

## La gestion des risques

### Le risque

Le risque<sup>1</sup> de sécurité des systèmes d'information (SSI) est une combinaison d'une menace et des pertes qu'elle peut engendrer.

La menace SSI peut être considérée comme un scénario envisageable, avec une certaine opportunité (représentant l'incertitude).

Ce scénario met en jeu :

- une méthode d'attaque (action ou événement, accidentel ou délibéré),
- les éléments menaçants (naturels ou humains, qui agissent de manière accidentelle ou délibérée) susceptibles de l'employer,
- les vulnérabilités des entités (matériels, logiciels, réseaux, organisations, personnels, locaux), qui vont pouvoir être exploitées par les éléments menaçants dans le cadre de la méthode d'attaque.

Les pertes sont généralement estimées en termes d'atteinte des besoins de sécurité des éléments essentiels (le patrimoine informationnel et les processus associés) et d'impacts induits sur l'organisme.

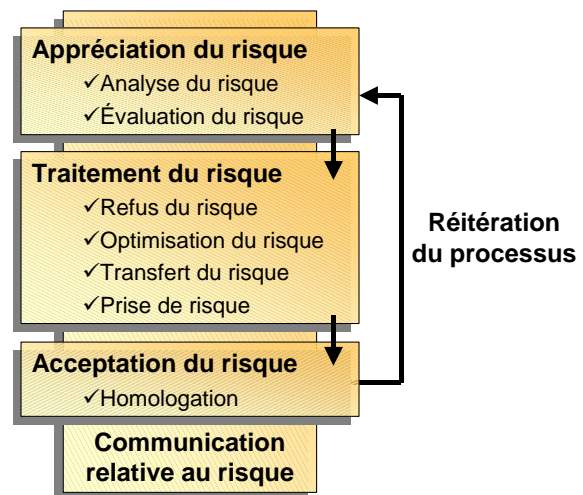
#### Exemple de risque décomposé :

Méthode d'attaque	piégeage du logiciel (introduction d'un ver)
Élément menaçant	un pirate expérimenté engagé par un concurrent
Entité	réseau WiFi
Vulnérabilité	possibilité d'administrer le réseau à distance
Opportunité	jugée moyenne
Atteinte des éléments essentiels	atteinte à la confidentialité (vol d'informations)
Impact sur l'organisme	perte d'avantages concurrentiels

<sup>1</sup> Le vocabulaire lié au risque et à la gestion des risques SSI est décliné du Guide ISO 73 – *Management du risque – Vocabulaire – Principes directeurs pour l'utilisation dans les normes* – International Organization for Standardization (ISO) (2002).

### La gestion des risques

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.



#### L'appréciation des risques

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

L'appréciation des risques consiste tout d'abord à décrire le contexte : l'organisme, le système d'information (SI), les éléments essentiels à protéger (informations, fonctions...), les entités sur lesquelles ils reposent, les enjeux liés au SI, les contraintes à prendre en compte...

Les besoins de sécurité des éléments essentiels doivent ensuite être exprimés (couramment en termes de disponibilité, d'intégrité et de confidentialité).

Les menaces pesant sur le SI doivent être identifiées et caractérisées en terme d'opportunité (représentant l'incertitude de ces menaces).

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

## Le traitement des risques

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 en déterminant le mode de traitement (refus, optimisation, transfert ou prise de risque) et en tenant compte des éléments du contexte. Ces objectifs représentent un cahier des charges exprimant la volonté de traiter les risques et ne préjugant pas des solutions à mettre en œuvre.

Le traitement des risques se poursuit par la détermination d'exigences de sécurité, techniques ou non, satisfaisant les objectifs de sécurité identifiés et décrivant la manière de traiter les risques (dissuasion, protection, détection, récupération, restauration, compensation...).

Enfin, les mesures de sécurité, techniques ou non techniques, spécifiées par les exigences de sécurité peuvent être mises en œuvre.

À l'issue, les risques ont été soit réduits, soit transférés (vers des tiers) et un ensemble de risques résiduels peut subsister. Il convient de les mettre en évidence et d'exprimer explicitement le choix de prendre ces risques.

## L'acceptation des risques

L'acceptation des risques SSI représente la décision d'accepter les risques traités.

Cette activité consiste en une homologation de sécurité. Elle est prononcée pour une durée déterminée, par une autorité d'homologation, qui doit être désignée et qui peut se reposer sur une Commission d'homologation qu'elle préside.

L'homologation de sécurité se base sur un dossier de sécurité dont le contenu doit être défini. Généralement, il est composé de l'étude des risques SSI, d'un document faisant état des objectifs de sécurité, d'une cible de sécurité précisant les exigences de sécurité et de la politique de sécurité (avec éventuellement ses documents d'application).

## La communication relative aux risques

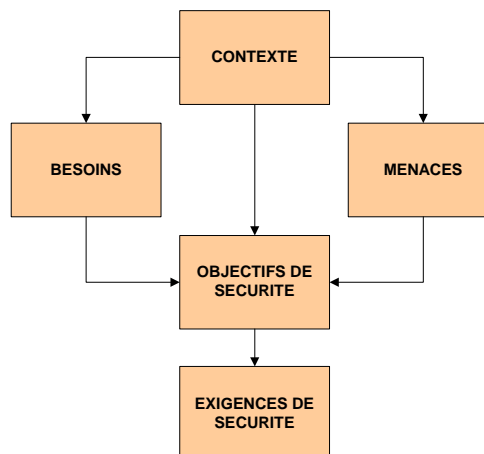
La communication relative aux risques SSI représente l'échange ou le partage d'informations concernant les risques.

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

# EBIOS : la méthode de gestion des risques SSI

## La méthode EBIOS et son logiciel

EBIOS (Expression des Besoins et Identification des Objectifs de sécurité) est la méthode de gestion des risques SSI diffusée gratuitement par la DCSSI.



Elle permet d'apprécier les risques SSI, de contribuer à leur traitement en spécifiant les exigences de sécurité à mettre en œuvre, de préparer l'ensemble du dossier de sécurité nécessaire à l'acceptation des risques et de fournir les éléments utiles à la communication relative aux risques.

EBIOS est actuellement employée dans le secteur public, dans le secteur privé, en France et à l'international.

Le logiciel libre EBIOS permet de suivre la démarche méthodologique, de personnaliser des bases de connaissances et de produire des livrables appropriés.

Par ailleurs, le Club EBIOS assure la pérennité de la méthode et des outils associés. Il réunit les experts du secteur public et du secteur privé en gestion des risques SSI.

Enfin, le centre de formation de la DCSSI propose des séances d'information et de formation sur la méthode EBIOS aux agents de l'État.

## Informations et contacts

[ebios.dcssi@sgdn.pm.gouv.fr](mailto:ebios.dcssi@sgdn.pm.gouv.fr)  
[conseil.dcssi@sgdn.pm.gouv.fr](mailto:conseil.dcssi@sgdn.pm.gouv.fr)  
<http://www.ssi.gouv.fr/fr/confiance/methodes>