LES DOSSIERS TECHNIQUES

LA GESTION DES RISQUES

-

Concepts et méthodes

Révision 1 du 28 janvier 2009

Espace Méthodes

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard, 75009 PARIS

Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88 – e-mail : clusif@clusif.asso.fr
Web : http://www.clusif.asso.fr

Table des Matières

REMERCIEMENTS

Le CLUSIF tient à remercier particulièrement les membres de l'espace Méthodes qui ont rendu possible la réalisation de ce document, à savoir :

Dominique	**BUC**	*BUC SA*
Olivier	**CORBIER**	*DOC@POST*
Éric	**DERONZIER**	*YSOSECURE*
Jean-Philippe	**JOUAS**	*CLUSIF*
Gérard	**MOLINES**	*MOLINES CONSULTANTS*
Jean-Louis	**ROULE**	*CLUSIF*

Merci également à notre partenaire du Québec, Martine **GAGNE**, dont la relecture attentive et pertinente a été précieuse.

1 INTRODUCTION

On peut affirmer qu'il n'y a pas d'entreprise ni de développement sans prise de risque.

Partant de ce constat, il est clair que les risques pris doivent être identifiés, analysés, maîtrisés et gérés et qu'il est alors raisonnable et sensé de le faire dans un cadre méthodologique.

Diverses méthodes se proposent comme méthode d'analyse et de gestion des risques, mais la notion de gestion des risques n'a pas le même sens selon les méthodes, ce qui conduit à une certaine confusion.

Le but de ce document est de tenter de définir des typologies de gestion des risques, d'en décrire les étapes.

Ainsi présenté, le domaine d'application de cette étude est très large et couvre tous les types de risques. Cependant, l'émergence et l'importance de normes spécifiques pour la gestion des risques liés à la sécurité de l'information fait que nous y ferons fréquemment référence et que les exemples pris le seront souvent dans ce domaine particulier.

A contrario, cette étude, strictement centrée sur la gestion des risques, n'a pas pour objectif de porter quelque jugement que ce soit sur les avantages et inconvénients respectifs des divers types de méthodes comme outil de management de la sécurité dans tel ou tel contexte.

2 RESUME

L'étude présentée dans ce document met en évidence de grandes différences entre les diverses méthodes possibles de gestion des risques.

Les points clés de différenciations sont décrits sommairement ci-dessous.

2.1 Identification des situations de risque

Les processus d'identification des situations de risque peuvent impliquer fortement le management et être orientés « stratégie » et « objectifs fondamentaux de l'entité » ou, au contraire, être déclinés à un niveau opérationnel et technique.

La manière même de définir les risques n'est pas neutre quant à cette orientation.

2.2 Options dans le mode de gestion des risques

Deux options principales se présentent pour la gestion des risques :

- celle qui consiste à analyser chaque situation de risque identifiée et à prendre des décisions spécifiques et adaptées à chacune d'elles, avec une forte implication du management dans la gestion des risques

- celle, au contraire, qui s'appuie sur une analyse plus générale afin de définir des objectifs et des directives de sécurité propres à réduire globalement les risques, sans gestion directe et individualisée des risques, et sans doute avec une moindre intervention du management

Le premier mode de gestion des risques exige un modèle évolué d'analyse des risques que ne demande pas le second.

Ces options relatives à la gestion des risques ont des conséquences directes au niveau de chaque étape du processus correspondant. Ces conséquences sont décrites dans la suite du document.

2.3 Options d'outillages et de bases de connaissances

Les outils pouvant venir en appui de la gestion des risques sont très variés et vont du strict minimum à des ensembles méthodologiques complets incluant des bases de connaissances, voire d'expertise, des outils d'audit, des outils de simulation des niveaux de risques atteints en fonction des options de mesures de sécurité, des outils de suivi de tableau de bord, etc.

La possible personnalisation de ces outils est en outre un élément à prendre en compte.

3 PRINCIPES GENERAUX ET DEFINITIONS DU RISQUE

Le premier point à tenter d'éclaircir, avant même de parler de gestion, est celui de la définition du « risque » qui n'est pas la même selon les méthodes.

Cette définition repose sur un nombre limité de concepts qui font à peu près consensus et que nous présenterons d'abord, avant d'exposer les points pour lesquels il existe des différences et des espaces de décision.

3.1 Concepts de base

Un risque provient du fait que l'entité, entreprise ou organisation, possède des « valeurs », matérielles ou non, qui pourraient subir une dégradation ou un dommage, dégradation ayant des conséquences pour l'entité considérée.

Ceci fait appel à quatre notions :

- Celle de « valeur », qu'il est d'usage d'appeler « actif » (traduction de « asset[1] ») dans le domaine de la sécurité de l'information
- Celle de dégradation ou de dommage subi par l'actif
- Celle de conséquences pour l'entité
- Celle qui suggère une cause possible mais non certaine

3.1.1 Les actifs

D'une manière très générale, on désigne sous ce terme tout ce qui peut représenter une valeur ou un enjeu pour l'entité.

En ce qui concerne la sécurité de l'information, la norme ISO/IEC 27005 distingue :

- Les actifs primaires ou primordiaux qui comprennent :
    - Les processus et activités
    - L'information
- Les actifs de support qui comprennent :
    - Le matériel
    - Le logiciel
    - Les réseaux

[1] Le terme « asset » est explicitement défini et commenté dans les normes de la série ISO/IEC 27000 qui s'adressent spécifiquement aux risques liés à la sécurité de l'information, alors qu'il n'est pas cité dans les normes plus générales telles que le guide 73 de l'ISO ou la norme ISO 31000. Il a néanmoins été retenu dans ce document, avec sa traduction sous le nom de « actif » car il évoque bien toutes les valeurs de l'entreprise, et ses immobilisations, tant matérielles qu'immatérielles, et parce qu'il est largement utilisé par maints responsables.

- Le personnel
- Le site
- Le support organisationnel

Il s'agit à l'évidence d'une définition très générale qui, pour être commune à toutes les méthodes, n'en recouvre pas moins des déclinaisons pratiques très variées.

3.1.2 La dégradation subie par un actif

Il est clair que le risque est différent (et ses conséquences différentes) selon le type de dommage subi.

Le type de dommage possible dépend des catégories d'actifs et autant il est facile de lister les principaux types de dommages subis par des informations (perte de disponibilité, d'intégrité ou de confidentialité, et éventuellement d'autres types de dégradations), autant il y a peu de typologies standards dès qu'il s'agit de processus, ou de certains actifs de support.

Il est à noter que le type de dégradation subi n'est pas explicitement cité par la norme ISO/IEC 27005 qui ne le distingue pas des conséquences. Il nous semble pourtant important de distinguer les conséquences primaires, constituées par les dégradations d'actifs, des conséquences secondaires ou indirectes pouvant être subies au niveau des processus et des activités de l'entité.

3.1.3 Les conséquences subies par l'entité

Ces conséquences peuvent être de natures très diverses et dépendent fortement du type d'entité, société commerciale, organisme de service public, organisation à but non lucratif, etc.

La seule chose importante à considérer, à ce stade, est que ces conséquences auront à être évaluées au niveau de l'entité et non à celui des systèmes d'information ou du périmètre technique de l'analyse et que l'évaluation du risque devra comprendre une évaluation de l'impact sur l'organisme de la dégradation considérée de l'actif concerné.

3.1.4 La cause, non certaine, de la dégradation subie par un actif

On inclut généralement, dans la définition du risque, une référence à la cause ou à un type de cause, par essence non certaine, pouvant conduire à la dégradation de l'actif. Le guide 73 de l'ISO parle d' « événement » pour évoquer cette cause.

On retient généralement que :

- Il n'y a risque (par opposition à un constat ou à une certitude) que s'il y a une action ou un événement non certains qui conduisent à la réalisation du risque (à son occurrence) c'est-à-dire à la dégradation considérée de l'actif concerné

- L'évaluation du risque devra comprendre une évaluation de la probabilité de survenance de cette action ou de cet événement

Le terme de cause que nous avons employé peut être ambigu car il peut y avoir des causes directes (événement au sens du guide 73) et des causes indirectes (source au sens du guide 73), mais représente bien l'idée générale de quelque chose qui va conduire à la réalisation de la dégradation redoutée.

3.1.5 La notion de menace

Les normes ISO/IEC 2700x traitant des risques liés aux systèmes d'information font référence à la notion de « menace » (« threat[2] ») qui n'est pas véritablement définie sauf par ce qu'elle est capable de causer, à savoir « causer un dommage à des actifs tel que information, processus ou systèmes et donc aux organisations » (« A threat has the potential to harm assets such as information, processes, and systems and therefore organizations » selon l'ISO/IEC 27005).

On pourrait penser que cette notion de menace est proche de celle de « cause » évoquée plus haut. Elle est, en fait, bien différente car les menaces peuvent recouvrir des aspects bien divers et, en particulier :

- Des événements ou actions qui peuvent conduire à l'occurrence du risque (par exemple, un accident, un incendie, le vol de media, etc.)

- Des actions ou modes d'action rendant possible l'occurrence du risque, sans en être le moteur (par exemple l'abus de droit, l'acquisition illicite de droits ou l'usurpation d'identité)

- Des effets caractéristiques et significatifs de causes indéterminées (par exemple la saturation du système d'information)

- Des comportements (par exemple l'utilisation non autorisée d'équipements) qui ne sont pas, en tant que tels, des événements conduisant à l'occurrence du risque

Il ressort de ces quelques exemples que la menace n'est pas strictement liée à la cause du risque mais permet de définir, en fonction de listes de menaces types, des typologies de risques.

3.1.6 La notion de vulnérabilité

La notion de vulnérabilité est parfois utilisée en analyse de risque et, plus généralement, dès que l'on aborde la sécurité des systèmes d'information[3].

---

[2] Le terme « threat » est explicitement défini et commenté dans les normes de la série 27000 qui s'adressent spécifiquement aux risques liés à la sécurité de l'information, alors qu'il n'est pas cité dans les normes plus générales telles que le guide 73 de l'ISO ou la norme ISO 31000. Il a néanmoins été retenu dans ce document, avec sa traduction sous le nom de « menace » car il est utilisé de manière importante par certaines méthodes de gestion des risques.

3 Ici encore, on peut noter que le terme de vulnérabilité n'est pas utilisé dans les normes générales traitant de la gestion des risques, en particulier le guide 73 de l'ISO, mais l'est par contre abondamment par certaines méthodes de gestion des risques

On peut définir ce qu'est une vulnérabilité de deux manières.

La plus correcte, au plan linguistique, est de la définir comme une **caractéristique d'un système, d'un objet ou d'un actif constituant un point d'application potentiel de menaces**.

Ainsi, si on parle d'un document écrit ou manuscrit, et si la menace considérée est la pluie ou plus généralement des intempéries, les vulnérabilités peuvent être, par exemple, que :

- l'encre n'est pas indélébile
- le papier est sensible à l'eau
- le support est dégradable.

Il est souvent plus utile d'adopter une vision des vulnérabilités orientée sur les processus de sécurisation et sur leurs défauts éventuels. **On définit alors une vulnérabilité comme un défaut ou une faille dans les dispositifs de sécurité pouvant être exploité par une menace pour atteindre un système, un objet ou un actif cible**.

Dans l'exemple précédent la vulnérabilité exploitée est : l'absence de protection contre les intempéries.

Cette vision conduit à une arborescence de vulnérabilités. En effet, toute solution de sécurité a ses faiblesses et donc toute solution apportée pour réduire une vulnérabilité comporte elle-même des vulnérabilités.

Exemple du document écrit sur support dégradable :

Solution de premier niveau : stockage à l'abri des intempéries

- Vulnérabilités induites :
    - Canalisations internes du bâtiment défectueuses
    - Procédures de mise à l'abri inappliquées ou inadéquates
    - Déclenchement de la protection incendie par sprinkler
    - Etc.

Ces deux visions des vulnérabilités ne sont pas équivalentes et il pourra être utile d'en tenir compte lorsqu'il est fait appel à cette notion.

* * * * *

En s'appuyant sur ces concepts généraux, plusieurs définitions du risque restent possibles et sont, de fait, proposées par les diverses méthodes de gestion de risques, tout en restant compatibles avec les documents normatifs.

3.2 Définition du risque

Si le concept général de risque ne pose pas de problème, il n'en est pas de même dès que l'on en recherche une définition formelle, c'est-à-dire une définition qui précise chacun des éléments constitutifs du risque. Or ces éléments vont intervenir, d'abord dans le processus d'identification des risques, puis dans celui de leur estimation.

Paradoxalement, les méthodes de gestion de risques donnent rarement une telle définition formelle. Les définitions que l'on peut reconstituer se classent en deux grandes catégories :

- Les définitions du risque basées sur la notion de menace, associée ou non à des vulnérabilités

- Les définitions du risque basées sur la notion de scénario

3.2.1 Le risque défini par l'ensemble « actif, menace » ou « actif, menace, vulnérabilités exploitées »

Une première définition du risque serait :

Le risque est la conjonction d'un actif et d'une menace susceptible de faire subir un dommage à cet actif.

Les méthodes de gestion des risques qui utilisent cette définition fournissent, le plus souvent une typologie[4] de menaces.

Il est possible, et certaines méthodes le font, d'inclure dans la définition du risque certaines vulnérabilités exploitées par la menace. Cette vision se base sur l'idée que sans vulnérabilité exploitable il n'y a pas de risque.

La définition du risque devient alors :

Le risque est la conjonction d'un actif, d'une menace susceptible de faire subir un dommage à cet actif et de vulnérabilités exploitées par la menace pour faire subir à l'actif ce dommage.

Ces définitions du risque conduisent à une notion de « risques types » résultant de types de menaces, de types d'actifs et, éventuellement, de types de vulnérabilités.

Il s'agit donc d'une **vision « statique » des risques**, au sens où les éléments pris en compte ne font pas intervenir la variable « temps » et ne permettent pas de décrire des enchaînements d'événements, de causes ou de conséquences.

3.2.2 Le risque défini par un scénario

Une autre définition du risque revient à considérer que le dommage subi et que la description des circonstances de survenance du dommage subi par l'actif doivent faire partie de la définition du risque.

Ces circonstances peuvent recouvrir des notions de :

- Lieux : par exemple, vol de media dans tel ou tel type de local

- Temps : par exemple, action menée en dehors ou pendant des heures ouvrables

- Processus ou étapes de processus : par exemple, altération de fichiers lors de la maintenance

La définition du risque devient alors :

[4] L'annexe C de la norme ISO/IEC 27005 donne une liste d'exemples de menaces types.

Le risque est la conjonction d'un actif, d'un type de dommage pouvant être subi par cet actif et de circonstances dans lesquelles ce dommage pourrait survenir.

On peut employer encore le terme de menace en lui donnant le sens de la description générale de types de circonstances dans lesquelles le risque pourrait se matérialiser. Les circonstances seront alors décrites par :

- une menace générique décrivant une typologie de circonstances et
- des circonstances particulières précisant la menace générique.

Cette définition conduit, en pratique, à définir des « **situations de risque** » ou des « **scénarios de risque** » qui décrivent, à la fois, le dommage subi et les circonstances dans lesquelles se produit ce dommage.

Cette vision du risque est, en fait, exactement celle que décrit le guide 73 de l'ISO quand il définit un risque comme comportant des sources ou phénomènes dangereux (circonstances), des événements déclencheurs et des conséquences.

Il s'agit donc d'une **vision « dynamique » des risques**, dans laquelle le temps peut intervenir, ce qui peut donner lieu à des actions différenciées en fonction de phases du scénario de risque. Cette vision dynamique permet de décrire et de tenir compte d'enchaînements d'événements, de causes ou de conséquences.

On notera par ailleurs que la norme ISO/IEC 27005 fait appel à une notion de « scénarios d'incident », notion très proche de ce que nous avons appelé ci-dessus « scénario de risque », sans être rigoureusement équivalente. En effet, la définition du scénario d'incident se réfère explicitement à l'exploitation d'une certaine vulnérabilité ou d'un ensemble de vulnérabilités, alors que les circonstances particulières de survenance du risque peuvent être liées à des notions diverses, ainsi qu'expliqué ci-dessus, qui ne sont pas forcément liées à des vulnérabilités.

* * * * *

* * *

*

Il est certainement possible de proposer d'autres manières de définir le risque et ses éléments constituants, mais nous retiendrons ces deux définitions caractéristiques et significatives en termes de gestion des risques.

4 OPTIONS FONDAMENTALES DE GESTION DES RISQUES

Indépendamment de la définition du risque, les objectifs que l'on peut assigner à la gestion des risques peuvent être très différents.

En pratique, on peut distinguer deux objectifs qui se révèlent, à l'analyse, fondamentalement différents :

- La gestion directe et individualisée de chaque risque, dans le cadre d'une politique de gestion des risques.

- La gestion globale et indirecte des risques par le biais d'une politique de sécurité adaptée aux risques encourus.

Remarque : Le contenu de cette politique et son niveau de détail sera abordé au chapitre 8.

4.1 La gestion directe et individualisée des risques

L'objectif d'une telle gestion, défini et caractérisé par une politique de gestion des risques, vise à :

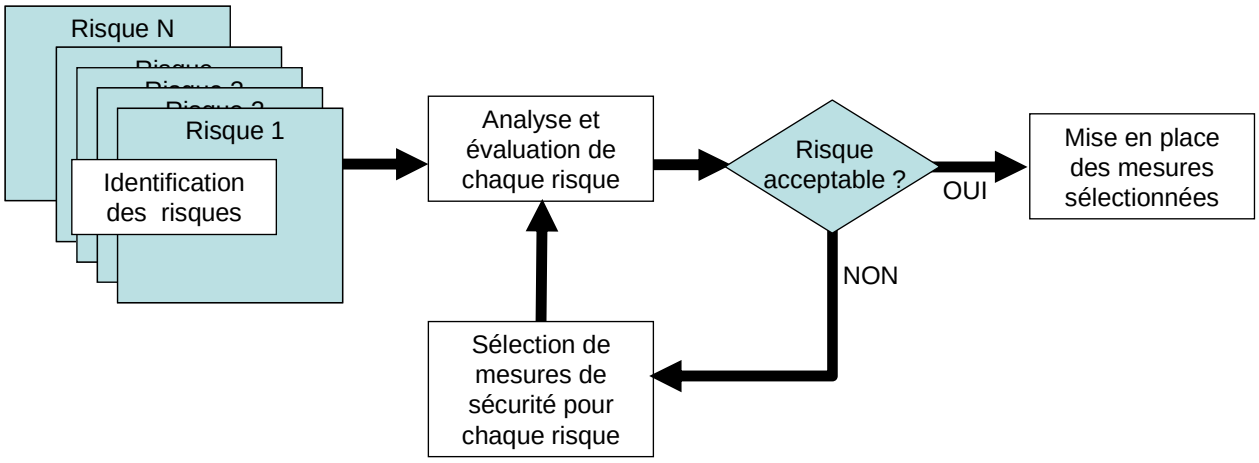
- Identifier tous les risques auxquels l'entreprise est exposée.

- Quantifier le niveau de chaque risque.

- Prendre, pour chaque risque considéré comme inadmissible, des mesures pour que le niveau de ce risque soit ramené à un niveau acceptable.

- Mettre en place, comme outil de pilotage, un suivi permanent des risques et de leur niveau.

- S'assurer que chaque risque, pris individuellement, est bien pris en charge et a fait l'objet d'une décision soit d'acceptation soit de réduction, voire de transfert.



Ce mode de management est donc très fortement tourné vers les activités de l'entité et ses enjeux fondamentaux et ne peut être choisi et mené à bien qu'en plein accord avec la Direction et avec sa participation active.

Il est aussi très bien adapté à toutes les organisations par projet dans lesquelles la gestion des risques est déléguée aux chefs de projet.

Principe sous-jacent et condition préalable

Il est clair que pour pouvoir gérer individuellement chaque risque, il faudra à un moment savoir prendre en compte les effets de toutes les mesures de sécurité, existantes ou prévues, susceptibles d'avoir une influence sur le niveau de risque.

Un tel mode de management exige donc, par principe et comme condition préalable, que soit défini un modèle de risque permettant d'expliciter et de quantifier, pour chaque risque identifié :

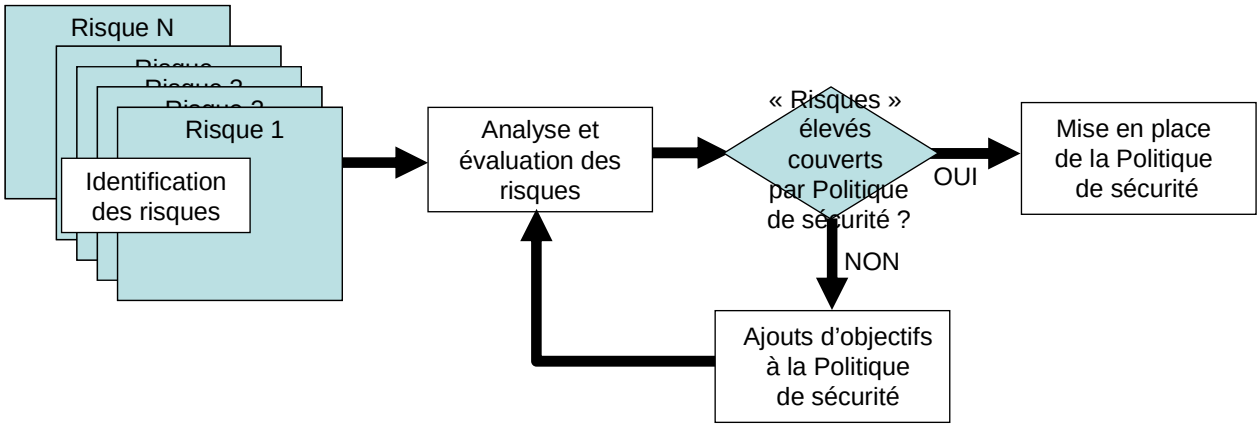
- Les facteurs de risque structurels liés au contexte et à l'activité de l'entité et donc indépendants des mesures de sécurité
- Les rôles et effets des mesures de sécurité sur le risque considéré
- Le niveau de risque global en résultant

Sans un tel modèle, il serait effectivement impossible d'établir un lien entre les décisions de mise en place de mesures de sécurité et un niveau de risque résiduel en résultant. Or ce lien est nécessaire pour une gestion individuelle des risques.

4.2 La gestion globale et indirecte des risques

L'objectif est, dans ce cas, de définir une politique de sécurité qui s'appuie sur une évaluation des risques. Le but visé est ainsi de :

- Identifier certains éléments pouvant conduire à des risques.
- Hiérarchiser ces éléments.
- En déduire une politique et des objectifs de sécurité.
- Mettre en place, comme outil de pilotage, un suivi permanent des objectifs de sécurité ou des éléments de la politique de sécurité.



Ce mode de management fait moins intervenir la Direction de l'entité et peut être mené à un niveau technique.

Principe sous-jacent et condition préalable

Le principe même de ce type de management est de définir des besoins ou des objectifs de sécurité en s'appuyant sur l'attribution aux risques d'un niveau qui tienne compte de l'atteinte (ou non) de ces objectifs ou de la satisfaction (ou non) de ces besoins.

La vision du risque peut être partielle et ne considérer qu'une partie des éléments ayant une influence sur le niveau réel de risque, en particulier certaines vulnérabilités (ou types de vulnérabilités) exploitées par des menaces types.

Un tel mode de management exige donc, par principe et comme condition préalable, que soit défini un modèle permettant de quantifier, pour chaque risque identifié :

- Un niveau de risque fonction des éléments cités dans la description de ce risque
- L'influence du choix d'objectifs dans la politique de sécurité
- Un niveau « relatif » du risque en résultant.

Il faut bien noter que le niveau de risque ainsi évalué l'est « compte tenu des seuls éléments cités dans l'identification du risque » et « compte tenu de l'influence de la politique de sécurité sur ces éléments ». Il ne peut donc pas être retenu comme valeur de jugement du niveau de risque réel pour l'entité, mais comme une valeur relative de l'importance des objectifs de sécurité retenus dans la politique de sécurité.

4.3 Définition du risque et type de management

Il est clair qu'une définition des risques basée sur la notion de scénario est particulièrement adaptée à une gestion directe et individualisée des risques et qu'une définition des risques basée sur les menaces et les vulnérabilités est, a priori, adaptée à une gestion globale et indirecte des risques.

Il n'y a, cependant, pas d'obstacle théorique à ce qu'une définition des risques basée sur des scénarios soit utilisée pour une gestion indirecte des risques par le biais d'une politique de sécurité.

De même, il n'y a pas d'obstacle absolu à ce qu'une définition des risques fondée sur des menaces et des vulnérabilités soit utilisée pour une gestion directe et individualisée ; cela reporte au niveau de l'évaluation des risques et du choix des mesures de sécurité la recherche des divers scénarios pouvant conduire au risque considéré ou appartenir à cette famille de risque.

Remarque sur le lien entre les vulnérabilités et le type de gestion des risques

La question du lien entre l'introduction des vulnérabilités dans l'identification des

risques et le type de management mérite d'être posée.

En effet, l'introduction des vulnérabilités dans la définition des risques (par comparaison avec leur introduction uniquement en phase d'analyse des risques) a plusieurs conséquences auxquelles il peut être utile de réfléchir :

- Ne pas faire intervenir les vulnérabilités dans l'identification des risques revient à considérer qu'un risque naît de la simple conjonction d'un élément d'actif qui a une valeur et de circonstances dans lesquelles cette valeur pourrait être mise en cause et que c'est cette situation que l'on entend gérer, les vulnérabilités étant alors prises en compte lors de l'analyse de cette situation de risque.

  Il s'agit donc bien d'une démarche de gestion directe des risques. Par contre, introduire les vulnérabilités dans la définition des risques revient à considérer que ce sont bien elles que l'on entend évaluer et gérer. Il s'agit bien alors d'une gestion indirecte des risques.

- D'autre part, pour une situation de risque donnée, ce n'est pas une vulnérabilité qui est concernée et exploitée mais souvent plusieurs. Il est clair, par exemple, qu'un scénario de piratage depuis l'extérieur de l'entreprise débouchant sur un détournement de données applicatives peut exploiter simultanément, comme vulnérabilités, la faiblesse du contrôle d'accès au réseau, l'absence de partitionnement du réseau et de confinement des fichiers sensibles, la faiblesse du contrôle d'accès au système, la faiblesse du contrôle d'accès applicatif, l'absence de chiffrement des fichiers, etc.

  Dans ces conditions, introduire dans la définition des risques la liste des vulnérabilités exploitées serait incontestablement une source de difficulté pour une gestion directe des risques et obligerait en outre à introduire dans une tâche qui est normalement une tâche de management (l'identification des risques) une tâche d'analyse technique (la recherche de l'ensemble des vulnérabilités concernées par cette situation de risque).

On peut donc considérer que l'introduction des vulnérabilités dans l'identification des risques est compatible avec une gestion globale et indirecte des risques, mais qu'elle l'est beaucoup moins avec une gestion directe et individualisée des risques.

* * * * *

* * *

*

Ces orientations fondamentales étant esquissées, nous allons analyser, dans les chapitres ci-dessous, en quoi elles sont déterminantes quant au contenu de différentes étapes décrites par les normes, et en particulier par le guide 73 de l'ISO, que nous rappelons ci-dessous (en gras les étapes qui seront analysées en détail, l'enchaînement entre ces étapes n'étant pas particulièrement traité).

MANAGEMENT DU RISQUE			
	APPRECIATION DU RISQUE		
		ANALYSE DU RISQUE	
			IDENTIFICATION DES RISQUES
			ESTIMATION DU RISQUE
		EVALUATION DU RISQUE	
	TRAITEMENT DU RISQUE		
		REFUS DU RISQUE	
		OPTIMISATION DU RISQUE (sa réduction)	
		TRANSFERT DU RISQUE	
		PRISE DE RISQUE	
	ACCEPTATION DU RISQUE		
	COMMUNICATION RELATIVE AU RISQUE		

5 L'IDENTIFICATION DES RISQUES

Ce que contient l'étape d'identification des risques dépend bien entendu de la définition retenue pour le risque.

Quelle que soit la définition retenue, le risque naît de l'existence de valeurs ou d'éléments d'actifs qui représentent, pour l'entreprise ou l'organisme, un enjeu, c'est-à-dire dont le maintien de certaines qualités est important pour le bon fonctionnement de l'entité.

Cette étape d'identification des actifs pouvant être critiques est donc la première et est commune à toutes les méthodes d'analyse de risque.

La deuxième étape, qui dépend de la définition du risque retenue, consiste donc à rechercher :

- Soit quelles menaces seraient susceptibles de causer un dommage à ces actifs, et éventuellement quelles vulnérabilités pourraient être exploitées, dans le cas d'une identification de risques basée sur la notion de menace et de vulnérabilités

- Soit quelles dégradations pourraient affecter ces actifs et dans quelles circonstances ces dégradations pourraient survenir, pour une identification de situations ou de scénarios de risque

Nous analyserons successivement les étapes d'identification des actifs, puis celle d'identification des menaces et vulnérabilités et celle d'identification des scénarios de risque.

5.1 L'identification des actifs critiques (ou susceptibles de l'être)

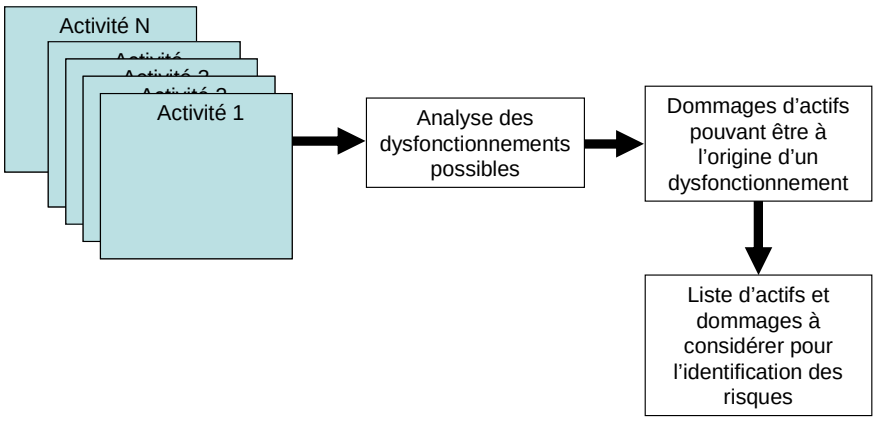
Cette étape est, incontestablement, essentielle dans l'identification des risques et on peut distinguer deux grands types de démarches.

La première consiste, selon le schéma indiqué ci-dessous, à :

- Analyser les processus et les activités de l'entreprise ou de l'entité et rechercher les dysfonctionnements de ces processus qui pourraient impacter les objectifs ou les résultats attendus de l'entité

- Rechercher les actifs et les dommages subis par ces actifs qui pourraient induire de tels dysfonctionnements

- En déduire une liste d'actifs (il peut être utile alors de distinguer les actifs les plus importants, que l'on considérera comme « critiques », pour ne pas alourdir inutilement le reste des étapes de gestion des risques).



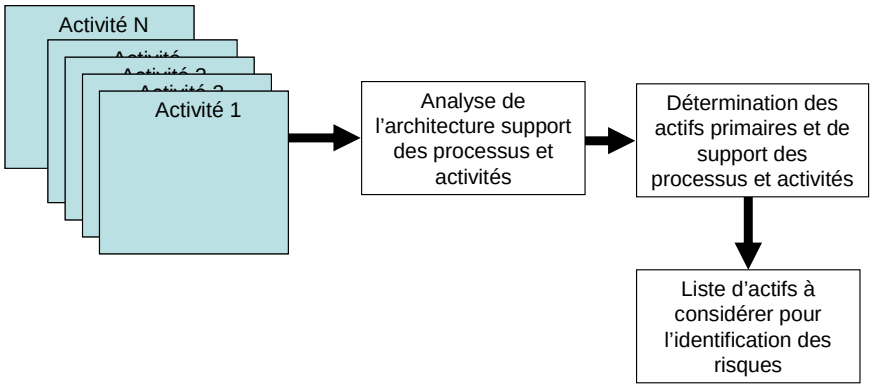
Il s'agit d'une démarche centrée sur les enjeux des diverses activités de l'entité, et menée de préférence à un niveau élevé de management. Cette démarche débouche assez naturellement sur une recherche des circonstances dans lesquelles les dommages pourraient survenir et donc sur une définition de scénarios de risques.

La deuxième démarche consiste à :

- Analyser l'architecture des moyens primaires supportant l'activité (qu'il s'agisse du système d'information ou de tout autre type de moyens, tels que les moyens de production, de logistique, de communication, etc.)

- Rechercher éventuellement les moyens supports des moyens primaires (tels que l'énergie, les moyens nécessaires à l'organisation, etc.)

- En déduire une liste d'actifs à considérer pour l'identification des risques.



Il s'agit d'une démarche beaucoup plus technique, pouvant être menée sans l'aide du management de haut niveau. Cette démarche débouche assez naturellement sur une recherche des menaces pouvant agir sur ces actifs et donc sur une identification de risques définis par les menaces et vulnérabilités.

Une différence essentielle réside dans le fait qu'avec une définition du risque basée sur la notion de scénario, le type de dommage éventuellement subi par l'actif en cas d'occurrence du risque fait partie de la recherche des actifs critiques.

Autrement dit, les critères utilisés pour valoriser les actifs, lors de la phase d'estimation des risques, avec une définition des risques basée sur les menaces,

sont introduits dès l'identification des actifs, quand on veut identifier des scénarios de risque.

Pour éclairer nos propos, nous prendrons quelques exemples, concernant trois types d'actifs.

Dans le cadre d'une vision statique des risques, des actifs identifiés pourraient être :

- Un document de planification stratégique
- La base de données d'un domaine métier.
- Le serveur de données de la Direction XXX

Dans une vision dynamique des risques par scénarios, les éléments identifiés seront en plus caractérisés par un type de dommage :

A. Document de planification stratégique confidentiel
B. Base de données de tel ou tel domaine dont l'intégrité doit être maintenue.
C. Serveur de données de la Direction XXX **dont la disponibilité doit être maintenue**

5.2 L'identification des menaces et vulnérabilités

Dans le cas de définition des risques basée sur les menaces, la démarche consistera, le plus souvent, à sélectionner dans une liste de menaces types, des éléments standards pertinents pour le type d'actif considéré.

Si nous reprenons les éléments d'actifs correspondant aux trois exemples ci-dessus, nous trouverons ainsi (exemples non limitatifs issus de la norme ISO/IEC 27005) :

1. Document stratégique

   Menaces pertinentes
   - Vol de media ou de document
   - Divulgation
2. Base de données

   Menaces pertinentes
   - Falsification par logiciel
   - Dysfonctionnement de logiciel
3. Serveur de données

   Menaces pertinentes
   - Incendie
   - Dégâts des eaux
   - Accident majeur
   - Destruction d'équipement

- Inondation
- Etc.

Si les vulnérabilités exploitées font partie de la définition des risques, la démarche consistera, le plus souvent, à sélectionner dans une liste de vulnérabilités, éventuellement pré-classées par type de menaces, des vulnérabilités pertinentes et, en reprenant les exemples ci-dessus, nous pourrions obtenir (toujours en prenant les exemples donnés dans les annexes du projet de norme ISO/IEC 27005) :

1. Document stratégique

   Menace et vulnérabilité :

   - Vol de media ou de document dû à un manque de protection du stockage

2. Base de données

   Menace et vulnérabilité :

   - Falsification par logiciel dû à un téléchargement et un usage incontrôlé de logiciel

3. Serveur de données

   Menace et vulnérabilité :

   - Destruction d'équipement dû à un manque de schéma périodique de remplacement

5.3 L'identification des scénarios de risque

Dans ce cas, la démarche consistera à analyser, dans les processus mis en œuvre impliquant l'élément d'actif considéré ou dans le cycle de vie de cet élément, ou dans son architecture, ce qui pourrait conduire à mettre en cause la qualité considérée.

Cette recherche s'effectuera soit directement soit en s'appuyant sur une base de connaissance décrivant des scénarios de risques fréquemment rencontrés, si la méthode le permet.

Ainsi pour reprendre les mêmes exemples

1. Document stratégique confidentiel

   On analysera le processus d'élaboration, de contrôle et de diffusion de ce type de document et on pourra mettre en évidence diverses circonstances conduisant à des risques particuliers :

   - Lors de son élaboration (fichier informatique sur le PC du responsable ou de son assistante ou sur un serveur partagé)
   - Lors de sa sauvegarde
   - Lors de son impression (sur imprimante partagée)
   - Lors de sa diffusion par mail
   - Lors de sa diffusion par courrier
   - Lors de son archivage

2. Base de données dont l'intégrité doit être maintenue

   On analysera également les divers processus impliquant la base de données et pouvant conduire à une mise en cause de son intégrité et on pourra mettre en

évidence diverses circonstances conduisant à des risques particuliers :

- Lors d'accès concurrents (risques logiciels)
- Lors d'accès malveillants
- Lors de maintenance logicielle
- Lors de tests de développement ou de maintenance
- Lors de maintenance à chaud

3. Serveur de données dont la disponibilité doit être maintenue

On analysera et listera les divers types de causes possibles et les divers processus internes impliquant cet élément d'actif, pouvant conduire à une mise en cause de sa disponibilité :

- Accidents physiques (incendie, dégâts des eaux, etc.) et leur origine :
  - Incendie provoqué par un court-circuit dans le câblage,
  - Incendie provoqué par une négligence interne (cendrier, appareil de chauffage annexe, etc.)
- Pannes courantes ou exceptionnelles et leurs conditions particulières :
  - Pannes courantes traitées par la maintenance
  - Pannes nécessitant une escalade
  - Etc.
- Attaques en déni de service
- Erreur de maintenance matérielle ou logicielle
  - Due à un défaut de formation
  - Due à un défaut de documentation
  - Etc.

Il est important de noter que le fait d'inclure dans l'identification d'un risque les circonstances dans lesquelles il pourrait se produire permet de mettre en lumière que, de par le contexte et les processus mis en œuvre, tel élément d'actif se trouve bien, à un moment donné, dans une situation de risque particulière.

Les différences de résultats obtenus sur ces trois exemples montrent bien qu'au-delà des mots et des termes employés, il y a une profonde différence de conception de la définition d'un risque.

Identifier les menaces pesant sur un actif et les vulnérabilités que ces menaces peuvent exploiter pour atteindre l'actif permet de caractériser un type de risque, mais n'a pas pour objectif, et ne permet en aucun cas, d'identifier directement des « situations de risque » susceptibles de réclamer des actions spécifiques lors d'un processus de gestion directe des risques.

6 L'ESTIMATION DES RISQUES IDENTIFIES

L'étape que les normes ISO appellent « estimation des risques » ou "Risk estimation" est, en fait, une étape de quantification des risques.

Ce que recouvre cette étape est très différent selon les modes de gestion des risques.

6.1 L'estimation des risques pour leur gestion individualisée

L'objectif est d'obtenir, pour chaque risque identifié, une évaluation du niveau de risque auquel l'entité est exposée.

Il y a un consensus général sur le fait que ce niveau dépend de deux facteurs qui sont l'impact (ou le niveau de conséquence du risque) et sa potentialité (ou probabilité). Pour faire ces évaluations, dans un contexte où des mesures de sécurité ont déjà été prises, il faudra en outre tenir compte de la qualité de ces mesures.

Ainsi qu'il a déjà été dit, un modèle de risque est nécessaire et est un préalable. Cependant, quelque soit le modèle proposé par telle ou telle méthode, quelques éléments permanents, toujours nécessaires, peuvent être dégagés. Ce sont :

- L'analyse des enjeux ou des conséquences du risque
- L'analyse de la probabilité de survenance du scénario de risque
- L'effet des mesures de sécurité

6.1.1 L'évaluation des enjeux ou des conséquences du risque

Sachant que la définition et la description du risque comprennent celle de l'élément d'actif impliqué et le type de dommage subi, la question est bien celle d'évaluer la gravité de ce dommage.

On est bien dans une problématique de méthode et ce n'est pas le lieu ici d'en décrire une plus particulièrement.

On peut néanmoins mettre en lumière les principes généraux qui doivent être respectés.

L'évaluation des conséquences maximales du dommage subi

Le premier principe à respecter est de rechercher les conséquences maximales du dommage subi.

Cela se fera souvent lors d'une démarche dite de classification qui devra comprendre les éléments décrits ci-après.

a. Etablir une échelle de gravité

L'échelle de gravité est sans doute une des premières choses à faire.

Cette échelle doit exprimer des niveaux de gravité de conséquences (telles que mort ou perte de l'entité, séquelles durables, perte de compétitivité momentanée, etc.) au même titre que l'on pourrait parler de risque accidentel pour l'homme (risque vital, risque d'invalidité permanente, obligation de soins permanents, maladie courante invalidant quelques semaines, etc.).

Dans le cas de services publics, le niveau de gravité peut se référer à des niveaux de perte de service rendu (en durée, en pourcentage du public touché, etc..).

b. Évaluer la gravité des conséquences en la distinguant bien de la gêne ressentie (par les responsables de l'entité)

Ce que l'on recherche est bien une évaluation de la gravité des conséquences du risque pour l'entité. C'est donc bien au niveau des processus de l'entité que cette évaluation doit être faite et que les conséquences du risque doivent être analysées. Il est important, lors de cette analyse, de ne pas survaloriser la gêne ressentie par les responsables de l'entité (mais de correctement valoriser la gêne ressentie par les clients).

c. Faire valider les niveaux de gravité par la Direction

Les conséquences des risques devraient être évaluées au niveau business par les responsables d'activité eux-mêmes et devraient être validées par un comité de Direction.

Ne pas respecter ce principe peut conduire et conduit généralement à des résultats surévalués. Ainsi, des événements considérés comme graves à des niveaux hiérarchiques bas ou moyens sont souvent considérés comme tolérables voire non significatifs à niveau élevé.

Plus généralement, la gestion des risques étant principalement destiné aux Dirigeants d'entreprise, c'est à eux de se déterminer sur la gravité réelle de tel ou tel risque.

L'évaluation des conséquences particulières du risque analysé

L'évaluation décrite ci-dessus, parfois résumée dans une classification des actifs, est le niveau de conséquences maximum encouru par l'entité pour le type de dommage subi par l'élément d'actif concerné.

Il se peut néanmoins que, pour les circonstances particulières du risque ou que pour le type de menace, les conséquences soient moindres.

La méthode supportant le management direct des risques doit alors proposer une étape ou un moyen de corriger, le cas échéant, l'évaluation de l'impact pour tenir compte de cet éventuel amoindrissement des conséquences.

6.1.2 L'évaluation de la probabilité de survenance du risque

Le fondement de « l'estimation » d'un risque reposant, pour partie, sur une notion de probabilité de survenance, il est clair que l'on doit passer par une évaluation de la probabilité de survenance a priori qui permettra un premier jugement sur cette probabilité en l'absence de toute mesure de sécurité.

L'idéal serait, bien entendu, de disposer d'une base statistique suffisante pour

pouvoir asseoir ces probabilités a priori sur des chiffres excluant toute partialité ou subjectivité.

En pratique, cela n'est guère possible pour diverses raisons :

- Les organismes collecteurs de chiffres relatifs aux sinistres sont réticents à les divulguer (les assurances en particulier)

- Ces chiffres ont eux-mêmes porteurs de biais car tous les sinistres ne sont pas déclarés (en particulier ceux qui peuvent porter atteinte à l'image des sinistrés)

- Certains sinistres ne sont même pas connus de ceux qui les ont subis (en particulier nombre de vols de données).

On en est donc réduit à porter un jugement relativement subjectif sur ces probabilités a priori en notant :

- Qu'un consensus de groupe de travail limite le caractère subjectif

- Que les méthodes du marché proposent des chiffres qui sont une base de départ appréciable

Ceci étant la méthode pour définir ces probabilités a priori doit faire partie du modèle de risque propre à ce type de management et doit comprendre les éléments décrits ci-dessous.

a. Établir une échelle de probabilité

L'échelle de probabilité est sans doute une des premières choses à faire.

Cette échelle doit exprimer des niveaux de probabilité aisés à comprendre par tous les participants au processus d'analyse des risques.

Le nombre de niveaux ne devrait pas être trop élevé pour qu'un consensus puisse être facilement atteint sur les niveaux de probabilité de chaque menace.

b. Évaluer la probabilité « a priori » du scénario de risque

L'évaluation de la probabilité maximale et a priori, en l'absence de toute mesure de sécurité, sera le plus souvent associée à une typologie de scénarios.

Ce sera effectivement le cas si la méthode propose une base de connaissances structurée. A défaut, il est conseillé de regrouper les scénarios en types de probabilité voisine, ce qui revient, de fait, à distinguer des menaces types communes à plusieurs types de scénarios.

Cette probabilité correspond souvent, en pratique à une probabilité de menace, indépendamment du contexte propre de l'entité.

c. L'évaluation de l'exposition de l'entité au scénario analysé

Cette notion d'exposition (parfois aussi appelée exposition naturelle) est fondamentale. Quelle que soit, en effet, la probabilité d'occurrence de la menace, en général, ce qui compte est de savoir si l'entité est plus particulièrement exposée ou non à ce type de risque.

Cette exposition met en jeu divers facteurs tels que :

- l'intérêt que représente l'action, pour son auteur
- le caractère plus ou moins unique de l'entité en tant que cible de la menace
- le contexte social
- le contexte économique

Il est de même important de noter que cette exposition peut fluctuer dans le temps.

La méthode de gestion des risques doit ainsi permettre d'évaluer cette exposition, en fonction du contexte propre de l'entité, afin de définir, in fine, une « potentialité intrinsèque » du risque, en l'absence de toute mesure de sécurité.

6.1.3 L'évaluation des effets des mesures de sécurité

C'est, sans aucun doute, dans ce domaine que les divers modèles de risque propres à ce type de management peuvent apporter des aides significatives et très différenciées.

On peut cependant mettre en lumière quelques éléments incontournables, qui doivent être décrits et explicités dans tout modèle d'analyse de risque associé à une gestion directe des risques, qui sont :

- La différenciation des types d'effets des mesures de sécurité
- La prise en compte d'un niveau de qualité de ces mesures
- La mesure de l'efficacité d'une mesure de sécurité
- La prise en compte d'une notion d' « assurance sécurité » (au-delà de la qualité technique d'une mesure, quelle assurance peut-on avoir de son efficacité réelle ?)
- La manière de prendre en compte et de combiner les effets simultanés de plusieurs mesures de sécurité

La différenciation des types d'effets des mesures de sécurité

Les types d'effets des mesures de sécurité sont divers et doivent impérativement être distingués dans le modèle de risque, pour une bonne appréciation du risque.

Il est important, en effet, de faire la distinction entre les effets venant réduire la probabilité du risque et ceux venant en atténuer les conséquences.

Bien au-delà, d'autres nuances doivent être distinguées telles que :

- L'effet de dissuasion
- L'effet d'empêchement (de faire quelque chose ou de réussir dans l'action)
- L'effet de détection suivi d'empêchement

- L'effet de détection suivi de réaction limitant les conséquences
- L'effet de confinement limitant les conséquences
- L'effet de restauration
- L'effet palliatif de moyens de secours
- Etc.

Cette liste n'est certes pas exhaustive et le modèle de risque doit proposer une typologie de ces effets, en les regroupant éventuellement, pour décrire l'action des mesures de sécurité et permettre une évaluation individualisée de chaque risque.

La prise en compte du niveau de qualité des mesures de sécurité

Il est bien clair que l'effet ou que les effets d'une mesure de sécurité dépend de la qualité de cette mesure.

Tous les mécanismes ne sont pas équivalents, toutes les procédures ne sont pas aussi efficaces et il faut bien savoir porter un jugement sur un niveau de qualité.

Le modèle de risque devrait donc comporter une méthode d'évaluation.

La méthode d'évaluation elle-même peut être plus ou moins experte, mais il est fortement souhaitable qu'elle s'appuie sur une base de connaissances.

L'évaluation de l'efficacité d'une mesure de sécurité

La qualité intrinsèque d'une mesure de sécurité n'indique pas pour autant si elle sera efficace pour réduire un niveau d'un risque particulier, même si, d'évidence, elle peut jouer un rôle positif dans la réduction de ce risque.

En outre, l'efficacité d'une mesure peut dépendre du type d'effet, alors qu'une même mesure peut avoir plusieurs types d'effets.

Il y a donc une relation à établir, par le modèle de risque, entre la qualité d'une mesure de sécurité et son efficacité pour tel ou tel effet sur tel ou tel type de scénario de risque.

La notion d'assurance sécurité

Cette notion, parfaitement mise en évidence par les ITSEC et les critères communs, vise à faire une différence entre le niveau d'efficacité d'une mesure de sécurité et l'assurance que l'on peut avoir de cette efficacité.

Il s'agit, par exemple, d'évaluer séparément la force d'un mécanisme technique et la garantie de sa mise en œuvre et de sa permanence dans le temps.

La prise en compte ou non de cette notion par le modèle de risque est donc un paramètre à considérer.

Les effets combinés de plusieurs mesures de sécurité

Enfin, la manière de combiner les effets simultanés de plusieurs mesures de

sécurité doit être explicitée par le modèle de risque afin de pouvoir évaluer correctement le niveau de risque résiduel quand plusieurs mesures sont actives et pertinentes, ce qui est la très grande majorité des cas.

6.1.4 L'estimation des niveaux de risque

L'estimation des niveaux de risque doit faire la synthèse des estimations partielles et déboucher, a minima, sur :

- Une évaluation de la potentialité de survenance du risque (sa probabilité)
- Une évaluation de son impact (la gravité de ses conséquences)

Le modèle de risque doit bien entendu décrire la manière d'obtenir ces deux valeurs de synthèse.

6.1.5 Influence du mode de définition du risque

Il est bien clair que tout ce qui vient d'être développé convient parfaitement à une définition des risques par des scénarios.

Si les risques sont définis comme des risques types basés sur des notions de menaces et de vulnérabilités, il faudra, pour chaque risque ainsi défini, rechercher tous les scénarios possibles (scénarios d'incident au sens de l'ISO/IEC 27005) et estimer le niveau de risque pour chaque scénario. Les divers points développés plus haut seront alors nécessaires pour cette estimation.

Une méthode d'élaboration d'une synthèse pour chaque risque sera en outre nécessaire.

6.2 L'estimation des risques pour leur gestion globale

Il est bien entendu possible d'utiliser un modèle de risque complet tel qu'abordé précédemment pour faire une estimation individuelle de chaque risque identifié comme un scénario de risque et d'en déduire une politique de sécurité et des objectifs adaptés à une gestion globale des risques.

Nous nous placerons néanmoins dans une optique où les risques sont décrits par une menace et une vulnérabilité (ou éventuellement un groupe de vulnérabilités) exploitée.

Ce qui est très significatif de cette représentation du risque est qu'elle donne une vue partielle du risque en ne citant qu'une partie des vulnérabilités. Ne prenant pas en compte l'ensemble des mesures de sécurité qui pourraient avoir un effet sur le niveau de risque, elle permet de donner une certaine valeur au risque (compte tenu de la vulnérabilité exploitée mais sans tenir compte des autres mesures de sécurité qui pourraient réduire le risque), valeur qui peut être utilisée pour hiérarchiser des vulnérabilités, bien qu'elle ne représente pas une évaluation complète du niveau de risque auquel l'organisme est exposé.

Ceci étant, le modèle d'estimation du risque « relatif » doit comprendre plusieurs éléments :

- L'estimation des enjeux ou des conséquences du risque
- L'estimation du niveau de la menace

- L'estimation du niveau des vulnérabilités citées dans la description du risque, niveau éventuellement fonction de la politique de sécurité.

6.2.1 L'estimation des enjeux ou des conséquences du risque

L'estimation du risque doit, bien entendu, tenir compte du dommage subi par l'élément d'actif lors de la survenance du risque.

Sachant que la description du risque comprend celle de l'élément d'actif impliqué et le type de dommage subi (bien que ce dommage ne soit pas cité explicitement et qu'il faille le rechercher dans le type de menace), la question est bien celle d'évaluer la gravité de ce dommage.

On est, comme précédemment, dans une problématique de méthode et ce n'est pas le lieu ici d'en décrire une plus particulièrement.

On peut néanmoins mettre en lumière les principes généraux qui doivent être respectés et qui sont influencés par le fait qu'on ne cherche pas une valeur absolue du niveau de risque.

Décrire la référence en matière de gravité des conséquences des risques

Dans la mesure où l'on ne rechercha pas une valeur absolue des niveaux de risque, la référence en matière de gravité peut être plus libre.

On peut ainsi prendre comme référence pour définir une échelle de gravité :

- la gravité réelle des conséquences pour l'entité (comme au chapitre 6.1.1)
- la gêne occasionnée aux utilisateurs,
- la gêne ressentie par la Direction
- les coûts de recouvrement
- tout autre critère reflétant une certaine hiérarchie dans les conséquences (telle que la durée d'une interruption de service)

Définir une échelle de gravité

Une fois la référence fixée une échelle devra l'être également.

Le nombre de niveaux importe relativement peu dans ce type de management et une échelle à faible nombre de niveaux facilitera la suite des quantifications.

6.2.2 L'estimation du niveau de menace

La valeur attribuée au risque doit, bien entendu, tenir compte du niveau de la menace.

La manière d'évaluer ce niveau doit être décrite dans le modèle d'estimation du risque et peut prendre en compte divers paramètres tels que :

- La probabilité de survenance « a priori » de l'événement déclencheur de la menace

- Le potentiel de nuisance de la menace
- L'exposition relative de l'entité à ce type de menace
- La « facilité de réalisation » de la menace
- Etc.

Certes, une fonction combinée de la probabilité de survenance a priori et de l'exposition relative de l'entité à ce type de menace semble se rapprocher au mieux d'une notion de probabilité, mais, dans ce processus d'estimation du risque « relatif », l'essentiel est que le processus d'évaluation du niveau de la menace permette une bonne communication et soit comprise par les décideurs, le validité théorique de cette évaluation n'ayant pas une importance majeure.

6.2.3 L'estimation du niveau de vulnérabilité

L'estimation du risque doit, enfin, tenir compte du niveau des vulnérabilités concernées puisque celles-ci sont un élément central du risque identifié.

Les points suivants devraient être abordés et décrits par le modèle de management :

- La mesure du niveau de chaque vulnérabilité
- La manière de prendre en compte et de valoriser la combinaison de plusieurs vulnérabilités, si plusieurs vulnérabilités sont décrites dans l'identification du risque.

La mesure du niveau de vulnérabilité

Pour pouvoir gérer dans le temps les risques encourus, même dans cette vision partielle des risques, il est nécessaire d'évaluer un niveau de vulnérabilité.

La manière de faire cette évaluation peut être :

- Subjective
- Basée sur un audit des vulnérabilités et sur une base de connaissance

Dans un cas comme dans l'autre la méthode doit décrire le processus d'évaluation et ce processus doit permettre la prise en compte des éléments de la politique de sécurité.

La mesure de plusieurs vulnérabilités cumulées

En outre, si plusieurs vulnérabilités sont décrites dans un type de risque, la manière de faire une évaluation globale du niveau de vulnérabilité doit être décrite et devrait comprendre :

- Une typologie de vulnérabilités (peut-on comparer des vulnérabilités aussi différentes que la faiblesse d'un contrôle d'accès et celle des sauvegardes ?)

- La manière de combiner des vulnérabilités de même type (leur minimum, leur maximum, une autre formule ?)

- La manière de combiner des vulnérabilités de types différents.

6.2.4 L'estimation du niveau de risque

L'estimation du niveau de risque doit tenir compte de l'ensemble des évaluations précédentes et déboucher sur une hiérarchisation des risques partiels ou relatifs décrits.

7 L'EVALUATION DES RISQUES IDENTIFIES

L'étape que les normes ISO appellent évaluation des risques ("Risk evaluation") est, en fait, une étape de jugement sur le caractère acceptable ou non des risques tels qu'ils sont décrits.

7.1 L'évaluation des risques pour leur gestion individualisée

Le résultat de l'étape d'estimation est, pour ce type de management, une évaluation de l'impact (I) et de la probabilité (P) de chaque risque.

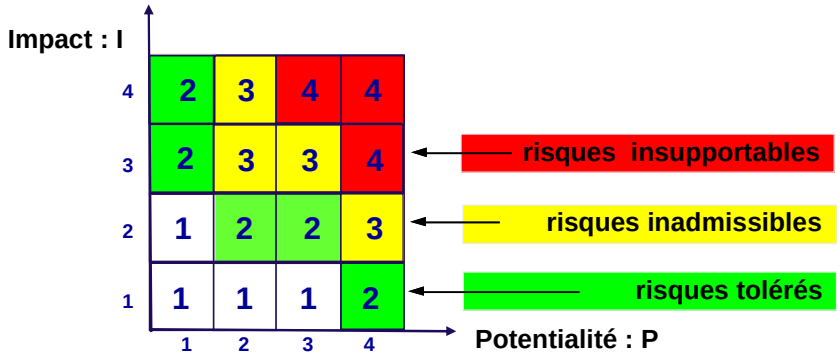
Il ne reste plus qu'à passer à une note globale ou, plus simplement, qu'à décider des plages d'acceptabilité des risques.

Compte tenu du caractère facilement accessible des deux notions de base, le management peut aisément conclure sur ce point.

Le support de décision peut ainsi être :

- Une fonction de Gravité du risque G = f(P, I)

- Une table d'acceptabilité fonction de P et de I, par exemple comme celle indiquée ci-dessous.



7.2 L'évaluation des risques pour leur gestion globale

Le résultat de l'étape d'évaluation est, pour ce type de management, une note globale permettant une hiérarchisation des risques.

La décision de traiter le risque ou non dépend alors d'un seuil de décision qui doit être fixé par un comité ad hoc.

8 LE TRAITEMENT DES RISQUES

Les risques ayant été estimés, il reste à les traiter, c'est-à-dire à :

- Les accepter en l'état
- Les éviter totalement par des évolutions structurelles telles que le risque ne se présente plus
- Les optimiser, c'est-à-dire les réduire
- Les transférer ou les partager avec une tierce partie

Nous aborderons ici les deux dernières options, à savoir la réduction des risques ou leur transfert vers un tiers.

Il est bien clair que la réduction des risques identifiés et considérés comme critiques est liée au mode de management choisi, mais aussi, et peut-être principalement, à la définition même de ces risques.

8.1 La réduction directe des situations de risque critiques

Comme son nom l'indique, la gestion directe des situations de risque consiste à décider, scénario par scénario, des mesures à prendre.

Ceci étant, en fonction de ce que permet la méthode support, bien des options sont encore possibles, dont deux principales :

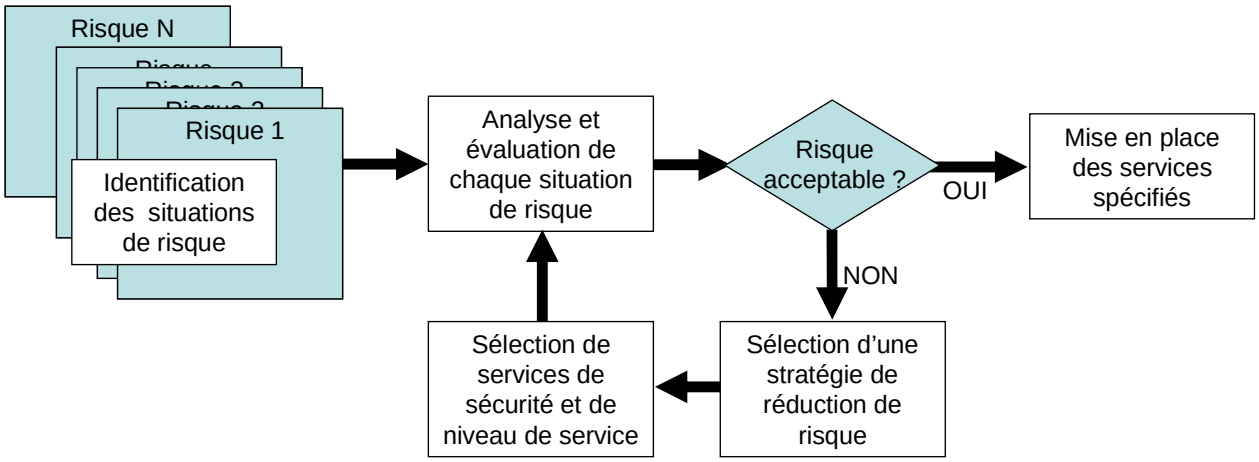
- L'appui sur une base de connaissances de scénarios de risque référençant les mesures de sécurité pertinentes et permettant l'évaluation de leur effet en termes de réduction du niveau de risque
- La gestion directe des situations de risque par les responsables d'activité, de projets ou de processus

8.1.1 La réduction directe des risques s'appuyant sur une base de connaissances

Le cas le plus intéressant est celui d'une base de connaissances de scénarios de risque qui référence, pour chaque scénario, les mesures de sécurité pertinentes et qui permet d'évaluer l'effet de ces mesures en termes de réduction du niveau de risque.

La question qui peut alors se poser est celle des aides additionnelles proposées par la méthode de gestion des risques et, en particulier le choix ou la proposition de stratégies de réduction de risques. Il est, en effet, possible que la méthode ne propose rien de particulier et que le responsable de la gestion des risques soit libre de travailler comme il l'entend pour sélectionner les mesures de sécurité à mettre en place ou, au contraire, qu'il lui soit proposé des stratégies permettant d'optimiser son action.

Le schéma de gestion des risques donné au chapitre 4.1 devient alors plus précisément le suivant :



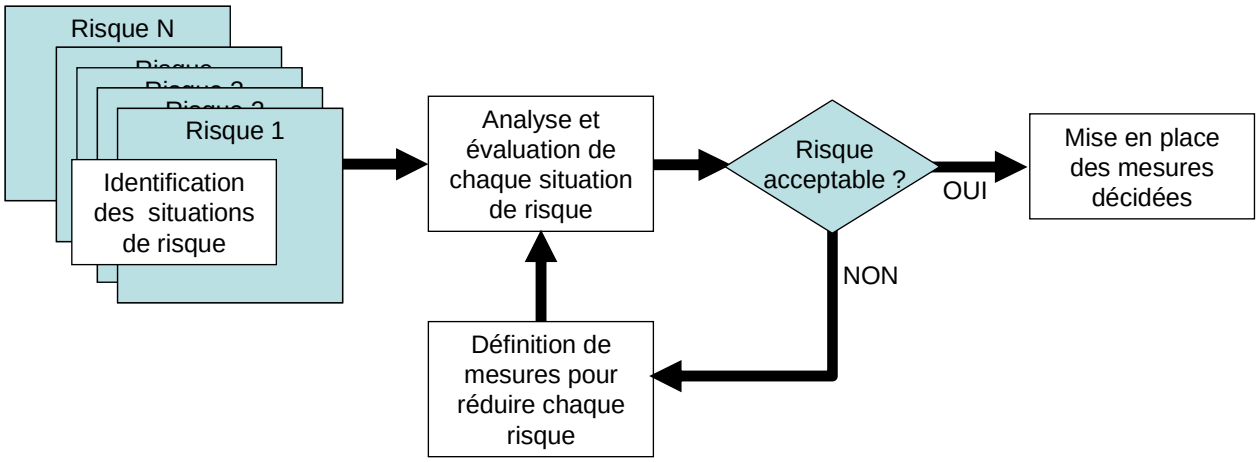
8.1.2 La réduction directe des risques par les responsables d'activité, de projet ou de processus

L'inclusion, dans la définition des risques, des circonstances particulières de survenance de chaque risque conduit à la possibilité de gestion directe des solutions à mettre en œuvre par les responsables d'activité, de projet ou de processus.

Bien des solutions, en effet, sont aisées à prendre au niveau de l'activité même et se révèlent généralement, dans ce cas, très économiques.

A titre d'exemple, si nous prenons le cas du détournement d'un dossier stratégique confidentiel lors de son impression sur une imprimante partagée, la décision pourrait simplement être de modifier le processus et d'imprimer ce même document en local sur une imprimante non partagée, plutôt que de se préoccuper de sécuriser le processus d'impression sur une imprimante partagée.

Le schéma de gestion des risques donné au chapitre 4.1 devient alors plus précisément le suivant :



8.2 Le traitement indirect des risques types critiques

Dans le cadre d'une démarche dans laquelle les risques critiques identifiés sont définis par les menaces et vulnérabilités, il est clair que ce sont ces vulnérabilités qu'il convient de réduire.

La question est alors de savoir jusqu'à quel niveau de détail la méthode de gestion des risques permet de descendre.

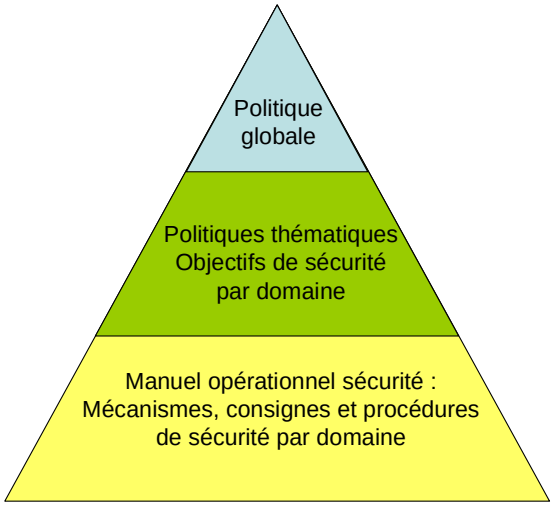
En effet, les décisions que l'on peut prendre, en matière de traitement des risques, et les orientations que l'on peut fixer, peuvent se situer à différents niveaux.

Ainsi que l'indique le schéma ci-dessous, elles peuvent se situer au niveau :

- D'une politique globale de sécurité définissant les grandes orientations générales

- De politiques thématiques de sécurité, définissant les objectifs de sécurité à atteindre, pour les différents thèmes ou domaines de la sécurité

- D'un manuel opérationnel de sécurité, définissant en détail les mécanismes à mettre en œuvre et les consignes de sécurité.



Ainsi, par exemple, le traitement de certains risques peut consister à :

- Décider, dans une politique thématique, la mise en place de procédures pour le traitement et le stockage de l'information, afin de protéger cette information contre des usages et des divulgations non autorisées, en se situant donc au niveau des objectifs de contrôle, le contenu de ces procédures et même les têtes de chapitre n'étant pas définies et décidées à ce niveau

- Analyser chacun des éléments à considérer pour atteindre l'objectif de protection de l'information et prendre une décision relative à chacun de ces éléments, dans un manuel opérationnel de sécurité, et par exemple (liste non limitative indiquée par la norme ISO/IEC 27002) :

    - La labellisation de tous les media en fonction de leur classification
    - L'établissement de restrictions d'accès
    - L'enregistrement et la maintenance de la liste des personnes autorisées à recevoir des données
    - La mise en place de contrôles de la complétude des données entrées et de la validation des sorties
    - La protection des données en attente d'édition ou de transmission
    - Le stockage des media en conformité avec les spécifications des fournisseurs
    - La restriction de la diffusion d'information
    - Le marquage des copies de media
    - La revue périodique des listes de diffusion et de distribution
    - Etc.

Deux options s'offrent alors aux méthodes de management indirect des risques types :

- Transformer directement les vulnérabilités à réduire en objectifs de sécurité fixés dans des politiques thématiques et reporter à une étape ultérieure la transformation de ces objectifs de sécurité en éléments pratiques d'un manuel opérationnel de sécurité

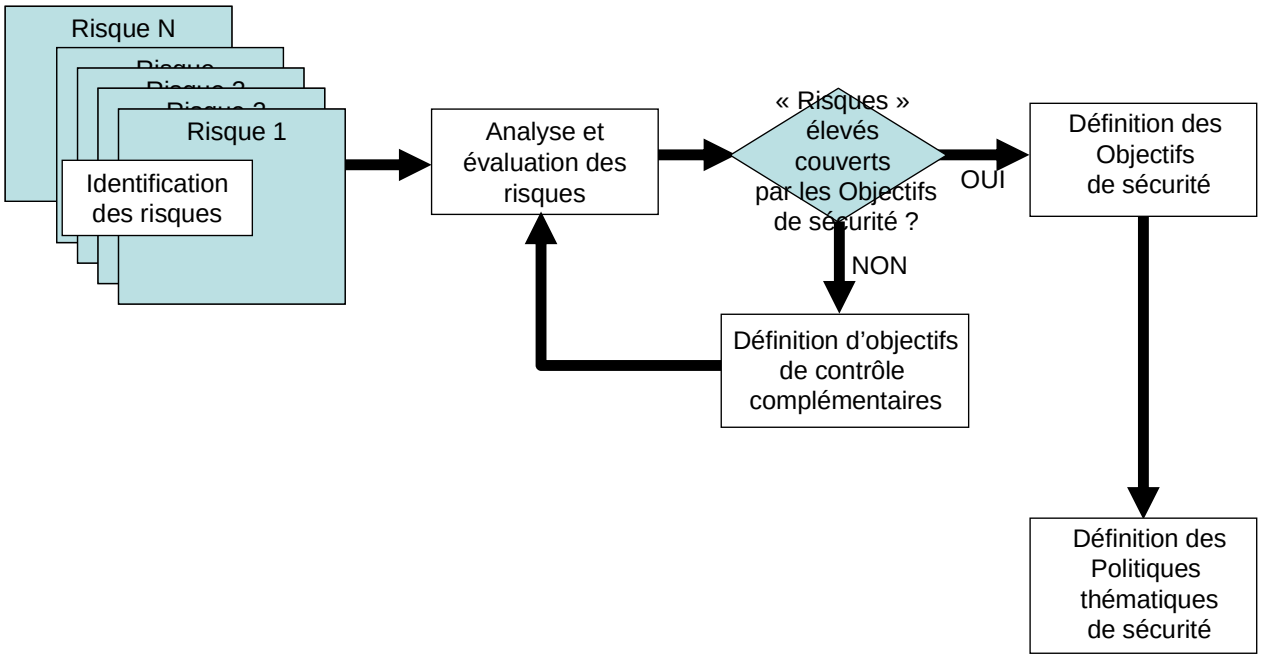
- Analyser plus en détail ces vulnérabilités pour en déduire, dès cette phase de management, les éléments pratiques d'un manuel opérationnel de sécurité à mettre en place.

8.2.1 Transformation des vulnérabilités à réduire en objectifs de sécurité

Cette transformation est relativement simple et ne demande pas d'outil particulier, les listes de vulnérabilités types utilisées étant le plus souvent de même niveau que les listes d'objectifs de contrôle.

Remarque : on pourrait imaginer de travailler avec des vulnérabilités types très détaillées et définies au même niveau que les éléments d'un manuel opérationnel de sécurité. Cela compliquerait beaucoup l'identification des risques et leur analyse, par la multiplication des vulnérabilités à prendre en compte pour chaque risque type, sans pour autant simplifier leur traitement.

Le schéma de gestion des risques donné au chapitre 4.2 devient alors plus précisément le suivant :



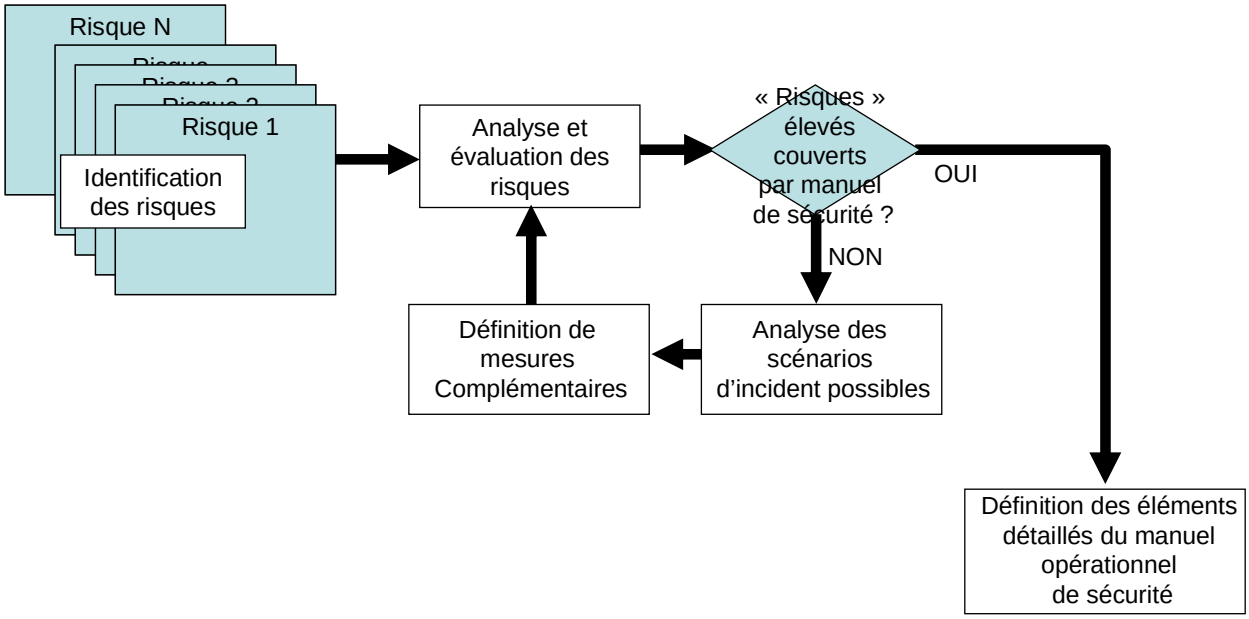
Les méthodes relevant de ce schéma sont, en fait, des méthodes de management des objectifs de sécurité, basées sur une évaluation de niveau de risques types, susceptibles d'exploiter les vulnérabilités non couvertes par les objectifs de sécurité.

8.2.2 Analyse détaillée des vulnérabilités à réduire pour décider des éléments d'une politique de sécurité

Les éléments d'un manuel opérationnel de sécurité, à décider puis à mettre en place, ne peuvent résulter, en pratique, que d'une analyse des scénarios d'incident ou scénarios de risque possibles et compatibles avec les caractéristiques du risque analysé : la menace et les vulnérabilités.

Le traitement des risques consiste alors à rechercher ces scénarios, puis à décider des mesures pertinentes pour réduire le niveau de risque et enfin à inclure des mesures dans le manuel opérationnel de sécurité.

Le schéma de gestion des risques donné au chapitre 4.2 devient alors plus précisément le suivant :



Les méthodes relevant de ce schéma sont, en fait, des méthodes de management des éléments du manuel opérationnel de sécurité, basées sur une évaluation de niveau de risques types prenant en compte des scénarios d'incident susceptibles d'exploiter les vulnérabilités non couvertes par le manuel de sécurité.

8.3 Le transfert du risque

Ce que l'on appelle transfert du risque consiste, le plus souvent, à contractualiser un certain partage de responsabilités entre l'entité et une ou plusieurs tierces parties.

Le cas le plus typique est celui de l'assurance, mais bien d'autres types d'accords et d'agréments sont possibles.

Les méthodes ne sont pas d'une grande aide dans ce domaine et les agréments sont à étudier et conclure au cas par cas.

Dans beaucoup de cas, néanmoins, une analyse approfondie des situations de risque sera plus utile et plus directement exploitable qu'une étude des menaces et des vulnérabilités.

9 COMMUNICATION SUR LES RISQUES

Les textes qui font référence, dans le domaine de la gestion des risques, insistent tous sur la communication relative aux risques.

Il nous parait, effectivement, essentiel que lorsqu'une entité s'engage dans une véritable gestion des risques, il y ait un consensus et une connaissance partagée sur :

- Les risques tolérés parce que leur niveau a été jugé admissible, ce qui ne veut pas dire qu ils ne surviendront pas et qu'il ne faudra pas réagir alors,

- Les risques que l'on a décidé de réduire, mais qui ne le seront qu'à plus ou moins long terme (le temps que les projets correspondants soient lancés et aboutissent),

- Les risques élevés et théoriquement inadmissibles qu'il faut bien supporter parce qu'il n'y a pas de solution d'évitement ni de réduction possible.

- Cette connaissance partagée ne peut que reposer sur une communication adaptée.

Au-delà des outils de communication, il est certain que communiquer sur des situations de risque a un sens et peut engendrer des comportements responsables, alors que communiquer sur des menaces et des vulnérabilités sera plus difficile à maîtriser et peut ne pas susciter l'adhésion du management.

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS
30, rue Pierre Sémard
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Téléchargez les productions du CLUSIF sur
www.clusif.asso.fr