METHODES

MEHARI 2010

Principes fondamentaux et spécifications fonctionnelles

Janvier 2010

Espace Méthodes

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard, 75009 PARIS
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88 – e-mail : clusif@clusif.asso.fr
Web : http://www.clusif.asso.fr

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Jean-Philippe	Jouas	Responsable de l'Espace Méthodes Responsable du Groupe de Travail Principes, Mécanismes et Bases de connaissances de MEHARI
Jean-Louis	Roule	Responsable du Groupe de Travail Documentation de MEHARI
Dominique	Buc	BUC S.A.
Olivier	Corbier	Docapost
Louise	Doucet	Ministère des Services gouvernementaux du Québec
Martine	Gagné	HydroQuébec
Moïse	Hazzan	Ministère des Services gouvernementaux du Québec
Gérard	Molines	Molines Consultants
Chantale	Pineault	AGRM
Luc	Poulin	CRIM
Pierre	Sasseville	Ministère des Services gouvernementaux du Québec
Claude	Taillon	Ministère de l'Éducation, du Loisir et du Sport du Québec
Marc	Touboul	BULL SA

Sommaire

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.

1. 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 à respecter pour une méthode support et de mettre en évidence les spécifications fonctionnelles qui en découlent.

MEHARI qui a été développé dans cette optique est conforme à ces spécifications et la manière de se conformer à ces spécifications est présentée.

1.1 Objectifs fondamentaux d'une méthode de gestion directe des risques

Les objectifs fondamentaux d'une gestion directe et individuelle des risques auxquels l'entreprise ou l'organisation est exposée, sont :

- 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.

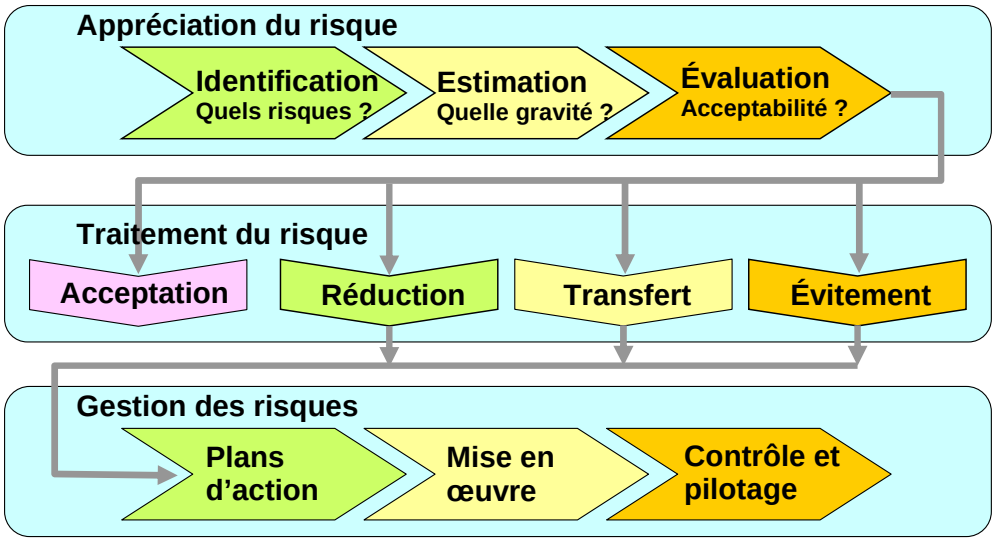
En fonction de ces objectifs, l'ensemble des processus et étapes décrits dans la norme ISO/IEC 27005 doivent être précisés et spécifiés. C'est précisément le but de ce document que de décrire les principes et spécifications fonctionnelles induits par les objectifs fondamentaux cités plus haut et d'expliquer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

1.2 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.



2. 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

3. Termes et définitions

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

3.1 Enjeu de la sécurité

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

3.2 Impact

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

3.3 Impact intrinsèque

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

3.4 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.

3.5 Potentialité

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

3.6 Potentialité intrinsèque

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

3.7 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.

3.8 Service de sécurité

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

3.9 Vulnérabilité intrinsèque

Caractéristique intrinsèque d'un système, d'un objet ou d'un actif constituant un point d'application potentiel de menaces.

3.10 Vulnérabilité contextuelle

Défaut ou faille dans les dispositifs de sécurité pouvant être exploité par une menace pour atteindre un système, un objet ou un actif cible

4. L'appréciation des risques

4.1 Introduction

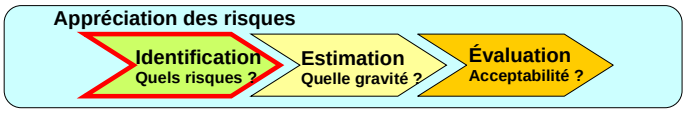
L'appréciation des risques consiste à identifier, aussi exhaustivement que possible, tous les risques auxquels l'entreprise ou l'organisation est exposée, à en estimer individuellement la gravité et à juger du caractère acceptable ou non de chaque risque ainsi évalué.

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.

4.2 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 ?

4.2.1 Les éléments caractéristiques des risques

Les paragraphes ci-dessous définissent et décrivent les éléments qui doivent faire partie de la description des risques et en justifient la nécessité. Ces éléments sont :

- L'actif,
- La vulnérabilité intrinsèque de cet actif mise en cause par le risque,
- Le dommage subi,
- La menace.

4.2.1.1 L'actif

Justification

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 seront 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.

MEHARI est conforme à cette spécification et la typologie d'actifs primaires à partir de laquelle a été créée la base de connaissances de MEHARI 2010 est donnée dans l'annexe A1.

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.

Spécification

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

MEHARI est conforme à cette spécification et la typologie d'actifs secondaires à partir de laquelle a été créée la base de connaissances de MEHARI 2010 est donnée dans l'annexe A2.

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 issus des tableaux d'actifs de MEHARI 2010 donnés en annexes A1 et A2 :

- 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 doit comprendre la description de l'actif concerné et cette description doit préciser le type d'actif primaire ainsi que le type d'actif secondaire.

4.2.1.2 La vulnérabilité intrinsèque et la vulnérabilité contextuelle

Le risque naît du fait que l'actif considéré possède une ou plusieurs vulnérabilités.

Il est cependant nécessaire de préciser le sens donné au mot vulnérabilité. En effet, on peut définir ce qu'est une vulnérabilité de deux manières :

La première est de la définir comme une caractéristique intrinsèque d'un système, d'un objet ou d'un actif constituant un point d'application potentiel de menaces (par exemple : le fait que le support d'un document soit dégradable).

C'est ce que nous appellerons une vulnérabilité intrinsèque.

La deuxième est orientée sur les processus de sécurisation et sur leurs défauts éventuels. On définit alors une vulnérabilité comme un défaut ou une faille dans les dispositifs de sécurité pouvant être exploité par une menace pour atteindre un système, un objet ou un actif cible (par exemple : l'absence de protection contre les intempéries).

C'est ce que nous appellerons une vulnérabilité contextuelle.

L'utilisation de cette deuxième conception des vulnérabilités n'est pas bien adaptée pour l'identification des risques car elle a l'inconvénient majeur de faire dépendre les risques identifiés et gérés des mesures de sécurité, donc de la connaissance de ces mesures, ce qui n'est pas toujours le cas.

Les vulnérabilités intrinsèques des actifs sont, par contre, essentielles pour décrire des risques et doivent être recherchées et identifiées.

Ces vulnérabilités dépendent du type d'actif secondaire. En effet, les vulnérabilités intrinsèques sont essentiellement dues à la forme de l'actif (support matériel, support logiciel, etc.) forme qui est définie par le type d'actif secondaire.

On notera par ailleurs que la vulnérabilité intrinsèque d'un actif peut être décrite comme une possibilité particulière de dommage subi par cet actif. Il revient ainsi au même de décrire le dommage subi ou la vulnérabilité intrinsèque.

La liste des vulnérabilités intrinsèques à partir de laquelle a été créée la base de connaissances de MEHARI 2010 est donnée en annexe B. Cette liste indique, pour chaque type d'actif secondaire, le type de dommage subi et, d'une manière plus littérale mais rigoureusement équivalente, la possibilité de ce dommage.

Il faut noter que pour un risque donné, c'est une seule vulnérabilité intrinsèque qui est concernée.

Spécification fonctionnelle

Chaque risque identifié doit comprendre la description de la vulnérabilité intrinsèque mise en cause.

MEHARI est conforme à cette spécification.

4.2.1.3 Le dommage subi

Le type de conséquence peut être implicitement donné par la vulnérabilité exploitée, 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, il n'y a pas toujours de liste précise de critère à préciser, le dommage subi précisant directement ce point.

Dans un cas comme dans l'autre, le dommage subi doit être précisé.

Spécification fonctionnelle

Chaque risque identifié doit préciser le type de dommage subi.

MEHARI est conforme à cette spécification.

4.2.1.4 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 la vulnérabilité intrinsèque de l'actif est effectivement exploitée. 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 de vulnérabilité)
- 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 :

- Le 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 a été créée la base de connaissances de MEHARI 2010 est donnée en annexe C1

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.

Le tableau donné en annexe C2 met en évidence les catégories d'acteurs à partir desquelles a été créée la base de connaissances de MEHARI 2010.

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 doit comprendre une description détaillée de la menace comprenant :

- **L'événement déclencheur et son caractère volontaire ou accidentel**

- **L'acteur déclenchant cet événement**
- **Les circonstances dans lesquelles survient cet événement**

MEHARI est conforme à cette spécification.

4.2.1.5 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 la base de scénarios de la base de connaissances de MEHARI 2010 comprend une description libre de chaque scénario.

4.2.2 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.

Certes, il est possible de se référer à une liste de risques génériques décrits dans une base de données, telle que celle de MEHARI, mais il est alors nécessaire, pour pouvoir se fier à une telle liste, de savoir sur la base de quels principes 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.

4.2.2.1 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 vulnérabilités intrinsèques attachées 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 seront établies pour chaque type d'élément de risque, ainsi que listé ci-dessus.

MEHARI est conforme à cette spécification.

4.2.2.2 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.

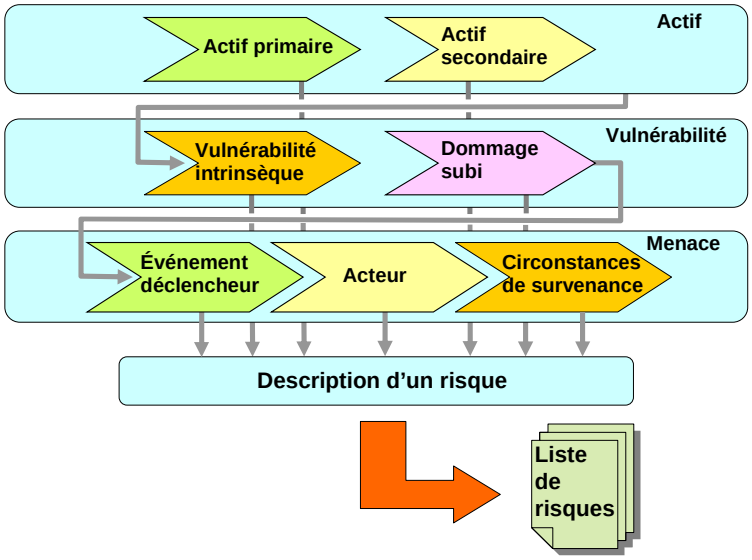
En effet, c'est le plus souvent en se référant à des actifs primaires ou secondaires, que l'on sera à même de mettre en évidence des circonstances particulières de risque telles que des phases de processus, des périodes calendaires ou des périodes de temps, voire des situations géographiques particulières.

Spécification

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

MEHARI est conforme à cette spécification.

Le processus global est représenté ci-dessous.



4.2.2.3 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.

MEHARI inclut ainsi une base de risques types appelés base de « scénarios de risque ».

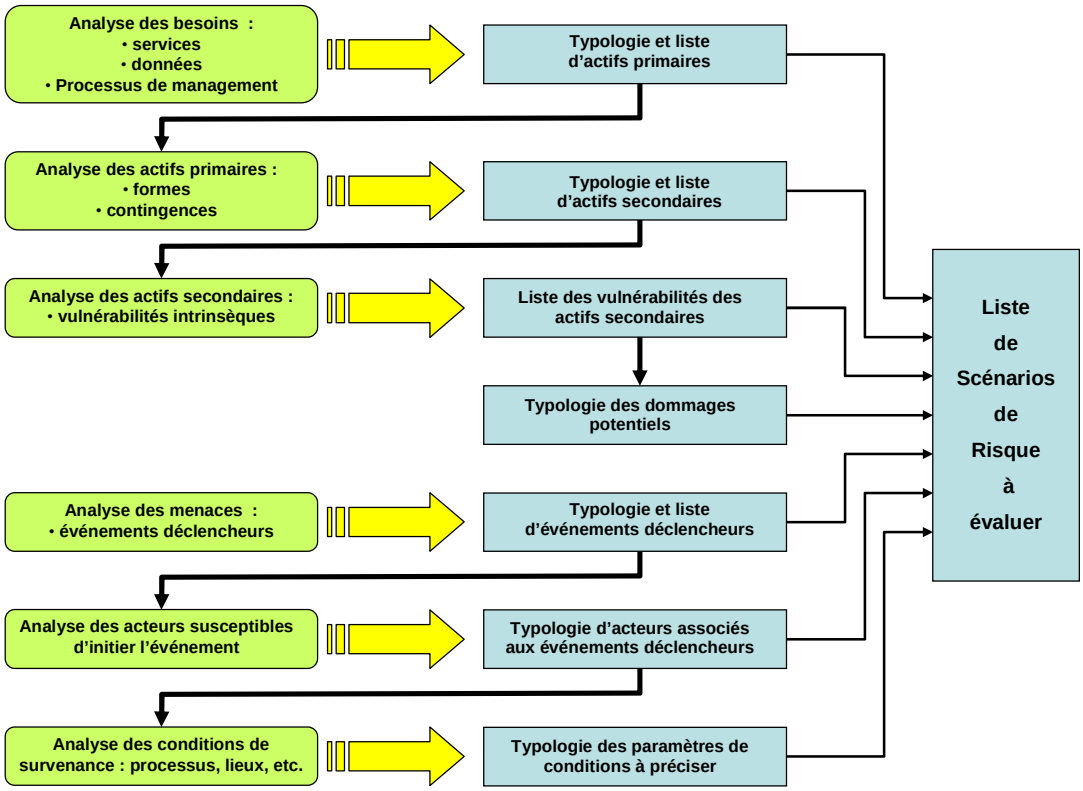
4.2.2.4 Sélection des risques à prendre en compte

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.

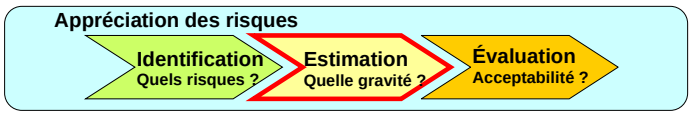
Ceci s'applique particulièrement dans le cas d'utilisation d'une base de risques types telle que celle proposée par MEHARI.

4.2.3 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.



4.3 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 », 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 ?

4.3.1 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.

4.3.1.1 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.

MEHARI est conforme à cette spécification.

4.3.1.2 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.

MEHARI est conforme à cette spécification.

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

4.3.1.3 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.

MEHARI est conforme à cette spécification.

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.

MEHARI est conforme à cette spécification.

4.3.1.4 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.

Il ne s'agit de rien d'autre que d'évaluer le niveau de vulnérabilité contextuelle[1] associée à chaque risque.

4.3.1.5 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 sa base 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 (reportées en annexe G1),
- Un manuel de référence des services de sécurité,
- 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.

Remarque : les questionnaires de diagnostic de la qualité des services de sécurité peuvent également être appelés questionnaires d'audit des vulnérabilités (contextuelles).

4.3.2 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

4.3.2.1 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.

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.

[1] Voir définition de ce terme aux paragraphes 3.9 et 4.2.1.2

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.

MEHARI est conforme à cette spécification et comprend les commentaires souhaités.

Nous donnons en annexe D les définitions correspondant à l'échelle à 4 niveaux proposée comme standard par MEHARI 2010.

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.

MEHARI est conforme à cette spécification et comprend les commentaires souhaités.

Nous donnons en annexe D les définitions correspondant à l'échelle à 4 niveaux proposée comme standard par MEHARI 2010.

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 2010 sont données en annexe E1 et E2.

Spécification

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

MEHARI est conforme à cette spécification.

4.3.2.2 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 des vulnérabilités contextuelles des services de sécurité.

L'utilisation de la base 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 la base.

L'évaluation de l'impact et de la potentialité (résiduels) 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 2010 sont données en annexe F1. 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 2010 sont données en annexe F2. 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.

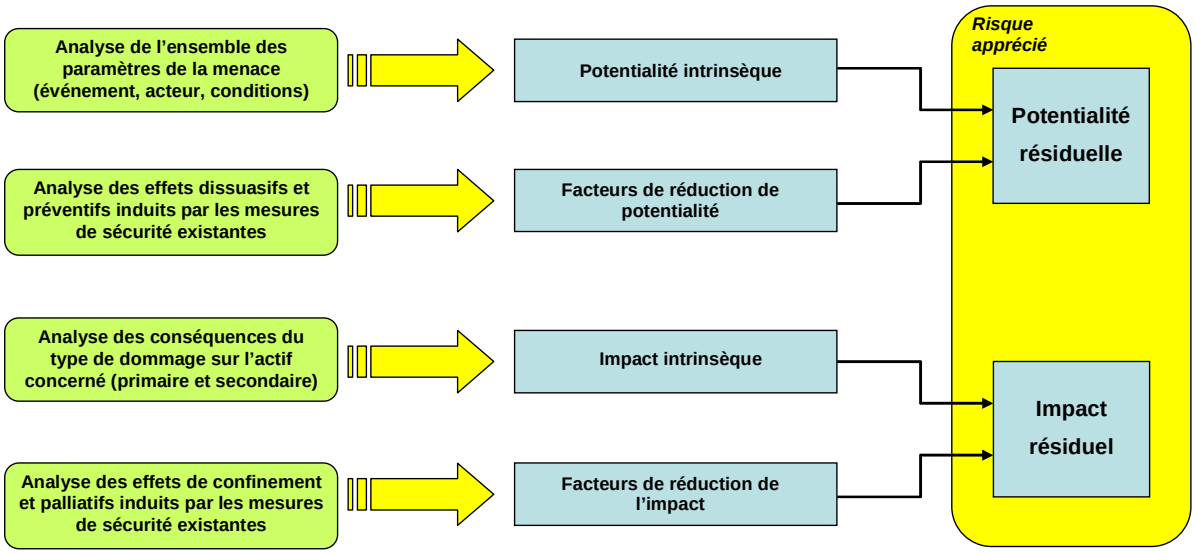
4.3.2.3 L'appréciation globale de chaque risque (géré)

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

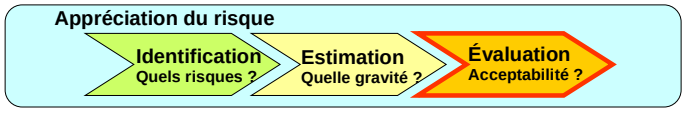
C'est en fonction de ces deux paramètres que les risques seront évalués, selon les processus décrits ci-dessous.

4.3.3 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.



4.4 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.

A titre d'exemple, il est proposé 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 2010 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

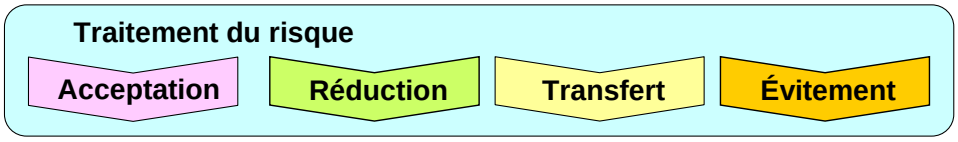
5. Le traitement des risques

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.



5.1 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.

5.2 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 dans l'annexe G1.

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

5.2.1.1 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 qui devrait comprendre au minimum :

- Une liste des services de sécurité,
- La finalité (ou les objectifs) de chaque service,
- Les mécanismes techniques et organisationnels envisageables pour la mise en œuvre du service.

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.

MEHARI est conforme à cette spécification

Nous donnons en annexe G2 la liste de services de sécurité de MEHARI 2010.

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.

5.2.1.2 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 échelles de niveau, comme cela a été fait pour les paramètres du risque.

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 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.

MEHARI est conforme à cette spécification.

L'échelle des niveaux de qualité des services de sécurité de MEHARI 2010 est donnée dans l'annexe G3.

5.2.1.3 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 un 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 est en préparation.

5.2.1.4 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.

5.2.2 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.

5.3 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.

5.4 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.

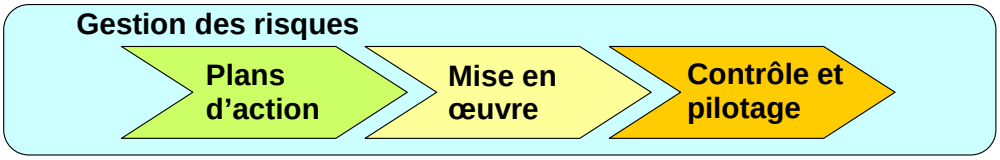
Ceci étant la caractérisation fine des scénarios, ainsi que nous l'avons spécifié, suffit à permettre cet évitement du risque.

6. 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.



6.1 L'élaboration des plans d'action

A 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 plans d'action concrets
- le choix des mesures structurelles éventuelles et des mesures d'évitement des risques
- la validation des décisions précédentes.

6.1.1 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 2010 propose un algorithme d'optimisation pour le choix des mesures à engager prioritairement.

6.1.2 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 que le 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 dépend fortement du degré de précision avec lequel ont été définis les services de sécurité.

Ces définitions devraient être l'objet d'un manuel de référence des services de sécurité

Le manuel de référence des services de sécurité

Un manuel de référence des services de sécurité doit indiquer, pour chaque service de sécurité :

- **l'objectif** du service,
- les **résultats attendus** de la mise en œuvre du service,
- la description des **mécanismes** associés à chaque service, en y incluant aussi bien les aspects techniques qu'organisationnels
- les éléments permettant d'évaluer la **qualité de** chaque service selon les trois critères d'analyse que sont son efficacité, sa robustesse et sa mise sous contrôle.

Justification

Le manuel de référence des services de sécurité est le garant de la cohérence et de la concordance entre les fonctionnalités attendues par les gestionnaires des risques et sur lesquelles ils se sont basés pour estimer les facteurs de réduction de risques objectifs, d'une part, et celles qui seront effectivement déployées, d'autre part.

Spécification

Le choix des mécanismes à déployer pour mettre en œuvre les services de sécurité sélectionnés et spécifiés par les gestionnaires de risques sera fait en s'appuyant sur un manuel de référence des services de sécurité, tel que défini ci-dessus.

MEHARI est conforme à cette spécification et comprend un manuel de référence des services de sécurité qui fait partie de la documentation de la méthode.

6.1.3 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.

6.1.4 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.

6.2 Mise en œuvre des plans d'action

La mise en œuvre des plans d'action 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

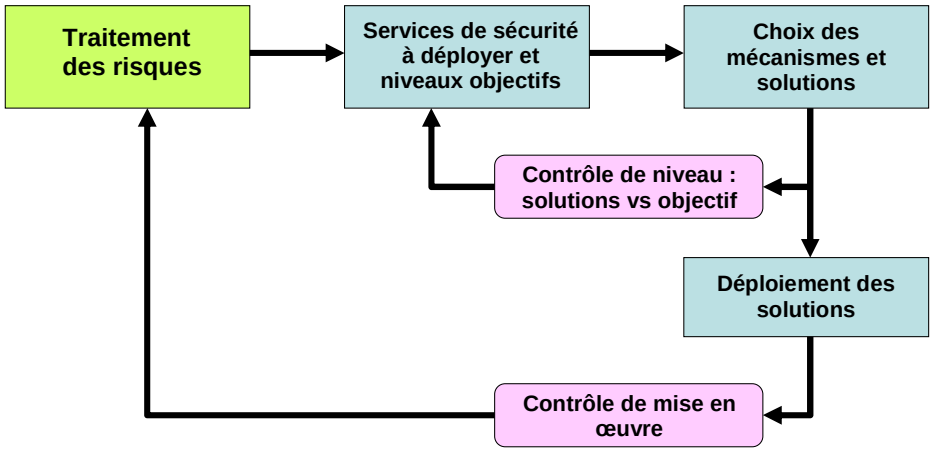
Spécification

Les risques adressés par les plans d'action seront référencés dans les plans d'action afin de pouvoir réagir au mieux en cas de difficulté.

A part cette précaution, il n'y a pas d'exigence particulière sur la méthode de gestion de risques due à la mise en œuvre des plans d'action.

6.3 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.

6.3.1 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 trois aspects que sont leur efficacité, leur robustesse et leur mise sous contrôle.

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 reproductive 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 2010 comprend une base de questionnaires et un système de pondération décrit dans le « Guide du diagnostic de l'état des services de sécurité »

6.3.2 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 reporting et d'en tenir compte dans le système de gestion des risques doit être précisée

6.3.3 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 reporting,
- Un système de revue périodique et de prise de décision relative aux actions correctives nécessaires.

Annexe A1
Typologie d'actifs primaires de la base de connaissances de MEHARI 2010

Catégorie d'actifs : Services
Services du réseau étendu
Services du réseau local
Services applicatifs
Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)
Services systèmes communs : messagerie, archivage, impression, édition, etc.
Services d'interface et terminaux mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)
Services de publication d'informations sur un site web interne ou public
Services généraux de l'environnement de travail du personnel (bureaux, énergie, climatisation, etc.)
Services de télécommunication (voix, télécopies, visioconférence, etc.)

Catégorie d'actifs : Données
Fichiers de données ou bases de données applicatives
Fichiers bureautiques partagés
Fichiers bureautiques personnels (gérés dans un environnement personnel)
Informations écrites ou imprimées détenues par les utilisateurs, archives personnelles
Listings ou états imprimés des applications informatiques
Données échangées, écrans applicatifs, données individuellement sensibles
Courrier électronique
Courrier postal et télécopies
Archives patrimoniales ou documentaires
Archives informatiques
Données et informations publiées sur un site web ou interne

Catégorie d'actifs : Processus de management
Conformité à la loi ou aux réglementations relatives à la protection des renseignements personnels
Conformité à la loi ou aux réglementations relatives à la communication financière
Conformité à la loi ou aux réglementations relatives à la vérification de la comptabilité informatisée
Conformité à la loi ou aux réglementations relatives à la propriété intellectuelle
Conformité à la loi relative à la protection des systèmes informatisés
Conformité aux réglementations relatives à la sécurité des personnes et à la protection de l'environnement

Annexe A2
Typologie d'actifs secondaires de la base de connaissances de MEHARI 2010

Le tableau suivant donne la liste de types d'actifs secondaires de la base de connaissances de MEHARI 2010, par catégorie d'actif primaire.

TYPES D'ACTIFS SECONDAIRES
Catégorie d'actifs : Services
Équipements matériels supports du service
Configurations logicielles
Media support de logiciel
Comptes et moyens nécessaires à l'accès au service
Services de sécurité associés au service
Moyens de servitude nécessaires au service
Locaux
Personnels et prestataires nécessaires pour le service (internes et externes)

Catégorie d'actifs : Données
Entités logiques : Fichiers ou bases de données
Entités logiques : Messages ou paquets de données en transit
Entités physiques : media et supports
Moyens d'accès aux données : clés et moyens divers, physiques ou logiques, nécessaires pour accéder aux données

Catégorie d'actifs : Processus de management
Procédures et directives internes (dispositifs organisationnels)
Moyens matériels nécessaires aux processus de management
Personnel et prestataires nécessaires aux processus de management

Annexe B
Typologie de vulnérabilités intrinsèques de la base de connaissances de MEHARI 2010

Tableau des vulnérabilités				
	Type d'actif secondaire	*Type de dommage subi*	*Type de vulnérabilité*	*Critère DICE*
Catégorie : Service				
	Equipement matériel	Destruction	Possibilité de destruction d'un équipement	D
		Non fonctionnement	Possibilité de non fonctionnement d'un équipement	D
		Non maintien en opération	Possibilité de non maintien en opération d'un équipement	D
	Configuration logicielle	Altération	Possibilité d'altération des configurations logicielles (logiciels et paramétrages)	D et I
		Non fonctionnement	Possibilité de non fonctionnement intrinsèque d'un logiciel (bug)	D
		Effacement	Possibilité d'effacement de configurations logicielles	D
		Défaut d'autorisation	Possibilité de blocage par défaut d'autorisation (défaut de licence)	I
		Pollution	Possibilité de pollution des configurations logicielles	I
		Divulgation de logiciel	Possibilité de diffusion de fichier de logiciel	D
	Media support de logiciel	Destruction	Possibilité de destruction de media support de logiciel	D
		Inexploitabilité	Possible inexploitabilité de media support de logiciel	D
		Disparition	Possibilité de disparition de media support de logiciel	D
		Echange	Possibilité de disparition de media support de logiciel	I
	Compte ou moyen d'accès au service	Blocage	Possibilité de blocage des comptes utilisateurs	D
		Disparition	Possibilité de perte des moyens nécessaires à la connexion au service	D
	Moyens de servitude	Indisponibilité	Possibilité d'indisponibilité de moyens de servitude nécessaires	I
	Locaux	Indisponibilité	Possibilité d'inaccessibilité des locaux	D
Catégorie : données				
	Fichier support de données	Effacement	Possibilité d'effacement du fichier support de données	D
		Pollution	Possibilité de pollution (lente) des données du fichier	D
		Altération	Possibilité d'altération du fichier support de données	I
		Divulgation	Possibilité de duplication ou diffusion (et divulgation) de fichier support de données	C
	Media support de données	Destruction	Possibilité de destruction de media support de données	D
		Inexploitabilité	Possible inexploitabilité de media support de données	D
		Disparition	Possibilité de disparition de media support de données	D et C
		Duplication	Possibilité de duplication (et divulgation) de media support de données	D et C
		Echange	Possibilité d'échange de media support de données	D et C
	Données en transit, messages, écrans	Perte	Possibilité de perte de données en transit ou messages	D et C
		Divulgation	Possibilité de duplication (et divulgation) de données en transit, messages, écrans	C
		Altération	Possibilité d'altération de données en transit ou messages	I
	Moyen d'accès aux données	Disparition	Possibilité de disparition d'un moyen nécessaire pour l'accès aux données (clés logiques ou physiques)	D
Catégorie : processus de management				
	Procédures et directives	Inefficience	Possibilité que les procédures appliquées soient inefficientes (vis-à-vis des obligations légales, réglementaires ou contractuelles)	E

Annexe C1
Typologie d'événements de la base MEHARI 2010

Tableau des événements		
Type	***Code type***	***Événement***
Absence accidentelle de personnel	AB.P	Absence de personnel de partenaire
		Absence de personnel interne
Absence ou indisponibilité accidentelle de service	AB.S	Absence de service : Énergie
		Absence de service : Climatisation
		Absence de service : Impossibilité d'accès aux locaux
		Absence de maintenance applicative ou maintenance applicative impossible
		Absence de maintenance système ou maintenance système impossible
Accident grave d'environnement	AC.E	Foudroiement
		Incendie
		Inondation
Accident matériel	AC.M	Panne d'équipement
		Panne d'équipement de servitude
Absence volontaire de personnel	AV.P	Conflit social avec grève
Erreur de conception	ER.L	Bug bloquant dû à une erreur de conception ou d'écriture de programme (interne)
Erreur matérielle ou de comportement du personnel	ER.P	Perte ou oubli de document ou de media
		Erreur de manipulation ou dans le suivi d'une procédure
		Erreur de saisie ou de frappe
Incident dû à l'environnement	IC.E	Dégât dû au vieillissement
		Dégât des eaux
		Surcharge électrique
		Dégât dû à la pollution
Incident logique ou fonctionnel	IF.L	Incident d'exploitation
		Bug bloquant dans un logiciel système ou un progiciel
		Saturation bloquante pour cause externe (ver)
		Virus
Malveillance menée par voie logique ou fonctionnelle	MA.L	Attaque en blocage de comptes
		Effacement volontaire ou polllution massive de configurations systèmes
		Effacement volontaire direct de supports logiques ou physiques
		Captation électromagnétique
		Falsification logique (données ou fonctions)
		Création de faux (messages ou données)
		Rejeu de transaction
		Saturation malveillante d'équipements informatiques ou réseaux
		Destruction logique totale (fichiers et leurs sauvegardes)
		Détournement logique de fichiers ou données (téléchargement ou copie)
Malveillance menée par voie physique	MA.P	Manipulation ou falsification matérielle d'équipement
		Terrorisme
		Vandalisme
		Vol physique
Procédures non conformes	PR.N	Procédures inadéquates
		Procédures inappliquées par manque de moyens
		Procédures inappliquées par méconnaissance
		Procédures inappliquées volontairement

Annexe C2
Typologie d'acteurs de la base de connaissances de MEHARI 2010

Tableau des acteurs

Catégorie	***Typologie***
Membre du personnel, utilisateur du système d'information	Utilisateur autorisé légitimement
	Utilisateur autorisé illégitimement
Personnel disposant d'un statut particulier	Membre du personnel d'exploitation
	Membre du personnel de développement
	Membre du personnel de maintenance
	Membre du personnel de service (entretien, services généraux, sécurité, etc.)
Personnel autorisé dans l'établissement	Personnel (permanent ou non)
	Visiteur
Personnel non autorisé dans l'établissement	Tiers non autorisé
	Vandale ou terroriste

Annexe D
Échelles standards de niveaux d'impact et de potentialité de MEHARI 2010

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 E1
Échelles standards de niveaux des facteurs de réduction de potentialité de MEHARI 2010

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 E2
Échelles standards de niveaux des facteurs de réduction d'impact de MEHARI 2010

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.

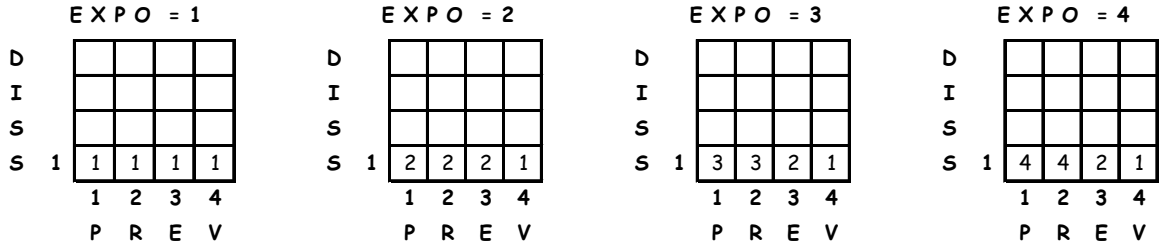
Niveau 1 : L'effet de limitation des conséquences indirectes est très faible ou nul.

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

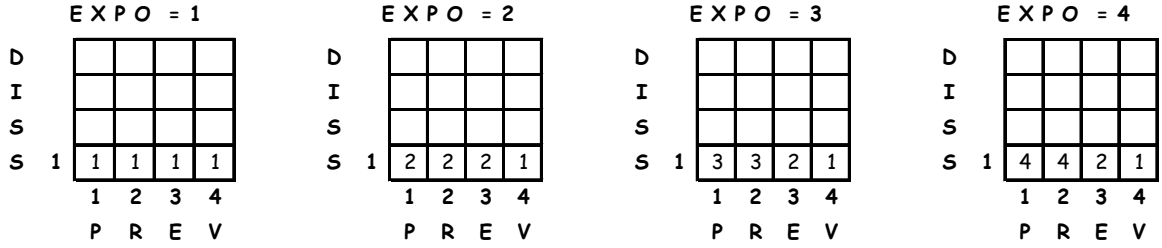
Annexe F1
Grilles de décision standards de MEHARI 2010

Grilles d'évaluation de potentialité

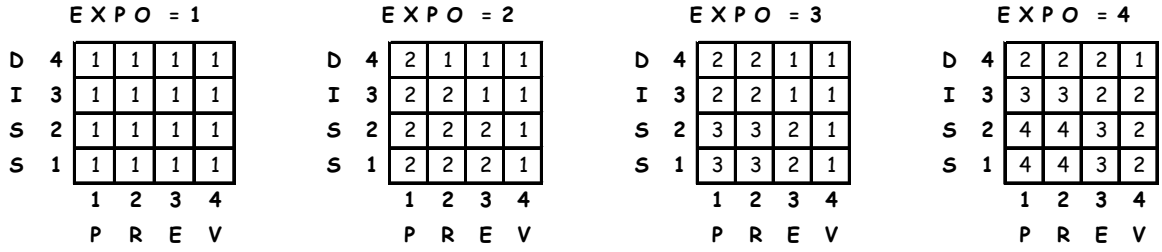
1. Scénarios de type Accident



2. Scénarios de type Erreur



3. Scénarios de type action Volontaire



Annexe F2
Grilles de décision standards de MEHARI 2010

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

Les scénarios non confinables sont évalués sur la ligne nc

1. Scénarios de type Disponibilité

II = 1

C	P	A	L	L
4	1	1	1	1
3	1	1	1	1
2	1	1	1	1
1	1	1	1	1
nc	1	1	1	1

II = 2

C	P	A	L	L
4	2	2	1	1
3	2	2	1	1
2	2	2	2	1
1	2	2	2	1
nc	2	2	2	1

II = 3

C	P	A	L	L
4	2	2	1	1
3	3	2	2	1
2	3	3	2	1
1	3	3	2	1
nc	3	3	2	1

II = 4

C	P	A	L	L
4	2	2	2	1
3	3	3	2	1
2	4	3	2	1
1	4	3	2	1
nc	4	3	2	1

2. Scénarios de type Intégrité

II = 1

C	P	A	L	L
4	1	1	1	1
3	1	1	1	1
2	1	1	1	1
1	1	1	1	1
nc	1	1	1	1

II = 2

C	P	A	L	L
4	1	1	1	1
3	2	2	1	1
2	2	2	2	1
1	2	2	2	1
nc	2	2	2	2

II = 3

C	P	A	L	L
4	1	1	1	1
3	2	2	1	1
2	3	3	2	1
1	3	3	2	1
nc	3	3	2	2

II = 4

C	P	A	L	L
4	1	1	1	1
3	2	2	2	1
2	3	3	2	1
1	4	3	2	1
nc	4	4	4	4

3. Scénarios de type Confidentialité

II = 1

C	P
4	1
3	1
2	1
1	1
nc	1

II = 2

C	P
4	2
3	2
2	2
1	2
nc	2

II = 3

C	P
4	2
3	2
2	3
1	3
nc	3

II = 4

C	P
4	2
3	2
2	3
1	4
nc	4

4. Scénarios de type Limitable

II = 1

C	P
4	1
3	1
2	1
1	1

II = 2

C	P
4	1
3	2
2	2
1	2

II = 3

C	P
4	1
3	2
2	3
1	3

II = 4

C	P
4	1
3	2
2	3
1	4

Annexe G1
Spécification des services de sécurité

1. Définitions

1.1 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.

1.2 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.

1.3 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.

1.4 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.

1.5 Base de connaissance des services de sécurité

MEHARI comprend une base de connaissance de services et 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.

2. 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.

2.1 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.

2.1.1 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.

2.1.2 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.

2.1.3 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

2.2 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 cotation 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.

2.2.1 Types de questionnaires

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

2.2.2 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.

2.2.2.1 Mesures contributives

Certaines questions ont trait à des mesures qui ont un certain rôle, au sens où elles contribuent à la qualité de service sans, pour autant, que leur mise en œuvre soit indispensable.

En termes quantitatifs, une pondération classique de ces mesures reflète bien cette notion de contribution. Dans ce cas, certaines mesures, plus importantes que d'autres, ont des poids différents. La base de connaissance MEHARI indique les poids attribués à chaque question.

Le tableau ci-dessous est un extrait de la base MEHARI, dans lequel une colonne est réservée pour la réponse aux questions (1 pour Oui et 0 pour Non), avant la colonne indiquant le poids de chaque question.

Questionnaire d'audit : Domaine des Systèmes (07)			
Service : A. Contrôle d'accès aux systèmes et applications **Sous-service : A02. Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)**			
N° Question	**Libellé de la question**	**Rép.**	**Poids**
07A02-01	La procédure d'attribution des autorisations d'accès nécessite-t-elle l'accord formel de la hiérarchie (à un niveau suffisant) ?	0	4
07A02-02	Les autorisations sont-elles attribuées nominativement en fonction du seul profil des utilisateurs ?	1	2
07A02-03	Le processus d'attribution (ou modification ou retrait) effectif d'autorisations à un individu (directement ou par le biais de profils) est-il strictement contrôlé ? *Un contrôle strict requiert une identification formelle du demandeur (reconnaissance de sa signature, signature électronique, etc.), que la matérialisation des profils attribués aux utilisateurs (par exemple sous forme de tables) soit strictement sécurisée lors de leur transmission et de leur stockage et qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que ces modifications soient journalisées et auditées.*	1	4
07A02-04	Y a-t-il un processus de remise à jour systématique de la table des autorisations d'accès lors de départs de personnel interne ou externe à l'entreprise ou de changements de fonctions ?	0	2
07A02-05	Y a-t-il un processus strictement contrôlé (voir ci-dessus) permettant de déléguer ses propres autorisations, en tout ou en partie, à une personne de son choix, pour une période déterminée (en cas d'absence) ? *Dans ce cas les autorisations déléguées ne doivent plus être autorisées à la personne qui les a déléguées. Cette dernière doit cependant avoir la possibilité de les reprendre, en annulant ou en suspendant la délégation.*	0	4
07A02-06	Peut-on contrôler à tout moment, pour tous les utilisateurs, les habilitations, autorisations et privilèges en cours ?	1	1
07A02-07	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des profils ou des autorisations attribués aux utilisateurs et des procédures de gestion des profils attribués ?	0	1

La moyenne pondérée est alors un simple cumul des poids des mesures actives (pour lesquelles il a été répondu affirmativement), ramené à la somme des poids possibles et normé sur l'échelle 0 à 4.

Soit en notant R_i la réponse à la question i, P_i le poids de la question i et Mp la moyenne pondérée :

$Mp = 4 \times \Sigma R_i.P_i / \Sigma P_i$

Dans l'exemple de réponses donné dans le tableau ci-dessus la moyenne pondérée serait ainsi :

$Mp = 4 \times 7/18 = 1,6$

et la qualité de service $Q = Mp = 1,6$

2.2.2.2 Mesures majeures ou « suffisantes »

D'autres mesures peuvent être jugées suffisantes pour atteindre un certain niveau de qualité. Ainsi, l'existence d'un système de détection incendie peut être considérée comme suffisante pour atteindre le niveau 2 pour le sous-service correspondant.

Il a donc été introduit un seuil minimum, qui est le minimum atteint, pour la qualité de service, si une mesure est active.

La colonne "Seuil min" indique que s'il est répondu oui à une question pour laquelle un seuil min a été fixé, alors le sous-service atteint au moins ce palier.

Un deuxième extrait de la base, avec la colonne Min est présenté ci-dessous :

Questionnaire d'audit : Domaine des Systèmes (07)				
Service : A. Contrôle d'accès aux systèmes et applications **Sous-service : A02. Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)**				
N° Quest.	**Libellé de la question**	**R**	**P**	**Min**
07A02-01	La procédure d'attribution des autorisations d'accès nécessite-t-elle l'accord formel de la hiérarchie (à un niveau suffisant) ?	0	4	
07A02-02	Les autorisations sont-elles attribuées nominativement en fonction du seul profil des utilisateurs ?	1	2	
07A02-03	Le processus d'attribution (ou modification ou retrait) effectif d'autorisations à un individu (directement ou par le biais de profils) est-il strictement contrôlé ? …	1	4	3
07A02-04	Y a-t-il un processus de remise à jour systématique de la table des autorisations d'accès lors de départs de personnel interne ou externe à l'entreprise ou de changements de fonctions ?	0	2	
07A02-05	Y a-t-il un processus strictement contrôlé (voir ci-dessus) permettant de déléguer ses propres autorisations, en tout ou en partie, à une personne de son choix, pour une période déterminée (en cas d'absence) ? …	0	4	
07A02-06	Peut-on contrôler à tout moment, pour tous les utilisateurs, les habilitations, autorisations et privilèges en cours ?	1	1	
07A02-07	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des profils ou des autorisations attribués aux utilisateurs et des procédures de gestion des profils attribués ?	0	1	

Dans l'exemple donné, le fait que le processus d'attribution, modification ou retrait de droits (question 3) soit strictement contrôlé a été jugé suffisant pour augmenter la cotation de la qualité du service au palier minimum de 3.

2.2.2.3 Mesures indispensables

Par contre, d'autres mesures peuvent être jugées indispensables pour atteindre un certain degré de qualité de service.

A ces mesures indispensables pour obtenir un certain niveau de qualité, et donc aux questions correspondantes, MEHARI associe donc un seuil de qualité pour aller au-delà duquel la mesure est indispensable.

En d'autres termes, le seuil indiqué dans la colonne "Max" est la limite maximum de niveau de qualité que peut atteindre le sous-service si la mesure n'est pas mise en œuvre.

En cas de conflit entre un seuil min et un seuil max, le seuil max prévaut.

Le tableau précédent devient alors le tableau final suivant :

Questionnaire d'audit : Domaine des Systèmes (07)					
Service : A. Contrôle d'accès aux systèmes et applications **Sous-service : A02. Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)**					
N° Quest.	**Libellé de la question**	**R**	**P**	**Max**	**Min**
07A02-01	La procédure d'attribution des autorisations d'accès nécessite-t-elle l'accord formel de la hiérarchie (à un niveau suffisant) ?	0	4	2	
07A02-02	Les autorisations sont-elles attribuées nominativement en fonction du seul profil des utilisateurs ?	1	2		
07A02-03	Le processus d'attribution (ou modification ou retrait) effectif d'autorisations à un individu (directement ou par le biais de profils) est-il strictement contrôlé ? …	1	4	2	3
07A02-04	Y a-t-il un processus de remise à jour systématique de la table des autorisations d'accès lors de départs de personnel interne ou externe à l'entreprise ou de changements de fonctions ?	0	2		
07A02-05	Y a-t-il un processus strictement contrôlé (voir ci-dessus) permettant de déléguer ses propres autorisations, en tout ou en partie, à une personne de son choix, pour une période déterminée (en cas d'absence) ? …	0	4		
07A02-06	Peut-on contrôler à tout moment, pour tous les utilisateurs, les habilitations, autorisations et privilèges en cours ?	1	1		
07A02-07	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des profils ou des autorisations attribués aux utilisateurs et des procédures de gestion des profils attribués ?	0	1	2	

Dans l'exemple ci-dessus, l'opinion d'experts est que les réponses négatives aux questions 1 et 7 font que le niveau de qualité de service ne peut excéder le niveau 2. Cette limitation prévaut sur le niveau 3 évalué précédemment.

Ce triple système de mesure de la qualité de service évite le risque de voir une série de mesures faiblement efficaces surévaluer un niveau de qualité si les mesures essentielles ne sont pas actives ou, au contraire, une série de mesures de poids faible sous-évaluer la qualité de service, alors qu'une mesure essentielle est effectivement en place. Cette approche est une valeur distinctive de MEHARI et s'appuie sur l'expertise des personnes qui tiennent à jour les bases de connaissance.

6.3.3.1.1 Questions sans objet

Certaines questions peuvent être « sans objet » pour certaines unités. Dans ce cas, il suffit d'indiquer « SO » dans la réponse pour que la question ne soit pas prise en compte.

Il conviendra de faire très attention cependant à ce qu'une question sans objet doit le rester quelles que soient les évolutions prévisibles du système d'information et des services de sécurité.

Annexe G2
Liste des services de sécurité de la base de connaissances de MEHARI 2010

SERVICES ET SOUS-SERVICES DE SECURITE

DOMAINES / SERVICES / SOUS-SERVICES	
01 Organisation de la sécurité (01 Org)	
A - Rôles et structures de la sécurité	
01A01	Organisation du management et du pilotage de la sécurité générale
01A02	Organisation du management et du pilotage de la sécurité des systèmes d'information
01A03	Système général de reporting et de suivi des incidents
01A04	Organisation des audits et du plan d'audit
01A05	Gestion de crise liée à la sécurité de l'information
B - Référentiel de sécurité	
01B01	Devoirs et responsabilités du personnel et du management
01B02	Directives générales relatives à la protection de l'information
01B03	Classification les ressources
01B04	Gestion des actifs
01B05	Protection des actifs ayant valeur de preuve
C - Gestion des ressources humaines	
01C01	Engagement du personnel - clauses contractuelles
01C02	Gestion du personnel et des partenaires ou prestataires stratégiques
01C03	Procédure d'habilitation du personnel
01C04	Sensibilisation et formation à la sécurité
01C05	Gestion des tierces parties
01C06	Enregistrement des personnes
D - Assurances	
01D01	Assurance des dommages matériels
01D02	Assurance des dommages immatériels
01D03	Assurance RC
01D04	Assurance Perte de Personnages clés
01D05	Gestion des contrats d'assurance
E - Continuité de l'activité	
01E01	Prise en compte des besoins de continuité de l'activité
01E02	Plans de continuité de l'activité
01E03	Plans de Reprise de l'Environnement de Travail
02 Sécurité des sites (02 Sit)	
A - Contrôle d'accès physique au site et aux bâtiments	
02A01	Gestion des droits d'accès au site ou à l'immeuble
02A02	Gestion des autorisations d'accès au site ou à l'immeuble
02A03	Contrôle d'accès au site ou à l'immeuble
02A04	Détection des intrusions sur le site ou dans l'immeuble
02A05	Accès aux zones de déchargement ou chargement
B - Protection contre les risques environnementaux divers	
02B01	Analyse des risques environnementaux divers
C - Contrôle des accès aux zones de bureaux	
02C01	Partitionnement des zones de bureaux en zones protégées
02C02	Contrôle d'accès physique aux zones de bureaux protégées
02C03	Gestion des autorisations d'accès aux zones de bureaux protégées
02C04	Détection des intrusions dans les zones de bureaux protégées
02C05	Surveillance des zones de bureaux protégées
02C06	Contrôle de la circulation des visiteurs et des prestataires occasionnels amenés à intervenir dans les bureaux

D - Protection de l'information écrite

02D01	Conservation et protection des documents courants importants
02D02	Protection des documents et supports amovibles
02D03	Ramassage des corbeilles à papier et destruction des documents
02D04	Sécurité du courrier
02D05	Sécurité des télécopies
02D06	Conservation et protection des pièces originales et éléments de preuve
02D07	Gestion des archives documentaires

03 Sécurité des locaux (03 Loc)

A - Services techniques

03A01	Qualité de la fourniture de l'énergie
03A02	Continuité de la fourniture de l'énergie
03A03	Sécurité de la climatisation
03A04	Qualité du câblage
03A05	Protection contre la foudre
03A06	Sécurité des équipements de servitude

B - Contrôle d'accès aux locaux sensibles

03B01	Gestion des droits d'accès aux locaux sensibles
03B02	Gestion des autorisations d'accès aux locaux sensibles
03B03	Contrôle des accès aux locaux sensibles
03B04	Détection des intrusions dans les locaux sensibles
03B05	Surveillance périmétrique (surveillance des issues et des abords immédiats des locaux sensibles)
03B06	Surveillance des locaux sensibles
03B07	Contrôle d'accès au câblage
03B08	Localisation des locaux sensibles

C - Sécurité contre les dégâts des eaux

03C01	Prévention des risques de dégâts des eaux
03C02	Détection des dégâts des eaux
03C03	Évacuation de l'eau

D - Sécurité incendie

03D01	Prévention des risques d'incendie
03D02	Détection d'incendie
03D03	Extinction d'incendie

04 Réseau étendu intersites (04 Wan)

A - Sécurité de l'architecture réseau et continuité du service

04A01	Sûreté de fonctionnement des éléments d'architecture du réseau étendu
04A02	Organisation de la maintenance des équipements du réseau étendu
04A03	Procédures et plans de reprise du réseau étendu sur incidents
04A04	Plan de sauvegarde des configurations du réseau étendu
04A05	Plan de Reprise d'Activité (PRA) du réseau étendu
04A06	Gestion des fournisseurs critiques vis-à-vis de la permanence de la maintenance

B - Contrôle des connexions sur le réseau étendu

04B01	Profils de sécurité des entités connectées au réseau étendu
04B02	Authentification de l'entité accédante lors des accès entrants depuis le réseau étendu
04B03	Authentification de l'entité accédée lors des accès sortants vers d'autres entités par le réseau étendu

C - Sécurité des données lors des échanges et des communications

04C01	Chiffrement des échanges sur le réseau étendu
04C02	Contrôle de l'intégrité des échanges sur le réseau étendu

D - Contrôle, détection et traitement des incidents sur le réseau étendu

04D01	Surveillance (en temps réel) du réseau étendu
04D02	Analyse (en temps différé) des traces, logs et journaux d'événements sur le réseau étendu
04D03	Traitement des incidents du réseau étendu

05 Réseau local (05 Lan)

A - Sécurité de l'architecture du réseau local

05A01	Partitionnement du réseau local en domaines de sécurité
05A02	Sûreté de fonctionnement des éléments d'architecture du réseau local
05A03	Organisation de la maintenance des équipements du réseau local
05A04	Procédures et plans de reprise du réseau local sur incidents
05A05	Plan de sauvegarde des configurations du réseau local
05A06	Plan de Reprise d'Activité (PRA) du réseau local
05A07	Gestion des fournisseurs critiques vis-à-vis de la permanence de la maintenance

B - Contrôles d'accès sur le réseau local de "données"

05B01	Gestion des profils d'accès au réseau local de données
05B02	Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)
05B03	Authentification de l'accédant lors des accès au réseau local depuis un point d'accès interne Ce mécanisme correspond à l'authentification réalisée sous Windows par un contrôleur de domaine
05B04	Authentification de l'accédant lors des accès au réseau local depuis un site distant via le réseau étendu
05B05	Authentification de l'accédant lors des accès au réseau local depuis l'extérieur (depuis le Réseau Téléphonique Commuté, X25, RNIS, ADSL, Internet, etc.)
05B06	Authentification de l'accédant lors des accès au réseau local depuis un sous-réseau WiFi
05B07	Filtrage général des accès au réseau local
05B08	Contrôle du routage des accès sortants
05B09	Authentification de l'entité accédée lors des accès sortants vers des sites sensibles

C - Sécurité des données lors des échanges et des communications sur le réseau local

05C01	Chiffrement des échanges sur le réseau local
05C02	Protection de l'intégrité des échanges sur le réseau local
05C03	Chiffrement des échanges lors des accès distants au réseau local
05C04	Protection de l'intégrité des échanges lors des accès distants au réseau local

D - Contrôle, détection et traitement des incidents du réseau local

05D01	Surveillance (en temps réel) du réseau local
05D02	Analyse (en temps différé) des traces, logs et journaux d'événements sur le réseau local
05D03	Traitement des incidents du réseau local

06 Exploitation des réseaux (06 Exr)

A - Sécurité des procédures d'exploitation

06A01	Prise en compte de la sécurité dans les relations avec le personnel d'exploitation (salariés et prestataires)
06A02	Contrôle de la mise en production de nouveaux logiciels ou matériels ou d'évolutions de logiciels ou matériels
06A03	Contrôle des opérations de maintenance
06A04	Contrôle de la télémaintenance
06A05	Gestion des procédures opérationnelles d'exploitation des réseaux
06A06	Gestion des prestataires de services liés aux réseaux
06A07	Prise en compte de la confidentialité lors des opérations de maintenance sur les équipements de réseau
06A08	Gestion des contrats de services réseaux

B - Paramétrage et contrôle des configurations matérielles et logicielles

06B01	Paramétrage des équipements de réseau et contrôle de la conformité des configurations
06B02	Contrôle de la conformité des accès réseaux des postes utilisateurs

C - Contrôle des droits d'administration

06C01	Gestion des droits privilégiés sur les équipements de réseau
06C02	Authentification des administrateurs et personnels d'exploitation des réseaux
06C03	Surveillance des actions d'administration des réseaux
06C04	Contrôle des outils et utilitaires de l'exploitation du réseau

D - Procédures d'audit et de contrôle des réseaux

06D01	Fonctionnement des contrôles d'audit
06D02	Protection des outils et résultats d'audit

07 Sécurité des systèmes et de leur architecture (07 Sys)

A - Contrôle d'accès aux systèmes et applications

07A01	Gestion des profils d'accès (droits et privilèges accordés en fonction des profils de fonction)
07A02	Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)
07A03	Authentification de l'accédant
07A04	Filtrage des accès et gestion des associations
07A05	Authentification du serveur lors des accès à des serveurs sensibles

B - Confinement des environnements

07B01	Contrôle des accès aux résidus

C - Gestion et enregistrement des traces

07C01	Enregistrement des accès aux ressources sensibles
07C02	Enregistrement des appels aux procédures privilégiées

D - Sécurité de l'architecture

07D01	Sûreté de fonctionnement des éléments d'architecture
07D02	Isolement des systèmes sensibles

08 Production informatique (08 Exs)

A - Sécurité des procédures d'exploitation

08A01	Prise en compte de la sécurité dans les relations avec le personnel d'exploitation (salariés et prestataires)
08A02	Contrôle des outils et utilitaires de l'exploitation
08A03	Contrôle de la mise en production de nouveaux systèmes ou d'évolutions de systèmes existants
08A04	Contrôle des opérations de maintenance
08A05	Prise en compte de la confidentialité lors des opérations de maintenance
08A06	Contrôle de la télémaintenance
08A07	Protection des états imprimés sensibles
08A08	Gestion des procédures opérationnelles d'exploitation informatique
08A09	Gestion des prestataires de services liés à la production informatique

B - Contrôle des configurations matérielles et logicielles

08B01	Paramétrage des systèmes et contrôle de la conformité des configurations systèmes
08B02	Contrôle de la conformité des configurations applicatives (logiciels et progiciels)
08B03	Contrôle de la conformité des programmes de référence (Sources et exécutables)

C - Gestion des supports informatiques de données et programmes

08C01	Administration des supports
08C02	Marquage des supports de production (vivants, sauvegardes et archives)
08C03	Sécurité physique des supports stockés sur site
08C04	Sécurité physique des supports externalisés (stockés sur un site externe)
08C05	Vérification et rotation des supports d'archivage
08C06	Protection des réseaux de stockage
08C07	Sécurité physique des media en transit

D - Continuité de fonctionnement

08D01	Organisation de la maintenance du matériel
08D02	Organisation de la maintenance du logiciel (système, middleware et progiciel applicatif)
08D03	Procédures et plans de reprise des applications sur incidents
08D04	Sauvegarde des configurations logicielles (logiciels de base et applicatifs et paramètres de configuration)
08D05	Sauvegarde des données applicatives
08D06	Plans de Reprise d'Activité
08D07	Protection antivirale des serveurs de production
08D08	Gestion des systèmes critiques (vis-à-vis de la permanence de la maintenance)
08D09	Sauvegardes de recours externalisées
08D10	Maintien des comptes d'accès

E - Gestion et traitement des incidents

08E01	Détection et traitement (en temps réel) des anomalies et incidents
08E02	Surveillance, en temps différé, des traces, logs et journaux
08E03	Gestion et traitement des incidents systèmes et applicatifs

F - Contrôle des droits d'administration

08F01	Gestion des attributions de droits privilégiés sur les systèmes (droits d'administrateur)
08F02	Authentification des administrateurs et personnels d'exploitation

08F03	Surveillance des actions d'administration des systèmes
G - Procédures d'audit et de contrôle des systèmes de traitement de l'information	
08G01	Fonctionnement des contrôles d'audit
08G02	Protection des outils et résultats d'audit
H - Gestion des archives informatiques	
08H01	Organisation de gestion des archives informatiques
08H02	Gestion des accès aux archives
08H03	Gestion de la sécurité des archives
09	**Sécurité applicative (09 App)**
A - Contrôle d'accès applicatif	
09A01	Gestion des profils d'accès aux données applicatives
09A02	Gestion des autorisations d'accès aux données applicatives (attribution, délégation, retrait)
09A03	Authentification de l'accédant
09A04	Filtrage des accès et gestion des associations
09A05	Authentification de l'application lors des accès à des applications sensibles
B - Contrôle de l'intégrité des données	
09B01	Scellement des données sensibles
09B02	Protection de l'intégrité des données échangées
09B03	Contrôle de la saisie des données
09B04	Contrôles permanents (vraisemblance, ...) sur les données
09B05	Contrôles permanents (vraisemblance, ...) sur les traitements
C - Contrôle de la confidentialité des données	
09C01	Chiffrement des échanges (ponctuel ou en totalité)
09C02	Chiffrement des données stockées
09C03	Dispositif anti-rayonnement
D - Disponibilité des données	
09D01	Enregistrements de Très Haute Sécurité (THS)
09D02	Gestion des moyens d'accès aux données applicatives
E - Continuité de fonctionnement	
09E01	Reconfiguration matérielle
09E02	Plans de Continuité des processus applicatifs
09E03	Gestion des applications critiques (vis-à-vis de la permanence de la maintenance)
F - Contrôle de l'émission et de la réception de données	
09F01	Garantie d'origine, signature, électronique
09F02	Individualisation des messages empêchant leur duplication (numérotation, séquencement,...)
09F03	Accusé de réception
G - Détection et gestion des incidents et anomalies applicatifs	
09G01	Détection des anomalies applicatives
H - Commerce électronique	
09H01	Sécurité des sites de commerce électroniques
10	**Sécurité des projets et développements applicatifs (10 Dev)**
A - Organisation des développements, de la maintenance et de la gestion des changements	
10A01	Prise en compte de la sécurité dans les méthodes de développement
10A02	Gestion des changements
10A03	Externalisation du développement logiciel
10A04	Organisation de la maintenance applicative
10A05	Modification des progiciels
B - Sécurité des processus de développement et de maintenance	
10B01	Sécurité des processus des développements applicatifs
10B02	Protection de la confidentialité des développements applicatifs
10B03	Sécurité relative aux traitements internes des applications
10B04	Protection des données d'essai
10B05	Sécurité de la maintenance applicative
10B06	Maintenance à chaud

11 Protection des postes de travail utilisateurs (11 Mic)

A - Sécurité des procédures d'exploitation du parc de postes utilisateurs

11A01	Contrôle de l'installation de nouvelles versions de progiciels ou systèmes sur les postes utilisateurs
11A02	Contrôle de la conformité des configurations utilisateurs
11A03	Contrôle des licences des logiciels et progiciels
11A04	Contrôle de la conformité des programmes de référence (Sources et exécutables) des logiciels utilisateurs
11A05	Gestion des prestataires ou fournisseurs de services de gestion et d'administration du parc de postes utilisateurs

B - Protection des postes de travail

11B01	Contrôle d'accès au poste de travail
11B02	Travail en dehors des locaux de l'entreprise
11B03	Utilisation d'équipements personnels ou externes (n'appartenant pas à l'entreprise)

C - Protection des données du poste de travail

11C01	Protection de la confidentialité des données contenues dans le poste de travail ou sur un serveur de données (disque logique pour le poste de travail)
11C02	Protection de la confidentialité des données de l'environnement de travail personnel stockées sur support amovible
11C03	Prise en compte de la confidentialité lors des opérations de maintenance des postes utilisateurs
11C04	Protection de l'intégrité des fichiers contenus sur le poste de travail ou sur un serveur de données (disque logique pour le poste de travail)
11C05	Sécurité de la messagerie électronique et des échanges électroniques d'information
11C06	Protection des impressions sur imprimantes partagées

D - Continuité de service de l'environnement de travail

11D01	Organisation de la maintenance du matériel mis à la disposition du personnel
11D02	Organisation de la maintenance du logiciel utilisateurs (système, middleware et applicatif)
11D03	Plans de sauvegardes des configurations utilisateurs
11D04	Plan de sauvegardes des données utilisateurs (bureautiques) stockées sur serveur de données
11D05	Plan de sauvegardes des données utilisateurs (bureautiques) stockées sur les postes de travail
11D06	Protection des postes utilisateurs contre des codes malveillants ou des codes exécutables non autorisés
11D07	Plan de Reprise d'Activité des postes utilisateurs
11D08	Gestion des moyens nécessaires à l'accès aux fichiers bureautiques

E - Contrôle des droits d'administration

11E01	Gestion des attributions de droits privilégiés sur les postes utilisateurs (droits d'administrateur)
11E02	Authentification et contrôle des droits d'accès des administrateurs et personnels d'exploitation
11E03	Surveillance des actions d'administration du parc de postes utilisateurs

12 Exploitation des télécommunications (12 Ext)

A - Sécurité des procédures d'exploitation

12A01	Prise en compte de la sécurité dans les relations avec le personnel d'exploitation (salariés et prestataires)
12A02	Contrôle de la mise en production de nouveaux systèmes ou d'évolutions de systèmes existants
12A03	Contrôle des opérations de maintenance
12A04	Contrôle de la télémaintenance
12A05	Gestion des procédures opérationnelles d'exploitation des télécommunications
12A06	Gestion des prestataires ou fournisseurs de services télécoms

B - Contrôle des configurations matérielles et logicielles

12B01	Paramétrage des équipements et contrôle de la conformité des configurations
12B02	Contrôle de la conformité des programmes de référence (Sources et exécutables)

C - Continuité de fonctionnement

12C01	Organisation de la maintenance des équipements
12C02	Organisation de la maintenance du logiciel (système et services attachés)
12C03	Sauvegarde des configurations logicielles (logiciels de base, middleware et/ou paramètres de configuration)
12C04	Plans de Reprise d'Activité
12C05	Gestion des systèmes critiques (vis-à-vis de la permanence de la maintenance)

D – Utilisation des équipements terminaux

12D01	Contrôle des configurations utilisateurs mises en oeuvre
12D02	Formation et sensibilisation des utilisateurs

12D01	Utilisation de terminaux chiffrants
E - Contrôle des droits d'administration	
12E01	Gestion des attributions de droits privilégiés sur les systèmes (droits d'administrateur)
12E02	Authentification et contrôle des droits d'accès des administrateurs et personnels d'exploitation
12E03	Surveillance des actions d'administration des systèmes

13 Processus de management (13 Man)

A - Protection des renseignements personnels	
13A01	Politique et directives relatives à la PRP
13A02	Programme de formation et de sensibilisation à la PRP
13A03	Applicabilité de la politique relative à la Prp
13A04	Contrôle de l'application de la politique relative à la Prp
B - Communication financière	
13B01	Politique et directives relatives à la Communication financière
13B02	Programme de formation et de sensibilisation à la Communication financière
13B03	Applicabilité de la politique relative à la Communication financière
13B04	Contrôle de l'application de la politique relative à la Communication financière
C - Respect de la législation concernant la Vérification de la Comptabilité Informatisée (VCI)	
13C01	Conservation des données et traitements
13C02	Documentation des données , procédures et traitements liés à la comptabilité
13C03	Programme de formation et de sensibilisation aux contraintes de la Vérification de la comptabilité informatisée
13C04	Applicabilité de la politique relative à la Vérification de la comptabilité informatisée
13C05	Contrôle de l'application de la politique relative à la Vérification de la comptabilité informatisée
D - Protection de la propriété intellectuelle	
13D01	Politique et directives relatives à la Protection de la propriété intellectuelle
13D02	Programme de formation et de sensibilisation à la Protection de la propriété intellectuelle
13D03	Applicabilité de la politique relative à la Protection de la propriété intellectuelle
13D04	Contrôle de l'application de la politique relative à la Protection de la propriété intellectuelle
E - Protection des systèmes informatisés	
13E01	Politique et directives relatives à la Protection des systèmes informatisés
13E02	Programme de formation et de sensibilisation à la Protection des systèmes informatisés
13E03	Applicabilité de la politique relative à la Protection des systèmes informatisés
13E04	Contrôle de l'application de la politique relative à la Protection des systèmes informatisés
F - Sécurité des personnes et protection de l'environnement	
13F01	Politique et directives relatives à la sécurité des personnes et à la protection de l'environnement
13F02	Programme de formation et de sensibilisation à la Sécurité des personnes et à la protection de l'environnement
13F03	Applicabilité de la politique relative à la Sécurité des personnes et protection de l'environnement
13F04	Contrôle de l'application de la politique relative à la Sécurité des personnes et protection de l'environnement
G – Règles relatives à l'utilisation de moyens cryptologiques	
13F01	Politique et directives relatives à l'utilisation de moyens cryptologiques
13F02	Programme de formation et de sensibilisation à l'utilisation de moyens cryptologiques
13F03	Applicabilité de la politique relative à l'utilisation de moyens cryptologiques
13F04	Contrôle de l'application de la politique relative à l'utilisation de moyens cryptologiques

14 Management de la sécurité de l'information (14 Msi)

A - Planification du système de management

14A01	Définition du périmètre du SMSI
14A02	Définition de la politique du SMSI
14A03	Approche de l'analyse des risques et des métriques associées
14A04	Identification des risques
14A05	Analyse et évaluation des risques
14A06	Sélection des options de traitement des risques
14A07	Sélection des mesures de réduction des risques
14A08	Sélection des mesures de sécurité et construction d'une déclaration d'applicabilité

B - Déploiement du système de management

14B01	Formulation d'un plan de traitement des risques
14B02	Mise en oeuvre du plan de traitement des risques
14B03	Choix et mise en place des indicateurs pour le SMSI
14B04	Mise en place d'un plan de formation et de sensibilisation
14B05	Détection et réactions aux incidents

C - Mise sous Contrôle du système de management

14C01	Contrôle de l'exécution des procédures et des mesures de sécurité
14C02	Pilotage du programme d'audit
14C03	Revue des risques et des mesures de sécurité

D - Amélioration du système de management

14D01	Amélioration continue
14D02	Actions de correction des non-conformités
14D03	Actions de prévention des non-conformités
14D04	Communication vers les parties prenantes

E - Documentation

14E01	Gestion de la documentation
14E02	Approbation des documents
14E03	Mises à jour
14E04	Identification et gestion des versions des documents
14E05	Mise à disposition de la documentation
14E06	Retrait des documents qui ne sont plus valides

Annexe G3
Échelle de niveaux utilisable pour évaluer la qualité des services de sécurité

Bien que cette échelle puisse être continue, il n'est pas inutile de donner quelques valeurs de référence 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.

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Téléchargez les productions du CLUSIF sur

www.clusif.asso.fr