



MEHARI

Principes fondamentaux et spécifications fonctionnelles

Mai 2017

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11, rue Mogador, 75009 PARIS

Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88 – e-mail : clusif@clusif.fr

Web : <http://www.clusif.fr>

MEHARI est une marque déposée par le CLUSIF.

La loi du 11 mars 1957 n'autorisant, aux termes des alinéas 2 et 3 de l'article 41, d'une part, que les "copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective" et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, "toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ayants droit ou ayants cause est illicite" (alinéa 1er de l'article 40)
Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal

Remerciements

La mise à jour de ce document, initialement publié par le CLUSIF, a été réalisée par le CLUSIQ, Club de la Sécurité de l'Information du Québec.

Que les personnes qui ont rendu possible la réalisation de ce document, en soient remerciées, tout particulièrement :

Jean-Philippe	Jouas	Ancien président du CLUSIF Ancien Responsable de l'Espace Méthodes du CLUSIF Créateur de la méthode
Jean-René	Blanchet	CAA-Québec
Guirec	Duperrin	GDC-Conseil
Gilles	Gouin	MAX2G
Christophe	Jolivet	PR4GM4
Benoît	Laliberté	VICTRIX
Chantale	Pineault	VICTRIX
Jean-Louis	Roule	

Sommaire

1	Introduction	8
2	Objectif de ce document.....	9
2.1	Objectifs fondamentaux de MEHARI	9
2.2	Plan du document	9
3	Références normatives	10
4	Termes et définitions	11
4.1	Actif.....	11
4.2	Enjeu de la sécurité.....	11
4.3	Impact.....	11
4.4	Impact intrinsèque	11
4.5	Incident.....	11
4.6	Menace.....	11
4.7	Potentialité	11
4.8	Potentialité intrinsèque.....	11
4.9	Scénario de risque	11
4.10	Service de sécurité.....	11
5	L'appréciation des risques.....	12
5.1	Introduction.....	12
5.2	L'identification des risques	12
5.2.1	Les éléments caractéristiques des risques.....	12
5.2.1.1	L'actif.....	12
5.2.1.2	L'incident à l'origine du risque	14
5.2.1.3	Le dommage subi	14
5.2.1.4	La menace provoquant l'occurrence du risque	15
5.2.1.5	Le scénario de risque.....	16
5.2.2	Le processus d'identification des risques	16
5.2.2.1	Élaboration des éléments caractéristiques des risques.....	17
5.2.2.2	Élaboration de la liste des risques possibles.....	17
5.2.2.3	Développement d'une base de connaissances de risques types	18
5.2.2.4	Sélection des risques à prendre en compte.....	18
5.2.3	Synthèse de l'identification des risques	18
5.3	L'estimation des risques	19
5.3.1	Les éléments mesurables et la métrique des risques.....	20
5.3.1.1	L'impact intrinsèque.....	20
5.3.1.2	La potentialité intrinsèque.....	21
5.3.1.3	L'effet des mesures de sécurité : facteurs de réduction des risques.....	22
5.3.1.4	Influence du niveau de qualité des mesures de sécurité existantes.....	24
5.3.1.5	Utilisation d'une base de connaissance des risques.....	24
5.3.2	Processus d'estimation des risques	24
5.3.2.1	L'élaboration des éléments de référence.....	24
5.3.2.2	Élaboration de l'échelle d'impact.....	25
5.3.2.3	Élaboration de l'échelle de potentialité	25

5.3.2.4	L'estimation des risques.....	26
5.3.2.5	L'appréciation globale de chaque risque (géré).....	28
5.3.3	Synthèse de l'appréciation de chaque scénario de risque	28
5.4	L'évaluation des risques	28
6	Le traitement des risques	30
6.1	L'acceptation du risque	30
6.2	La réduction du risque.....	31
6.2.1	Le choix de services de sécurité à mettre en place pour augmenter certains facteurs de réduction du risque.....	31
6.2.1.1	Les services de sécurité pertinents ou adaptés à un risque donné	31
6.2.1.2	Le choix de niveau de qualité cible pour un service de sécurité à mettre en place	31
6.2.1.3	L'évaluation de l'effet combiné de plusieurs services de sécurité	32
6.2.1.4	Processus de décision propre à la réduction des risques	32
6.2.2	Cas particulier de l'emploi de mesures structurelles.....	32
6.3	Le transfert du risque	33
6.4	L'évitement du risque	33
7	La gestion des risques	34
7.1	L'élaboration des plans d'action	34
7.1.1	Choix des objectifs prioritaires et optimisation	34
7.1.2	Le choix des solutions : mécanismes techniques et organisationnels.....	35
7.1.3	Choix de mesures structurelles et de mesures d'évitement de risques	35
7.1.4	Validation et prise de décision.....	35
7.2	Mise en œuvre des plans d'action.....	35
7.3	Contrôle et pilotage de la gestion directe des risques.....	35
7.3.1	Contrôle du niveau de qualité de service	36
7.3.2	Contrôle de la mise en œuvre des services de sécurité	36
7.3.3	Pilotage global associé à la gestion des risques	37
Annexe A	38
Échelles standards de niveaux d'impact et de potentialité		38
Annexe B1.....		39
Échelles standards de niveaux des facteurs de réduction de potentialité		39
Annexe B2.....		40
Échelles standards de niveaux des facteurs de réduction d'impact		40
Annexe C1.....		41
Grilles de décision standards de MEHARI.....		41
Annexe C2.....		42
Grilles de décision standards de MEHARI		42
Annexe D		43
Spécification des services de sécurité		43
A. Définitions		43
7.3.4 Services de sécurité.....		43
7.3.5 Services et sous-services de sécurité.....		43

7.3.6	Mécanismes et solutions de sécurité.....	43
7.3.7	Typologie des services de sécurité	43
7.3.8	Bases de connaissances des services de sécurité.....	44
B.	Mesure de la qualité des services de sécurité	44
7.3.9	Paramètres à prendre en compte.....	44
7.3.9.1	Efficacité d'un service de sécurité.....	44
7.3.9.2	Robustesse d'un service de sécurité.....	45
7.3.9.3	Mise sous contrôle d'un service de sécurité.....	45
C.	Évaluation de la qualité des services de sécurité basée sur les questionnaires MEHARI	45
7.3.9.4	Types de questionnaires	45
7.3.9.5	Système de pondération des questions.....	45
D.	Échelle de niveaux utilisable pour évaluer la qualité des services de sécurité	46

1 Introduction

L'analyse des risques est citée et considérée comme devant être la base des actions de sécurité par nombre d'ouvrages sur la sécurité.

Il en est de même dans les normes les plus récentes sur les systèmes de gestion de la sécurité de l'information et notamment l'ISO/IEC 27001 qui fait explicitement référence aux processus d'identification, d'évaluation et de traitement des risques.

La nécessité d'une méthode, en complément des normes

Ces mêmes normes qui font explicitement appel à la notion de risque et à la nécessité d'évaluer et de maîtriser les risques ne proposent pas de méthodes d'analyse de risque mais précisent qu'une méthode doit être choisie par l'organisation.

Certes un cadre général pour la gestion des risques est fourni par la norme ISO/IEC 27005, mais ce cadre laisse encore la place à bien des interprétations et à bien des modes de gestion des risques.

Dans ces conditions, il est clair qu'une méthode formelle est nécessaire et que le choix de cette méthode doit répondre à des spécifications, elles-mêmes fonctions du type de gestion de risque souhaité par l'organisme.

Il s'avère en effet que le sens donné à l'expression « gestion des risques » peut varier d'une organisation à une autre et qu'en fonction des objectifs poursuivis, les méthodes supports peuvent être notablement différentes.

2 Objectif de ce document

Ce document est établi à l'usage des organisations qui souhaitent choisir, mettre en place, définir ou développer un processus de gestion directe de leurs risques et a pour objectif de préciser, dans cette optique, les principes qui sont la base de la méthode MEHARI et de mettre en évidence les spécifications fonctionnelles qui en découlent.

2.1 Objectifs fondamentaux de MEHARI

Les objectifs fondamentaux de MEHARI sont de permettre une gestion directe et individuelle des risques auxquels l'entreprise ou l'organisation est exposée, et peuvent donc se décliner ainsi :

- 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 d'acceptation, de réduction, d'évitement ou de transfert.

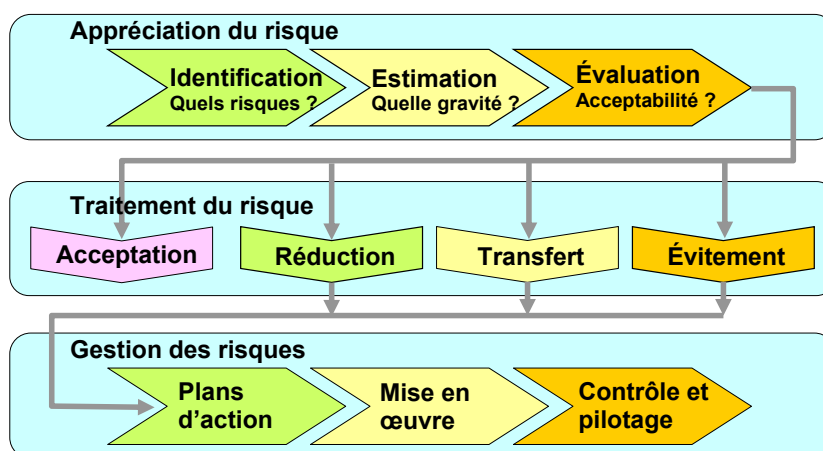
En fonction de ces objectifs, l'ensemble des processus et étapes décrits dans la norme ISO/IEC 27005 doivent être précisés et spécifiés. C'est précisément le but de ce document que de décrire les principes et spécifications fonctionnelles induits par les objectifs fondamentaux cités plus haut et d'expliquer, si nécessaire, leur nécessité pour atteindre les buts recherchés.

2.2 Plan du document

Nous présenterons ces différents aspects en suivant un plan proche de celui de l'ISO/IEC 27005 en traitant successivement :

- L'appréciation des risques
- Le traitement des risques
- Les processus de gestion des risques.

Le plan d'ensemble et les différents aspects abordés sont représentés schématiquement ci-dessous.



3 Références normatives

Les documents référencés ci-dessous, sont utiles pour l'application de ce document :

ISO/IEC 27001 :2005, Information technology – Security techniques – Information security management systems - Requirements

ISO/IEC 27005 :2008, Information technology – Security techniques – Information security risk management

4 Termes et définitions

Les termes cités ci-dessous ont une définition spécifique introduite dans ce document et nécessaire à la compréhension de ce document.

4.1 Actif

Tout élément du système d'information, qu'il s'agisse de l'information proprement dite, quelle que soit sa forme, ou de tout ce qui peut être nécessaire pour la communiquer, la traiter ou la stocker.

4.2 Enjeu de la sécurité

Conséquences d'un incident de sécurité sur les objectifs de l'organisme.

4.3 Impact

Conséquence, pour l'organisme concerné, de l'occurrence du risque considéré.

4.4 Impact intrinsèque

Conséquence, pour l'organisme concerné, de l'occurrence du risque considéré en l'absence de toute mesure de sécurité.

4.5 Incident

Manifestation concrète de l'occurrence du risque, sous forme d'une atteinte à la disponibilité, à l'intégrité ou à la confidentialité de données ou de services.

4.6 Menace

Description de l'ensemble des éléments conduisant à l'occurrence du risque incluant l'événement déclencheur et son caractère volontaire ou accidentel, l'acteur déclenchant cet événement et les circonstances dans lesquelles survient cet événement.

4.7 Potentialité

Probabilité de l'occurrence du risque considéré, dans le contexte l'organisme concerné ;

4.8 Potentialité intrinsèque

Probabilité de l'occurrence du risque considéré, dans le contexte l'organisme concerné, en l'absence de toute mesure de sécurité.

4.9 Scénario de risque

Description de l'ensemble des caractéristiques d'un risque, incluant l'actif concerné, la vulnérabilité intrinsèque de cet actif mise en cause et la menace conduisant à l'occurrence du risque.

4.10 Service de sécurité

Description d'une fonction de sécurité répondant à un besoin.

5 L'appréciation des risques

5.1 Introduction

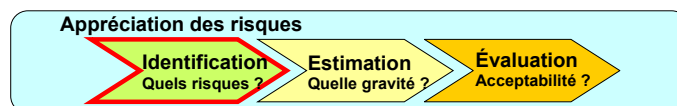
L'appréciation des risques consiste à identifier, aussi exhaustivement que possible, tous les risques auxquels l'entreprise ou l'organisation est exposée, à en estimer individuellement la gravité et à juger du caractère acceptable ou non de chaque risque ainsi évalué.

Chacune des étapes constituant ce processus doit ainsi être conduite avec cette exigence d'être à même de porter un jugement précis sur la gravité de chaque risque, en fonction du contexte, et notamment des mesures de sécurité existantes.

Nous reprenons ci-dessous les trois étapes du processus global d'appréciation des risques que sont :

- L'identification des risques,
- L'estimation des risques,
- L'évaluation des risques.

5.2 L'identification des risques



Le but de cette étape est non seulement la recherche et la reconnaissance de situations de risques, c'est-à-dire de certains types de risques, mais une caractérisation de chacun de ces risques suffisamment précise pour être à même d'en estimer la gravité.

Ceci pose deux questions :

- Quels sont les éléments caractéristiques des risques qu'il est nécessaire de mettre en évidence et avec quel degré de détail doivent-ils être précisés ?
- Quel est le meilleur processus pour y arriver ?

5.2.1 Les éléments caractéristiques des risques

Les paragraphes ci-dessous définissent et décrivent les éléments qui ont été définis, dans MEHARI, comme devant faire partie de la description des risques et en justifient la nécessité. Ces éléments sont :

- L'actif,
- L'incident,
- Le dommage subi,
- La menace.

5.2.1.1 L'actif

Rappelons que nous définissons, sous le terme d'actif, tout élément du système d'information, qu'il s'agisse de l'information proprement dite, quelle que soit sa forme, ou de tout ce qui peut être nécessaire pour la communiquer, la traiter ou la stocker.

Les actifs sont le sujet principal du risque : ce sont eux qui vont subir un dommage et le risque naît bien du fait qu'une certaine forme d'actif est susceptible de subir un dommage.

Il est bien clair, dès lors, que les conséquences et que la gravité de la survenance du risque dépendent de la nature de ces actifs et donc que celle-ci doit faire partie de la caractérisation du risque.

Mode de description des actifs

a. Les actifs primaires

La description des actifs devant servir à évaluer les conséquences des risques auxquels ils sont exposés, les éléments clés doivent se référer aux **besoins** des organisations que l'on peut, dans un premier temps, classer dans trois catégories :

- Les services (informatiques, de télécommunication et généraux),
- Les données nécessaires au fonctionnement des services,
- Les processus de gestion.

Dans chaque catégorie, des types d'actifs primaires doivent être distingués, en fonction :

- De la nature des besoins,
- De la nature des prestataires de service.

Et éventuellement :

- Du domaine d'activité et de domaines de responsabilité différents,
- De la technologie employée,
- Des utilisateurs concernés.

Ces typologies doivent correspondre à des types de besoins et être décrites au niveau fonctionnel.

Spécification

Les actifs primaires sont décrits selon des catégories de services, de données et de processus de gestion et, dans chaque catégorie, selon des typologies correspondant à des besoins fonctionnels.

La typologie des actifs primaires de MEHARI est différente selon les versions de bases de connaissances mais se réfère systématiquement à cette spécification.

Remarque : Les actifs primaires correspondent aux besoins des organisations et c'est donc à ce niveau qu'il conviendra d'évaluer (voir plus loin) l'importance de ce besoin, importance dont il sera tenu compte pour juger du niveau de risque.

b. Les actifs secondaires ou actifs de support

Les actifs ont des vulnérabilités et ce sont elles dont l'exploitation conduit au risque.

Pour rechercher ces vulnérabilités, il est essentiel, cependant, de distinguer, pour chaque actif primaire :

- les diverses formes qu'il peut revêtir,
- les diverses contingences dont il peut dépendre.

Ces formes et contingences peuvent être regroupées sous l'appellation d'actifs secondaires ou d'actifs de support.

Autant les actifs primaires correspondent à des besoins fonctionnels, autant les actifs secondaires correspondent à un niveau matériel et concret et aux moyens nécessaires à la réalisation des besoins fonctionnels.

Pour prendre deux exemples, si un résultat comptable est bien à classer dans les actifs primaires, les formes qu'il peut revêtir, à savoir une donnée dans un fichier, une écriture sur une édition papier ou un écran dans une page Internet sont bien à considérer comme des actifs secondaires. De même, si le service de comptabilité qui permet d'obtenir ce résultat est bien un actif primaire, le serveur, les

programmes, et toute l'infrastructure nécessaire au fonctionnement de la comptabilité sont des actifs secondaires associés.

Spécification

Les actifs secondaires sont décrits en typologies correspondant à des moyens nécessaires à la réalisation des besoins fonctionnels décrits par les actifs primaires.

La typologie des actifs secondaires de MEHARI est différente selon les versions de bases de connaissances et dépend, bien entendu de celle des actifs primaires, mais se réfère systématiquement à cette spécification. En outre cette typologie découle d'une recherche systématique visant à décrire exhaustivement tous les moyens nécessaires à la réalisation des besoins fonctionnels

c. Caractérisation de l'actif soumis à risque

L'objectif de gestion directe des risques conduit ainsi à caractériser chaque risque par un actif et cet actif par sa catégorie, son type d'actif primaire et son type d'actif secondaire.

Exemples d'actifs de MEHARI utilisés par les bases de connaissance :

- Serveur support d'un service applicatif,
- Configuration logicielle support de la messagerie,
- Compte utilisateur nécessaire à l'accès aux services bureautiques.

Spécification

Chaque risque identifié comprend la description de l'actif concerné et cette description précise le type d'actif primaire ainsi que le type d'actif secondaire.

5.2.1.2 L'incident à l'origine du risque

Le risque naît du fait que l'actif considéré peut être victime d'un incident qui va mettre en cause sa disponibilité, son intégrité ou sa confidentialité.

Les types d'incidents possibles, pour un actif donné, sont essentiels pour décrire des risques et doivent être recherchés et identifiés.

Ces types d'incidents dépendent du type d'actif secondaire. En effet, ils sont essentiellement liées à la forme de l'actif (support matériel, support logiciel, etc.) forme qui est définie par le type d'actif secondaire.

La liste des incidents types à partir de laquelle ont été créées les bases de connaissances de MEHARI est précisée dans chaque base.

Il faut noter que pour un risque donné, un seul incident est concerné.

Spécification fonctionnelle

Chaque risque identifié comprend la description de l'incident mis en cause.

5.2.1.3 Le dommage subi

Le type de conséquence peut être implicitement donné par l'incident à l'origine du risque, mais il est des cas où il est encore nécessaire de le préciser (par exemple en cas de vol, la conséquence redoutée peut-être la perte de disponibilité ou la perte de confidentialité).

Il s'agit là, pour les actifs de type Données ou Services de préciser un des critères de conséquence Disponibilité, Intégrité ou Confidentialité a minima, éventuellement en se référant à d'autres critères de conséquences tels que la valeur de preuve.

Pour les actifs de type Processus de gestion, Méhari ne considère qu'un critère : leur Efficience, et plus précisément leur efficacité pour assurer la conformité aux diverses exigences légales ou contractuelles.

Spécification fonctionnelle

Chaque risque identifié précise le type de dommage subi.

Dans les bases de connaissances de MEHARI, les dommages subis pour chaque risque sont précisés.

5.2.1.4 La menace provoquant l'occurrence du risque

Il n'y a pas de risque s'il n'y a pas une cause, qui fait que l'incident que peut subir l'actif se produit effectivement. Les normes et référentiels de sécurité, dont l'ISO/IEC 27005, font appel à la notion de menace pour décrire cette cause.

Il est cependant nécessaire d'inclure dans la menace d'autres aspects que la simple cause.

Justification

Il est nécessaire de préciser également tout ce qui peut décrire la manière dont le dommage pourrait survenir et, notamment, tout ce qui peut avoir une influence sur la probabilité d'occurrence du risque.

C'est ainsi qu'il est nécessaire de décrire :

- L'événement déclenchant l'occurrence du risque (cet événement est souvent déjà décrit par le type d'incident)
- Le caractère volontaire ou accidentel de cet événement
- L'acteur déclenchant cet événement
- Les circonstances dans lesquelles survient cet événement

Il est clair, en effet, que chacun de ces paramètres influe sur la probabilité d'occurrence du risque.

Description

Les deux premières catégories sont souvent réunies dans le même descriptif, ce que nous ferons ici.

a. Événements

Les événements peuvent être décrits par catégories et par types au sein de chaque catégorie.

Les catégories minimales à considérer devraient être :

- Les accidents
- Les erreurs
- Les actes volontaires, malveillants ou non

Dans chaque catégorie, des types d'événements devraient être définis et décrits en fonction d'aspects tels que :

- La cause interne ou externe à l'entité
- L'aspect matériel ou immatériel
- Tout élément pouvant avoir une influence sur la probabilité de survenance de l'événement

La typologie d'événements à partir de laquelle ont été créées les bases de connaissances de MEHARI est précisée dans chaque base.

b. Les acteurs déclenchant la menace

Pour les menaces mises à exécution par des personnes, il est important de distinguer des catégories de personnes en fonction de leurs droits et privilèges.

En effet, en fonction de ces droits :

- Leurs capacités à déclencher la menace seront plus ou moins grandes et donc la probabilité d'occurrence plus ou moins forte.
- Les mesures de sécurité à mettre en œuvre seront différentes et donc, en fonction des mesures effectivement mises en œuvre ou non, les probabilités d'occurrence seront plus ou moins grandes.

Les typologies d'acteurs dépendent des versions de bases de connaissances (en remarquant que plus la typologie d'acteurs sera détaillée, plus on distinguera de menaces et plus le nombre de situations de risque à analyser sera grand).

c. Les circonstances de survenance du risque

Les circonstances peuvent recouvrir des notions de :

- Processus ou étapes de processus : par exemple, altération de fichiers lors de la maintenance
- Lieux : par exemple, vol de media dans tel ou tel type de local, à l'intérieur ou à l'extérieur de l'entreprise
- Temps : par exemple, action menée en dehors ou pendant des heures ouvrables

La recherche des circonstances particulières dignes d'intérêt est à entreprendre pour finaliser la description de chaque risque.

Spécification

Chaque risque identifié comprend une description détaillée de la menace incluant :

- **L'événement déclencheur et son caractère volontaire ou accidentel**
- **L'acteur déclenchant cet événement**
- **Les circonstances dans lesquelles survient cet événement**

Tous ces éléments sont présents dans les bases de connaissances de MEHARI.

5.2.1.5 Le scénario de risque

Les différents éléments requis pour la description d'un risque peuvent être rassemblés sous la forme d'un **scénario de risque** reprenant sous une forme libre les divers aspects cités plus haut.

C'est ainsi que les bases de scénarios des bases de connaissances de MEHARI comprennent une description libre de chaque scénario.

5.2.2 Le processus d'identification des risques

Le processus d'identification des risques est, de toute évidence, essentiel, puisque tout risque ignoré lors de ce processus ne fera l'objet d'aucune analyse ni d'aucun plan de traitement.

Pour pouvoir se référer et se fier à une liste de risques génériques décrits dans une base de données, telle que celle de MEHARI, il est nécessaire de préciser et de spécifier les principes sur la base desquels elle a été établie.

Il est donc nécessaire de spécifier le processus d'identification des risques.

L'objectif étant de s'assurer que la liste des risques obtenue sera aussi exhaustive que possible, trois étapes doivent être distinguées :

- L'élaboration de la liste des éléments caractéristiques des risques
- L'élaboration de la liste des risques théoriquement possibles
- La sélection dans cette liste, de tous les risques possibles dans le contexte précis de la gestion des risques en cours.

Chacune de ces étapes est précisée et spécifiée ci-dessous.

5.2.2.1 Élaboration des éléments caractéristiques des risques

Il s'agit là de préciser et de spécifier les typologies de chaque catégorie d'éléments évoquée plus haut dans ce document, à savoir :

- Les types d'actifs primaires
- Les types d'actifs secondaires
- Les types d'incidents attachés à chaque type d'actif secondaire
- Les types d'événements déclencheurs
- Les types d'acteurs

A noter que les circonstances de survenance du risque seront plus facilement décrites lors de l'étape suivante d'élaboration des risques possibles.

Justification

Il est important, en effet, lors de l'élaboration de la liste de risques, de lister séparément tous les composants élémentaires pour garantir que toute la combinatoire possible sera prise en compte lors de l'étape suivante.

Spécification

Des typologies sont établies pour chaque type d'élément de risque, ainsi que listé ci-dessus.

Les typologies utilisées par MEHARI sont précisées dans chaque version de base de connaissances.

5.2.2.2 Élaboration de la liste des risques possibles

Il s'agit là de rechercher toutes les combinaisons possibles et plausibles d'éléments et de les préciser éventuellement par des circonstances de survenance du risque.

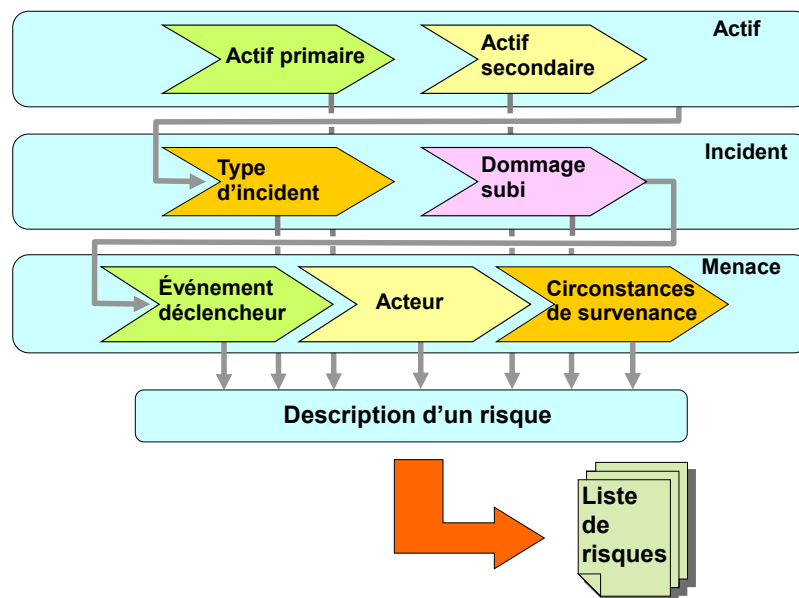
Pour établir cette liste, il est recommandé de partir des actifs.

En effet, c'est le plus souvent en se référant à des actifs primaires ou secondaires, que l'on sera à même de mettre en évidence des circonstances particulières de risque telles que des phases de processus, des périodes calendaires ou des périodes de temps, voire des situations géographiques particulières.

Spécification

Toutes les combinaisons « possibles » sont listées et, à chaque fois que nécessaire, précisées par les circonstances de survenance du risque

Le processus global est représenté ci-dessous.



5.2.2.3 Développement d'une base de connaissances de risques types

La plus grande partie, si ce n'est l'intégralité, du processus ci-dessus est très générale et peut donner le même résultat pour de nombreuses entités. Il est, dès lors, naturel de dérouler ce processus de manière générique afin de développer une base de connaissances de risques types qui sera utilisable par de nombreuses entités, soit intégralement, soit avec quelques adaptations.

Les avantages procurés par une telle base de connaissances sont la mutualisation des moyens de développement et l'enrichissement de la base par une communauté d'utilisateurs.

Chaque base MEHARI inclut ainsi une base de risques types appelés base de « scénarios de risque ». Ces bases sont plus ou moins détaillées selon les versions, mais découlent du même processus et de la même analyse fonctionnelle.

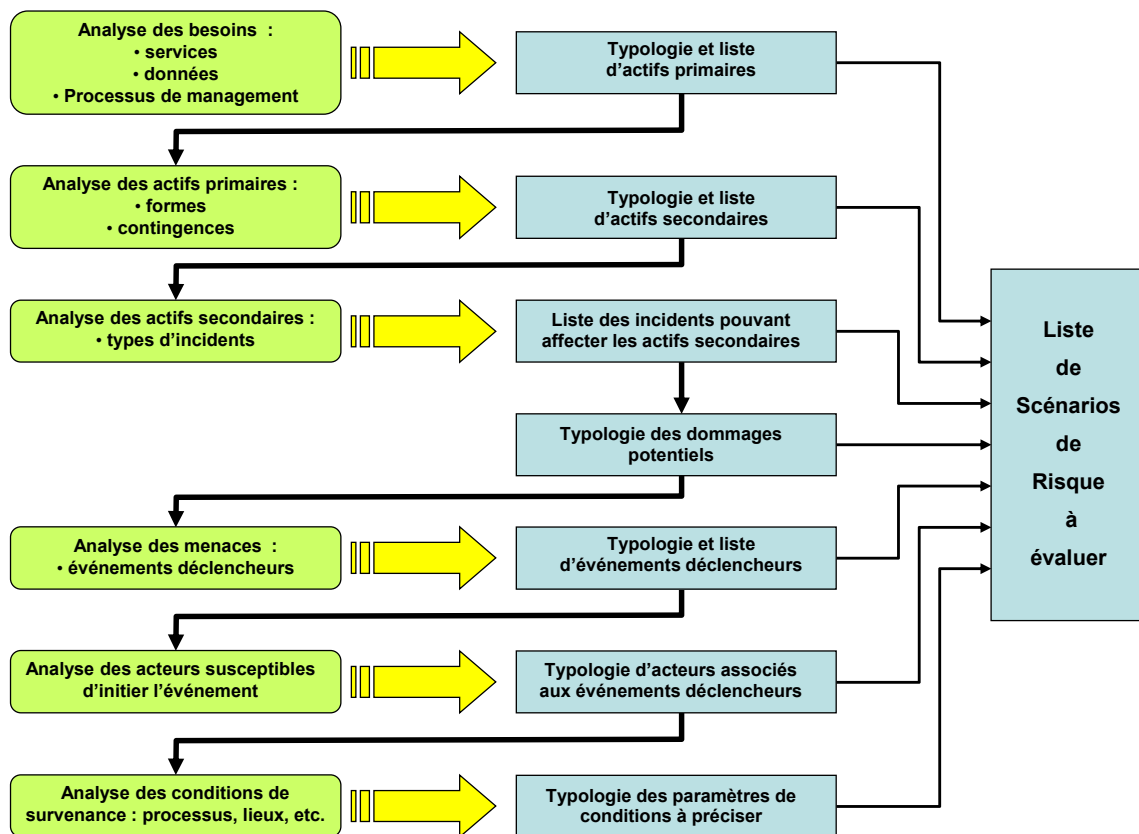
5.2.2.4 Sélection des risques à prendre en compte

Une dernière étape, dans le processus d'identification des risques, consiste à éliminer de la liste ci-dessus, les risques impossibles dans le contexte précis de l'organisation concernée ou sortant du cadre de la gestion des risques concernée.

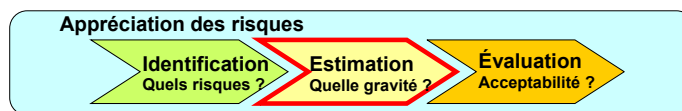
Ceci s'applique particulièrement dans le cas d'utilisation d'une base de risques types telle que celle proposée par MEHARI.

5.2.3 Synthèse de l'identification des risques

L'identification des risques est ainsi un processus qui comprend différentes étapes, chacune ayant des livrables bien définis et contribuant à l'élaboration d'une liste de scénarios de risque à évaluer, ainsi que montré schématiquement ci-dessous.



5.3 L'estimation des risques



Le but de cette étape est d'estimer la gravité de chaque risque précédemment identifié, et ceci en tenant compte des mesures de sécurité mises en place.

Ceci étant, il se peut que la liste des scénarios de risques soit importante et qu'il soit souhaité de faire une première sélection pour limiter la gestion des risques à une liste réduite de risques, notamment les risques estimés a priori comme « majeurs ».

Par ailleurs, il peut également être souhaitable de sélectionner les risques qui seront maintenus sous contrôle et « gérés », sans tenir compte des mesures de sécurité, pour éviter, en particulier, de perdre le contrôle d'une situation de risque actuellement réduite à un niveau acceptable mais qui pourrait, par l'évolution du contexte ou de la technologie, redevenir critique.

Il est donc nécessaire de définir et de pouvoir estimer :

- Une gravité de risque « intrinsèque », c'est-à-dire sans tenir compte des mesures de sécurité
- Une gravité de risque « résiduelle » ou « actuelle », tenant compte des mesures de sécurité en place

Ceci pose deux questions :

- Quels sont les éléments mesurables des risques et quelle métrique d'ensemble est nécessaire pour estimer les gravités intrinsèque et résiduelle des risques?
- Quel est le meilleur processus pour y arriver ?

5.3.1 Les éléments mesurables et la métrique des risques

La mesure du risque, classiquement, repose sur deux paramètres :

- Le niveau de gravité des conséquences, que nous appellerons « impact »
- Le niveau de vraisemblance ou probabilité, que nous appellerons « potentialité »

Une appréciation globale et directe de ces deux paramètres s'avère généralement difficile ; il est donc préférable de recourir à une approche plus analytique en décomposant ces paramètres en plusieurs niveaux et en évaluant séparément :

- L'impact intrinsèque, hors toute mesure de sécurité
- La potentialité intrinsèque, hors toute mesure de sécurité
- L'effet des mesures de sécurité sur ces deux premiers paramètres

Nous analysons ci-dessous les principes qui sous-tendent ces estimations.

5.3.1.1 L'impact intrinsèque

L'impact intrinsèque est défini par le niveau **maximum** des conséquences possibles pour l'organisation, en l'absence de toute mesure de sécurité visant, précisément, à amoindrir ces conséquences.

Justification

En effet, on pourrait envisager d'évaluer directement le niveau d'impact en tenant compte des mesures de sécurité. Le passage par l'impact intrinsèque est justifié par une plus grande facilité d'analyse et par deux raisons complémentaires :

- D'une part les mesures prises ou envisagées pour amoindrir ces conséquences peuvent se révéler non pérennes ou inopérantes et l'impact intrinsèque permet d'évaluer le niveau de conséquences atteint dans cette hypothèse.
- D'autre part, les dirigeants peuvent avoir tendance à sous-estimer les risques par surestimation de l'effet des mesures de sécurité existantes ; ils auront un meilleur jugement sur la situation de risque et sa gravité en commençant par se placer dans l'hypothèse où il n'y a aucune mesure de sécurité.

Plus précisément, si l'impact intrinsèque s'avère important, la question de la qualité et de l'efficacité des moyens à utiliser pour l'amoindrir sera inévitablement posée, alors que seule l'existence de moyens pertinents aurait pu être évoquée si l'on était passé par une évaluation directe de l'impact résiduel.

Considérations complémentaires à prendre en compte

Ceci étant, deux considérations sont à prendre en compte :

- Une fois un sinistre survenu, l'organisation aura des réactions « naturelles » de défense qui, même en l'absence de mesures « organisées » et prévues, permettront de minimiser les conséquences du sinistre.
- De même, il peut exister des mesures limitant les conséquences et non susceptibles d'être remises en cause parce qu'externes ou liées à un contexte permanent.

Dans ces cas précis et dans ces cas seulement, on peut tenir compte de ces mesures pour évaluer l'impact intrinsèque d'un risque.

Spécification

L'impact intrinsèque d'un risque doit être évalué sans tenir compte des mesures de sécurité visant à amoindrir cet impact. Il se réfère à un type d'actif, primaire ou secondaire, et à un type de conséquence.

5.3.1.2 La potentialité intrinsèque

La potentialité intrinsèque est définie comme la probabilité maximale de survenance du risque, en l'absence de toute mesure de sécurité visant, précisément, à amoindrir cette probabilité.

Justification

En effet, on pourrait envisager d'évaluer directement le niveau de potentialité en tenant compte des mesures de sécurité. Le passage par la potentialité intrinsèque est justifié, comme pour l'impact intrinsèque, par une plus grande facilité d'analyse et par les deux raisons complémentaires évoquées plus haut et rappelées ci-dessous :

- D'une part les mesures prises ou envisagées pour amoindrir la probabilité de survenance peuvent se révéler non pérennes ou inopérantes et la potentialité intrinsèque permet d'évaluer le niveau de probabilité atteint dans ce cas.
- D'autre part, les dirigeants peuvent avoir tendance à sous-estimer les risques par surestimation de l'effet des mesures de sécurité existantes ; ils auront un meilleur jugement sur la situation de risque et sa probabilité de survenance en commençant par se placer dans l'hypothèse où il n'y a aucune mesure de sécurité.

Plus précisément, si la potentialité intrinsèque d'un scénario de risque s'avère importante, la question de la qualité et de l'efficacité des moyens à utiliser pour que sa probabilité de survenance soit faible sera inévitablement posée, alors que seule l'existence de moyens pertinents aurait pu être évoquée si l'on était passé par une évaluation directe de la potentialité.

Les acteurs et conditions de survenance seront importants lors de la prise en compte des mesures de sécurité (l'efficacité en dépendant) mais les mesures déjà en place ne sont pas à considérer pour la potentialité intrinsèque, puisque par définition on ne prend en compte aucune mesure de sécurité à ce stade.

Description

L'activité de chaque entreprise, son contexte économique, social, géographique, ... font que chacune est plus ou moins exposée à chaque type de risque, indépendamment de toute mesure prise :

- Une entreprise de haute technologie et leader sur son marché est plus exposée qu'une autre au risque de piratage ou d'espionnage.
- Une entreprise localisée en bordure de rivière est plus exposée qu'une autre au risque d'inondation
- Une entreprise traitant des flux financiers importants est plus exposée qu'une autre à des tentatives de fraude.

Il s'agit donc de s'interroger sur l'existence de facteurs pouvant favoriser l'exposition de l'entreprise au type de risque considéré et donc à l'événement qui le déclenche.

La potentialité intrinsèque d'un événement donné peut dépendre :

- de sa localisation et de son environnement, pour les risques naturels,
- de l'enjeu potentiel d'un acte volontaire, pour son auteur (vol, détournement, satisfaction intellectuelle, etc.)
- de la probabilité qu'une action volontaire vise spécifiquement l'entreprise (inversement proportionnelle au nombre de cibles potentielles : notion de ciblage)

Spécification

La potentialité intrinsèque d'un risque est celle de l'événement qui le déclenche. Elle doit être évaluée en faisant abstraction des mesures de sécurité existantes qui auraient comme effet de réduire sa probabilité d'occurrence.

Remarque : La potentialité intrinsèque peut également être appelée « **Exposition naturelle** » au risque considéré

5.3.1.3 L'effet des mesures de sécurité : facteurs de réduction des risques

Les mesures de sécurité mises en place sont susceptibles d'intervenir comme des facteurs de réduction des risques et il est nécessaire, pour pouvoir gérer les risques, de comprendre comment, par quels effets, et à quel degré ces mesures peuvent réduire le niveau de risque.

Certaines mesures ont une influence sur la potentialité, d'autres sur le niveau de conséquences, ou impact, et ceci de plusieurs manières qu'il est important de distinguer.

Les facteurs de réduction de potentialité

Les mécanismes par lesquels des mesures adéquates peuvent réduire la potentialité du risque sont divers, peuvent se cumuler ou non et ne s'adressent pas tous aux mêmes acteurs.

Il est possible de distinguer, par exemple :

- Le fait d'empêcher totalement un événement de survenir
- Le fait d'empêcher ou non un événement de survenir, en fonction de la sévérité de cet événement
- Le fait de rendre plus difficile à réaliser un acte malveillant (et donc de le rendre réalisable par un moindre nombre de personnes)
- Le fait d'interdire une action humaine
- Le fait d'interdire et d'exercer un contrôle
- Le fait d'interdire, de contrôler et de punir sévèrement le non-respect de la règle

Les mesures ci-dessus relèvent, en fait, de deux ordres ou de deux types de mécanismes :

- La dissuasion, qui a comme objectif, pour les actions humaines, de rendre moins probable que l'acteur passe réellement à l'action.
- La prévention qui a pour objectif de rendre moins probable que l'action, humaine ou non, aboutisse à la réalisation du risque

La dissuasion

La dissuasion repose, de fait, sur trois principes :

- L'imputabilité de l'action à son auteur, ce qui met en jeu des mécanismes techniques et organisationnels évaluables (existence de traces, authentification de l'auteur, solidité de la preuve, ...).
- L'existence de sanctions dont la sévérité est également évaluable.
- La connaissance, par l'auteur, des possibilités d'imputation et des sanctions alors encourues.

Le niveau de dissuasion est, ainsi, susceptible d'être évalué et quantifié. Il convient pour cela de se référer à une échelle de niveaux de dissuasion, à définir ou au moins à valider pour chaque entreprise, ainsi que cela sera développé plus loin.

La prévention

La prévention dépend, bien évidemment, des événements que l'on veut empêcher de survenir. Il s'agit, le plus souvent, de mesures techniques et de mécanismes de contrôle dont il est possible d'évaluer l'efficacité et la robustesse.

Le niveau de prévention est ainsi susceptible d'être évalué et quantifié. Il convient pour cela de se référer à une échelle de niveaux de prévention, à définir ou au moins à valider pour chaque entreprise, ainsi que cela sera développé plus loin.

Spécification

Les facteurs de réduction de la potentialité sont la dissuasion et la prévention. Ces facteurs doivent être évalués et quantifiés en se référant à des échelles de niveau, qu'il convient de définir préalablement.

Les facteurs de réduction d'impact

Les mécanismes par lesquels des mesures adéquates peuvent réduire l'impact du risque (le niveau de ses conséquences) sont divers, peuvent se cumuler ou non et ne s'adressent pas tous aux mêmes types de conséquences.

Il est possible de distinguer, par exemple :

- Le fait de limiter dans l'absolu le niveau maximum des conséquences directes possibles,
- Le fait d'empêcher la propagation d'un sinistre initial,
- Le fait de prévoir la réparation d'un équipement suite à un sinistre matériel,
- Le fait de prévoir la restauration d'un état d'origine suite à un sinistre immatériel,
- Le fait de prévoir des moyens de secours,

Les mesures ci-dessus relèvent, en fait, de deux ordres ou de deux types de mécanismes :

- Le confinement, qui a comme objectif de limiter l'ampleur des conséquences directes,
- L'effet palliatif qui a pour objectif de minimiser les conséquences indirectes du risque par une anticipation de la gestion de crise.

Le confinement

Le confinement repose sur divers types de mécanismes ayant en commun d'imposer des limites aux conséquences du risque :

- La fixation de limites à des événements pouvant se propager, telles que des limites physiques à certains types de sinistres (cloisons anti-feu, par exemple),
- La fixation de points de contrôle intermédiaires dans des processus pour éviter la propagation d'erreurs ou d'anomalies,
- La surveillance du déroulement de processus pour limiter les conséquences d'une dérive pouvant occasionner des conséquences plus sévères,
- La fixation de limites aux variations possibles de paramètres (limitation des montants de versements, limitation des écarts entre deux états avec déclenchement de contrôles en cas de dépassement, par exemple).

Le niveau de confinement est susceptible d'être évalué et quantifié. Il convient pour cela de se référer à une échelle de niveaux de confinement, à définir ou au moins à valider pour chaque entreprise, ainsi que cela sera développé plus loin.

L'effet palliatif

Cet effet, parfois appelé *palliation*, ne change rien aux conséquences directes, c'est-à-dire au sinistre lui-même, mais conduit à minimiser les conséquences indirectes du sinistre. Les mesures correspondantes reposent sur divers types de mécanismes :

- Les plans de maintenance matérielle ou logicielle,
- Les plans de sauvegarde et de restauration de données,
- Les plans de secours et plans de continuité d'activité,
- Les plans de gestion et de communication de crise.

Le niveau d'effet palliatif est susceptible d'être évalué et quantifié. Il convient pour cela de se référer à une échelle de niveaux de palliation, à définir ou au moins à valider pour chaque entreprise, ainsi que cela sera développé plus loin.

Spécification

Les facteurs de réduction d'impact sont le confinement et la palliation (ou facteur palliatif). Ces facteurs doivent être évalués et quantifiés en se référant à des échelles de niveau, qu'il convient de définir préalablement.

5.3.1.4 Influence du niveau de qualité des mesures de sécurité existantes

Il est bien clair que ces facteurs de réduction de risque ne dépendent pas uniquement de la nature des mesures de sécurité existantes mais aussi de leur niveau de qualité. Certaines implémentations peuvent comprendre des mécanismes plus efficaces que d'autres et il convient, bien entendu, de pouvoir en tenir compte.

Spécification

Le processus d'évaluation des facteurs de réduction des risques doit permettre de tenir compte des niveaux de qualité des mesures de sécurité pertinentes pour chaque risque.

En pratique, cette mesure de niveau de qualité revient à rechercher les faiblesses éventuelles, non seulement des mécanismes mis en œuvre, mais également des conditions et du contexte de cette mise en œuvre.

5.3.1.5 Utilisation d'une base de connaissance des risques

Si les risques sont identifiés avec l'aide d'une base de connaissance des risques types, telle qu'elle a été évoquée au paragraphe 4.2.2.3, il est alors possible de compléter cette base pour inclure, au-delà de la simple description des éléments caractéristiques de chaque risque, des informations sur les mesures de sécurité pertinentes pour chaque risque type, sur les critères permettant de juger de la qualité de ces mesures et sur les relations entre ces niveaux de qualité et le niveau des facteurs de réduction des risques.

MEHARI et ses bases de connaissances contiennent effectivement tous ces éléments et, en particulier :

- Une spécification des « services de sécurité » incluant des critères de jugement de niveau de qualité et une métrique de mesure (reportée en annexe),
- Une base experte de questionnaires de diagnostic de la qualité des services de sécurité,
- La référence, pour chaque facteur de réduction de risque de chaque risque de la base de connaissances, des services de sécurité pertinents et des formules permettant d'évaluer les effets combinés de ces services.

5.3.2 Processus d'estimation des risques

Le processus d'estimation des risques comprend deux phases :

- Une phase que l'on pourrait qualifier de « stratégique » dans la mesure où elle correspond à la mise en place des bases et références d'évaluation.
- Une phase plus opérationnelle, pendant laquelle les estimations des risques seront menées à bien en s'appuyant sur les bases et références évoquées plus haut

5.3.2.1 L'élaboration des éléments de référence

Il s'agit là de bâtir les différentes définitions de niveaux qui serviront à évaluer les divers paramètres de chaque risque évoqués précédemment et, plus précisément de définir :

- L'échelle d'impact,

- L'échelle de potentialité,
- Les échelles de niveau des différents facteurs de réduction des risques.

5.3.2.2 Élaboration de l'échelle d'impact

L'échelle d'impact a pour objectif de hiérarchiser des niveaux de conséquences.

Justification

Le niveau de conséquences étant un élément majeur de l'estimation des risques, une définition aussi claire que possible et dénuée d'ambiguïté doit être recherchée et établie.

Description

Il s'agira forcément d'estimation et non de « mesure » et il serait donc illusoire d'avoir trop de niveaux de conséquences. Le choix de 4 niveaux semble un bon compromis.

Spécification

Il est nécessaire de définir le nombre de niveaux d'impact et d'en donner une définition. Cette définition doit se référer à des niveaux de gravité de conséquences.

Toute définition reliée à autre chose que des niveaux de gravité serait impropre à la gestion directe des risques.

Les commentaires et explications sont souhaitables pour favoriser les prises de décisions quant au niveau de gravité qui pourrait être atteint.

Nous donnons en annexe les définitions correspondant à l'échelle à 4 niveaux proposée comme standard par MEHARI.

5.3.2.3 Élaboration de l'échelle de potentialité

L'échelle de potentialité a pour objectif de hiérarchiser des niveaux de probabilité.

Justification

Le niveau de potentialité étant un élément majeur de l'estimation des risques, une définition aussi claire que possible et dénuée d'ambiguïté doit être recherchée et établie.

Description

Il s'agira forcément d'estimation et non de « mesure » et il serait donc illusoire d'avoir trop de niveaux de potentialité. Le choix de 4 niveaux semble, là encore, un bon compromis.

Spécification

Il est nécessaire de définir le nombre de niveaux de potentialité et d'en donner une définition. Cette définition doit se référer à des niveaux de probabilité.

Toute définition reliée à autre chose que des niveaux de probabilité serait impropre à la gestion directe des risques.

Les commentaires et explications sont souhaitables pour favoriser les prises de décisions quant au niveau de potentialité qui pourrait être atteint.

Nous donnons en annexe les définitions correspondant à l'échelle à 4 niveaux proposée comme standard par MEHARI.

Élaboration des échelles de niveau des facteurs de réduction des risques

Chaque facteur de réduction de risque peut être évalué en se référant à une échelle de niveau qu'il faut donc au préalable fixer.

De même que pour les échelles d'impact et de potentialité, le choix de quatre niveaux semble être un bon compromis entre une précision excessive et une précision insuffisante. Le point important est que la définition de chaque niveau soit telle que l'on puisse aisément choisir entre un niveau et un autre.

Les échelles proposées comme standard par MEHARI sont données en annexe.

Spécification

Pour chaque facteur de réduction de risque, des niveaux sont définis en se référant à l'efficacité des mesures correspondantes : mesures dissuasives, mesures préventives, mesures de confinement et mesures palliatives.

5.3.2.4 L'estimation des risques

L'estimation des risques, qui s'appuie sur les éléments de référence définis préalablement comme décrit ci-dessus, comprend, pour chaque risque :

- L'évaluation de l'impact intrinsèque et de la potentialité intrinsèque,
- L'évaluation des facteurs de réduction de risque,
- L'évaluation de l'impact et de la potentialité des risques, compte tenu de l'existence et de la valeur de ces facteurs de réduction.

L'évaluation de l'impact intrinsèque et de la potentialité intrinsèque

Ces deux évaluations sont à faire en se référant aux définitions de niveaux et en faisant abstraction de toute mesure de sécurité, ainsi que cela a été précisé plus haut.

Pour MEHARI, les processus détaillés correspondants sont décrits dans la documentation : Guide de l'analyse des enjeux, d'une part, et guide de l'analyse et du traitement des risques, d'autre part.

L'évaluation des facteurs de réduction des risques

L'évaluation de chaque facteur de réduction de risque est à faire selon le processus suivant :

- Rechercher les mesures ou services de sécurité pertinents pour chaque scénario de risque
- Déterminer les effets (dissuasif, préventif, de confinement, palliatif) induits par chaque mesure ou service de sécurité
- Pour chaque effet et pour chaque mesure, déterminer le niveau atteint en se référant aux échelles de niveaux
- Pour chaque effet, déterminer le niveau maximum atteint pour l'ensemble des mesures retenues comme pertinentes pour ce risque,
- Ce sont ces niveaux maximums qui fixent le niveau de chaque facteur de réduction de risque (pour le risque analysé).

L'utilisation d'une base de connaissance des risques telle que celle évoquée au paragraphe 4.3.1.5 est, dans ce processus, fortement souhaitable, si ce n'est nécessaire. Les arguments qui militent pour l'emploi d'une base de connaissance sont, en effet, les suivants :

- L'identification des mesures de sécurité pertinentes à même de réduire les facteurs de réduction de risque doit tenir compte d'un principe de précaution : on ne doit prendre en compte des mesures que si l'on peut garantir qu'elles auront un effet. L'aide des experts qui ont élaboré une base de connaissances comprenant des mesures de sécurité et des questionnaires d'audit associés sera alors bien utile.
- La manière dont peuvent se combiner, se compléter ou dépendre l'une de l'autre plusieurs mesures de sécurité est une affaire d'experts que l'on n'a pas forcément sous la main lors de l'évaluation de facteurs de réduction de risques.

- La prise en compte des niveaux de qualité des mesures de sécurité (ou des niveaux de vulnérabilité contextuelle) demande que l'on ait défini des questionnaires permettant d'évaluer ces niveaux, ce qui n'est pas du ressort d'un processus d'évaluation,
- La relation entre niveaux des mesures de sécurité et niveaux de facteurs de réduction de risque est également une affaire d'experts.

C'est pour tenir compte tenu de tous ces aspects que MEHARI s'appuie sur une base de connaissance qui comprend une base de « services de sécurité », des questionnaires d'évaluation de la qualité de ces services et des formules permettant d'évaluer les facteurs de réduction de risques à partir des résultats d'un audit de la qualité des services de sécurité.

L'utilisation des bases MEHARI permet ainsi, après un diagnostic de la qualité des services de sécurité, une évaluation du niveau des facteurs de réduction de risque de chaque scénario de risque de chaque base.

L'évaluation de l'impact et de la potentialité (résiduels ou actuels) des risques

Ces deux évaluations se font à partir des évaluations d'impact intrinsèque, de potentialité intrinsèque et des facteurs de réduction de risque.

Évaluation de la potentialité

Il s'agit, pour la potentialité, d'un jugement porté sur le niveau de potentialité en fonction des éléments du scénario de risque et qui revient à poser la question suivante :

Compte tenu de la potentialité intrinsèque (ou de l'exposition naturelle au risque), compte tenu du niveau des mesures dissuasives (pour une action humaine) et compte tenu du niveau des mesures préventives, à quel niveau évalue-t-on la potentialité réelle du risque ?

Cette évaluation est de l'ordre de la décision, mais afin de rendre les jugements correspondants reproductibles, il est conseillé de s'appuyer sur des grilles de décision (qui auront pu être définies lors de la phase stratégique, avec les échelles de niveau).

De telles grilles devraient alors être fonction du type de scénario : accident, erreur ou action volontaire humaine.

Les grilles de décision proposées comme standard par MEHARI sont données en annexe. Cette annexe indique, pour divers types de scénarios, et pour chaque niveau d'exposition naturelle (EXPO), en fonction des niveaux de mesures dissuasives (DISS) et des mesures préventives (PREV) le niveau de potentialité résultant.

Évaluation de l'impact

Il s'agit, pour l'impact, d'un jugement porté sur le niveau d'impact en fonction des éléments du scénario de risque et qui revient à poser la question suivante :

Compte tenu de l'impact intrinsèque, compte tenu du niveau des mesures de confinement (pour les scénarios qui peuvent l'être) et compte tenu du niveau des mesures palliatives, à quel niveau évalue-t-on l'impact réel du risque ?

Cette évaluation est de l'ordre de la décision, mais afin de rendre les jugements correspondants reproductibles, il est conseillé de s'appuyer sur des grilles de décision (qui auront pu être définies lors de la phase stratégique, avec les échelles de niveau).

De telles grilles devraient alors être fonction du type de scénario : atteinte à la disponibilité, à la confidentialité ou à l'intégrité, avec éventuellement un cas particulier pour des scénarios à impact limitable sans mesures palliatives possibles.

Les grilles de décision proposées comme standard par MEHARI sont données en annexe. Cette annexe indique, pour divers types de scénarios, et pour chaque niveau d'impact intrinsèque (II), en fonction

des niveaux de mesures de confinement (CONF) et des mesures palliatives (PALL) le niveau d'impact résultant.

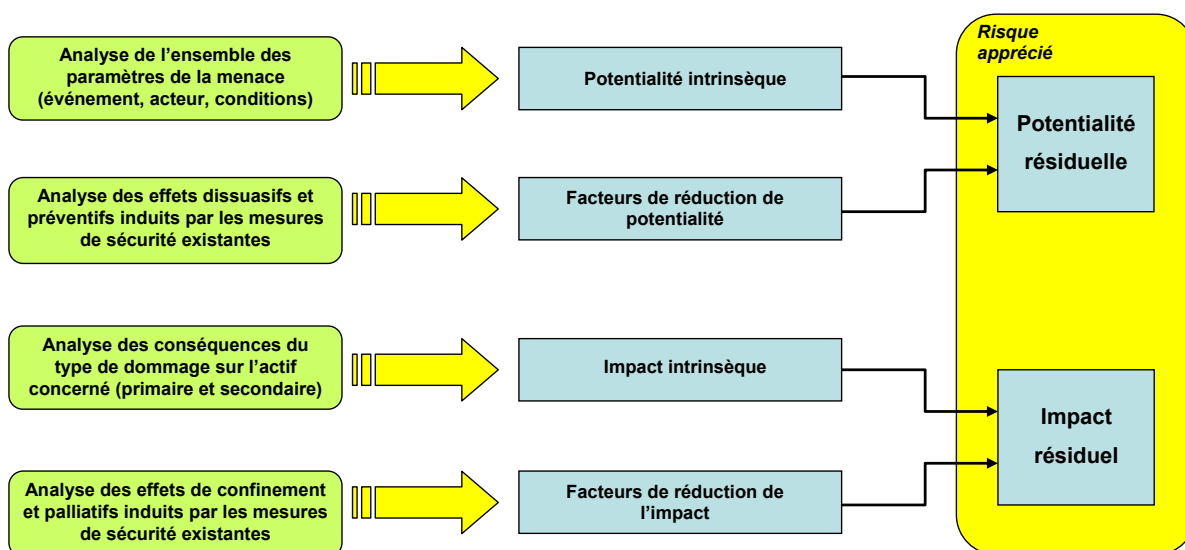
5.3.2.5 L'appréciation globale de chaque risque (géré)

L'appréciation de chaque risque repose ainsi sur une double évaluation, celle de sa potentialité et celle de son impact.

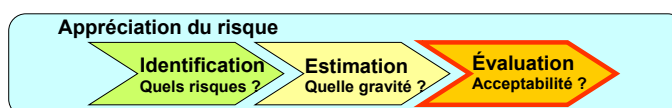
C'est en fonction de ces deux paramètres que les risques seront évalués, selon les processus décrits ci-dessous.

5.3.3 Synthèse de l'appréciation de chaque scénario de risque

L'appréciation de chaque scénario de risque est ainsi un processus qui comprend différentes étapes, chacune contribuant à l'élaboration d'un jugement individualisé sur la potentialité et l'impact de chaque scénario de risque, ainsi que montré schématiquement ci-dessous.



5.4 L'évaluation des risques



La gravité du scénario ou de la situation de risque résulte à la fois de sa potentialité et de son impact (résiduels).

Il ne s'agit pas, cependant, d'une opération mathématique entre ces deux valeurs mais d'un simple jugement sur le caractère acceptable ou non de la situation.

La seule question à se poser, en fonction de la potentialité et de l'impact du risque analysé, est celle-ci :

Cette situation de risque est-elle acceptable en l'état et sinon que proposer ?

La décision d'accepter un risque ou de le déclarer inacceptable doit être prise par un processus qui garantisse la constance de telle décision.

A cette fin, il est nécessaire d'établir une table de décision qui assurera la cohérence des décisions prises à des instants différents ou par des personnes différentes.

Ces tables de décisions peuvent être représentées par des grilles « d'acceptabilité des risques » qui définissent, en fonction de l'impact et de la potentialité estimés, si le risque est acceptable ou non.

MEHARI propose de définir trois types de risques :

- Les risques insupportables, qui devraient faire l'objet de mesures d'urgence, en dehors de tout cycle budgétaire.
- Les risques inadmissibles qui devraient être réduits ou éliminés à une échéance à déterminer, donc à prendre en compte dans une planification (plan de sécurité).
- Les risques tolérés.

Les deux premières catégories correspondent à ce que nous avons appelé les risques inacceptables.

La grille de gravité standard de MEHARI est donnée ci-dessous. Dans cet exemple, G est la gravité globale évaluée par la grille en fonction de l'impact (I) et de la potentialité (P), une gravité de 4 correspond à un risque insupportable, une gravité de 3 à un risque inadmissible et les gravités inférieures à des risques tolérés.

I = 4	G = 2	G = 3	G = 4	G = 4
I = 3	G = 2	G = 3	G = 3	G = 4
I = 2	G = 1	G = 2	G = 2	G = 3
I = 1	G = 1	G = 1	G = 1	G = 2
	P = 1	P = 2	P = 3	P = 4

Grille d'acceptabilité des risques

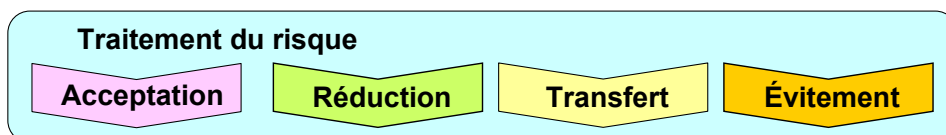
6 Le traitement des risques

Le traitement des risques comprend les différentes options possibles, une fois que les risques ont été identifiés, répertoriés et évalués, c'est-à-dire une fois que l'on a porté sur chacun d'entre eux un jugement sur son caractère acceptable ou non.

Il ne s'agit pas ici de décrire en détail chacune des options, mais de faire ressortir ce que chaque option peut entraîner comme exigence vis-à-vis des méthodes de gestion des risques liés à l'information, afin de spécifier ce que doivent contenir ces méthodes pour être à même de supporter une gestion directe et individuelle des risques.

Nous aborderons donc successivement les quatre options principales de traitement des risques, décrites en particulier par la norme ISO/IEC 27005, et représentées par le schéma ci-dessous, à savoir :

- L'acceptation du risque,
- La réduction du risque,
- Le transfert du risque,
- L'évitement du risque.



6.1 L'acceptation du risque

L'acceptation du risque consiste, bien entendu, à accepter la situation de risque décrite par le scénario de risque tel qu'explicité plus haut dans ce document.

En fait, il serait plus correct et plus général de considérer que l'entreprise ou l'organisme accepte de ne rien faire vis-à-vis de cette situation.

Les raisons de cette décision sont de deux ordres :

- Cela couvre tous les cas où le risque a été évalué comme acceptable au sens de la grille d'acceptabilité des risques parce que la combinaison de son impact et de sa potentialité a été jugée acceptable,
- Cela couvre également les cas où, bien que théoriquement inacceptable, il a été jugé impossible d'y remédier par une autre voie ou que toute solution a été écartée pour des raisons économiques.

Quoi qu'il en soit, il importe dans ces cas, et surtout dans le second, que cette acceptation du risque fasse l'objet d'un consensus et qu'une communication sur cette acceptation soit assurée.

Cependant, cette communication ne requiert rien de plus qu'une description précise de la situation de risque, ce qui est déjà assuré par les spécifications décrites dans les chapitres précédents.

Il n'y a donc pas d'exigences supplémentaires au titre de l'acceptation du risque sauf, probablement, à mettre en place des indicateurs de suivi pour s'assurer que les conditions éventuelles de cette acceptation demeurent valables dans le temps.

6.2 La réduction du risque

La réduction du risque consiste à réduire un des deux paramètres caractéristiques du risque, potentialité ou impact, voire les deux simultanément, par des actions précises décidées pour chaque risque identifié comme inacceptable.

Ces actions consistent essentiellement à améliorer certains facteurs de réduction de risques par la mise en place de mesures de sécurité adaptées.

Le choix direct de solutions concrètes serait inadapté au processus de décision que constitue la réduction du risque, car il ferait dépendre la pertinence de la solution des évolutions des technologies. Il importe donc, à ce stade de spécifier un besoin fonctionnel et de le faire tant au niveau des finalités attendues que du niveau de performance visé. Cela conduit à une notion de « service de sécurité », notion essentielle pour le traitement des risques. Les services de sécurité, tels qu'utilisés par MEHARI, sont définis en annexe.

6.2.1 Le choix de services de sécurité à mettre en place pour augmenter certains facteurs de réduction du risque

6.2.1.1 Les services de sécurité pertinents ou adaptés à un risque donné

Le processus de décision relatif à la réduction du risque consiste d'abord à sélectionner des services de sécurité pertinents pour le scénario de risque concerné et pour le facteur de réduction de risque que l'on souhaite améliorer.

Cela nécessite de pouvoir s'appuyer sur une base de connaissances des services de sécurité définis au plan fonctionnel, c'est-à-dire en termes d'objectifs.

Spécification

Une méthode de gestion des risques doit proposer une base de connaissance des services de sécurité, définis au plan fonctionnel et à celui des objectifs attendus de chaque service.

La liste des services de sécurité de MEHARI dépend des versions de la base de connaissances.

Etant admis le principe d'existence de cette base de connaissances, il conviendra de choisir les facteurs de réduction de risque et les services pertinents pour ce faire.

Le processus correspondant n'est pas unique et il peut y avoir plusieurs manières de présenter les principales options stratégiques. Par ailleurs ce document n'a pas pour objet de spécifier un processus de choix particulier.

6.2.1.2 Le choix de niveau de qualité cible pour un service de sécurité à mettre en place

Par contre, il ne fait pas de doute que l'ampleur de l'amélioration des facteurs de réduction de risque concernés dépend fortement des performances des services de sécurité sélectionnés, ce qui exige de pouvoir définir un niveau de qualité des services de sécurité.

Il convient pour cela de définir :

- Des critères d'évaluation de la qualité des services de sécurité
- Des échelles de niveau, comme cela a été fait pour les paramètres du risque.

Il ne suffit pas, en effet, de juger de l'efficacité d'un service pour atteindre son objectif, mais il convient de s'assurer également qu'il a les mécanismes suffisants pour résister à ceux qui voudraient le court-circuiter ou l'inhiber et qu'il existe des mécanismes de contrôle de sa permanence.

Spécification

Il est nécessaire de définir des niveaux de qualité des services de sécurité et d'en donner une définition. Cette définition doit se référer à des critères d'évaluation et à des niveaux de force ou de compétence qu'il faut avoir pour violer le service, le contourner, le court-circuiter et/ou l'inhiber ou rendre inefficace la détection de sa mise hors circuit.

L'échelle des niveaux de qualité des services de sécurité de MEHARI ainsi que les critères pris en compte sont donnés en annexe.

6.2.1.3 L'évaluation de l'effet combiné de plusieurs services de sécurité

L'évaluation de l'effet combiné de plusieurs services de sécurité projetés ou existants demeure une étape importante du choix des services à mettre en place dans une optique de gestion des risques.

Cela demande que des aides soient fournies et c'est bien l'objet d'une base de connaissances des risques telle que présentée aux paragraphes 4.2.2.3, 4.3.1.5 et 4.3.2.2.

Spécification

Une base de connaissance incluant les risques et leurs éléments caractéristiques, les services de sécurité, les questionnaires d'évaluation de la qualité des services de sécurité et des aides à l'évaluation des facteurs de réduction de risque en fonction de la qualité des services de sécurité doit faire partie de la méthode d'analyse et de traitement des risques.

Si une telle base n'est pas fournie ou n'est pas applicable dans un contexte donné, la méthode doit fournir les éléments et les guides nécessaires à son élaboration.

MEHARI contient une base adaptée au domaine des systèmes d'information. Un guide de développement d'une base de connaissance a été développé et est disponible.

6.2.1.4 Processus de décision propre à la réduction des risques

Le processus de réduction de risque consiste donc à :

- sélectionner des services de sécurité adaptés,
- sélectionner un niveau cible pour ces services,
- en déduire de nouvelles valeurs pour les facteurs de réduction de risque,
- vérifier qu'avec ces nouvelles valeurs le risque est ramené à un niveau de gravité acceptable.

6.2.2 Cas particulier de l'emploi de mesures structurelles

Certaines mesures, que nous appellerons « structurelles » peuvent avoir une influence sur la potentialité intrinsèque ou sur l'impact intrinsèque du risque encouru.

Il s'agit alors de changer « structurellement » certains aspects du contexte de l'entreprise ou de son lien avec l'environnement. Nous prendrons deux exemples :

Une entreprise donnée peut être exposée à des risques environnementaux tels que des risques d'inondation, des risques sismiques, etc. Elle peut réduire le niveau de tels risques par la mise en œuvre de services de sécurité adaptés, mais elle peut aussi décider, tout simplement, de déménager. Il s'agira alors de mesures dites structurelles car pouvant changer « structurellement » la nature ou le niveau de risque.

Telle entreprise bancaire peut être exposée au risque de hold-up. Elle peut limiter le risque par des services de sécurité adaptés, mais aussi par des mesures structurelles consistant à limiter les encours disponibles.

6.3 Le transfert du risque

Le transfert du risque consiste, en pratique, à se placer sur un plan financier et à transférer une partie de la charge financière occasionnée par la survenance du risque sur un tiers.

Il s'agit le plus souvent de l'assurance, mais il peut également s'agir de transférer la charge sur un tiers (responsable) par une action en justice.

Une telle décision, pour ne pas faire appel aux mêmes mécanismes d'évaluation, n'en réclame pas moins la mise en œuvre de services de sécurité spécifiques (au niveau de la collecte de preuves en particulier) et ce qui a été spécifié plus haut reste valable sans exigences supplémentaires.

6.4 L'évitement du risque

L'évitement du risque est proche de sa réduction par des mesures structurelles.

La différence vient du fait qu'au lieu de jouer sur les rapports entre l'entreprise ou l'organisme et son environnement, on joue sur ses processus internes pour que la situation de risque n'existe plus du tout.

Prenons, là encore un exemple.

Telle entreprise peut être exposée à un risque de divulgation grave lors de l'élaboration de son plan stratégique qui contient rassemblées, beaucoup d'informations extrêmement sensibles. Une des solutions consiste à ne plus établir un tel plan stratégique : c'est une solution d'évitement du risque.

D'une manière générale l'évitement du risque consiste à jouer sur les paramètres de description fine du scénario de risque, en modifiant ces paramètres.

On peut en conclure que cette solution n'est véritablement possible qu'à la condition que les risques aient été décrits très finement dans leurs scénarios, ainsi que cela a été spécifié plus haut dans ce document.

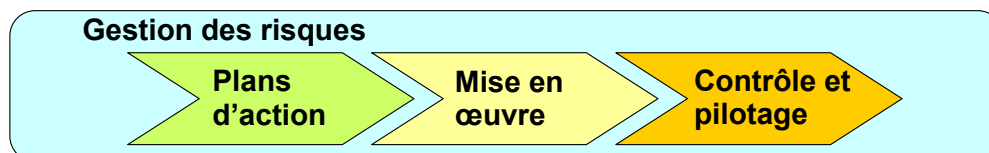
Ceci étant la caractérisation fine des scénarios, ainsi que nous l'avons spécifié, suffit à permettre cet évitement du risque.

7 La gestion des risques

La gestion des risques comprend l'ensemble des processus qui vont permettre, une fois les décisions de traitement des risques prises, de mettre en œuvre ces décisions, d'en contrôler l'effet et de les améliorer, si nécessaire.

La question qui se pose ici, compte tenu de l'objectif de ce document, est de savoir si ces processus induisent des exigences particulières qu'il conviendrait de spécifier pour garantir l'efficacité d'une méthode de gestion des risques liés à l'information.

En partant du schéma global présenté en début de document et rappelé ci-dessous, nous allons analyser les exigences propres à chaque phase.



7.1 L'élaboration des plans d'action

À l'issue de la phase d'analyse des risques et des prises de décision concernant le traitement des risques, l'entreprise ou l'organisme a décidé du principe d'un certain nombre d'actions qui relèvent, selon le type de traitement retenu :

- De la mise en place de services de sécurité, avec pour chacun, un objectif de niveau de qualité
- De mesures structurelles visant à réduire certaines expositions au risque
- De mesures organisationnelles visant à éviter certains risques

Ceci étant, il doit être clair que toutes ces actions ne seront sans doute pas menées simultanément ni toutes engagées immédiatement, pour diverses raisons telles que la limitation des moyens budgétaires, le manque de disponibilité des moyens humains, etc.

Dans ces conditions la phase d'élaboration des plans d'action doit comprendre les étapes suivantes :

- le choix des objectifs prioritaires, en termes de services de sécurité à mettre en œuvre et l'optimisation de ce choix
- la transformation des choix de services de sécurité en projets concrets
- le choix des mesures structurelles éventuelles et des mesures d'évitement des risques
- la validation des décisions précédentes.

7.1.1 Choix des objectifs prioritaires et optimisation

Si toutes les actions ne peuvent être engagées simultanément, pour des raisons économiques, de moyens disponibles ou pour toute autre raison, il y a un choix à faire en ce qui concerne les mesures à engager prioritairement.

Les éléments à prendre en compte pour effectuer ces choix sont :

- Les niveaux de gravité des risques que les mesures prioritaires permettront de réduire (les risques de niveau le plus élevé devant être traités en premier)
- Le nombre de risques qui seront traités et le nombre de risques dont le traitement sera remis à plus tard
- La rapidité avec laquelle les premiers résultats pourront être observés

- L'incidence de ces choix sur la sensibilisation du personnel
- Etc.

Selon l'importance accordée à l'un ou l'autre de ces critères, des outils d'optimisation peuvent s'avérer souhaitables.

MEHARI propose des processus d'optimisation pour le choix des mesures à engager prioritairement.

7.1.2 Le choix des solutions : mécanismes techniques et organisationnels

Le choix des solutions concrètes à déployer, que ces solutions s'appuient sur des mécanismes techniques ou organisationnels revient, bien entendu, aux équipes spécialisées telles que Direction des systèmes d'information, responsables réseaux, responsables de la sécurité physique, RSSI, etc.

Il n'en reste pas moins qu'il s'agit d'un transfert de responsabilités entre les responsables de la gestion des risques qui ont sélectionné des services de sécurité à mettre en œuvre avec un certain degré de qualité et les responsables de la définition des mécanismes et de leur déploiement et que ce transfert doit reposer sur des définitions et des spécifications claires.

Ces définitions devraient couvrir, comme nous l'avons dit plus haut dans ce document, tant les critères d'évaluation de la qualité des services que les niveaux eux-mêmes.

Les définitions utilisées par MEHARI sont reportées en annexe.

7.1.3 Choix de mesures structurelles et de mesures d'évitement de risques

Ces choix, essentiellement basés sur des particularités de situations ou de processus opératoires, ne conduisent pas à des exigences particulières en ce qui concerne les méthodes de gestion de risque et n'ont pas d'incidence directe sur les bases de connaissances ni les principes de MEHARI.

7.1.4 Validation et prise de décision

Les différents choix explicités ci-dessus doivent, bien entendu être chiffrés et faire l'objet d'une planification avant d'être présentés aux instances de décision pour validation. Cette étape n'est pas spécifique à la gestion directe des risques et n'a pas d'exigence particulière en ce qui concerne la méthode de gestion de risques.

7.2 Mise en œuvre des plans d'action

La mise en œuvre des plans d'action et des projets de sécurité peut révéler des difficultés d'application dues à un contexte particulier.

Il importe alors de pouvoir se référer aux risques que chaque plan d'action était destiné à réduire afin de pouvoir réagir au mieux et ceci ne sera possible que si des outils de simulation permettent de mettre en évidence l'influence individuelle de chaque plan d'action ou projet sur les niveaux de risques.

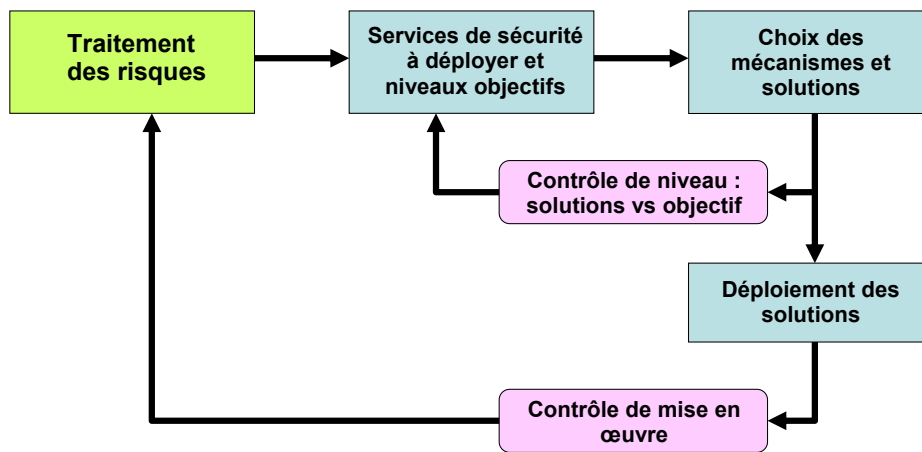
Spécification

L'influence des projets et plans d'action sur les niveaux de risques doit pouvoir être simulée afin de pouvoir réagir au mieux en cas de difficulté.

Les bases de connaissances de MEHARI, toutes versions confondues, offrent cette possibilité.

7.3 Contrôle et pilotage de la gestion directe des risques

Les contrôles à effectuer pour piloter la gestion directe des risques sont multiples et sont représentés par le schéma ci-dessous.



Le premier niveau de contrôle à effectuer est que les mécanismes et solutions de sécurité planifiés et décidés correspondent bien aux niveaux de qualité de service retenus en phase de traitement des risques.

Le deuxième contrôle est un contrôle de mise en œuvre.

7.3.1 Contrôle du niveau de qualité de service

Il devrait s'agir d'autocontrôle le plus souvent. Ceci pose la question de savoir comment les personnels techniques en charge de définir les mécanismes et solutions à mettre en œuvre vont pouvoir le faire avec une connaissance suffisante de l'incidence de leurs décisions sur le niveau de qualité de service qui sera obtenu in fine.

Par ailleurs, un contrôle a posteriori sera nécessaire et ce contrôle devra être effectué par du personnel qui ne sera pas obligatoirement un technicien confirmé et d'expérience.

Cela conduit à la nécessité d'une base d'expertise ou base d'audit des services de sécurité qui permettra des choix appropriés lors de la phase de définition des mécanismes et solutions à mettre en œuvre, d'une part et un contrôle a posteriori, d'autre part.

Justification de la nécessité d'une base d'audit des services de sécurité

Ainsi que nous l'avons vu, la qualité des services de sécurité comprend plusieurs aspects, décrits en détail en annexe.

Pour pouvoir vérifier chacun de ces aspects, des questions spécifiques devront être posées.

Il est alors nécessaire qu'il y ait une ligne directrice et un répertoire des questions à poser et qu'à ces questions soit associé un système de cotation des réponses pour pouvoir qualifier de manière fiable et reproductible la qualité de chaque service de sécurité.

Spécification

La définition et le contrôle de la qualité des services de sécurité devront s'appuyer sur une base de questionnaires relatifs à chaque service de sécurité et sur un système de pondération associé.

MEHARI comprend des bases de questionnaires et un système de pondération décrits dans le « Guide du diagnostic de l'état des services de sécurité »

7.3.2 Contrôle de la mise en œuvre des services de sécurité

Il est bien clair que la mise en œuvre effective des services définis précédemment devra être contrôlée.

On sera souvent amené à constater des situations dans lesquelles des services de sécurité ont été partiellement déployés et où leur mise en œuvre n'est pas totalement conforme aux décisions prises au préalable.

Du point de vue de la gestion des risques la conduite à tenir dans de tels cas doit être définie.

Spécification

La manière de traiter les cas de déploiements incomplets des services de sécurité, d'en faire le rapport et d'en tenir compte dans le système de gestion des risques doit être précisée

7.3.3 Pilotage global associé à la gestion des risques

Le pilotage global de la gestion directe des risques ressemble à tout pilotage de projet et suppose :

- Des indicateurs et un tableau de bord,
- Un système de compte-rendu,
- Un système de revue périodique et de prise de décision relative aux actions correctives nécessaires.

Les bases de connaissances de Méhari, au format Excel, permettent de définir et de mettre en place de tels indicateurs et des tableaux de bord.

Leur variété et leur adaptation aux tableaux de bord généraux des entreprises et organismes font que leur description sort du cadre du présent document.

Annexe A

Échelles standards de niveaux d'impact et de potentialité

Échelle d'impact

Niveau 4 : Vital

A ce niveau l'impact est extrêmement grave et met en danger l'existence même ou la survie de l'entité ou de l'une de ses activités majeures.

En cas de survie de l'entreprise ou de l'organisme, les séquelles sont importantes et durables.

Niveau 3 : Très Grave

Il s'agit là d'impact très grave au niveau de l'entité, sans que son avenir soit compromis.

En termes financiers, cela peut amputer sérieusement le résultat de l'exercice, sans que les actionnaires se dégagent massivement.

En termes d'image, on considérera souvent à ce niveau une perte d'image dommageable qu'il faudra plusieurs mois à remonter, même si l'impact financier ne peut être évalué avec précision.

Des sinistres conduisant à une désorganisation notable de l'entreprise pendant une durée de plusieurs mois seront aussi souvent évalués à ce niveau.

Niveau 2 : Important

Il s'agit là de sinistres ayant un impact notable au niveau des opérations de l'entité, de ses résultats ou de son image, mais restant globalement supportables.

Niveau 1 : Non significatif

A ce niveau les dommages encourus n'ont pratiquement pas d'impact sur les résultats de l'entité ni sur son image, même si certaines personnes sont fortement impliquées dans le rétablissement de la situation d'origine.

Échelle de potentialité

Niveau 4 : Très probable

A ce niveau, il est raisonnable de penser que le scénario se produira très certainement et vraisemblablement à court terme.

Quand le risque est survenu, personne n'est surpris.

Niveau 3 : Probable

Il s'agit là des scénarios dont il est raisonnable de penser qu'ils pourraient bien se produire, à plus ou moins court terme. L'espoir que le risque ne survienne pas n'est pas insensé mais dénote un certain optimisme.

La survenance du risque déçoit, mais ne surprend pas.

Niveau 2 : Improbable

Il s'agit là de scénarios dont il est raisonnable de penser qu'ils ne surviendront pas. L'expérience passée montre souvent d'ailleurs qu'ils ne sont pas survenus.

Ils demeurent néanmoins « possibles » et ne sont pas complètement invraisemblables

Niveau 1 : Très improbable

A ce niveau l'occurrence du risque est tout à fait improbable. De tels scénarios ne sont pas strictement impossibles car il existe toujours une infime probabilité pour que cela se produise.

Annexe B1

Échelles standards de niveaux des facteurs de réduction de potentialité

Efficacité des mesures dissuasives

Niveau 4 : L'effet dissuasif est très important.

Un acteur rationnel devrait logiquement abandonner toute idée d'action. Il devrait savoir qu'il sera presque certainement démasqué et que les sanctions encourues seront hors de proportion avec le gain espéré.

Niveau 3 : L'effet dissuasif est important.

Un acteur rationnel devrait logiquement penser qu'il encourt un risque important : il devrait savoir qu'il serait sans doute identifié et que les préjudices qu'il aurait à subir seraient graves.

Niveau 2 : L'effet dissuasif est moyen.

L'acteur peut logiquement penser qu'il encourrait un risque faible et qu'en tout état de cause les préjudices personnels qu'il aurait à subir resteraient supportables.

Niveau 1 : L'effet dissuasif est très faible ou nul.

L'acteur peut logiquement penser qu'il n'encourrait aucun risque personnel : il peut penser qu'il ne serait pas identifié ou qu'il aurait de très sérieux arguments pour réfuter toute imputation de l'action ou que les sanctions seraient très faibles.

Efficacité des mesures préventives

Niveau 4 : L'effet préventif est très important.

Seuls quelques experts, dotés de moyens très importants, peuvent aboutir.

Seuls des concours exceptionnels de circonstances exceptionnelles peuvent conduire à ce scénario.

Niveau 3 : L'effet préventif est important.

Seul un spécialiste, un professionnel doté de moyens très importants, ou une collusion entre plusieurs professionnels ayant des domaines différents peuvent aboutir.

Concours de circonstances rares ou circonstances exceptionnelles exigées.

Niveau 2 : L'effet préventif est moyen.

Le scénario peut être mis en œuvre par un professionnel sans autres moyens que ceux dont disposent les personnels de la profession.

Des circonstances naturelles rares peuvent aboutir à ce résultat.

Niveau 1 : L'effet préventif est très faible ou nul.

Toute personne proche ou appartenant à l'entreprise ou tout initié la connaissant un minimum est capable de déclencher un tel scénario, avec des moyens qu'il est facile d'acquérir.

Des circonstances tout à fait courantes (maladresse, erreur, conditions défavorables non exceptionnelles) peuvent être à l'origine d'un tel scénario.

Annexe B2

Échelles standards de niveaux des facteurs de réduction d'impact

Efficacité des mesures de confinement

Niveau 4 : L'effet est très important.

Les conséquences directes seront très limitées dans leur ampleur. L'impact résiduel sera très faible, voire non significatif.

Niveau 3 : L'effet de confinement et de limitation des conséquences directes est important.

Les limites imposées au sinistre en amoindriront notablement les conséquences et si cela dépend d'action humaine, le délai de détection et de réaction sera rapide.

Les mesures prises auront une influence réelle sur l'impact direct, qui restera limité et circonscrit.

Niveau 2 : L'effet de confinement et de limitation des conséquences directes est moyen.

Soit le sinistre peut être faiblement limité dans ses conséquences directes, soit il pourrait l'être à condition d'être détecté mais le délai de détection ou de réaction ne sera pas rapide.

Les mesures prises auront une influence réelle sur l'impact, mais l'ampleur des conséquences directes restera importante.

Niveau 1 : L'effet de confinement et de limitation des conséquences directes est très faible ou nul.

Soit le sinistre ne peut être limité dans ses conséquences directes, soit, s'il peut l'être à condition d'être détecté, il ne sera détecté qu'au bout d'un délai important.

Les mesures prises n'auront qu'une influence très limitée sur le niveau des conséquences directes.

Efficacité des mesures palliatives

Niveau 4 : L'effet de limitation des conséquences indirectes est très important.

Le fonctionnement normal de l'activité est assuré sans discontinuité notable.

Niveau 3 : L'effet de limitation des conséquences indirectes est important.

Les mesures ont été analysées et organisées dans le détail, puis validées. Le délai de reprise du fonctionnement normal de l'activité peut être estimé ou connu avec précision et est tel que cela réduira notablement la gravité des conséquences indirectes du scénario.

Niveau 2 : L'effet de limitation des conséquences indirectes est moyen.

Les solutions de secours ou moyens palliatifs ont été prévus globalement et pour l'essentiel, mais l'organisation de détail n'a pas été faite. Il est raisonnable de penser qu'il résultera de ce manque de préparation un manque d'efficacité très net des mesures prévues. Le délai de reprise du fonctionnement normal de l'activité ne peut être connu avec précision ou ne changera pas fondamentalement le niveau de gravité du sinistre.

Niveau 1 : L'effet de limitation des conséquences indirectes est très faible ou nul.

Les mesures seront totalement improvisées et/ou il est raisonnable de penser que leur effet en sera très faible

Annexe C1

Grilles de décision standards de MEHARI

Grilles d'évaluation de potentialité

Grilles d'élaboration des STATUS-P																			
1. Scénarios de type Accident																			
	EXPO = 1				EXPO = 2				EXPO = 3				EXPO = 4						
D					D					D					D				
I					I					I					I				
S					S					S					S				
S 1	1	1	1	1	S 1	2	2	2	1	S 1	3	3	2	1	S 1	4	4	2	1
	1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4
	P	R	E	V		P	R	E	V		P	R	E	V		P	R	E	V
2. Scénarios de type Erreur																			
	EXPO = 1				EXPO = 2				EXPO = 3				EXPO = 4						
D					D					D					D				
I					I					I					I				
S					S					S					S				
S 1	1	1	1	1	S 1	2	2	2	1	S 1	3	3	2	1	S 1	4	4	2	1
	1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4
	P	R	E	V		P	R	E	V		P	R	E	V		P	R	E	V
3. Scénarios de type action Volontaire																			
	EXPO = 1				EXPO = 2				EXPO = 3				EXPO = 4						
D 4	1	1	1	1	D 4	1	1	1	1	D 4	2	2	1	1	D 4	2	2	2	1
I 3	1	1	1	1	I 3	2	2	1	1	I 3	2	2	1	1	I 3	3	3	2	2
S 2	1	1	1	1	S 2	2	2	2	1	S 2	3	3	2	1	S 2	4	4	3	2
S 1	1	1	1	1	S 1	2	2	2	1	S 1	3	3	2	1	S 1	4	4	3	2
	1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4
	P	R	E	V		P	R	E	V		P	R	E	V		P	R	E	V

Annexe C2

Grilles de décision standards de MEHARI

Grilles d'évaluation d'impact (II étant l'impact intrinsèque)

Grilles d'élaboration des STATUS-I																			
1. Scénarios de type Disponibilité																			
II = 1				II = 2				II = 3				II = 4							
C 4	1	1	1	1	C 4	2	2	1	1	C 4	2	2	1	1	C 4	2	2	2	1
O 3	1	1	1	1	O 3	2	2	1	1	O 3	3	2	2	1	O 3	3	3	2	1
N 2	1	1	1	1	N 2	2	2	2	1	N 2	3	3	2	1	N 2	4	3	2	1
F 1	1	1	1	1	F 1	2	2	2	1	F 1	3	3	2	1	F 1	4	3	2	1
	1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4
	P	A	L	L		P	A	L	L		P	A	L	L		P	A	L	L
2. Scénarios de type Intégrité																			
II = 1				II = 2				II = 3				II = 4							
C 4	1	1	1	1	C 4	1	1	1	1	C 4	1	1	1	1	C 4	1	1	1	1
O 3	1	1	1	1	O 3	2	2	1	1	O 3	2	2	1	1	O 3	2	2	2	1
N 2	1	1	1	1	N 2	2	2	2	1	N 2	3	3	2	1	N 2	3	3	2	1
F 1	1	1	1	1	F 1	2	2	2	1	F 1	3	3	2	1	F 1	4	3	2	1
	1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4
	P	A	L	L		P	A	L	L		P	A	L	L		P	A	L	L
3. Scénarios de type Confidentialité																			
II = 1				II = 2				II = 3				II = 4							
C 4	1				C 4	2				C 4	2				C 4	2			
O 3	1				O 3	2				O 3	2				O 3	2			
N 2	1				N 2	2				N 2	3				N 2	3			
F 1	1				F 1	2				F 1	3				F 1	4			
	1					1					1					1			
	P	A	L	L		P	A	L	L		P	A	L	L		P	A	L	L
4. Scénarios de type Efficience																			
II = 1				II = 2				II = 3				II = 4							
C 4	1	1	1	1	C 4	1	1	1	1	C 4	1	1	1	1	C 4	1	1	1	1
O 3	1	1	1	1	O 3	2	2	1	1	O 3	2	2	1	1	O 3	2	2	2	1
N 2	1	1	1	1	N 2	2	2	2	1	N 2	3	3	2	1	N 2	3	3	2	1
F 1	1	1	1	1	F 1	2	2	2	1	F 1	3	3	2	1	F 1	4	3	2	1
	1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4
	P	A	L	L		P	A	L	L		P	A	L	L		P	A	L	L

Annexe D

Spécification des services de sécurité

A. Définitions

7.3.4 Services de sécurité

Un **service de sécurité** est une réponse à un besoin de sécurité, exprimée en termes génériques et fonctionnels décrivant la finalité du service, généralement en référence à certains types de menaces.

Un service de sécurité décrit une fonction de sécurité.

Cette **fonction** est **indépendante des mécanismes et solutions concrètes** permettant la réalisation effective du service.

Exemple : le service « Contrôle d'accès », dont la finalité ou fonction, décrite implicitement par son titre, est de contrôler les accès, c'est à dire de ne laisser passer que les personnes autorisées.

7.3.5 Services et sous-services de sécurité

La fonction assurée par un service de sécurité peut, elle-même, nécessiter plusieurs éléments complémentaires, qui peuvent être considérés comme des « sous-fonctions ». Dans l'exemple ci-dessus, le contrôle d'accès nécessite la connaissance de ce qui est autorisé, ce qui fait appel à une fonction d'autorisation, la reconnaissance d'une personne, ce qui fait appel à une fonction d'authentification, et le filtrage des accès, ce qui fait appel à une troisième fonction de filtrage.

Un service de sécurité peut ainsi lui-même être constitué de plusieurs autres services de sécurité pour répondre à un besoin ou une finalité déterminée. *Chacun des constituants est un sous-service de sécurité* du service en question, tout en conservant, vis-à-vis d'une fonction qui lui est propre, les caractéristiques d'un service, telles que définies plus haut.

7.3.6 Mécanismes et solutions de sécurité

Un "**Mécanisme**" est une manière particulière d'assurer, totalement ou partiellement, la fonction du service ou du sous-service. Il peut s'agir de procédure spécifique, d'algorithme, de technologie, etc.

Pour le sous-service d'authentification abordé précédemment, les mécanismes possibles (pour l'authentification aux systèmes d'information) sont les mots de passe, les jetons, les processus reposant sur des algorithmes contenus dans des cartes à puce, les systèmes biométriques, etc.

Pour un sous-service donné, plusieurs mécanismes sont généralement possibles. Leur choix a très souvent un effet direct sur la qualité du sous-service concerné.

Une **solution de sécurité** est la réalisation concrète d'un mécanisme de sécurité et comprend les matériels et logiciels nécessaires à son déploiement, les procédures de déploiement et de support opérationnel ainsi que les structures organisationnelles nécessaires.

7.3.7 Typologie des services de sécurité

Certains services peuvent être considérés comme des mesures générales, d'autres comme des services techniques :

- Les mesures générales sont des mesures de sécurité reconnues comme utiles, voire nécessaires, à la sécurité des systèmes d'information, mais dont l'effet se situe davantage au plan

de l'organisation, du pilotage de la sécurité ou de la sensibilisation, sans influence directe sur des situations de risques précises.

- Les mesures techniques ont un rôle précis, une finalité directe et ont un effet immédiat sur certaines situations de risque qu'il est possible de préciser.

7.3.8 Bases de connaissances des services de sécurité

MEHARI comprend plusieurs bases de connaissances, chacune ayant sa propre base de services et de sous-services de sécurité adaptés à la sécurité des systèmes d'information.

Ce sont ces sous-services dont la qualité sera évaluée lors d'un diagnostic.

B. Mesure de la qualité des services de sécurité

Les services de sécurité peuvent avoir des niveaux de performance très différents selon les mécanismes et les processus employés. Il est donc essentiel de pouvoir mesurer la qualité ou la performance d'ensemble d'un service de sécurité.

7.3.9 Paramètres à prendre en compte

Pour mesurer la performance d'un service de sécurité, plusieurs paramètres devront être pris en compte :

- L'efficacité du service,
- Sa robustesse,
- Les moyens de contrôle du maintien dans le temps des caractéristiques précédentes.

7.3.9.1 Efficacité d'un service de sécurité

Pour les services dits techniques, l'efficacité mesure leur capacité à assurer effectivement la fonction demandée face à des acteurs ayant des compétences plus ou moins fortes ou des circonstances plus ou moins courantes.

Pour prendre l'exemple du sous-service "Gestion des autorisations d'accès au système d'information", qui attribue des droits à des utilisateurs, la fonction du service est de faire en sorte que seules les personnes dûment habilitées par leur hiérarchie aient effectivement les droits correspondants. En pratique, l'efficacité du service dépendra de la rigueur du contrôle de l'authenticité de la demande et du contrôle de la position du demandeur vis-à-vis de l'utilisateur. S'il s'agit d'un simple courrier signé sans qu'il y ait dépôt de signature ni compte rendu à la hiérarchie, n'importe quelle personne connaissant un peu le circuit d'autorisation sera capable de se faire attribuer indûment des droits et la qualité du sous-service pourra être considérée comme faible.

L'efficacité d'un service contrôlant des actions humaines est ainsi la mesure des compétences nécessaires pour qu'un acteur puisse passer au travers des contrôles mis en place ou pour les abuser.

Pour les services visant des événements naturels (tels que la détection incendie, l'extinction incendie, etc.), l'efficacité est la mesure de la « force » de l'événement pour lequel ils gardent leur effet.

S'il s'agit, par exemple, d'une digue destinée à empêcher une inondation due à la crue d'une rivière, l'efficacité sera directement liée à la hauteur de la crue (sa force) à laquelle la digue résiste. *En pratique cette force sera souvent évaluée en fonction du caractère plus ou moins exceptionnel de l'événement.*

Les services qui sont des mesures générales ne peuvent pas, par principe, être évalués en fonction de leur finalité directe mais en fonction de leur rôle indirect.

L'efficacité des mesures générales mesure leur capacité à générer des plans d'action ou des changements significatifs de comportement.

7.3.9.2 Robustesse d'un service de sécurité

La robustesse d'un service mesure sa capacité à résister à une action visant à le court-circuiter ou à l'inhiber.

La robustesse ne concerne que les services dits techniques.

Dans l'exemple précédent de gestion des autorisations, la robustesse du sous-service dépend, en particulier, des possibilités d'accès direct à la table des droits attribués aux utilisateurs et donc de se faire attribuer des droits sans passer par les processus normaux de contrôle mis en place.

Dans le cas de services visant des accidents ou des événements naturels (système de détection et d'extinction automatique d'incendie, par exemple), leur robustesse tiendra compte de leur capacité à résister à une mise hors circuit volontaire ou accidentelle.

7.3.9.3 Mise sous contrôle d'un service de sécurité

La qualité globale d'un service de sécurité doit enfin prendre en compte sa permanence dans le temps.

Pour cela, il convient que toute interruption de service ou que tout changement de paramétrage soit détecté et que des mesures palliatives soient alors décidées. La qualité de ce paramètre dépend donc de la capacité et de la rapidité de détection et des moyens de réaction.

Pour les mesures générales, la mise sous contrôle représente d'une part leur aptitude à être mesurées en termes de mise en œuvre ou d'effet, et d'autre part la mise en place effective d'indicateurs et de systèmes de contrôle

C. Évaluation de la qualité des services de sécurité basée sur les questionnaires MEHARI

L'ensemble méthodologique MEHARI comporte, outre la méthode proprement dite, des bases de connaissance. Une de ces bases de connaissance consiste en une base d'audit des services de sécurité, sous la forme de questionnaires et d'un système de pondération des réponses.

Les questionnaires comprennent un **lot de questions auxquelles il est demandé de répondre par oui ou par non**, avec des conventions de notation et de pondération que nous étudierons plus loin.

Les questionnaires comprennent à la fois des questions axées sur l'efficacité des mesures de sécurité (par exemple : fréquence des sauvegardes, type de contrôle d'accès physique : lecteur de carte, digicode, etc., existence d'un système de détection d'incendie, etc.), des questions axées sur la robustesse des mesures de sécurité (par exemple : localisation et protection d'accès au lieu de stockage des sauvegardes, existence d'un sas d'entrée ou solidité de la porte, protection du système de détection incendie, etc.) et, généralement, une ou deux questions sur le contrôle ou l'audit des fonctionnalités attendues du service.

7.3.9.4 Types de questionnaires

Les bases de connaissance de MEHARI comprennent plusieurs questionnaires, spécialisés par domaines techniques correspondant à des interlocuteurs différents.

7.3.9.5 Système de pondération des questions

Les questions à se poser au sujet d'un service de sécurité sont relatives à des mesures de sécurité utiles ou nécessaires au service. Or, ces mesures ne jouent pas toutes le même rôle, et les mesures contributives, les mesures majeures ou suffisantes et les mesures indispensables seront à distinguer.

Le système de pondération utilisé par MEHARI est décrit en détail dans le document : « *Guide du diagnostic de l'état des services de sécurité* »

D. Échelle de niveaux utilisable pour évaluer la qualité des services de sécurité

Les valeurs de référence suivantes sont données à titre indicatif pour la qualité de service.

Qualité de service évaluée à 4

Il s'agit du niveau le plus élevé et le service de sécurité reste efficace et résiste aux agresseurs et événements décrits ci-dessus. Il reste qu'il pourrait être mis en brèche par des circonstances exceptionnelles : meilleurs experts mondiaux dotés d'outils exceptionnels (moyens pouvant être mis en œuvre par des États importants) ou concours exceptionnels de circonstances elles-mêmes exceptionnelles.

Qualité de service évaluée à 3

Le service reste efficace et résiste aux agresseurs et événements décrits ci-dessus, mais pourrait être insuffisant contre des spécialistes (hackers chevronnés et équipés, ingénieurs systèmes fortement spécialisés sur un domaine donné et dotés d'outils spéciaux qu'ils maîtrisent, espions professionnels, agences de renseignement, etc.) ou des événements exceptionnels (catastrophes naturelles). Une mesure organisationnelle de ce niveau aura un effet certain dans la très grande majorité des circonstances, mais peut-être pas dans des circonstances exceptionnelles.

Qualité de service évaluée à 2

Le service reste efficace et résiste à un agresseur moyen, voire initié, mais pourrait être insuffisant contre un bon professionnel du domaine concerné (un informaticien professionnel pour un service de sécurité logique, un cambrioleur normalement équipé ou un "casseur" pour un service de sécurité physique des accès). Dans le domaine des événements naturels, un tel service pourrait être insuffisant pour des événements très sérieux, considérés comme rares. Pour les mesures organisationnelles, un tel service n'apportera une amélioration des comportements que dans des cas courants.

Qualité de service évaluée à 1

Le service a une qualité minimale. Il peut ne pas être efficace (ou ne pas résister) face à une personne quelconque, sans qualification particulière, ou tant soit peu initiée, ou, dans le domaine des événements naturels, ne pas être efficace face à un événement relativement banal. Pour une mesure organisationnelle, elle aura très peu d'effet sur les comportements ou l'efficacité de l'organisation.



Téléchargez les bases de connaissances et la documentation de Méhari

www.meharipedia.org