaité : refus (changement structurel faisant en sorte que le risque n'existe plus), optimisation (réduction), transfert (partage des pertes avec un tiers) ou prise de risque ("ne rien faire").

Il convient également de garder une liberté de formulation par rapport à la proposition faite ci-dessus afin de la rendre "parlante".

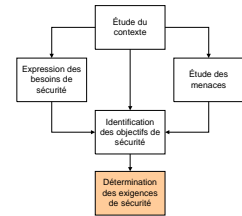
La formulation peut orienter le traitement du risque. Néanmoins, ceci empêche d'imaginer de traiter le risque d'une autre manière (on peut traiter les vulnérabilités, mais aussi et parfois uniquement, les conséquences ou l'origine du risque).

Les références réglementaires et les contraintes peuvent être traitées comme les hypothèses et règles de sécurité.

### Exemples de formulations

- ❑ Optimiser ou transférer le risque suivant en prenant en compte le fait que des dépenses supplémentaires ne sont pas envisageables : une personne en visite ou un personnel de nettoyage (potentiel d'attaque faible) vole des supports ou des documents en profitant de la facilité de pénétrer dans les locaux du site du cabinet d'études pendant les heures ouvrables (opportunité élevée) ; ceci porte atteinte à la disponibilité de plusieurs éléments essentiels et à la confidentialité d'informations sensibles (devis, dossier de contentieux...) ; l'impact résultant est une perte notable d'image de marque
- ❑ Optimiser le risque suivant : un pirate expérimenté et bien équipé, payé par un concurrent (potentiel d'attaque élevé), pratique une écoute passive en exploitant les media et supports (ex. : Ethernet, systèmes de communication sans fil) disposant des caractéristiques permettant l'écoute passive (opportunité faible) ; ceci porte atteinte à la confidentialité d'informations sensibles (devis, dossier de contentieux...) ; l'impact résultant est une perte de clientèle (réutilisation par le concurrent)
- ❑ Garantir la conformité avec la politique de sécurité
- ❑ Les interfaces de communication doivent protéger les transmissions en confidentialité, intégrité et disponibilité
- ❑ Les exigences de sécurité doivent intégrer une infrastructure de gestion de clés (décision prise a priori)

## 2.5 La détermination des exigences de sécurité



### 2.5.1 L'exigence de sécurité fonctionnelle

**Rappel de la définition** Spécification fonctionnelle des fonctions de sécurité à mettre en œuvre afin de participer à la couverture d'un ou plusieurs objectifs de sécurité portant sur le système-cible.

**Proposition de rédaction**

**{groupe nominal} + {"devoir" au présent} + {complément}**

**Notes**

C'est généralement la réponse de la maîtrise d'œuvre à la maîtrise d'ouvrage qui, d'une manière générale, propose des moyens de traiter le risque.

Dans la mesure du possible, la formulation des exigences de sécurité fonctionnelles doit être spécifique, mesurable, atteignable, réaliste et liée au temps.

Bien que la formulation d'une exigence puisse être issue d'un catalogue de meilleures pratiques, il convient généralement de l'adapter à son contexte et aux lecteurs.

**Exemples de formulations**

- ❑ Les personnes en visite doivent systématiquement être accompagnées par un membre du personnel d'ici la fin de l'année
- ❑ Les supports et documents sur lesquels sont contenues des informations confidentielles doivent systématiquement être rangés sous clé dès lors qu'ils ne sont pas utilisés à compter de la validation de la politique de sécurité
- ❑ Un plan de communication doit être élaboré afin d'améliorer la réaction vis-à-vis des clients en cas de vol d'informations confidentielles
- ❑ 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
- ❑ Le cabinet d'études doit être abonné chez au moins deux fournisseurs d'accès à Internet distincts
- ❑ Une politique sur l'utilisation des commandes cryptographiques pour la protection des informations doit être élaborée et suivie
- ❑ Le câblage électrique et de télécommunication transmettant des données ou supportant des services d'information doit être protégé contre les interceptions
- ❑ Les opérations cryptographiques doivent être exécutées conformément à un algorithme cryptographique (à définir) et avec des tailles de clés cryptographiques spécifiées (à définir) qui satisfont à des normes identifiées (à définir)
- ❑ Les matériels informatiques doivent être assurés

## 2.5.2 Le risque résiduel

<b>Rappel de la définition</b>	Risque subsistant après le traitement du risque.
<b>Proposition de rédaction</b>	<div style="border: 1px solid black; padding: 10px; text-align: center;">{risque}</div>
<b>Notes</b>	<p>Des risques résiduels peuvent apparaître dès l'identification des objectifs de sécurité (risques partiellement optimisés ou pris), mais la plupart sera mise en évidence au niveau de la détermination des exigences de sécurité.</p> <p>Ils reflètent souvent les limites des exigences de sécurité déterminées.</p> <p>Il convient de garder une liberté de formulation par rapport à la proposition faite ci-dessus (même formulation que le risque) afin de la rendre "parlante".</p>
<b>Exemples de formulations</b>	<ul style="list-style-type: none"><li>❑ Une personne en visite ou un personnel de nettoyage (potentiel d'attaque faible) vole des supports ou des documents en profitant de l'inattention de la personne l'accompagnant dans les locaux du site du cabinet d'études pendant les heures ouvrables (opportunité faible) ; ceci porte atteinte à la disponibilité de plusieurs éléments essentiels et à la confidentialité d'informations sensibles (devis, dossier de contentieux...) ; l'impact résultant est une perte notable d'image de marque</li> <li>❑ On ne peut totalement exclure la possibilité qu'un utilisateur du système d'information dévoile son mot de passe à un collègue et que ce dernier porte atteinte à la disponibilité, à l'intégrité ou à la confidentialité de toutes les informations et les fonctions auxquelles l'utilisateur a accès légitimement, ce qui pourrait impacter les activités de l'organisme et l'image de l'utilisateur</li></ul>

### 2.5.3 L'exigence de sécurité d'assurance

<b>Rappel de la définition</b>	Spécification d'assurance des fonctions de sécurité à mettre en œuvre pour participer à la couverture d'un ou plusieurs objectifs de sécurité, et portant généralement sur l'environnement de développement du système.
<b>Proposition de rédaction</b>	<b>{groupe nominal} + {"devoir" au présent} + {complément}</b>
<b>Notes</b>	<p>Ce type d'exigence tend à améliorer la confiance envers la mise en œuvre des mesures spécifiées à l'aide des exigences de sécurité fonctionnelles.</p> <p>Dans la mesure du possible, la formulation des exigences de sécurité d'assurance doit être spécifique, mesurable, atteignable, réaliste et liée au temps.</p> <p>Bien que la formulation d'une exigence puisse être issue d'un catalogue de meilleures pratiques, il convient généralement de l'adapter à son contexte et aux lecteurs.</p>
<b>Exemples de formulations</b>	<ul style="list-style-type: none"><li>❑ Le développeur doit documenter les procédures de livraison à l'utilisateur du système-cible ou de parties de celle-ci</li><li>❑ La documentation de livraison doit décrire toutes les procédures qui sont nécessaires pour maintenir la sécurité lors de la distribution de versions du système-cible vers le site d'un utilisateur</li><li>❑ La conception de haut niveau doit décrire les fonctionnalités de sécurité fournies par chaque sous-système de l'ensemble des fonctions de sécurité du système-cible</li></ul>

## 3 Exercices

### 3.1 Questions à choix multiples

**Question 1 – Le "devis du cabinet d'architecture @rchimed" est :**

1. un élément essentiel
2. une hypothèse
3. une règle de sécurité
4. une entité
5. un objectif de sécurité

**Question 2 – "Les utilisateurs du système d'information d'@rchimed ont connaissance des valeurs et des axes stratégiques exprimés par le directeur. En particulier, l'innovation et la réactivité sont des valeurs partagées. Dans ce contexte, chacun sait la valeur que représentent les logiciels de conception." Il s'agit :**

1. d'un élément essentiel
2. d'une hypothèse
3. d'une règle de sécurité
4. d'un objectif de sécurité
5. d'une exigence de sécurité fonctionnelle

**Question 3 – "La preuve, l'opposabilité et la traçabilité" sont :**

1. des critères de sécurité au même titre que disponibilité, intégrité ou confidentialité
2. des hypothèses
3. des objectifs de sécurité
4. des exigences de sécurité fonctionnelle
5. des exigences de sécurité d'assurance

**Question 4 – "L'incendie" est :**

1. une vulnérabilité
2. une menace
3. un risque
4. une méthode d'attaque
5. un élément menaçant

**Question 5 – La menace est constituée :**

1. d'un élément menaçant et des vulnérabilités des entités
2. d'une méthode d'attaque et des vulnérabilités des entités
3. d'un élément menaçant et d'une méthode d'attaque
4. d'un élément menaçant, d'une méthode d'attaque et des vulnérabilités des entités
5. d'un élément menaçant, d'une méthode d'attaque, des vulnérabilités des entités et d'une opportunité

**Question 6 – Un risque est la combinaison :**

1. de la méthode d'attaque et des éléments menaçants
2. de la menace et de l'impact sur les besoins de sécurité et l'organisme
3. de la menace et des vulnérabilités
4. des prédictions météorologiques
5. des éléments du contexte

**Question 7 – Le traitement des risques est :**

1. l'utilisation systématique de données pour l'identification des origines des attaques et l'estimation du risque
2. l'ensemble du processus d'analyse du risque et d'évaluation du risque
3. le processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance d'un risque
4. le processus permettant de trouver, recenser et caractériser les origines des attaques (éléments menaçants et méthodes d'attaque)
5. le processus de sélection et de mise en œuvre des mesures visant à modifier le risque, ce qui signifie une réduction du risque, un transfert du risque ou une prise de risque

**Question 8 – "Un utilisateur légitime du système d'information ne doit pas pouvoir amorcer involontairement un matériel à partir d'un périphérique." Il s'agit :**

1. d'un objectif de sécurité
2. d'une hypothèse
3. d'une règle de bon sens
4. d'une exigence de sécurité fonctionnelle
5. d'une exigence de sécurité d'assurance

**Question 9 – "Mettre en oeuvre deux antivirus compatibles et les mettre régulièrement à jour", c'est :**

1. une exigence de sécurité
2. un objectif de sécurité
3. une vulnérabilité
4. une menace
5. un risque

**Question 10 – Laquelle des formulations suivantes décrivant le risque de manière théorique est-elle fausse ?**

1. l'organisme est impacté par l'atteinte des besoins de sécurité des éléments essentiels du fait de l'exploitation de vulnérabilités d'entités par un élément menaçant dans le cadre d'une méthode d'attaque avec une opportunité donnée
2. un élément menaçant exploite les vulnérabilités des éléments essentiels dans le cadre d'une méthode d'attaque avec une opportunité donnée afin de porter atteinte aux besoins de sécurité des entités et ainsi impacter l'organisme
3. il existe une opportunité donnée pour qu'un élément menaçant emploie une méthode d'attaque en s'appuyant sur les vulnérabilités des entités, porte ainsi atteinte aux besoins de sécurité des éléments essentiels et impacte l'organisme
4. une vulnérabilité d'une entité est utilisée dans le cadre d'une méthode d'attaque employée par un élément menaçant avec une opportunité donnée, ce qui provoque un impact dû à l'atteinte des besoins de sécurité des éléments essentiels
5. une méthode d'attaque est employée par un élément menaçant qui exploite les vulnérabilités des entités avec une opportunité donnée pour porter atteinte aux besoins de sécurité des éléments essentiels et ainsi impacter l'organisme

## 3.2 Réponses commentées

Les bonnes réponses apparaissent en texte gras et souligné.

**Question 1 – Le "devis du cabinet d'architecture @rchimed" est :**

1. **un élément essentiel**
2. une hypothèse
3. une règle de sécurité
4. une entité
5. un objectif de sécurité

Commentaires : le devis en lui-même est un élément essentiel, une information à protéger ; celle-ci repose sur plusieurs entités de types matériel, logiciel, réseaux, personnel, organisation et locaux.

**Question 2 – "Les utilisateurs du système d'information d'@rchimed ont connaissance des valeurs et des axes stratégiques exprimés par le directeur. En particulier, l'innovation et la réactivité sont des valeurs partagées. Dans ce contexte, chacun sait la valeur que représentent les logiciels de conception." Il s'agit :**

1. d'un élément essentiel
2. **d'une hypothèse**
3. d'une règle de sécurité
4. d'un objectif de sécurité
5. d'une exigence de sécurité fonctionnelle

Commentaires : il s'agit en effet d'un postulat, posé sur l'environnement opérationnel du système, permettant de procurer les fonctionnalités de sécurité attendues.

**Question 3 – "La preuve, l'opposabilité et la traçabilité" sont :**

6. des critères de sécurité au même titre que disponibilité, intégrité ou confidentialité
7. des hypothèses
8. des objectifs de sécurité
9. **des exigences de sécurité fonctionnelle**
10. des exigences de sécurité d'assurance

Commentaires : il est possible de considérer la preuve, l'opposabilité et la traçabilité comme des critères de sécurité au même titre que disponibilité, intégrité et confidentialité si cela correspond à un élément fort de la culture de l'organisme, mais il s'agit en fait d'exigences de sécurité permettant d'optimiser des risques généralement liés à l'intégrité et à des méthodes d'attaque telles que "reniement d'actions" ou "informations sans garantie de l'origine" [EBIOS].

**Question 4 – "L'incendie" est :**

1. une vulnérabilité
2. une menace
3. un risque
4. **une méthode d'attaque**
5. un élément menaçant

Commentaires : il s'agit d'une des 42 méthodes d'attaque types proposées dans la méthode [EBIOS].

**Question 5 – La menace est constituée :**

1. d'un élément menaçant et des vulnérabilités des entités
2. d'une méthode d'attaque et des vulnérabilités des entités
3. d'un élément menaçant et d'une méthode d'attaque
4. d'un élément menaçant, d'une méthode d'attaque et des vulnérabilités des entités
5. **d'un élément menaçant, d'une méthode d'attaque, des vulnérabilités des entités et d'une opportunité**

Commentaires : cela correspond à la description de la menace de l'[ISO 15408] ; les autres propositions sont incomplètes.

**Question 6 – Un risque est la combinaison :**

1. de la méthode d'attaque et des éléments menaçants
2. **de la menace et de l'impact sur les besoins de sécurité et l'organisme**
3. de la menace et des vulnérabilités
4. des prédictions météorologiques
5. des éléments du contexte

Commentaires : cela correspond à la définition de la méthode [EBIOS] (application du [Guide ISO 73] à la SSI) ; les autres propositions sont incomplètes.

**Question 7 – Le traitement des risques est :**

1. l'utilisation systématique de données pour l'identification des origines des attaques et l'estimation du risque
2. l'ensemble du processus d'analyse du risque et d'évaluation du risque
3. le processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance d'un risque
4. le processus permettant de trouver, recenser et caractériser les origines des attaques (éléments menaçants et méthodes d'attaque)
5. **le processus de sélection et de mise en œuvre des mesures visant à modifier le risque, ce qui signifie une réduction du risque, un transfert du risque ou une prise de risque**

Commentaires : cela correspond à la définition de la méthode [EBIOS] (application du [Guide ISO 73] à la SSI) ; les autres propositions correspondent respectivement à l'acceptation du risque (1), à l'appréciation du risque (2), à l'évaluation du risque (3) et à l'identification des origines des attaques (4).

**Question 8 – "Un utilisateur légitime du système d'information ne doit pas pouvoir amorcer involontairement un matériel à partir d'un périphérique." Il s'agit :**

1. **d'un objectif de sécurité**
2. d'une hypothèse
3. d'une règle de bon sens
4. d'une exigence de sécurité fonctionnelle
5. d'une exigence de sécurité d'assurance

Commentaires : il s'agit d'un objectif de sécurité traitant précisément un aspect du risque : la vulnérabilité ; il oriente donc le traitement du risque et interdit de traiter le risque d'une autre manière s'il est le seul à couvrir ce risque ; une exigence de sécurité fonctionnelle expliquerait les moyens à mettre en œuvre pour empêcher le fait qu'un utilisateur amorce involontairement un matériel à partir d'un périphérique.

**Question 9 – "Mettre en œuvre deux antivirus compatibles et les mettre régulièrement à jour", c'est :**

1. **une exigence de sécurité**
2. un objectif de sécurité
3. une vulnérabilité
4. une menace
5. un risque

Commentaires : cette exigence de sécurité fonctionnelle pourrait être encore plus affinée en spécifiant les antivirus et en précisant la fréquence de mise à jour et les procédures associées.

**Question 10 – Laquelle des formulations suivantes décrivant le risque de manière théorique est-elle fausse ?**

1. l'organisme est impacté par l'atteinte des besoins de sécurité des éléments essentiels du fait de l'exploitation de vulnérabilités d'entités par un élément menaçant dans le cadre d'une méthode d'attaque avec une opportunité donnée
2. **un élément menaçant exploite les vulnérabilités des éléments essentiels dans le cadre d'une méthode d'attaque avec une opportunité donnée afin de porter atteinte aux besoins de sécurité des entités et ainsi impacter l'organisme**
3. il existe une opportunité donnée pour qu'un élément menaçant emploie une méthode d'attaque en s'appuyant sur les vulnérabilités des entités, porte ainsi atteinte aux besoins de sécurité des éléments essentiels et impacte l'organisme
4. une vulnérabilité d'une entité est utilisée dans le cadre d'une méthode d'attaque employée par un élément menaçant avec une opportunité donnée, ce qui provoque un impact dû à l'atteinte des besoins de sécurité des éléments essentiels
5. une méthode d'attaque est employée par un élément menaçant qui exploite les vulnérabilités des entités avec une opportunité donnée pour porter atteinte aux besoins de sécurité des éléments essentiels et ainsi impacter l'organisme

Commentaires : les vulnérabilités sont des caractéristiques des entités sur lesquelles reposent les éléments essentiels, qui eux, ont des besoins de sécurité.

## Acronymes

<b>DCSSI</b>	Direction Centrale de la Sécurité des Systèmes d'Information
<b>EBIOS</b>	Expression des Besoins et Identification des Objectifs de Sécurité
<b>FEROS</b>	Fiche d'Expression Rationnelle des Objectifs de Sécurité des SI
<b>PP</b>	Profil de protection
<b>PSSI</b>	Politique de Sécurité des Systèmes d'Information
<b>SDSSI</b>	Schéma Directeur de la Sécurité des Systèmes d'Information
<b>SGDN</b>	Secrétariat Général de la Défense Nationale
<b>SI</b>	Système d'Information
<b>SSI</b>	Sécurité des Systèmes d'Information

## Références bibliographiques

<b>[EBIOS]</b>	<i>Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) – SGDN/SCSSI (2004).</i>
<b>[FEROS]</b>	<i>Fiche d'Expression Rationnelle des Objectifs de Sécurité des systèmes d'information (FEROS) – SGDN/SCSSI (1991).</i>
<b>[ISO 13335]</b>	<i>Information technology – Security techniques – Guidelines for the management of IT security (GMITS) – International Organization for Standardization (ISO) (2001).</i>
<b>[ISO 15408]</b>	<i>Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information, – International Organization for Standardization (ISO) – version 3 (2005).</i>
<b>[ISO 15446]</b>	<i>Technologies de l'information – Techniques de sécurité – Guide pour la production de profils de protection et de cibles de sécurité, – International Organization for Standardization (ISO) (2004).</i>
<b>[ISO 17799]</b>	<i>Information technology – Code of practice for information security management – International Organization for Standardization (ISO) (2005).</i>
<b>[ISO 27001]</b>	<i>Information technology – Security Techniques – Information security management systems – Requirements – International Organization for Standardization (ISO) (2005).</i>
<b>[ISO Guide 73]</b>	<i>Management du risque – Vocabulaire – Principes directeurs pour l'utilisation dans les normes – International Organization for Standardization (ISO) (2002).</i>

## 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](mailto: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