ROYAUME DU MAROC

ADMINISTRATION DE LA DÉFENSE NATIONALE

DIRECTION GÉNÉRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

# GUIDE DE GESTION DES RISQUES

# DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

# INFORMATIONS

**AVERTISSEMENT**
Destiné à vous assister dans l'adoption d'une démarche cohérente et homogène pour la mise en conformité de la sécurité de vos systèmes d'information avec les règles de sécurité édictées par la Directive Nationale de la Sécurité des Systèmes d'information (DNSSI), ce guide élaboré par la DGSSI traite la démarche d'analyse de risques de la sécurité des systèmes d'information. Il est destiné à évoluer avec les usages, mais aussi avec vos contributions et retours d'expérience. Les recommandations citées dans ce guide sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, la DGSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par la DGSSI doit être soumise, au préalable, à la validation du Responsable de la Sécurité des Systèmes d'Information (RSSI) et de l'administrateur du système concerné.

**PERSONNES AYANT CONTRIBUÉ À LA RÉDACTION DE CE DOCUMENT :**

| Rédigé par | Version | Date |
|---|---|---|
| DGSSI | 1.0 | 12/12/2014 |

**ÉVOLUTION DU DOCUMENT :**

| Version | Date | Nature des modifications |
|---|---|---|
| 1.0 | 12/12/2014 | Version initiale |

**PUBLIC CONCERNÉ PAR CE DOCUMENT :**

| |
|---|
| Direction SI |
| RSSI |

**POUR TOUTE REMARQUE :**

| Contact | Email |
|---|---|
| DGSSI | contact@dgssi.gov.ma |

# Table des matières

# Introduction

Les organismes sont de plus en plus amenés à identifier leurs besoins organisationnels concernant les exigences en matière de sécurité de l'information, notamment pour se doter d'un système de management de la sécurité de l'information (SMSI) efficace tout en respectant les exigences contenues dans la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI).

Partant de ce constat, il est nécessaire de passer par une approche systématique qui soit au même temps adaptée à l'environnement de l'organisme et alignée sur la démarche générale de gestion du risque de l'organisme.

Le présent guide a pour but de donner un aperçu général sur le processus de gestion des risques en sécurité, d'en décrire les étapes qui viennent, notamment, en appui des exigences définies dans l'ISO/CEI 27001 (celles relatives au SMSI), et l'ISO/CEI 27005 qui décrit le système de management des risques liés à la sécurité de l'information.

Il s'adresse aux responsables et aux personnels concernés par la gestion des risques en sécurité de l'information au sein d'une organisation.

Sommairement, ce document décrit les activités liées à la gestion du risque en sécurité de l'information, et présente, à travers une étude de cas, le déroulement du processus de gestion du risque.

# 1 Concepts généraux

## 1.1 Termes et définitions

Pour les besoins du présent guide, les termes et définitions donnés dans l'ISO/-CEI 27001, l'ISO/CEI 27002 et les suivants s'appliquent.

**Impact :** Changement radical au niveau des objectifs métiers atteints.

**Risque de sécurité de l'information :** Possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et nuise donc à l'organisation. Le risque est mesuré en termes de combinaison entre la vraisemblance d'un événement et ses conséquences.

**Evitement du risque :** Décision de se retirer d'une situation à risque, ou de ne pas s'y engager.

**Communication du risque :** Echange ou partage de l'information concernant un risque entre le décideur et les autres parties prenantes.

**Estimation du risque :** Processus utilisé pour affecter des valeurs à la vraisemblance et aux conséquences d'un risque.

**Identification du risque :** Processus utilisé pour trouver, lister et caractériser les éléments à risque.
**Réduction du risque :** Mesures prises pour diminuer la vraisemblance, les conséquences négatives, ou les deux à la fois, associées à un risque.

**Maintien du risque :** Acceptation du poids de la perte ou du bénéfice de gain découlant d'un risque particulier. Dans le cadre des risques en sécurité de l'information, seules les conséquences négatives (pertes) sont prises en compte pour le maintien du risque.

**Transfert du risque :** Partage avec un tiers du poids de la perte ou du bénéfice de gain découlant d'un risque.

## 1.2 Présentation générale du processus de gestion du risque en sécurité de l'information

La DGSSI propose un processus simplifié de gestion du risque en sécurité de l'information déduit du modèle proposée dans la norme ISO/CEI 27005.

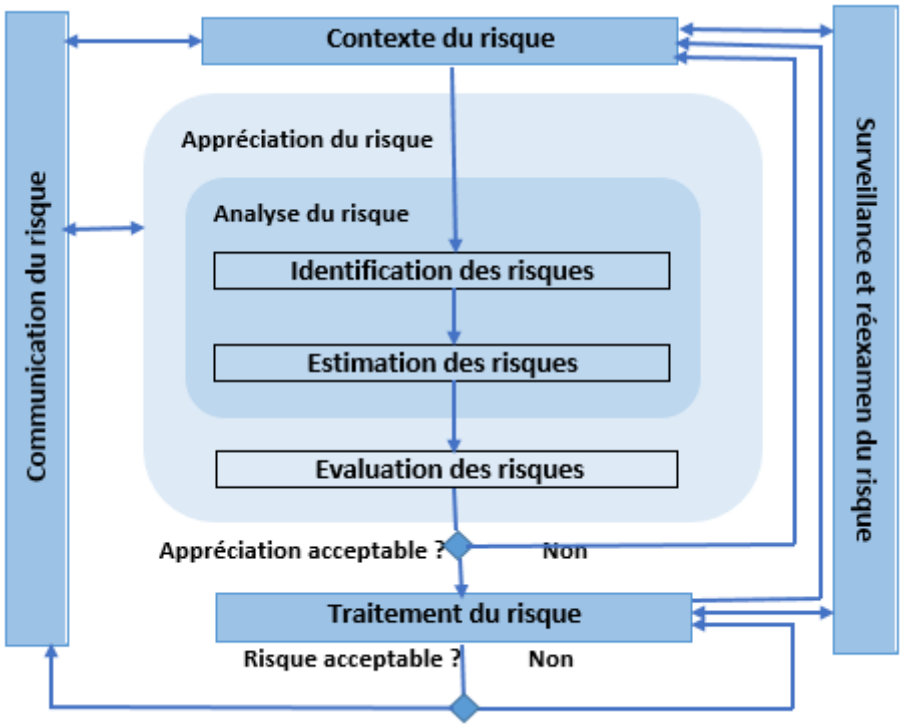


**FIGURE 1.1:** Processus de gestion du risque en sécurité de l'information

Comme illustré par la figure 1, le contexte est établi en premier lieu suivi d'une appréciation du risque. Si cette appréciation donne suffisamment d'informations pour déterminer correctement les actions nécessaires pour ramener les risques à un niveau acceptable, la tâche est alors terminée et suivie par le traitement du risque.

Si les informations ne sont pas suffisantes, une nouvelle itération de l'appréciation du risque s'exige et sera réalisée avec un contexte révisé (par exemple les critères d'évaluation du risque ou les critères d'impact).Au cours du processus de gestion du risque en sécurité de l'information, il est important que les risques et leur traitement soient validés par les dirigeants et communiqués aux personnes concernées.

# 2 Etablissement du contexte

## 2.1 Définitions des critères de base

Les organismes doivent établir dans un premier temps le contexte de la gestion du risque en sécurité de l'information et de déterminer les objectifs attendus de la gestion du risque en sécurité de l'information. Ces objectifs peuvent concerner, à titre d'exemples, la conformité avec la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI), la préparation d'un plan de continuité de l'activité, la préparation d'un plan de réponse aux incidents.
Ensuite, il est nécessaire de choisir ou d'élaborer une approche de gestion du risque adaptée précisant les critères d'évaluation du risque, les critères d'impact.

| **Etude de Cas** |
| --- |
| Le Directeur d'un organisme souhaite que les risques liés à la perte de confidentialité des informations pouvant empêcher l'organisme d'atteindre ses objectifs, soient gérés de manière continue. Et qu'une politique de sécurité de l'information soit produite, appliquée et contrôlée. |

**a. Critères d'évaluation du risque**

Il convient d'élaborer des critères d'évaluation du risque de l'organisme en sécurité de l'information en prenant en compte les éléments suivants :

- La valeur stratégique des processus informationnels,
- La criticité des actifs informationnels concernés,
- Les exigences légales et réglementaires ainsi que les obligations contractuelles,
- L'importance opérationnelle et métier de la disponibilité, de la confidentialité et de l'intégrité.

**Etude de Cas**

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de confidentialité :

| Niveau de l'échelle | Description détaillée de l'échelle |
|---|---|
| 1. Public | Informations publiques, destinées à être diffusées à l'extérieur de l'organisme. |
| 2. Interne | Informations destinées à être diffusées en interne à l'organisme. |
| 3. Confidentiel | La divulgation publique d'une information classée confidentielle peut nuire sérieusement à l'organisme. |
| 4. Très confidentiel | La divulgation publique d'une information classée très confidentielle peut causer un dommage grave. |

**a. Critères d'impact**

Il convient que les critères d'impact soient élaborés et spécifiés en fonction du niveau de dommages ou de coûts pour l'organisme et qui peuvent être causés par un événement lié à la sécurité de l'information, et ce en tenant compte des points suivants :

- Le niveau de classification de l'actif informationnel impacté,
- L'atteinte à la sécurité de l'information (par exemple une perte de confidentialité, d'intégrité et de disponibilité),
- Les erreurs opérationnelles (équipes internes ou tierces parties),
- La perturbation des plans d'actions et des délais,
- Le non-respect des exigences légales, réglementaires ou contractuelles.
- Les attentes et les perceptions des parties prenantes ainsi que la réputation de l'organisme et dans certains cas des conséquences négatives sur la valorisation financière.

**Etude de Cas :**

L'échelle suivante sera utilisée pour estimer l'impact des risques :

| Niveau de l'échelle | Description détaillée de l'échelle |
|---|---|
| 1. Négligeable | L'organisme surmontera les impacts sans aucune difficulté |
| 2. Limitée | L'organisme surmontera les impacts malgré quelques difficultés |
| 3. Importante | L'organisme surmontera les impacts avec de sérieuses difficultés |
| 4. Critiquel | L'organisme ne surmontera pas les impacts (sa survie est menacée) |

L'échelle suivante sera utilisée pour estimer la vraisemblance des scénarios de menaces et des risques :

| Niveau de l'échelle | Description détaillée de l'échelle |
|---|---|
| 1. Minime | Cela ne devrait pas se (re)produire |
| 2. Significative | Cela pourrait se (re)produire |
| 3. Forte | Cela devrait se (re)produire un jour ou l'autre |
| 4. Maximale | Cela va certainement se (re)produire prochainement |

## 2.2 Domaine d'application

Il est nécessaire de définir le domaine d'application du processus de gestion du risque en sécurité de l'information afin de garantir que tous les actifs concernés soient pris en compte dans l'appréciation du risque. En outre, il est nécessaire d'identifier les limites afin de traiter les risques susceptibles de survenir au travers de ces interfaces.

L'organisme devrait considérer les informations suivantes :
- Les objectifs stratégiques et les politiques de l'organisme,
- Les processus métier,
- Les fonctions et la structure de l'organisme,
- Les exigences légales, réglementaires et contractuelles applicables à l'organisme,
- La politique de sécurité de l'information de l'organisme,
- L'approche globale de l'organisme vis-à-vis de la gestion du risque,
- Les actifs informationnels,
- Les localisations de l'organisme et leurs caractéristiques géographiques,
- Les contraintes affectant l'organisme (liées aux processus métiers par exemple),
- Les attentes des parties prenantes,
- L'environnement socioculturel,
- Les interfaces (c'est-à-dire les échanges d'information avec l'environnement).

De plus, il convient que l'organisme justifie toute exclusion du domaine d'application.

**Etude de Cas :**

Il s'agit d'un organisme constitué d'une quinzaine de personnes, sa vocation principale est le développement de projets informatiques pour ses clients.

Ses **missions** consistent principalement à élaborer des projets informatiques.

Ses **valeurs** sont la réactivité, la précision des travaux, la créativité et la communication. Les **principaux métiers** représentés sont le développement informatique et l'administration des systèmes et réseaux.

Sa **structure organisationnelle** est fonctionnelle avec une direction, un secrétariat, un service informatique et un service comptabilité.

Ses **axes stratégiques** sont d'une part l'utilisation des nouvelles technologies dans un but d'ouverture vers l'extérieur et d'optimisation des moyens, et d'autre part la consolidation de l'image de marque (protection des projets sensibles).

Ses principaux processus métiers sont :
- Le développement des projets informatiques,
- L'administration des réseaux,
- La gestion des relations commerciales.

Le choix du périmètre d'étude est porté sur le service informatique uniquement.

## 2.3 Organisation de la gestion du risque en sécurité de l'Information

Les organismes sont tenus à déterminer et maintenir l'organisation et les responsabilités relatives au processus de gestion du risque en sécurité de l'information.
Les principaux rôles et responsabilités de cette organisation sont les suivants :

- Elaboration du processus de gestion du risque en sécurité de l'information adapté à l'organisme,
- Identification et analyse des parties prenantes,
- Définition des rôles et des responsabilités de toutes les parties, à la fois internes et externes à l'organisme,
- Etablissement des relations entre l'organisme et les parties prenantes, des interfaces avec les fonctions de gestion de risque de haut niveau de l'organisme (par exemple, gestion du risque opérationnel) ainsi que des interfaces avec d'autres projets ou activités, si cela est pertinent,
- Détermination des processus d'escalade,
- Spécification des différents livrables à conserver.

Il convient que cette forme organisationnelle soit approuvée par les dirigeants concernés au sein de l'organisme.

**Etude de Cas :**

Afin de réaliser cette mission, l'organisme en question prévoit de suivre le modèle RACI comme suit :

| Les rôles et responsabilités | Directeur | RSSI | Service informatique | Ressources éstimés en J/H |
|---|---|---|---|---|
| Définir le cadre de la gestion des risques | R | I | I | 2 |
| Préparer les critères de base | A | R | I | 2 |
| Identifier les biens | I | R | I | 3 |
| Identifier les menaces et vulnérabilités | I | R | C | 3 |
| Apprécier les risques | | R | I | 3 |
| Formaliser les mesures de sécurité à mettre en œuvre | I | R | I | 3 |
| Mettre en œuvre les mesures de sécurité | A | R | C | Cette action sera réalisée de suite |

"R" = Responsable de la mise en œuvre de l'activité,
"A" = Autorité légitime pour approuver l'activité,
"C" = Consulté pour obtenir les informations nécessaires à l'activité,
"I" = Informé des résultats de l'activité.

# 3 Appréciation du risque en sécurité de l'information

L'appréciation du risque comprend les activités suivantes :
- L'analyse du risque ;
- L'évaluation du risque.

L'appréciation du risque détermine la valeur des actifs informationnels, identifie les menaces et les vulnérabilités applicables existantes (ou susceptibles d'exister), identifie les mesures de sécurité existantes et leurs effets sur le risque identifié, détermine les conséquences potentielles puis classe les risques ainsi obtenus par ordre de priorité en cohérence avec les critères d'évaluation du risque tels que définis lors de l'établissement du contexte.

## 3.1 Analyse de risque

### 3.1.1 Identification de risque

L'objectif de l'identification du risque est de déterminer les événements susceptibles de se produire et causant une perte potentielle, et de donner un aperçu de comment, où, et quand cette perte pourrait survenir.

**a. Identification des actifs**

Un actif désigne tout élément ayant de la valeur pour l'organisme et nécessitant, par conséquent, une protection. Il convient d'identifier le propriétaire de chaque actif afin d'assurer la responsabilité comme l'indique la DNSSI. Les actifs peuvent être répartis en différents types, et sous types comme indiqué dans l'annexe 1.

**Etude de Cas :**

Le système d'information de l'organisme, objet de l'étude de cas, est en évolution permanente avec une très grande diversité d'informations gérées sur des systèmes hétérogènes (OS : [UNIX, SOLARIS, Windows Seven]), différentes bases de données [Oracle, Informix], et des applications.

Le bureau d'étude dispose d'un site web publié et géré par son service informatique.

L'architecture réseau est un siège fédérateur Gigabit Ethernet, composé de 2 VLAN. Le réseau informatique est découpé en plusieurs DMZ (zones intermédiaires entre Internet et le réseau interne) pour protéger les serveurs en production via des règles de filtrage des flux réseaux paramétrées au niveau firewall.

La Protection antivirale assurée par deux logiciels, maintenus avec mises à jour et qui n'est pas centralisée.

La qualité de service des applications informatiques est assurée par un moyen de monitoring qui permet et sans aucune installation lourde, de superviser les applications internet et extranet, et les systèmes de messagerie électronique.

**b. Identification d'un scenario de risque et ces conséquences**

Afin de déterminer les scénarios des risques, il est nécessaire d'identifier :

- **Les sources des menaces :** celles-ci peuvent être accidentelles, délibérées ou environnementales.
- **Les menaces :** peuvent survenir de l'intérieur ou de l'extérieur de l'organisme. Une liste de menaces pouvant être exploitée, est consignée dans l'annexe n 2.
- **Les vulnérabilités :** elles n'entraînent pas de dommage en elle-même, puisque la présence d'une menace est nécessaire pour l'exploiter. Une vulnérabilité à laquelle ne correspond aucune menace peut ne pas exiger la mise en œuvre d'une mesure de sécurité. Il convient de noter qu'une mesure de sécurité mal mise en œuvre, ou présentant un dysfonctionnement, ou encore utilisée de manière incorrecte peut constituer une vulnérabilité. Une liste de vulnérabilités pouvant être exploitée, est consignée dans l'annexe n 3.
- **Les conséquences des scénarios d'incident :** doivent être déterminées en tenant compte des critères d'impact définis lors de l'établissement du contexte.

**Etude de Cas :**

L'étude se focalisera sur le processus métier qui consiste au développement des projets informatiques contenant des informations sensibles, un scénario de menace susceptible d'atteindre au besoin de confidentialité, est déterminé comme suit :

| Processus | Développement des projets informatiques sensibles |
|---|---|
| Evaluateur | RSSI |
| Scénario de menace | Abus de droits |
| Type de menace | Compromission des fonctions |
| Sources de menace | Pirate informatique |
| Type d'actif | Logiciel |
| Vulnérabilité(s) | Failles bien connues dans le logiciel |
| Risque | Risque sur la confidentialité |
| Type d'impact | Image de marque |
| Niveau d'impact | Importante |
| Niveau de vraisemblance | Minime |

**c.Identification des mesures de sécurité existantes**

Les organismes doivent procéder à une identification des mesures de sécurité existantes pour éviter des travaux ou des coûts inutiles dus, par exemple, à une redondance des mesures de sécurité. En outre, tout en identifiant les mesures de sécurité existantes, il est nécessaire d'effectuer un contrôle afin de garantir que les mesures de sécurité puissent fonctionner correctement.

Les activités suivantes peuvent s'avérer utiles pour l'identification des mesures de sécurité existantes ou prévues :

- Le réexamen des documents contenant des informations relatives aux mesures de sécurité (par exemple, les plans de mise en œuvre du traitement du risque),
- La vérification avec les personnes responsables de la sécurité de l'information (par exemple un responsable de la sécurité du système d'information, un responsable de la sécurité physique) et avec les utilisateurs afin de vérifier quelles mesures de sécurité sont réellement mises en œuvre pour le processus d'information ou le système d'information considérés,
- La revue sur site des mesures de sécurité physiques, en comparant les mesures mises en œuvre avec la liste des mesures à déployer et en vérifiant les mesures mises en œuvre pour savoir si elles fonctionnent correctement et efficacement,
- L'examen des résultats des audits internes.

**Etude de Cas :**

Afin de se prémunir du risque de divulgation des informations liées au processus métier du développement des projets informatiques sensibles, l'organisme établit des mesures de sécurité telle que l'accès restreint au code source de ces projets informatiques.

### 3.1.2 Estimation du risque

**a. Méthodologie d'éstimation du risque**

L'estimation du risque attribue des valeurs à la vraisemblance et aux impacts (conséquences) d'un risque. Ces valeurs peuvent être quantitatives ou qualitatives, en pratique :

- L'estimation qualitative utilise une échelle d'attributs qualificatifs pour décrire l'ampleur des conséquences potentielles (par exemple : faible, moyenne et élevée) ainsi que la vraisemblance (probabilité de leur occurrence). Elle est souvent utilisée en premier lieu pour obtenir une indication générale du niveau de risque et pour mettre en exergue les principaux risques.
- L'estimation quantitative utilise une échelle comportant des valeurs, à la fois pour les impacts et pour la vraisemblance, à l'aide de données obtenues à partir de sources diverses.

Le risque estimé est une combinaison de la vraisemblance d'un scénario d'incident et de ses impacts.

Ci-après une présentation d'une méthode d'appréciation détaillée du niveau de risque.

**b. Appreciation détaillée du risque en sécurité de l'Information**

Le processus d'appréciation détaillée du risque en sécurité de l'information implique l'identification et l'évaluation approfondie des actifs, l'appréciation des menaces par rapport à ces actifs et l'appréciation des vulnérabilités. Les résultats obtenus grâce à ces activités sont alors utilisés pour apprécier les risques, puis pour identifier le traitement du risque.

Le tableau suivant est utilisé pour l'appréciation des risques identifiés :

| Type d'actifs | Libellé d'actifs | Besoin en DIC* | Libellé menace | Libellé vulnérabilité | Niveau d'impact | Niveau de vraisemblance | Gravité du risque | Commentaires |
|---|---|---|---|---|---|---|---|---|
| Logiciel | Logiciel de gestion de bases de données | Confidentialité | Abus de droits | Failles bien connues dans le logiciel | 3 | 1 | 2 | |
| | | | Usurpation de droits | Mauvaise gestion des mots de passe | 3 | 3 | 3 | |

**Gravité de risque :**

La valeur de la gravité du risque est l'intersection de la valeur d'impact et la valeur de vraisemblance d'un risque donné comme le montre le tableau suivant :

| | | | | |
|---|---|---|---|---|
| I=4 | G=3 | G=3 | G=4 | G=4 |
| I=3 | G=2 | G=3 | G=3 | G=4 |
| I=2 | G=1 | G=2 | G=3 | G=3 |
| I=1 | G=1 | G=1 | G=1 | G=3 |
| | V=1 | V=2 | V=3 | V=4 |

## 3.2 Evaluation du risque

Il convient que les critères d'évaluation du risque utilisés pour prendre des décisions soient cohérents avec le contexte interne et externe de gestion du risque en sécurité de l'information, et qu'ils tiennent compte des objectifs de l'organisme. Les décisions prises lors de l'activité d'évaluation du risque sont essentiellement basées sur le niveau acceptable du risque. Lors de l'étape d'évaluation du risque, les exigences légales et réglementaires sont des facteurs essentiels qu'il convient de prendre en compte en plus des risques estimés.

**Etude de Cas :**

L'organisme a décidé de considérer que les scénarios de gravité égale 4 sont intolérables, les scénarios de gravité égale à 3 sont inadmissibles et les scénarios de niveau de gravité inférieur sont tolérables.

| | | | | |
|---|---|---|---|---|
| I=4 | G=3 | G=3 | G=4 | G=4 |
| I=3 | G=2 | G=3 | G=3 | G=4 |
| I=2 | G=1 | G=2 | G=3 | G=3 |
| I=1 | G=1 | G=1 | G=1 | G=3 |
| | V=1 | V=2 | V=3 | V=4 |

# 4 Traitement du risque en sécurité de l'Information

Quatre options de traitement du risque sont possibles : la réduction du risque, le maintien du risque, l'évitement du risque ou le transfert de risque.

Il convient de choisir les options de traitement du risque sur la base des résultats de l'appréciation du risque, du coût prévu de mise en œuvre ainsi que des bénéfices attendus de ces options.

**a. Réduction du risque**

En général, les mesures de sécurité peuvent fournir un ou plusieurs types de protection : la correction, l'élimination, la prévention, l'atténuation des impacts, la dissuasion, la détection, la récupération, la surveillance et la sensibilisation.

Lors de la sélection des mesures de sécurité, il est important d'évaluer le coût d'acquisition, de mise en œuvre, d'administration, d'exploitation, de surveillance et de maintenance des mesures de sécurité par rapport à la valeur des actifs protégés.

En outre, il convient de considérer le retour sur investissement en termes de réduction du risque et de nouvelles opportunités offertes par certaines mesures de sécurité. De plus, il convient de prendre en compte les compétences spécifiques susceptibles d'être nécessaires pour définir et mettre en œuvre de nouvelles mesures de sécurité, ou pour modifier les mesures existantes.

**b. Maintien du risque**

Si le niveau de risque répond aux critères d'acceptation du risque, il n'est pas nécessaire de mettre en œuvre d'autres mesures de sécurité, le risque peut alors être conservé.

**c. Evitement du risque**

Lorsque les risques identifiés sont jugés trop élevés ou lorsque les coûts de mise en œuvre d'autres options de traitement du risque dépassent les bénéfices attendus, il est possible de prendre la décision d'éviter complètement le risque, en abandonnant une ou plusieurs activités prévues ou existantes, ou en modifiant les conditions dans lesquelles l'activité est effectuée. Par exemple, pour les risques découlant d'incidents naturels, il peut être plus rentable de déplacer physiquement les moyens de traitement de l'information à un endroit où le risque

n'existe pas ou est maîtrisé.

**d. Transfert du risque**

Le transfert du risque implique la décision de partager certains risques avec des parties externes. Il peut créer de nouveaux risques ou modifier les risques identifiés existants. Par conséquent, un autre traitement de risque peut s'avérer nécessaire.

# 5 Communication du risque en sécurité de l'information

La communication du risque consiste en une activité bidirectionnelle visant à atteindre un accord sur la manière de gérer les risques par un échange et/ou un partage des informations relatives au risque entre les décideurs et les autres parties prenantes. Ces informations comprennent, sans toutefois s'y limiter, l'existence, la nature, le type, la vraisemblance, la gravité, le traitement des risques.

Il convient qu'un organisme élabore des plans de communication du risque en fonctionnement normal ainsi que dans les situations d'urgence. Par conséquent, il convient de procéder de manière continue à l'activité de communication du risque.

La coordination entre les principaux décideurs et les principales parties prenantes peut être mise en œuvre en constituant un comité, de manière à ce qu'un débat sur les risques, sur leur niveau de priorité et le caractère adapté de leur traitement puisse avoir lieu.

# 6 Surveillance et réexamen du risque en sécurité de l'information

Les risques ne sont pas statiques. Les menaces, les vulnérabilités, la vraisemblance ou les conséquences peuvent changer brutalement sans aucune indication préalable. Par conséquent, une surveillance constante est nécessaire pour détecter ces changements (les nouveaux actifs ayant été inclus dans le domaine d'application de la gestion du risque, les nouvelles menaces et vulnérabilités susceptibles d'être actives à la fois à l'intérieur et à l'extérieur de l'organisme et qui n'ont pas été appréciées, les incidents liés à la sécurité de l'information, etc.).

Une surveillance et un réexamen permanents sont nécessaires pour garantir que le contexte, les résultats de l'appréciation et du traitement du risque, ainsi que les plans de gestion, restent adaptés aux circonstances.

## ANNEXE 1 : IDENTIFICATION DES ACTIFS

Il est possible de distinguer les actifs de la manière suivante :

| **Types d'actifs** | **Sous types** | **Description** |
|---|---|---|
| Actifs primordiaux : les processus centraux et informations de l'activité | • Processus | • Processus support et métier. |
| | • Informations | • Informations créées, traitées, stockées, archivées, etc. par l'entité. |
| Actifs en support : sur lesquels reposent les actifs primordiaux du domaine d'application | • Matériel | • Equipement de traitement des données (serveur, poste de travail fixe, ordinateur portable, etc.)<br>• Périphériques de traitement (imprimante, lecteur de disque amovible…)<br>• Support de données : Il s'agit de supports destinés à stocker des données ou des fonctions (CD ROM, cartouche de secours, disque dur amovible, clé USB, etc.),<br>• Autres supports (papier, diapositive, etc.). |
| | • Logiciels | • Systèmes d'exploitation,<br>• Applications métier ou supports. |
| | • Réseau | • Supports (Ethernet, VOIP, ADSL, spécifications de protocole sans fil (par exemple Wifi 802.11), etc.)<br>• Relais actif ou passif (pont, switch, routeur, concentrateur, sélecteur, central automatique, etc.)<br>• Interfaces de communication |
| | • Personnel | • Décideurs<br>• RSSI<br>• Développeurs<br>• Personnel d'exploitation / de maintenance<br>• Utilisateurs |
| | • Site | • Locaux de l'entité<br>• Environnement extérieur (tous les emplacements au sein desquels les moyens de sécurité de l'entité ne peuvent s'appliquer).<br>Exemples : résidence du personnel, locaux d'une autre entité, environnement situé à l'extérieur du site (zone urbaine, zone dangereuse).<br>• Zone<br>Une zone est formée par une limite physique de protection créant des cloisons dans les locaux d'une entité.<br>Exemples : bureaux, zone d'accès réservé, zone sécurisée.<br>• Services et moyens (sources et câblage) nécessaires pour alimenter le matériel et les périphériques de technologie de l'information (alimentation électrique basse tension, onduleur, appareil de climatisation, etc.). |
| | • structure de l'entité | • Autorités (entité responsable, siège de l'entité).<br>• Structure de l'entité (organigramme comprenant les différentes branches de l'entité)<br>• Tiers (sous-traitants, fournisseurs, fabricants, etc.). |

## ANNEXE 2 : TABLEAU DES MENACES

Le tableau suivant donne des exemples de menaces type. Cette liste peut être utilisée lors du processus d'appréciation des menaces. La liste suivante indique pour chaque type de menace si D (délibérée) pour les actions délibérées destinées aux actifs informationnels, A (accidentelle) pour toutes les actions humaines qui peuvent endommager les actifs informationnels de manière accidentelle, ou E (environnementale) pour tous les incidents qui ne reposent pas sur des actions humaines.

| Type | Menaces | Origine |
|---|---|---|
| Dommage physique | Incendie | A, D, E |
| | Dégât des eaux | A, D, E |
| | Pollution | A, D, E |
| | Accident majeur | A, D, E |
| | Destruction de matériel ou de support | A, D, E |
| | Poussière, corrosion, congélation | A, D, E |
| Catastrophes naturelles | Phénomène climatique | E |
| | Phénomène sismique | E |
| | Phénomène volcanique | E |
| | Phénomène météorologique | E |
| | Inondation | E |
| Perte de services essentiels | Panne du système de climatisation ou d'alimentation en eau | A, D |
| | Perte de la source d'alimentation en électricité | A, D, E |
| | Panne du matériel de télécommunications | A, D |
| Perturbation due à des rayonnements | Rayonnements électromagnétiques | A, D, E |
| | Rayonnements thermiques | A, D, E |
| | Impulsions électromagnétiques | A, D, E |
| Compromission d'informations | Interception de signaux d'interférence compromettants | D |
| | Espionnage à distance | D |
| | Ecoute | D |
| | Vol de supports ou de documents | D |
| | Vol de matériel | D |
| | Récupération de supports recyclés ou mis au rebut | D |
| | Divulgation | A, D |
| | Données provenant de sources douteuses | A, D |
| | Piégeage de matériel | D |
| | Piégeage de logiciel | A, D |
| | Géolocalisation | D |
| Défaillances techniques | Panne de matériel | A |
| | Dysfonctionnement du matériel | A |
| | Saturation du système d'information | A, D |
| | Dysfonctionnement du logiciel | A |
| | Violation de la maintenabilité du système d'information | A, D |

**ANNEXE 2 : TABLEAU DES MENACES**

| | | |
|---|---|---|
| Actions non autorisées | Utilisation non autorisée du matériel | D |
| | Reproduction frauduleuse de logiciel | D |
| | Utilisation de logiciels copiés ou de contrefaçon | A, D |
| | Corruption de données | D |
| | Traitement illégal de données | D |
| Compromission des fonctions | Erreur d'utilisation | A |
| | Abus des droits | A, D |
| | Usurpation de droits | D |
| | Déni d'actions | D |
| | Violation de la disponibilité du personnel | A, D, E |

## ANNEXE 3 : EXEMPLES DE VULNERABILITES

Des exemples de vulnérabilités sont consignés dans le tableau suivant :

| Types | Exemples de vulnérabilités | Exemples de menaces |
|---|---|---|
| Matériel | Maintenance insuffisante/mauvaise installation des supports de stockage | Violation de la maintenabilité du système d'information |
| | Absence de programmes de remplacement périodique | Destruction de matériel ou de support |
| | Sensibilité à l'humidité, à la poussière, aux salissures | Poussière, corrosion, congélation |
| | Sensibilité aux rayonnements électromagnétiques | Rayonnements électromagnétiques |
| | Absence de contrôle efficace de modification de configuration | Erreur d'utilisation |
| | Sensibilité aux variations de tension | Perte de la source d'alimentation en électricité |
| | Sensibilité aux variations de température | Phénomène météorologique |
| | Stockage non protégé | Vol de supports ou de documents |
| | Manque de prudence lors de la mise au rebut | Vol de supports ou de documents |
| | Reproduction non contrôlée | Vol de supports ou de documents |
| Logiciel | Tests de logiciel absents ou insuffisants | Abus de droits |
| | Failles bien connues dans le logiciel | Abus de droits |
| | Pas de fermeture de session en quittant le poste de travail | Abus de droits |
| | Mise au rebut et réutilisation de supports de stockage sans véritable effacement | Abus de droits |
| | Absence de traces d'audit | Abus de droits |
| | Attribution erronée des droits d'accès | Abus de droits |
| | Logiciel distribué à grande échelle | Corruption de données |
| | Application de programmes de gestion à de mauvaises données en termes de temps | Corruption de données |

**ANNEXE 3 : EXEMPLES DE VULNERABILITES**

| | | |
|---|---|---|
| | Interface utilisateur compliquée | Erreur d'utilisation |
| | Absence de documentation | Erreur d'utilisation |
| | Réglage incorrect de paramètres | Erreur d'utilisation |
| | Dates incorrectes | Erreur d'utilisation |
| | Absence de mécanismes d'identification et d'authentification tels que l'authentification des utilisateurs | Usurpation de droits |
| | Tableaux de mots de passe non protégés | Usurpation de droits |
| | Mauvaise gestion des mots de passe | Usurpation de droits |
| | Activation de services non nécessaires | Traitement illégal de données |
| | Logiciel neuf ou en phase de rodage | Dysfonctionnement du logiciel |
| | Spécifications des développeurs confuses ou incomplètes | Dysfonctionnement du logiciel |
| | Absence de contrôle efficace des modifications | Dysfonctionnement du logiciel |
| | Chargement et utilisation non contrôlés du logiciel | Piégeage de logiciel |
| | Absence de copies de sauvegarde | Piégeage de logiciel |
| | Absence de protection physique du bâtiment, des portes et des fenêtres | Vol de supports ou de documents |
| | Impossibilité de produire les comptes rendus de gestion | Utilisation non autorisée du matériel |
| Réseau | Absence de preuves d'envoi ou de réception d'un message | Déni d'actions |
| | Voies de communication non protégées | Ecoute |
| | Trafic sensible non protégé | Ecoute |
| | Mauvais câblage | Panne du matériel de télécommunications |
| | Point de défaillance unique | Panne du matériel de télécommunications |

**ANNEXE 3 : EXEMPLES DE VULNERABILITES**

| | | |
|---|---|---|
| | Absence d'identification et d'authentification de l'expéditeur et du destinataire | Usurpation de droits |
| | Architecture réseau non sécurisée | Espionnage à distance |
| | Transfert de mots de passe en clair | Espionnage à distance |
| | Gestion réseau inadaptée (résilience du routage) | Saturation du système d'information |
| | Connexions au réseau public non protégées | Utilisation non autorisée du matériel |
| Personnel | Absence de personnel | Violation de la disponibilité du personnel |
| | Procédures de recrutement inadaptées | Destruction de matériel ou de support |
| | Formation insuffisante à la sécurité | Erreur d'utilisation |
| | Utilisation incorrecte du logiciel et du matériel | Erreur d'utilisation |
| | Absence de sensibilisation à la sécurité | Erreur d'utilisation |
| | Absence de mécanismes de surveillance | Traitement illégal de données |
| | Travail non surveillé d'une équipe extérieure ou de l'équipe d'entretien | Vol de supports ou de documents |
| | Absence de politiques relatives à la bonne utilisation de supports de télécommunications et de la messagerie | Utilisation non autorisée du matériel |
| Site | Utilisation inadaptée ou négligente du contrôle d'accès physique aux bâtiments et aux salles | Destruction de matériel ou de support |
| | Emplacement situé dans une zone sujette aux inondations | Inondation |
| | Réseau électrique instable | Perte de la source d'alimentation en électricité |
| | Absence de protection physique du bâtiment, des portes et des fenêtres | Vol de matériel |

**ANNEXE 3 : EXEMPLES DE VULNERABILITES**

| | | |
|---|---|---|
| Organisme | Absence de procédure formelle relative à l'enregistrement et au retrait des utilisateurs | Abus de droits |
| | Absence de processus formel relatif au réexamen des droits d'accès (supervision) | Abus de droits |
| | Absence de dispositions suffisantes (relatives à la sécurité) dans les contrats avec des clients et/ou des tiers | Abus de droits |
| | Absence de procédure de surveillance des moyens de traitement de l'information | Abus de droits |
| | Absence d'audits réguliers (supervision) | Abus de droits |
| | Absence de procédures d'identification et d'appréciation du risque | Abus de droits |
| | Absence de rapports d'erreur enregistrés dans les journaux administrateurs et les journaux opérations | Abus de droits |
| | Réponse inadaptée du service de maintenance | Violation de la maintenabilité du système d'information |
| | Accord de service absent ou insuffisant | Violation de la maintenabilité du système d'information |
| | Absence de procédure de contrôle des modifications | Violation de la maintenabilité du système d'information |
| | Absence de procédure formelle du contrôle de la documentation SMSI | Corruption de données |
| | Absence de procédure formelle de supervision des enregistrements SMSI | Corruption de données |
| | Absence de processus formel d'autorisation des informations à disposition du public | Données provenant de sources douteuses |
| | Absence de bonne attribution des responsabilités en sécurité de l'information | Déni d'actions |

**ANNEXE 3 : EXEMPLES DE VULNERABILITES**

| | | |
|---|---|---|
| | Absence de plans de continuité | Panne de matériel |
| | Absence de politique relative à l'utilisation des emails | Erreur d'utilisation |
| | Absence de procédures d'introduction d'un logiciel dans des systèmes d'exploitation | Erreur d'utilisation |
| Organisme (fin) | Absence d'enregistrements dans les journaux administrateurs et journaux opérations | Erreur d'utilisation |
| | Absence de procédures relatives au traitement de l'information classée | Erreur d'utilisation |
| | Absence de responsabilités en sécurité de l'information dans les descriptions de poste | Erreur d'utilisation |
| | Dispositions absentes ou insuffisantes (relatives à la sécurité de l'information) dans les contrats avec les employés | Traitement illégal de données |
| | Absence de processus disciplinaire défini en cas d'incident en sécurité de l'information | Vol de matériel |
| | Absence de politique formelle relative à l'utilisation des ordinateurs portables | Vol de matériel |
| | Absence de contrôle des actifs situés hors des locaux | Vol de matériel |
| | Politique absente ou insuffisante relative au « bureau propre et à l'écran vide » | Vol de supports ou de documents |
| | Absence d'autorisation relative aux moyens de traitement de l'information | Vol de supports ou de documents |
| | Absence de mécanismes de surveillance établis pour des violations de sécurité | Vol de supports ou de documents |
| | Absence de revues de direction régulières | Utilisation non autorisée du matériel |

**ANNEXE 3 : EXEMPLES DE VULNERABILITES**

| | | |
|---|---|---|
| | Absence de procédures de signalement des failles de sécurité | Utilisation non autorisée du matériel |
| | Absence de procédures de la conformité des dispositions aux droits de propriété intellectuelle | Utilisation de logiciels copiés ou de contrefaçon |