

METHODES



MEHARI 2010

Guide de l'analyse et du traitement des risques

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>

MEHARI est une marque déposée par le CLUSIF.

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

Remerciements

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

| | | |
|-------|--|----|
| 1 | Introduction..... | 5 |
| 1.1 | Gestion directe et individuelle des risques ou gestion globale..... | 5 |
| 1.2 | Rappel des principes généraux de MEHARI..... | 6 |
| 1.3 | Schéma général de planification du traitement des risques..... | 7 |
| 2 | L'appréciation des risques | 8 |
| 2.1 | L'identification des risques | 8 |
| 2.1.1 | Les scénarios de risque de la base de connaissances..... | 8 |
| 2.1.2 | Sélection des scénarios de risque | 9 |
| 2.2 | L'estimation des risques identifiés | 9 |
| 2.2.1 | Évaluation de la potentialité intrinsèque..... | 10 |
| 2.2.2 | Évaluation de l'impact intrinsèque | 11 |
| 2.2.3 | Évaluation des facteurs de réduction de risque à partir d'un audit de sécurité MEHARI...13 | |
| 2.2.4 | Évaluation de la potentialité et de l'impact résiduels..... | 15 |
| 2.3 | Évaluation de la gravité du scénario..... | 17 |
| 3 | Le traitement des risques | 18 |
| 3.1 | Sélection de plans d'action par famille de scénarios | 18 |
| 3.2 | Définition et sélection de projets..... | 19 |
| 3.3 | Besoin de service..... | 19 |
| 3.4 | Autres démarches..... | 19 |
| 4 | Conseils pratiques | 20 |
| 4.1 | Esprit de la démarche d'analyse de risque..... | 20 |
| 4.2 | Composition du groupe d'évaluation des risques | 20 |
| 4.3 | Contrôle des automatismes | 20 |
| | Annexe 1 : Grille d'exposition naturelle standard | 21 |
| | Annexe 2 : Définition des niveaux d'exposition naturelle..... | 22 |
| | Annexe 3 : Tableau d'impact intrinsèque..... | 23 |
| | Annexe 4 : Définition des niveaux de facteurs de réduction de risque | 24 |
| | Annexe 5 : Grilles d'évaluation standards..... | 26 |

1 Introduction

Ce guide est destiné à aider les responsables souhaitant engager, avec l'aide de MEHARI, une démarche de gestion de risques dans leur entreprise ou organisme.

MEHARI se distingue par le fait qu'elle permet une gestion directe et individuelle des risques, par opposition aux méthodes de gestion globale et moins différenciée (des risques).

1.1 Gestion directe et individuelle des risques ou gestion globale

En effet, on peut distinguer deux grands types de gestion des risques :

- Un premier type de gestion consiste à identifier toutes les situations de risque, à analyser chaque situation de risque identifiée et à prendre des décisions spécifiques et adaptées à chacune d'elles, avec une forte implication de la Direction dans la gestion des risques
- Un deuxième type de gestion qui, au contraire, s'appuie sur une analyse plus générale afin de définir des objectifs et des directives de sécurité propres à réduire globalement les risques, sans gestion directe et individualisée des risques, et sans doute avec une moindre intervention de la Direction.

Une analyse détaillée de ces types de gestion est donnée dans le document: « La gestion des risques – Concepts et méthodes » publié en 2009 et disponible sur le site du Clusif.

Un tableau comparatif de ces deux types de gestion est donné ci-dessous.

| | Gestion directe et individuelle des risques | Gestion globale et indirecte des risques |
|---------------|--|---|
| Avantages | Identification et analyse de toutes les situations de risques Évaluation précise du niveau de risque de chaque situation Evaluation précise de l'effet des mesures de sécurité sur les niveaux de chaque situation de risque | Représentation simple des risques Facilité d'assimilation des concepts Facilité de communication sur les risques Passage aisé des risques aux mesures à mettre en œuvre |
| Inconvénients | Nécessité d'un modèle complet de représentation du risque Nécessité de représenter chaque situation de risque dans sa complexité | Possibilité d'ignorer des situations de risques éventuellement graves Absence de jugement précis sur les niveaux de gravité des risques Possibles surcoûts dans les traitements des risques |

MEHARI est clairement positionné comme un cadre méthodologique adapté à la gestion directe des risques des entreprises ou des organismes et les démarches que nous introduisons plus loin sont strictement dans ce cadre.

1.2 Rappel des principes généraux de MEHARI

Le choix de l'option de gestion directe des risques conduit à définir un certain nombre de principes et de spécifications, décrits dans le document « MEHARI 2010 – Principes fondamentaux et spécifications fonctionnelles ».

L'essentiel peut se résumer à ceci :

Les risques doivent être identifiés et décrits par des scénarios contenant un certain nombre d'éléments précis

Chaque scénario de risque peut être évalué quantitativement et cette évaluation prend en compte :

- L'impact intrinsèque du scénario de risque qui reflète le niveau de conséquence du scénario, s'il se réalise, en l'absence de toute mesure de sécurité
- La potentialité intrinsèque du scénario (ou exposition naturelle au scénario), qui reflète le niveau de probabilité de survenance du scénario, en l'absence de toute mesure de sécurité
- Des facteurs de réduction de risque, différenciés par leur type d'effet sur l'impact ou la potentialité, facteurs qui dépendent des mesures de sécurité et de la qualité de ces mesures

Le processus d'évaluation de chaque scénario de risque permet de sélectionner des mesures de sécurité, et des objectifs qualitatifs pour ces mesures, tels que le risque puisse être maintenu à un niveau acceptable.

Nous nous alignerons, pour présenter la démarche MEHARI, sur l'organisation décrite dans la norme ISO/IEC 27005 et représentée schématiquement ci-dessous.

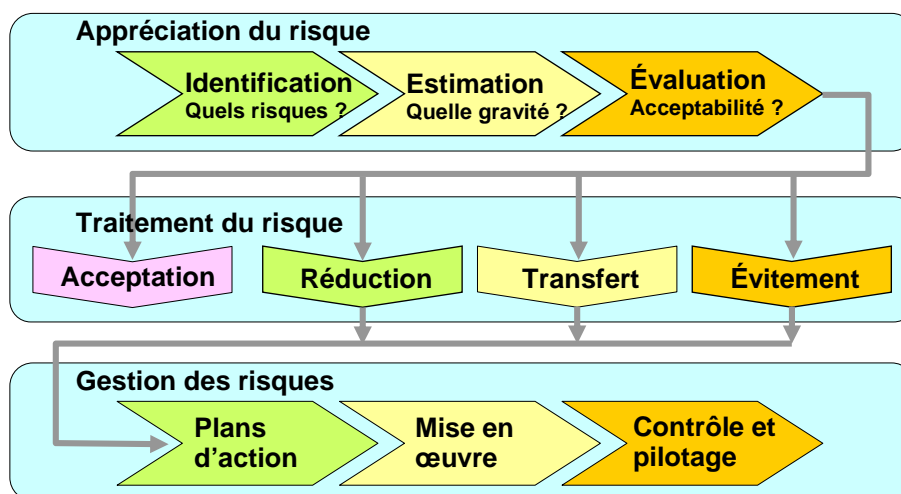


Figure 1 Etapes dans la gestion des risques

Ce schéma fait apparaître trois grandes phases, les deux premières constituées de l'appréciation des risques et de l'élaboration des plans de traitement des risques correspondant à la partie planification (plan) de la norme ISO/IEC 27001 et une phase de mise en œuvre qui comprend elle-même, au sens de cette même norme, les aspects de déploiement (« do »), de contrôle (« check »), et enfin d'amélioration et de correction éventuelle (« act »).

Les différences principales entre les diverses démarches adaptées à la gestion directe et individualisée des risques résident essentiellement dans la phase de planification, par la manière d'apprécier chaque risque et de définir le plan de traitement adapté à chacun.

1.3 Schéma général de planification du traitement des risques

La figure 2 décrit l'ensemble des étapes constituant les phases d'appréciation des risques et d'élaboration des plans de traitement correspondants.

Chacune de ces étapes est décrite, justifiée et commentée dans le document déjà cité « MEHARI 2010 – Principes fondamentaux et spécifications fonctionnelles ».

Etapes et exigences bases et actions Application particulière résultat

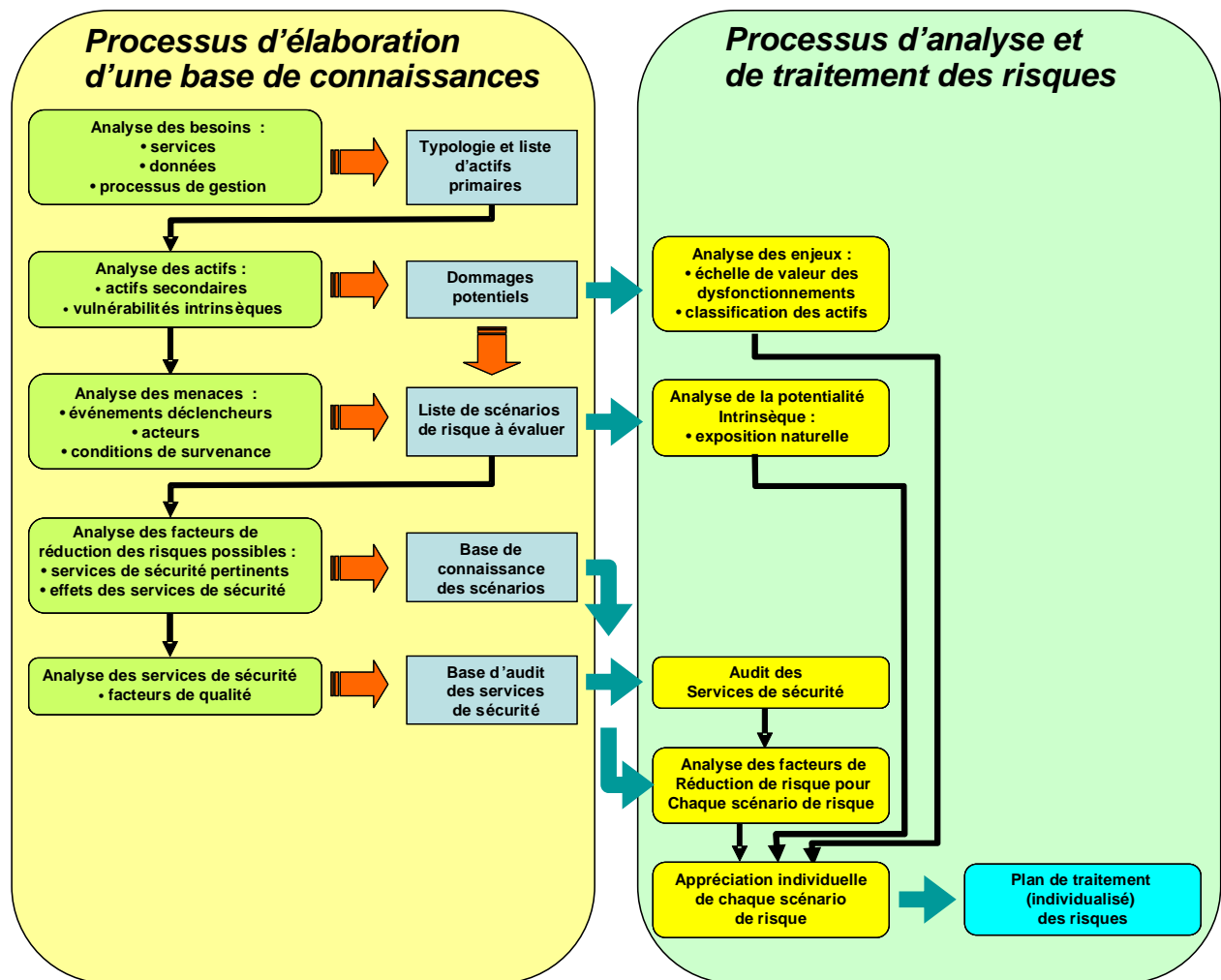


Figure 2 : Schéma général de planification du traitement des risques

Cette figure montre que les exigences et les étapes d'analyse sont communes à nombre d'entités et permettent de bâtir des démarches, des bases et des outils d'utilisation générale facilitant une application ultérieure à chaque environnement particulier. Ceci nous amène à considérer que les deux premières colonnes correspondent en fait à l'établissement d'une base de connaissances et qu'il convient dès lors de considérer séparément deux types d'activités :

- La construction d'une base de connaissances de scénarios de risque
- L'analyse et le traitement des risques avec l'aide de cette base de connaissances

Le présent document traite de la gestion des risques (analyse et élaboration des plans de traitement) en s'appuyant sur la base de connaissances de MEHARI, le guide relatif à la construction d'une base de connaissance étant reporté dans un autre document (à paraître).

2 L'appréciation des risques

L'appréciation des risques comprend :

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

2.1 L'identification des risques

L'identification des risques est un processus qui, pour l'essentiel, peut être réalisé à partir d'une base de connaissances. En effet, outre que peu de risques sont réellement spécifiques d'une entreprise ou d'une organisation, les situations de risque auxquelles l'entreprise ou l'organisme sont confrontées sont relativement peu évolutives.

MEHARI propose une base de connaissances de scénarios de risque utilisable par la très grande majorité des organismes. Il est néanmoins possible de développer des variantes, de compléter cette base, ou d'en développer de nouvelles, en s'appuyant sur un guide spécifique.

Pour la suite de ce document, nous considérerons que la base de connaissances MEHARI 2010 est utilisée.

2.1.1 Les scénarios de risque de la base de connaissances

Les situations de risque standards sont donc décrites par des scénarios de risque qui contiennent les éléments suivants :

- Un indicateur de classement des scénarios en familles de scénarios
- Le type d'actif (primaire)
- Le type de vulnérabilité intrinsèque, ceci incluant :
 - Le type d'actif secondaire
 - Le type de dommage subi
 - Le critère concerné (DIC)
- Le type de menace, ceci incluant :
 - Le type d'événement déclencheur
 - Les circonstances de déclenchement (éventuellement)
 - Le type d'acteur (éventuellement)
- Un descriptif du scénario, sous forme de texte

La justification de ces divers éléments est fournie dans le document « *MEHARI 2010, Principes fondamentaux et spécifications fonctionnelles* ».

La base de connaissances de MEHARI 2010 contient près de 800 scénarios de risque standards.

Parmi tous ces scénarios, certains peuvent être réellement critiques et méritent un examen détaillé, d'autres, au contraire, peuvent ne pas être pertinents pour l'entité ou ne pas mériter que l'on s'y attarde.

Une sélection peut donc s'avérer souhaitable.

2.1.2 Sélection des scénarios de risque

Il peut être jugé souhaitable d'effectuer une sélection de scénarios avant d'aborder une estimation approfondie de leur gravité et un plan de traitement des risques.

Les critères de sélection des scénarios pertinents peuvent être :

- La gravité intrinsèque des scénarios
- Certaines formes d'actifs
- Certains types d'événement
- Certains types de circonstances ou d'acteurs

La base de connaissances permet d'effectuer cette sélection.

Mise en pratique avec la base de connaissance MEHARI sous Excel

En pratique, la feuille de calcul « Scénarios » de la base comprend une colonne « Sélection » et des possibilités de filtrage (standard Excel).

Le processus est alors le suivant :

- ✚ Sélectionner le paramètre sur lequel on veut effectuer un filtrage et la valeur de ce paramètre à éliminer
- ✚ Forcer 0 dans la colonne « Sélection » une fois le filtrage effectué
- ✚ Supprimer le filtrage (sélectionner « tous » pour le paramètre)

2.2 L'estimation des risques identifiés

Rappelons, en introduction, le schéma global de l'estimation d'un risque, tel que cela a été présenté et justifié dans le document « MEHARI 2010 - Principes fondamentaux et spécifications fonctionnelles » :

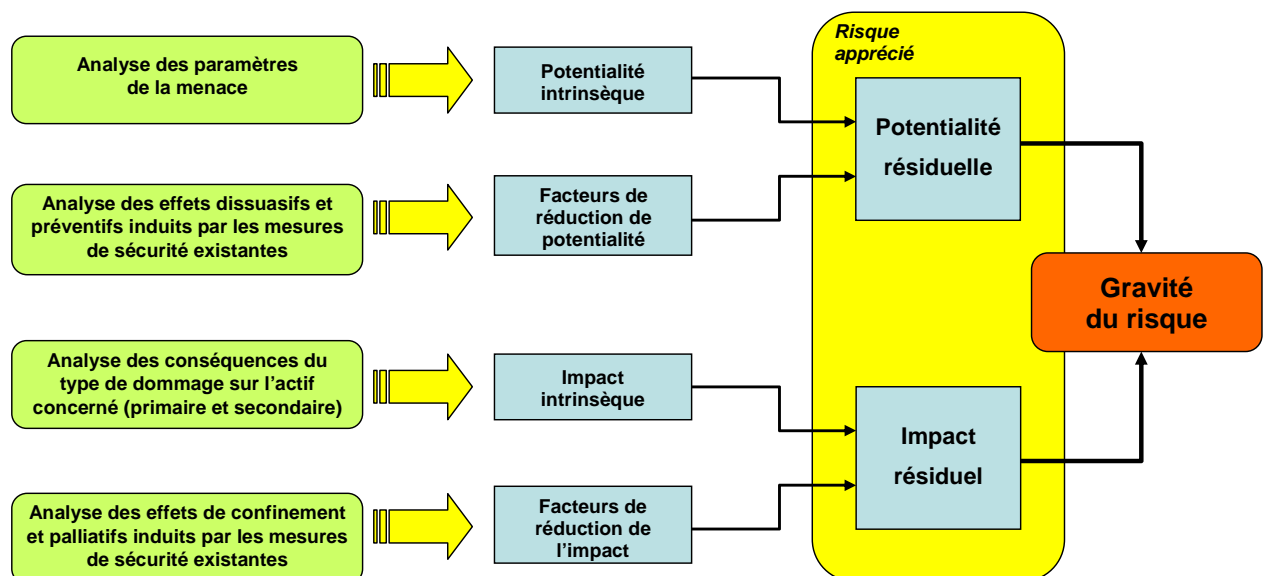


Figure 3 : Le processus d'estimation d'un risque

MEHARI propose, par ses bases de connaissances, plusieurs types d'assistance à l'estimation d'un risque :

- Une assistance à l'évaluation de la potentialité intrinsèque
- Un tableau générique d'impact intrinsèque pouvant être élaboré à la suite d'une classification ou directement à partir d'une échelle de valeurs de dysfonctionnements.
- Des automatismes d'évaluation des facteurs de réduction des risques (dissuasion, prévention, protection et palliation) en fonction de la qualité des services de sécurité, si celle-ci a été évaluée par un audit MEHARI.
- Des automatismes de calcul de la potentialité et de l'impact résiduels, en fonction de la potentialité intrinsèque, de l'impact intrinsèque et des facteurs d'atténuation des risques.
- Une assistance à l'évaluation de la gravité résultante du risque.

2.2.1 Évaluation de la potentialité intrinsèque

La potentialité intrinsèque est une évaluation de la probabilité de survenance de la menace, en dehors de toute mesure de sécurité.

Nous appelons également ce facteur « Exposition naturelle », ce qui dit bien le sens donné à cette expression.

La potentialité intrinsèque d'une menace n'est pas une constante absolue et peut varier d'une entreprise à une autre et, pour une même entreprise, en fonction de phénomènes conjoncturels.

Il s'agit bien de l'exposition naturelle **de l'entreprise ou de l'organisme** à la menace considérée.

Il reste, néanmoins, que pour beaucoup d'entreprises, l'exposition « normale » ou « standard » à un type de menace, c'est-à-dire en l'absence de phénomènes conjoncturels particuliers, est conforme à ce qui peut être constaté généralement et qu'une évaluation « a priori » peut donc être fournie.

2.2.1.1 Exposition naturelle (ou potentialité intrinsèque) standard

Les scénarios de la base de connaissances MEHARI se réfèrent ainsi à une liste limitée de menaces. Ces menaces sont elles-mêmes décrites par des événements types, et par des descriptions complémentaires de circonstances et d'acteurs (voir la justification de ces divers paramètres dans le document « *MEHARI 2010 – Principes fondamentaux et spécifications fonctionnelles* »).

La potentialité intrinsèque ou exposition naturelle (de valeur 1 à 4) dépend essentiellement du type d'événement, qu'il s'agisse d'accidents, d'erreurs ou d'actes volontaires (malveillants ou non), pour lesquels une évaluation a priori de l'exposition est donnée.

Ainsi, par exemple, il est estimé que l'exposition naturelle « standard » d'une entreprise à un incendie est de niveau 2 (plutôt improbable), à une panne d'équipement informatique de niveau 3 (plutôt probable) et à une erreur pendant un processus de saisie de niveau 4 (très probable).

La liste de ces événements et de l'exposition naturelle standard est donnée en annexe 1.

Chaque scénario fait ainsi référence à un type d'événement, pour lequel une valeur standard de potentialité intrinsèque est fournie.

2.2.1.2 Exposition naturelle spécifique de l'entreprise pour un risque donné

Il doit être clair que l'évaluation standard proposée n'est qu'une évaluation par défaut et que l'évaluation directe de l'exposition de l'entreprise à la situation de risque analysée est de loin préférable. Pour cette évaluation, il convient de se référer aux définitions des niveaux d'exposition qui ont été données dans le document « *MEHARI 2010 – Principes fondamentaux et spécifications fonctionnelles* » et qui sont rappelées en annexe 2.

Remarque :

S'il est décidé de procéder à une analyse systématique de situations de risque ou si plusieurs situations doivent être examinées, il est largement préférable de passer d'abord en revue l'ensemble des types d'événements et de porter un jugement d'ensemble sur l'exposition de l'entreprise à chacun d'eux.

Mise en pratique avec la base de connaissance MEHARI sous Excel

En pratique, le responsable de la gestion des risques devra valider ces valeurs ou les corriger en décidant au cas par cas des valeurs à retenir pour son entité.

Le processus est alors le suivant :

- ✚ Ouvrir la base de connaissance
- ✚ Aller dans la feuille « Mask » et vérifier que la feuille de paramétrages « événements types » n'est pas masquée
- ✚ Sélectionner la feuille « Evénements types »
- ✚ Remplir les nouvelles valeurs dans la colonne « Exposition naturelle décidée » (il est inutile de remplir ces valeurs si les valeurs standards sont acceptées)

2.2.2 Évaluation de l'impact intrinsèque

L'impact intrinsèque d'un scénario est l'évaluation des conséquences de l'occurrence du risque, indépendamment de toute mesure de sécurité, ainsi que cela a été décrit dans les principes de MEHARI.

Pour chaque scénario défini dans la base de connaissances de MEHARI, il existe un actif cible de ce scénario. Chaque scénario indique clairement le type d'actif primaire et le type d'actif secondaire (voir « *MEHARI 2010 – Principes fondamentaux et spécifications fonctionnelles* » pour la définition des actifs primaires et secondaires).

L'impact intrinsèque dépend, fondamentalement du type d'actif primaire..

Le scénario indique également le type de dommage subi.

Il peut s'agir d'un type de données dérobées, d'un type de service rendu indisponible ou d'un type de données altérées, selon qu'il s'agit d'un scénario mettant en cause la confidentialité, la disponibilité ou l'intégrité d'un actif, qui sont les trois critères de base pris en compte par MEHARI en standard. Un dernier critère, d'« efficacité », est considéré pour les actifs de type « processus de gestion ».

Dans ces conditions évaluer l'impact intrinsèque d'un scénario revient à évaluer le niveau de criticité ou de gravité résultant de la perte de disponibilité, d'intégrité, de confidentialité, ou de non-conformité selon le type de scénario, du type d'actif mis en cause par le scénario.

La démarche de classification utilisée par MEHARI permet d'établir un tableau générique de classification faisant apparaître les types d'actifs identifiés de manière spécifique par les scé-

narios de la base de connaissances. La démarche de classification est décrite dans le document « MEHARI 2010 - Principes fondamentaux et Spécifications fonctionnelles » et dans le « *Guide de l'analyse des enjeux et de la classification* ».

2.2.2.1 Le tableau d'impact intrinsèque

La démarche d'évaluation des impacts intrinsèques peut donc être organisée et permet de remplir un tableau d'impact intrinsèque, basé sur celui fourni en Annexe 3, dont un extrait est donné ci-dessous.

| Tableau d'impact intrinsèque | | | |
|--|---|---|---|
| Actifs de type données et informations | D | I | C |
| D01 Fichiers de données ou bases de données applicatives | | | |
| D07 Courrier électronique | | | |
| .../... | | | |
| Actifs de type services | | | |
| S01 Services applicatifs, ... | | | |

Le remplissage de ce tableau s'effectue en transcrivant (par une valeur de 1 à 4) le niveau de conséquence d'une atteinte à la disponibilité, l'intégrité ou la confidentialité de chaque type d'actif identifié (cependant certaines cases n'ont pas à être remplies : par exemple la confidentialité de certains services).

La démarche de base consiste à partir de tableaux de classification, tels que décrits dans le document « *Guide de l'analyse des enjeux et de la classification* ».

A défaut, il est possible de le faire directement, mais la démarche de classification décrite dans le guide cité ci-dessus est incontestablement à conseiller.

Le principe général de remplissage du tableau d'impact intrinsèque est de retenir, pour chaque type d'information et pour chaque critère, la classification la plus élevée trouvée lors du processus de classification. Le détail de la démarche de remplissage du tableau d'impact intrinsèque à partir de tableaux de classification est fourni dans le « *Guide de l'analyse des enjeux et de la classification* ».

Il s'agit donc d'une synthèse servant à définir le niveau d'impact intrinsèque de chaque scénario de la base de connaissances de MEHARI.

2.2.2.2 Extension du tableau d'impact intrinsèque

Le tableau standard de MEHARI ne fait référence qu'aux trois critères standards de Disponibilité, Intégrité et Confidentialité, pour les données et les services et qu'au critère d'efficacité pour les processus de gestion. D'autres critères peuvent, bien entendu, être utilisés. Il est ainsi possible d'étendre le tableau avec, par exemple, des critères de Preuve, de Traçabilité, d'Auditabilité, etc.

Il faudra alors créer des scénarios faisant appel à de tels critères (ou modifier des scénarios existants) et créer, en outre, les grilles d'évaluation correspondantes.

2.2.2.3 L'évaluation de l'impact intrinsèque des scénarios

L'évaluation de l'impact intrinsèque de chaque scénario de la base de connaissances sera faite très simplement, chaque scénario faisant référence à un type d'actif du tableau d'impact intrinsèque et au critère à utiliser (D, I ou C ou autre éventuellement).

2.2.2.4 Décomposition cartographique

Le tableau d'impact intrinsèque standard, fourni en annexe 3, ne comprend qu'une ligne pour l'ensemble des services applicatifs, qu'une ligne pour les bases de données applicatives, et, plus généralement, qu'une seule référence par type d'actif.

Cette démarche globale permet d'analyser des situations de risques en tenant compte de la sensibilité maximale des actifs concernés, sans qu'il soit requis de différencier ces actifs ni de les préciser. C'est une simplification qui limite les situations à analyser, sans conséquence au plan pratique car il sera toujours temps, lors de l'établissement des plans d'action, de limiter les actions correctrices aux actifs réellement sensibles.

Il est possible, cependant, de distinguer des variantes d'actifs, un peu de la même manière que l'on peut distinguer des variantes de services de sécurité lors d'un audit MEHARI (voir le schéma d'audit, dans le « *Guide du diagnostic de l'état des services de sécurité* »).

La création de variantes d'actifs dans le tableau d'impact intrinsèque s'appelle la ***décomposition cartographique***.

Cette décomposition permet de différencier, par exemple, les services applicatifs en plusieurs domaines de serveurs, les bases de données en domaines applicatifs, etc. L'utilisation de la décomposition cartographique permet de traiter spécifiquement un ou plusieurs domaines d'activité.

Cette possibilité n'est pas directement exploitable par les outils standards Excel fournis par le CLUSIF mais peut être réalisée avec RISICARE.

Attention, l'exploitation de cette possibilité peut cependant s'avérer lourde de conséquences quant au nombre de scénarios à analyser.

2.2.3 Évaluation des facteurs de réduction de risque à partir d'un audit de sécurité MEHARI

L'évaluation de la potentialité et de l'impact résiduels d'un scénario de risque repose sur une analyse de l'existence de facteurs de réduction du risque et sur une évaluation de leur niveau.

Ces facteurs sont la dissuasion et la prévention pour la potentialité, le confinement et la palliation pour l'impact.

MEHARI propose, dans sa base de connaissance des scénarios, des évaluations du niveau de ces facteurs en fonction de la qualité des services de sécurité pertinents pour le scénario analysé.

Cette évaluation automatisée est faite en deux temps :

- Le calcul d'indicateurs d'efficacité des services de sécurité, pour chaque type de mesure
- Le calcul des facteurs de réduction de risque proprement dits

2.2.3.1 Indicateurs d'efficacité des services de sécurité par scénario et type de mesure

MEHARI définit, pour chaque scénario et pour chaque type de mesure, un indicateur

d'efficacité.

L'efficacité des mesures d'un type donné est noté :

EFF-DISS pour l'efficacité des *mesures dissuasives*

EFF-PREV pour l'efficacité des *mesures de prévention*

EFF-CONF pour l'efficacité des *mesures de confinement*

EFF-PALL pour l'efficacité des *mesures palliatives*

Ces indicateurs sont calculés par le biais de formules faisant référence à des services de sécurité.

Les formules données dans la base de connaissances de MEHARI font appel :

- Soit directement à un service de sécurité, par son identifiant¹, quand ce service est le seul à avoir un effet de ce type pour ce scénario
- Soit par le biais de formules comprenant des fonctions MIN(arg1 ; arg2 ; ...) ou MAX(arg1 ; arg2 ; ...), les arguments (arg1 ; arg2, ...) étant les identifiants des services de sécurité de la base MEHARI.

Les formules peuvent être, par exemple, de la forme :

EFF-PALL = 06B01

EFF-PREV = MAX(04B04;MIN(04B01;04B02;04B03))

La première formule signifie que l'efficacité (proposée) des mesures palliatives est directement fonction du service 06B01 et a pour valeur le niveau (compris entre 1 et 4) de qualité de ce service.

La deuxième formule signifie que l'efficacité (proposée) des mesures préventives est égale à la plus grande valeur de la qualité du service 04B04 et de la fonction représentant le minimum des services 04B01, 04B02, 04B03

Il peut se trouver qu'il n'y ait pas de service de sécurité pouvant avoir un effet de type donné pour un scénario donné.

Remarque :

La fonction MIN signifie que les services appelés en arguments sont complémentaires et que si l'un d'eux est faible, l'ensemble sera faible. Ce peut être le cas, par exemple de la gestion des autorisations d'accès et de l'authentification ; si l'un d'eux est faible, le contrôle d'accès dans son ensemble est faible.

La fonction MAX signifie que les services appelés sont alternatifs : si l'un d'eux est de bonne qualité, l'ensemble le sera. Ce peut être le cas, par exemple et selon certains scénarios, du contrôle d'accès aux données et du chiffrement de ces données.

Les formules littérales sont données dans la base de connaissances de MEHARI

2.2.3.2 Facteurs de réduction de risque « calculés »

Il est clair que les coefficients d'efficacité évalués ci-dessus, de la forme EFF-XXXX, étant calculés à partir de valeurs de qualité de service qui n'ont aucune raison d'être des nombres entiers, ne sont pas eux-mêmes des nombres entiers. Afin de faciliter l'évaluation finale de la potentialité et de l'impact, MEHARI choisit de les transformer pour obtenir des évaluations de

¹ L'identifiant d'un sous-service est constitué d'un numéro de domaine, d'une lettre indiquant le service auquel il est attaché et d'un numéro de sous-service (ex. 06B01)

facteurs de réduction de risque exprimés par des valeurs entières. Dans ce but la qualité de service prise en compte dans les formules sera arrondie à l'entier le plus proche.

La base de connaissances de MEHARI fournit une valeur calculée (de 0 à 4) de ces facteurs de réduction de risque en se basant sur une valeur de qualité de service qui est indiquée dans la feuille « Services ».

En cas de domaine de services possédant plusieurs variantes dans le schéma d'audit (voir à ce sujet le « Guide de diagnostic des services de sécurité »), les formules fournies dans la base sous Excel retiennent, pour le calcul des facteurs de réduction de risque, le minimum des valeurs obtenues pour chaque variante de service de sécurité (RISICARE permettant de traiter fidèlement le schéma d'audit).

Mise en pratique avec la base de connaissance MEHARI sous Excel

En pratique, les valeurs des divers facteurs de réduction de risque calculés sont données, pour chaque scénario, dans les colonnes « Dissuasion », « Prévention », « Confinement » et « Palliation » de la feuille « Scénarios ».

Ces facteurs de réduction de risque sont ainsi des facteurs « calculés », ce qui veut dire que la valeur obtenue sera généralement pertinente mais qu'il se pourrait qu'elle ne le soit pas dans le contexte spécifique de l'entreprise ou de l'organisme. Il peut se trouver, par exemple, des situations dans lesquelles le personnel a un statut tel qu'il est peu sensible à la dissuasion ou dans lesquelles le personnel est particulièrement expert, ceci rendant fragiles les mesures de prévention, ou pour lesquelles les mesures de protection ou les mesures palliatives seraient sans effet réel sur le niveau d'impact réel.

MEHARI propose une assistance en fournissant des valeurs calculées à l'aide de formules standards pour les facteurs de réduction de risque ; il peut s'avérer pertinent de contrôler ces valeurs avant utilisation.

En cas de désaccord avec les valeurs calculées, il est conseillé de ne pas modifier ces valeurs directement dans la feuille scénarios, car cela supprimerait définitivement le calcul de base, mais de corriger les valeurs « décidées » de l'impact ou de la Potentialité.

Un cas particulier fréquent est celui de scénarios pour lesquels il peut être considéré que les mesures de confinement ne réduiront pas significativement l'impact intrinsèque du scénario (parce que la détection de la fraude ou de la divulgation, par exemple, ne réduiront pas la gravité du risque, quelles que soient les mesures prises alors). Il est alors possible de considérer le scénario comme non évolutif (ou non confinable) et de le déclarer comme tel.

2.2.4 Évaluation de la potentialité et de l'impact résiduels

2.2.4.1 Évaluation automatisée de la Potentialité : STATUS-P

MEHARI propose une évaluation automatisée de la potentialité en partant de l'évaluation de l'exposition naturelle, d'une part, et du niveau des mesures dissuasives et préventives, mesuré par les STATUS-DISS et STATUS-PREV, d'autre part.

MEHARI propose d'évaluer la « **potentialité résiduelle** », sous la forme d'un indicateur appelé STATUS-P, qui est déduit directement de l'exposition naturelle et des STATUS-DISS et STATUS-PREV par des grilles d'évaluation.

Trois grilles standards d'évaluation sont prévues par MEHARI, en fonction du type de cause conduisant au scénario :

- Événement naturel ou accident

- Erreur humaine
- Acte volontaire (malveillant ou non)

Ces grilles standards peuvent être modifiées si besoin est.

Remarque :

La logique de ces grilles d'évaluation est de considérer que pour un type de cause donné (accident, erreur ou acte volontaire), le même raisonnement devrait être suivi, indépendamment de la description précise du scénario : à exposition naturelle égale, dissuasion égale et prévention égale, il devrait être jugé que la potentialité de deux scénarios est la même.

2.2.4.2 Évaluation automatisée de l'impact : STATUS-I

MEHARI propose également une évaluation automatisée de l'impact en partant de l'impact intrinsèque du scénario d'une part et du niveau des mesures de confinement et palliatives, mesuré par les STATUS-CONF et STATUS-PALL, d'autre part.

MEHARI propose d'évaluer « **l'impact résiduel** » par un indicateur STATUS-I, déduit directement de l'impact intrinsèque et des STATUS-CONF et STATUS-PALL par des grilles d'évaluation.

Quatre grilles standards d'évaluation permettant d'évaluer le STATUS-I sont prévues par MEHARI, en fonction du type de conséquence du scénario :

- Scénarios de type Disponibilité
- Scénarios de type Intégrité
- Scénarios de type Confidentialité
- Scénarios de type Limitable²

Les grilles tiennent compte également du caractère évolutif ou non du scénario, ce caractère étant explicité dans la base de connaissances (et pouvant être forcé dans l'état non évolutif, pour les scénarios initialement déclarés comme évolutifs dans la base).

Ces grilles standards peuvent également être modifiées, si besoin est, par un expert de la méthodologie.

Remarque :

La logique de ces grilles d'évaluation est de considérer que pour un type de conséquence donné (atteinte à la disponibilité, à l'intégrité ou à la confidentialité), le même raisonnement devrait être suivi, indépendamment de la description précise du scénario : à impact intrinsèque égal, à mesures de confinement égales et mesures palliatives égales, il devrait être jugé que l'impact résiduel de deux scénarios est le même.

2.2.4.3 Principes de construction des grilles d'évaluation

En pratique, les grilles standards, aussi bien pour la potentialité que pour l'impact, ont été bâties en s'appuyant sur un certain nombre de principes décrits dans le guide de construction des bases de connaissances. Il est possible de modifier ces grilles, en partant d'un nouvel ensemble de principes.

Les grilles d'évaluation standards sont données en annexe 5.

² Cette typologie de scénarios correspond le plus souvent à des scénarios d'atteinte à l'intégrité pour lesquels il n'existe pas de mesure palliative mais dont l'impact peut être limité par des mesures de confinement spécifiques.

2.2.4.4 Évaluation de la potentialité et de l'impact

Comme pour les facteurs de réduction de risque, les automatismes fournis par les grilles de décision sont une assistance au jugement qui fournissent des indicateurs appelés, dans MEHARI, *STATUS*.

Les automatismes fournissent ainsi des évaluations de la potentialité et de l'impact résiduels sous la forme de STATUS-P et STATUS-I

Un jugement final sur la pertinence des niveaux de potentialité P et d'impact I, dans le cas de l'entité étudiée, devrait être la règle.

Mise en pratique avec la base de connaissance MEHARI sous Excel

En pratique, les valeurs calculées de la Potentialité et de l'Impact résiduels (après prise en compte des services de sécurité) sont indiqués dans les colonnes « I calculé » et « P calculé » de la feuille « Scénarios ».

Il est possible d'indiquer des valeurs différentes de ces valeurs calculées dans les colonnes « I décidé » et « P décidée ». Ce sont alors ces valeurs décidées qui seront prises en compte pour le calcul de la gravité résiduelle.

2.3 Évaluation de la gravité du scénario

La gravité du scénario sera déduite des évaluations de Potentialité et d'Impact résiduels, STATUS-P et STATUS-I.

Il s'agit d'un jugement porté sur le caractère acceptable ou non de chaque situation de risque, ainsi que cela a été présenté dans le document « *MEHARI 2010 – Principes fondamentaux et spécifications fonctionnelles* ».

Ce processus repose sur une grille d'acceptabilité des risques, ainsi que cela est indiqué dans le document cité ci-dessus.

Cette grille est un document stratégique essentiel et doit être définie pour chaque organisme. A défaut de réflexion spécifique, la base MEHARI contient une grille standard qu'il convient, a minima, de valider.

3 Le traitement des risques

Le traitement des risques consiste théoriquement à analyser chaque scénario de risque et à prendre des décisions spécifiques qui peuvent être de :

- Accepter le risque tel quel
- Réduire le risque c'est-à-dire prendre des mesures pour que l'impact ou la potentialité ou les deux soient réduits et diminuent la gravité résiduelle en conséquence
- Décider d'éviter le risque en supprimant la situation de risque par des mesures structurales ou organisationnelles
- Transférer le risque, essentiellement par l'assurance

En pratique, il est rationnel d'organiser le travail de manière structurée et, pour cela, plusieurs approches peuvent être envisagées, et, en particulier :

- Travailler par familles de scénarios ayant le même type d'actif et donc le même impact intrinsèque et sélectionner des plans d'action par famille
- Travailler par projets fédérateurs, chaque projet regroupant des services de finalités proches (contrôle d'accès physique, gestion des droits et des habilitations, etc.)
- Travailler par services en fonction d'une notion de « besoin de service ».

3.1 Sélection de plans d'action par famille de scénarios

Pour faciliter cette approche, les scénarios de la base de connaissances de MEHARI ont été regroupés en familles correspondant au même type d'actif et au même type de dommage.

Pour chaque famille, des plans d'action sont proposés (feuille Plans_d'action) et ce pour chaque type d'effet (dissuasion, prévention, confinement, palliation), chaque plan regroupant différents services pertinents pour la famille de scénarios considérée et fixant, pour chaque service, un niveau cible à l'issue du plan d'action.

Si l'option de prise en compte des objectifs pour l'appréciation des risques a été choisie, la sélection de plans d'action permet de simuler les niveaux de gravité des scénarios de risque à l'issue de ces plans.

Dès lors le processus conseillé consiste à

- sélectionner pour chaque famille les plans les plus efficaces (à cet effet, la base de connaissance donne, pour chaque plan, un indicateur d'efficacité reflétant le pourcentage de scénarios de la famille influencé par la mise en œuvre de ce plan)
- éventuellement modifier, pour le ou les plans sélectionnés, les cibles fixées aux services cités dans les plans sélectionnés,
- valider cette sélection de plans d'action (en visualisant les niveaux de risques à terme),
- puis à décider au cas par cas, pour les scénarios non réduits par cette première ou ces premières sélections, de :
 - sélectionner des mesures complémentaires
 - accepter le risque, au moins provisoirement
 - éviter le risque

- le transférer

Pour aider à dérouler ce processus, la base de connaissances de MEHARI propose différentes aides :

- Un panorama de l'ensemble des scénarios de risque par types d'actifs, faisant apparaître pour chaque classe d'actifs primaires et pour chaque critère de classification, le nombre de scénarios par niveaux de gravité. Des liens hypertexte permettent de passer facilement de ce panorama à telle ou telle classe d'actifs dans la feuille « Plans d'action »
- Un panorama des mêmes scénarios classés par types de menaces

3.2 Définition et sélection de projets

Il est également possible de définir des projets regroupant divers services, chaque projet indiquant :

- Les services dont l'amélioration fait partie du projet,
- Le niveau de qualité cible de ces services à l'issue du projet,
- La date d'achèvement du projet.

Ces projets sont pris en compte, pour évaluer le niveau des scénarios de risque, si l'option est choisie et si la date d'achèvement des projets est antérieure à une date de référence.

Ceci permet de faire des simulations à différentes époques et de définir ainsi un tableau de bord des risques.

La sélection des services et de leur cible dans chaque projet est libre et peut s'appuyer sur les plans d'action évoqués au paragraphe précédent ou sur toute autre notion telle que le besoin de service évoqué ci-dessous.

3.3 Besoin de service

On peut définir un indicateur de « besoin de service » tenant compte du nombre de scénarios faisant appel à un service donné, de la gravité de ces scénarios et de l'efficacité des plans dans lesquels ces services interviennent.

Il ne s'agit que d'un indicateur mais il est raisonnable d'envisager d'améliorer en priorité les services faisant apparaître le plus fort besoin.

3.4 Autres démarches

Bien d'autres démarches sont possibles, en particulier en sélectionnant des ensembles restreints de scénarios selon divers critères et en s'attaquant sélectivement à chaque sous-ensemble.

4 Conseils pratiques

4.1 Esprit de la démarche d'analyse de risque

Nous avons, volontairement, fait apparaître les automatismes de MEHARI comme des aides à l'évaluation du niveau de risque.

Il est fondamental de garder à l'esprit qu'il s'agit d'un processus d'évaluation et qu'un consensus obtenu par un groupe d'évaluation sera toujours plus fiable qu'un automatisme.

4.2 Composition du groupe d'évaluation des risques

La démarche telle que nous l'avons décrite, fonctionne d'autant mieux que l'évaluation des risques est faite par un groupe d'évaluation représentatif. La composition du groupe d'évaluation des risques a une certaine importance. Il devrait comprendre :

- Des utilisateurs du domaine concerné, et ceci à un niveau tel qu'ils puissent juger de l'atténuation réelle des conséquences pouvant être apportée par des mesures de sécurité.
- Des informaticiens capables d'éclairer le groupe d'évaluation sur l'efficacité réelle des diverses mesures de sécurité et sur les possibilités de contournement (robustesse et mise sous contrôle).
- Un animateur connaissant bien la méthode et compétent en sécurité des systèmes d'information.

4.3 Contrôle des automatismes

Nous avons dit que les automatismes ne devaient être considérés que comme des aides au processus d'évaluation. Ceci signifie qu'un contrôle a posteriori des calculs effectués devrait toujours être effectué afin que le groupe d'évaluation valide chaque résultat intermédiaire.

Ceci s'applique :

- A la cotation de la qualité des services de sécurité
- Aux facteurs de réduction des risques
- Aux évaluations d'impact résiduel calculé et de potentialité résiduelle calculée
- A la gravité résiduelle calculée des scénarios de risque

Pour ces contrôles, la confrontation des résultats calculés aux définitions données pour chaque niveau de chaque paramètre est la pratique à conseiller.

Annexe 1 :

Grille d'exposition naturelle standard

| Tableau des événements : types et exposition naturelle | | | | | | |
|---|-----------|---|----------|--------------------------------------|------------------------------|---------------------------------|
| Type | Code type | Événement | Code | Exposition naturelle standard CLUSIF | Exposition naturelle décidée | Exposition naturelle résultante |
| Absence accidentelle de personnel | AB.P | Absence de personnel de partenaire | AB.P.Pep | 3 | | 3 |
| | | Absence de personnel interne | AB.P.Per | 2 | | 2 |
| Absence ou indisponibilité accidentelle de service | AB.S | Absence de service : Énergie | AB.S.Ene | 3 | | 3 |
| | | Absence de service : Climatisation | AB.S.Cli | 2 | | 2 |
| | | Absence de service : Impossibilité d'accès aux locaux | AB.S.Loc | 2 | | 2 |
| | | Absence de maintenance applicative ou maintenance applicative impossible | AB.S.Maa | 3 | | 3 |
| | | Absence de maintenance système ou maintenance système impossible | AB.S.Mas | 2 | | 2 |
| Accident grave d'environnement | AC.E | Foudroiement | AC.E.Fou | 2 | | 2 |
| | | Incendie | AC.E.Inc | 2 | | 2 |
| | | Inondation | AC.E.Ino | 3 | | 3 |
| Accident matériel | AC.M | Panne d'équipement | AC.M.Equ | 3 | | 3 |
| | | Panne d'équipement de servitude | AC.M.Ser | 3 | | 3 |
| Absence volontaire de personnel | AV.P | Conflit social avec grève | AV.P.Gre | 2 | | 2 |
| Erreur de conception | ER.L | Bug bloquant dû à une erreur de conception ou d'écriture de programme (interne) | ER.L.Lin | 3 | | 3 |
| Erreur matérielle ou de comportement du personnel | ER.P | Perte ou oubli de document ou de media | ER.P.Peo | 3 | | 3 |
| | | Erreur de manipulation ou dans le suivi d'une procédure | ER.P.Pro | 3 | | 3 |
| | | Erreur de saisie ou de frappe | ER.P.Prs | 3 | | 3 |
| Incident dû à l'environnement | IC.E | Dégât dû au vieillissement | IC.E.Age | 2 | | 2 |
| | | Dégât des eaux | IC.E.De | 3 | | 3 |
| | | Surcharge électrique | IC.E.Se | 2 | | 2 |
| | | Dégât dû à la pollution | IC.E.Pol | 2 | | 2 |
| Incident logique ou fonctionnel | IF.L | Incident d'exploitation | IF.L.Exp | 3 | | 3 |
| | | Bug bloquant dans un logiciel système ou un progiciel | IF.L.Lsp | 2 | | 2 |
| | | Saturation bloquante pour cause externe (ver) | IF.L.Ver | 3 | | 3 |
| | | Virus | IF.L.Vir | 4 | | 4 |
| Malveillance menée par voie logique ou fonctionnelle | MA.L | Attaque en blocage de comptes | MA.L.Blo | 2 | | 2 |
| | | Effacement volontaire ou pollution massive de configurations systèmes | MA.L.Cfg | 2 | | 2 |
| | | Effacement volontaire direct de supports logiques ou physiques | MA.L.DeI | 2 | | 2 |
| | | Captation électromagnétique | MA.L.Ele | 3 | | 3 |
| | | Falsification logique (données ou fonctions) | MA.L.Fal | 3 | | 3 |
| | | Création de faux (messages ou données) | MA.L.Fau | 3 | | 3 |
| | | Rejeu de transaction | MA.L.Rej | 2 | | 2 |
| | | Saturation malveillante d'équipements informatiques ou réseaux | MA.L.Sam | 3 | | 3 |
| | | Destruction logique totale (fichiers et leurs sauvegardes) | MA.L.Tot | 2 | | 2 |
| Détournement logique de fichiers ou données (téléchargement ou copie) | MA.L.Vol | 3 | | 3 | | |
| Malveillance menée par voie physique | MA.P | Manipulation ou falsification matérielle d'équipement | MA.P.Fal | 2 | | 2 |
| | | Terrorisme | MA.P.Ter | 2 | | 2 |
| | | Vandalisme | MA.P.Van | 2 | | 2 |
| | | Vol physique | MA.P.Vol | 2 | | 2 |
| Procédures non conformes | PR.N | Procédures inadéquates | PR.N.Api | 2 | | 2 |
| | | Procédures inappliquées par manque de moyens | PR.N.Naa | 2 | | 2 |
| | | Procédures inappliquées par méconnaissance | PR.N.Nam | 2 | | 2 |
| | | Procédures inappliquées volontairement | PR.N.Nav | 2 | | 2 |

Annexe 2 :

Définition des niveaux d'exposition naturelle

Exposition naturelle au risque

Niveau 1 : L'exposition est très faible

Indépendamment de toute mesure de sécurité, la probabilité d'occurrence d'un tel scénario est extrêmement faible et pratiquement négligeable.

Niveau 2 : L'exposition est faible : l'unité est peu exposée.

Même en l'absence de toute mesure de sécurité, l'environnement (culturel, humain, géographique, ...) et le contexte (stratégique, concurrentiel, social, ...) font que la probabilité d'occurrence d'un tel scénario, à court ou moyen terme, est faible.

Niveau 3 : L'exposition est moyenne : l'unité n'est pas particulièrement exposée

L'environnement et le contexte de l'entreprise font que, si rien n'est fait pour l'empêcher, un tel scénario devrait se produire, à plus ou moins court terme.

Niveau 4 : L'exposition est forte : l'unité est particulièrement exposée.

L'environnement ou le contexte font que si rien n'est fait, un tel scénario se réalisera sûrement, vraisemblablement à court terme.

Annexe 3 :

Tableau d'impact intrinsèque

| Tableau d'Impact Intrinsèque | | | | |
|---|--|----------|----------|----------|
| Actifs de type Données et informations | | D | I | C |
| Données et informations | | | | |
| D01 | Fichiers de données ou bases de données applicatives | 3 | 3 | 4 |
| D02 | Fichiers bureautiques partagés | 3 | 3 | 3 |
| D03 | Fichiers bureautiques personnels (gérés dans environnement personnel) | 3 | 3 | 3 |
| D04 | Informations écrites ou imprimées détenues par les utilisateurs, archives personnelles | 3 | | 3 |
| D05 | Listings ou états imprimés des applications informatiques | | | 3 |
| D06 | Données échangées, écrans applicatifs, données individuellement sensibles | 3 | 3 | 4 |
| D07 | Courrier électronique | 3 | 3 | 4 |
| D08 | Courrier postal et télécopies | 3 | 3 | 4 |
| D09 | Archives patrimoniales ou documentaires | 3 | | 3 |
| D10 | Archives informatiques | 3 | 3 | 3 |
| D11 | Données et informations publiées sur des sites publics ou internes | 3 | 3 | 4 |
| Actifs de type Services | | D | I | C |
| Services généraux communs | | | | |
| G01 | Environnement de travail des utilisateurs | 3 | | |
| G02 | Services de télécommunication (voix, télécopies, visioconférence, etc.) | 3 | 2 | |
| Services informatiques et réseaux | | | | |
| R01 | Service du réseau étendu | 3 | 3 | |
| R02 | Service du réseau local | 3 | 3 | |
| S01 | Services applicatifs | 3 | 3 | 4 |
| S02 | Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.) | 3 | 3 | |
| S03 | Equipements mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.) Nota : Considérer ici la perte massive de ces services et non celle d'un seul utilisateur | 3 | | |
| S04 | Services systèmes communs : messagerie, archivage, impression, édition, etc. | 3 | 2 | |
| S05 | Services de publication d'informations sur un site web interne ou public | 3 | 2 | |
| Actifs de type Processus de gestion | | E | | |
| Processus de gestion de la conformité à la loi ou à la réglementation | | | | |
| C01 | Conformité à la loi ou aux réglementations relatives à la protection des renseignements personnels | 3 | | |
| C02 | Conformité à la loi ou aux réglementations relatives à la communication financière | 3 | | |
| C03 | Conformité à la loi ou aux réglementations relatives à la vérification de la comptabilité informatisée | 3 | | |
| C04 | Conformité à la loi ou aux réglementations relatives à la propriété intellectuelle | 3 | | |
| C05 | Conformité à la loi relative à la protection des systèmes informatisés | 3 | | |
| C06 | Conformité aux réglementations relatives à la sécurité des personnes et à la protection de l'environnement | 3 | | |
| Nota : Les cases grisées correspondent à des cas dans lesquels il n'y a généralement pas de classification à effectuer et pour lesquels il n'y a pas de scénario de risque dans la base Méhari. | | | | |
| Légende : | | | | |
| D | Disponibilité | | | |
| I | Intégrité | | | |
| C | Confidentialité | | | |
| E | Efficiencia (des processus de gestion, vis-à-vis de la conformité aux législations ou aux règlements). Pour ce critère, la grille de décision L pour l'impact sera utilisée. | | | |

Annexe 4 :

Définition des niveaux de facteurs de réduction de risque

Dissuasion

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

L'auteur 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.

Niveau 2 : L'effet dissuasif est moyen.

L'auteur 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 3 : L'effet dissuasif est important.

Un auteur 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 4 : L'effet dissuasif est très important.

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

Prévention

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.

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 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 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.

Confinement

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 il ne sera détecté qu'au bout d'un délai important.

Les mesures qui peuvent alors être prises n'ont qu'une influence très limitée sur le niveau des conséquences directes.

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

Si le sinistre pouvait être limité dans ses conséquences directes, le délai de détection n'est pas rapide et/ou les réactions sont tardives.

Les mesures qui peuvent alors être prises ont une influence réelle sur l'impact, mais l'ampleur des conséquences directes reste importante.

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

Le délai de détection est rapide et les réactions sont prises sans délai.

Les mesures qui peuvent alors être prises ont une influence réelle sur l'impact direct, qui est réel mais limité et circonscrit.

Niveau 4 : L'effet est très important.

Le début de sinistre est détecté en temps réel et les mesures déclenchées immédiatement.

Les conséquences directes seront limitées aux détériorations immédiates dues à l'accident, l'erreur ou l'acte volontaire.

Palliation

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

Les mesures seront totalement improvisées et/ou il est probable que leur effet en sera très faible.

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

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

Annexe 5 :

Grilles d'évaluation standards

Grilles d'élaboration des STATUS-P

1. Scénarios de type Accident

EXPO = 1

| | | | | |
|-----|---|---|---|---|
| D | | | | |
| I | | | | |
| S | | | | |
| S 1 | 1 | 1 | 1 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | R | E | V |

EXPO = 2

| | | | | |
|-----|---|---|---|---|
| D | | | | |
| I | | | | |
| S | | | | |
| S 1 | 2 | 2 | 2 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | R | E | V |

EXPO = 3

| | | | | |
|-----|---|---|---|---|
| D | | | | |
| I | | | | |
| S | | | | |
| S 1 | 3 | 3 | 2 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | R | E | V |

EXPO = 4

| | | | | |
|-----|---|---|---|---|
| D | | | | |
| I | | | | |
| S | | | | |
| S 1 | 4 | 4 | 2 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | R | E | V |

2. Scénarios de type Erreur

EXPO = 1

| | | | | |
|-----|---|---|---|---|
| D | | | | |
| I | | | | |
| S | | | | |
| S 1 | 1 | 1 | 1 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | R | E | V |

EXPO = 2

| | | | | |
|-----|---|---|---|---|
| D | | | | |
| I | | | | |
| S | | | | |
| S 1 | 2 | 2 | 2 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | R | E | V |

EXPO = 3

| | | | | |
|-----|---|---|---|---|
| D | | | | |
| I | | | | |
| S | | | | |
| S 1 | 3 | 3 | 2 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | R | E | V |

EXPO = 4

| | | | | |
|-----|---|---|---|---|
| D | | | | |
| I | | | | |
| S | | | | |
| S 1 | 4 | 4 | 2 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | R | E | V |

3. Scénarios de type action Volontaire

EXPO = 1

| | | | | |
|-----|---|---|---|---|
| D 4 | 1 | 1 | 1 | 1 |
| I 3 | 1 | 1 | 1 | 1 |
| S 2 | 1 | 1 | 1 | 1 |
| S 1 | 1 | 1 | 1 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | R | E | V |

EXPO = 2

| | | | | |
|-----|---|---|---|---|
| D 4 | 1 | 1 | 1 | 1 |
| I 3 | 2 | 2 | 1 | 1 |
| S 2 | 2 | 2 | 2 | 1 |
| S 1 | 2 | 2 | 2 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | R | E | V |

EXPO = 3

| | | | | |
|-----|---|---|---|---|
| D 4 | 2 | 2 | 1 | 1 |
| I 3 | 2 | 2 | 1 | 1 |
| S 2 | 3 | 3 | 2 | 1 |
| S 1 | 3 | 3 | 2 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | R | E | V |

EXPO = 4

| | | | | |
|-----|---|---|---|---|
| D 4 | 2 | 2 | 2 | 1 |
| I 3 | 3 | 3 | 2 | 2 |
| S 2 | 4 | 4 | 3 | 2 |
| S 1 | 4 | 4 | 3 | 2 |
| | 1 | 2 | 3 | 4 |
| | P | R | E | V |

Grilles d'élaboration des STATUS-I

Les scénarios non confinables sont évalués sur la ligne nc

1. Scénarios de type Disponibilité

II = 1

| | | | | |
|-----|---|---|---|---|
| C 4 | 1 | 1 | 1 | 1 |
| O 3 | 1 | 1 | 1 | 1 |
| N 2 | 1 | 1 | 1 | 1 |
| F 1 | 1 | 1 | 1 | 1 |
| nc | 1 | 1 | 1 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | A | L | L |

II = 2

| | | | | |
|-----|---|---|---|---|
| C 4 | 2 | 2 | 1 | 1 |
| O 3 | 2 | 2 | 1 | 1 |
| N 2 | 2 | 2 | 2 | 1 |
| F 1 | 2 | 2 | 2 | 1 |
| nc | 2 | 2 | 2 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | A | L | L |

II = 3

| | | | | |
|-----|---|---|---|---|
| C 4 | 2 | 2 | 1 | 1 |
| O 3 | 3 | 2 | 2 | 1 |
| N 2 | 3 | 3 | 2 | 1 |
| F 1 | 3 | 3 | 2 | 1 |
| nc | 3 | 3 | 2 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | A | L | L |

II = 4

| | | | | |
|-----|---|---|---|---|
| C 4 | 2 | 2 | 2 | 1 |
| O 3 | 3 | 3 | 2 | 1 |
| N 2 | 4 | 3 | 2 | 1 |
| F 1 | 4 | 3 | 2 | 1 |
| nc | 4 | 3 | 2 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | A | L | L |

2. Scénarios de type Intégrité

II = 1

| | | | | |
|-----|---|---|---|---|
| C 4 | 1 | 1 | 1 | 1 |
| O 3 | 1 | 1 | 1 | 1 |
| N 2 | 1 | 1 | 1 | 1 |
| F 1 | 1 | 1 | 1 | 1 |
| nc | 1 | 1 | 1 | 1 |
| | 1 | 2 | 3 | 4 |
| | P | A | L | L |

II = 2

| | | | | |
|-----|---|---|---|---|
| C 4 | 1 | 1 | 1 | 1 |
| O 3 | 2 | 2 | 1 | 1 |
| N 2 | 2 | 2 | 2 | 1 |
| F 1 | 2 | 2 | 2 | 1 |
| nc | 2 | 2 | 2 | 2 |
| | 1 | 2 | 3 | 4 |
| | P | A | L | L |

II = 3

| | | | | |
|-----|---|---|---|---|
| C 4 | 1 | 1 | 1 | 1 |
| O 3 | 2 | 2 | 1 | 1 |
| N 2 | 3 | 3 | 2 | 1 |
| F 1 | 3 | 3 | 2 | 1 |
| nc | 3 | 3 | 2 | 2 |
| | 1 | 2 | 3 | 4 |
| | P | A | L | L |

II = 4

| | | | | |
|-----|---|---|---|---|
| C 4 | 1 | 1 | 1 | 1 |
| O 3 | 2 | 2 | 2 | 1 |
| N 2 | 3 | 3 | 2 | 1 |
| F 1 | 4 | 3 | 2 | 1 |
| nc | 4 | 4 | 4 | 4 |
| | 1 | 2 | 3 | 4 |
| | P | A | L | L |

3. Scénarios de type Confidentialité

II = 1

| | | | | |
|-----|---|---|---|---|
| C 4 | 1 | | | |
| O 3 | 1 | | | |
| N 2 | 1 | | | |
| F 1 | 1 | | | |
| nc | 1 | | | |
| | 1 | | | |
| | P | A | L | L |

II = 2

| | | | | |
|-----|---|---|---|---|
| C 4 | 2 | | | |
| O 3 | 2 | | | |
| N 2 | 2 | | | |
| F 1 | 2 | | | |
| nc | 2 | | | |
| | 1 | | | |
| | P | A | L | L |

II = 3

| | | | | |
|-----|---|---|---|---|
| C 4 | 2 | | | |
| O 3 | 2 | | | |
| N 2 | 3 | | | |
| F 1 | 3 | | | |
| nc | 3 | | | |
| | 1 | | | |
| | P | A | L | L |

II = 4

| | | | | |
|-----|---|---|---|---|
| C 4 | 2 | | | |
| O 3 | 2 | | | |
| N 2 | 3 | | | |
| F 1 | 4 | | | |
| nc | 4 | | | |
| | 1 | | | |
| | P | A | L | L |

4. Scénarios de type Limitable

II = 1

| | | | | |
|-----|---|---|---|---|
| C 4 | 1 | | | |
| O 3 | 1 | | | |
| N 2 | 1 | | | |
| F 1 | 1 | | | |
| | 1 | | | |
| | P | A | L | L |

II = 2

| | | | | |
|-----|---|---|---|---|
| C 4 | 1 | | | |
| O 3 | 2 | | | |
| N 2 | 2 | | | |
| F 1 | 2 | | | |
| | 1 | | | |
| | P | A | L | L |

II = 3

| | | | | |
|-----|---|---|---|---|
| C 4 | 1 | | | |
| O 3 | 2 | | | |
| N 2 | 3 | | | |
| F 1 | 3 | | | |
| | 1 | | | |
| | P | A | L | L |

II = 4

| | | | | |
|-----|---|---|---|---|
| C 4 | 1 | | | |
| O 3 | 2 | | | |
| N 2 | 3 | | | |
| F 1 | 4 | | | |
| | 1 | | | |
| | P | A | L | L |



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