Gestion des risques (EBIOS)

Gestion des risques

D'après la documentation de l'ANSSI

Introduction

La gestion des risques est définie comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque.

On distingue 3 thèmes généraux :

Améliorer la sécurisation des systèmes d'information.
Justifier le budget alloué à la sécurisation du système d'information.
Prouver la crédibilité du système d'information à l'aide des analyses effectuées.

La méthode de gestion des risques permet de dégager une vision globale des aspects sécurité, d'acquérir et d'utiliser un vocabulaire commun. Elle permet également de savoir mener une évaluation des risques de sécurité du global (politique) au local (mesures techniques).

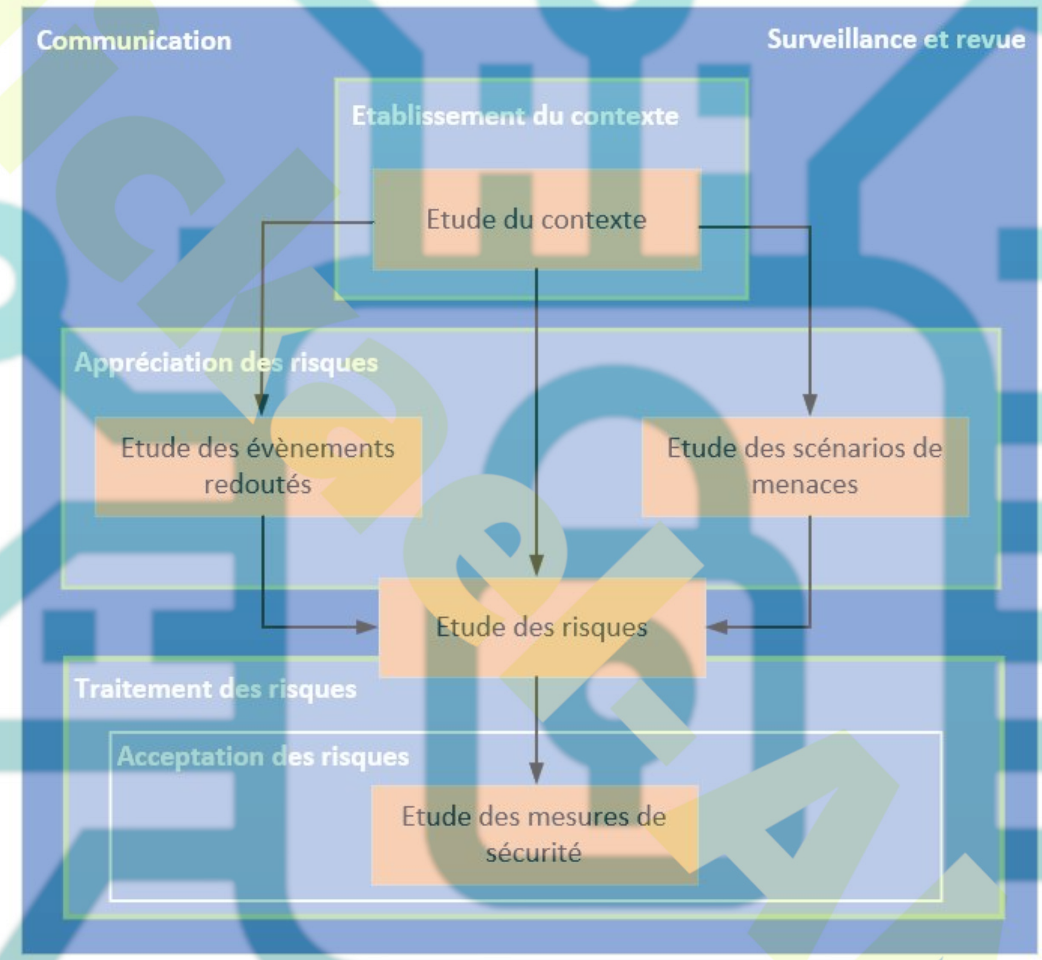
Les normes

ISO/IEC 31000 – décrit le processus de gestion des risques en général que les normes et méthodes doivent respecter.
ISO/IEC 27001 – fixe les exigences d'un système de management de la sécurité de l'information.
ISO/IEC 27002 – Catalogue de bonnes pratiques.
ISO/IEC 27005 – décrit le processus de gestion des risques que toutes les

méthodes doivent respecter.

EBIOS – décrit une démarche et des outils pratiques pour gérer les risques.

EBIOS



Le risque et le niveau de risque

Le risque

EBIOS utilise un scénario, avec un niveau donné, combinant un événement redouté et un ou plusieurs scénarios de menaces.

LES ÉLÉMENTS CONSTITUTIFS

Événement redouté

Scénario, avec un niveau donné, représentant une situation crainte par

l'organisme.

Scénarios de menaces

Scénario, avec un niveau donné, décrivant des modes opératoires.

1 – Un événement redouté combine :

- les sources de menace susceptibles d'en être à l'origine
  ex. : un acheteur agissant de manière délibérée par appât du gain
- un bien essentiel
  ex. : matériel acheté
- un critère de sécurité
  ex. : intégrité
- un besoin de sécurité concerné
  ex. : parfaite intégrité
- les impacts potentiels
  ex. : l'acheteur achète pour son propre compte , image de l'entreprise, perte d'argent

2 – Un scénario de menace combine :

- les sources de menaces susceptibles d'en être à l'origine
  ex. : l'acheteur
- un bien support
  ex. : système informatique de l'entreprise
- un critère de sécurité
  ex. : intégrité
- des menaces
  ex. : intrusion, élévation de privilèges et modification de contenu
- les vulnérabilités exploitables pour qu'elles se réalisent
  ex. : facilité d'accès aux données, possibilité de modifier les données.

Exemple réel

Les sujets de la première épreuve du baccalauréat 2018, pour la filière "sciences appliquées" ainsi que " philosophie et littérature arabe" , ont été diffusés sur internet. Il était possible pour les lycéens algériens de consulter les questions en avant-première en se rendant sur Facebook, à peine 10 minutes après la remise en marche du réseau.

Source de menace	Des enseignants
Menace	Divulgation
Bien support	Facebook
Vulnérabilité	Étourderie ou appât du gain
Bien essentiel	Informations sur le sujet de l'épreuve
Critère de sécurité	Confidentialité
Besoin de sécurité	Confidentialité
Impact	Annulation de l'épreuve

Le niveau de risque

Il correspond à l'estimation de sa gravité et de sa vraisemblance.

GRAVITÉ

Estimation de la hauteur des effets d'un événement redouté ou d'un risque. Elle représente ses conséquences. Elle dépend essentiellement :

- de la hauteur et du nombre des impacts
- de la valeur du bien considéré
- de la motivation des sources de menaces.

VRAISEMBLANCE

Estimation de la possibilité qu'un scénario de menace ou qu'un risque se produise. Elle représente sa force d'occurrence. Elle dépend essentiellement :

- de l'exposition aux menaces considérées
- de l'existence plus ou moins avérée de vulnérabilités
- de la facilité d'exploitation des vulnérabilités identifiées

- de la capacité des sources de
- menaces.

Les grands principes EBIOS

La notion de boîte à outils

EBIOS est une boîte à outils à multiple usages, qui n'est pas utilisée de la même façon selon :

- le sujet étudié
  ex. : un organisme dans son intégralité, une application particulière…
- les livrables attendus
  ex. : doctrine SSI, cible de sécurité…
- l'état du projet
  ex. : étude de faisabilité, maintien en conditions opérationnelles

Une réflexion préalable sur la stratégie de mise en œuvre est donc indispensable.

Une application souple

L'application d'EBIOS s'inscrit dans un cadre de référence

1 – Un cadre lié au sujet de l'étude

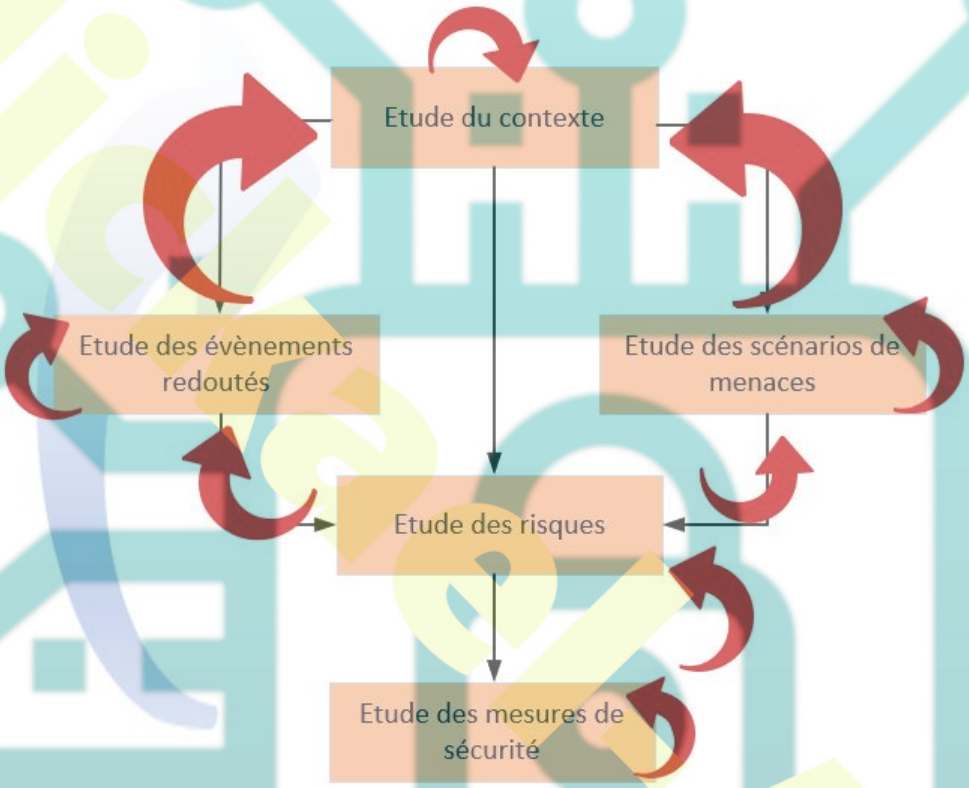
- Le niveau de maturité SSI
- Des référentiels applicables (réglementation, normes, méthodes internes…)
- Une culture spécifique à l'organisme

2 – Un cadre lié aux parties prenantes variées qui doivent être impliquées

- Responsables du périmètre de l'étude
- Responsable de la sécurité de l'information / RSSI
- Gestionnaire de risques
- Autorités de validation
- Dépositaire de biens essentiels (utilisateurs ou maîtrises d'ouvrage)
- Propriétaire de biens supports

Le vocabulaire et les pratiques employés doivent donc ê tre souples pour que la démarche soit efficace.

Un rebouclage nécessaire



Étude du contexte

Définir le cadre de la gestion des risques

- Savoir ce qui est dans le champ de l'étude et ce qui ne l'est pas
- Disposer des éléments contextuels susceptibles d'orienter les décision.

Les principales questions à se poser

Identifier les biens essentiels, leurs relations et leurs dépositaires	• Quels sont les informations et processus essentiels aux métiers ? • Quels sont les liens (inclusions, dépendances...) entre ces biens ? • Quel est le responsable de chacun de ces biens essentiels ?
Identifier les biens supports, leurs relations et leurs propriétaires	• Sur quoi reposent les biens essentiels (systèmes informatiques et de téléphonie, organisations, locaux) ? • Quels sont les liens (inclusions, dépendances...) entre ces biens ? • Quel est le responsable de chacun de ces biens supports ?
Déterminer le lien entre les biens essentiels et les biens supports	• Quel est le lien entre chaque bien essentiel et bien support ?
Identifier les mesures de sécurité existantes	• Quels sont les mesures de sécurité mises en œuvre ou prévues ? Sur quels biens supports reposent-elles ?

Étude des événements redoutés

Apprécier les événements redoutés

Obtenir une liste hiérarchisée de ce que craint l'organisme.

Les principales questions à se poser

Analyser tous les événements redoutés	• Quels sont les besoins de sécurité de chaque bien essentiel ? • Quelles sources de menaces peuvent les affecter ? • Quels seraient les impacts si l'événement se produisait ? • Quelle serait la gravité d'un tel événement ?
Évaluer chaque événement redouté	• Quelle est la hiérarchie des événements redoutés identifiés ?

Étude des scénarios de menaces

Apprécier les scénarios de menaces

Obtenir une liste hiérarchisée de tous les scénarios possible.

Les principales questions à se poser

Analyser tous les scénarios de menace	• Quelles menaces peuvent s'exercer sur chaque bien support ? • Quelles sources de menaces peuvent en être à l'origine ? • Quelles sont les vulnérabilités potentiellement utilisables ? • Y a-t-il des prérequis pour que la menace se réalise ? • Quelle est la vraisemblance des scénarios ?
Évaluer chaque scénario de menace	• Quelle est la hiérarchie des scénarios de menaces identifiés ?

Étude des risques

Apprécier les risques

Obtenir une liste hiérarchisée des risques réels pesant sur le sujet de l'étude.

Les principales questions à se poser

Analyser les risques	• Quels scénarios s'appliquent aux événements redoutés ? • Y a-t-il des mesures existantes pour traiter ces risques ? • Quelle est la gravité des risques ? • Quelle est la vraisemblance des risques ?
Évaluer les risques	• Quelle est la hiérarchie des risques identifiés ?

Identifier les objectifs de sécurité

Connaître les choix de traitement de chaque risque.

Les principales questions à se poser

Choisir les options de traitement de chaque risque	• Comment choisit-on de traiter chaque risque (réduire, transférer, éviter, prendre) ?
Analyser les risques résiduels	• Quels risques resteraient si les objectifs étaient satisfaits ?

Étude des mesures de sécurité

Formaliser les mesures de sécurité à mettre en œuvre

- Obtenir la liste des mesures de sécurité destinées à traiter les risques conformément aux objectifs de sécurité.
- Obtenir la liste des risques résiduels.

Les principales questions à se poser

Déterminer les mesures de sécurité	• Quelles mesures doivent être mise en place ? • Servent-elles à la prévention, la protection, ou la récupération ? • Sur quels biens supports reposent-elles ?
Analyser les risques résiduels	• Quelles sont les nouvelles valeurs de gravité et vraisemblance ? • Quels sont les scénarios toujours possibles ?
Établir une déclaration d'applicabilité	• Les paramètres à prendre en compte ont-ils bien été traités ?

Mettre en œuvre les mesures de sécurité

- Disposer d'un plan d'action
- Pouvoir décider de valider la manière dont les risques ont été gérés.

Les principales questions à se poser

Élaborer le plan d'action et suivre la réalisation des mesures de sécurité	• Comment planifie-t-on la mise en place des mesures ? • Où en est la mise en place des mesures de sécurité ?
Analyser les risques résiduels	• Quelles sont les nouvelles valeurs de gravité et vraisemblance ? • Quels sont les scénarios toujours possibles ?
Prononcer l'homologation de sécurité	• La manière dont les risques ont été gérés est-elle satisfaisante ? • Les risques résiduels sont-ils acceptables ?