MEHARI

Guide de l'analyse et du traitement des risques

Avril 2022

CLUSIF

Table des matières

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, en s'appuyant sur des principes et des spécifications fonctionnelles précis rappelés ci-dessous.

1.1 Rappel des principes généraux de MEHARI

La volonté de pouvoir gérer individuellement les risques auxquels l'entreprise ou l'organisme est confrontée conduit à définir un certain nombre de principes et de spécifications, décrits dans le document *« MEHARI – 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 maximal 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.

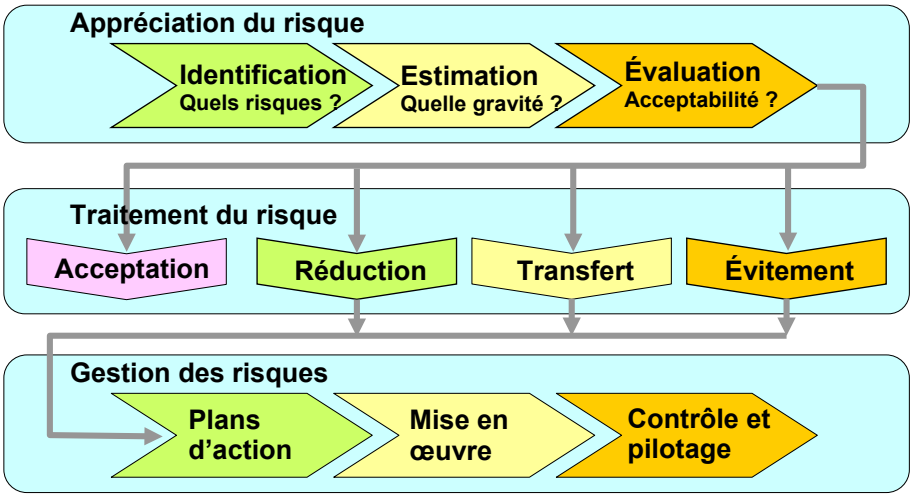

Figure 1 Etapes dans la gestion des risques

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 »).

1.2 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 – Principes fondamentaux et spécifications fonctionnelles »*.

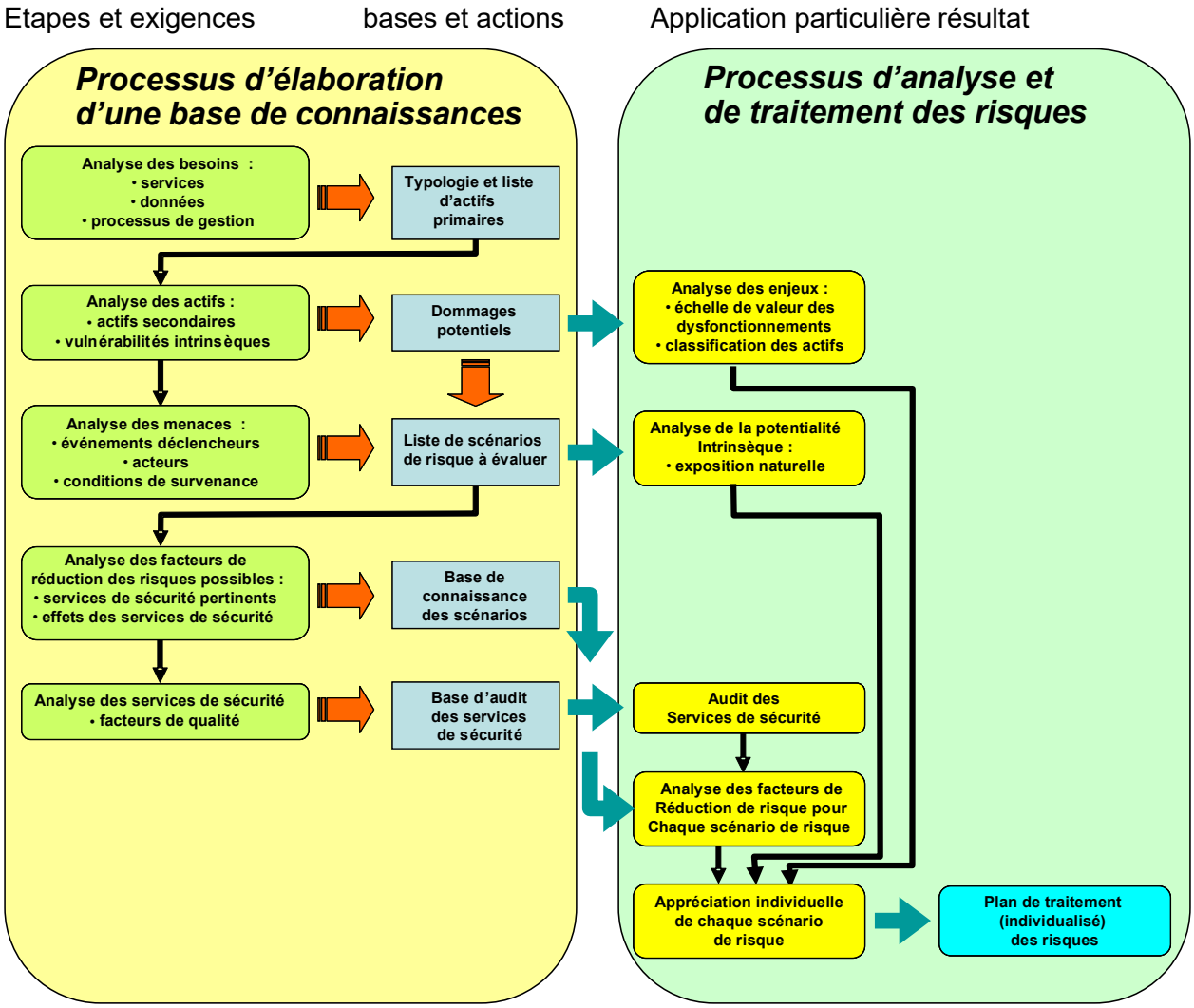

Figure 2 : Schéma général de planification du traitement des risques

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 une base de connaissances[1] de MEHARI, le guide relatif à la construction d'une base de connaissance étant reporté dans un autre document.

[1] Il existe plusieurs bases de connaissances Méhari (Méhari-Expert et Méhari-Standard) adaptées à des environnements divers et à des architectures plus ou moins complexes et étendues.

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 des bases de connaissances de scénarios de risque utilisables 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.

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
- Les types d'actif primaires concernés
- Le type d'incident, 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, Principes fondamentaux et spécifications fonctionnelles* ».

Les bases de connaissances de MEHARI contiennent un nombre variable de scénarios (180 environ pour MEHARI-Standard et près de 800 pour MEHARI-Expert).

Parmi 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, surtout pour les bases comportant un nombre important de scénarios, 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 :

- Certaines formes d'actifs
- Certains types d'événement

— Certains types d'incidents

La base de connaissances MEHARI-Standard et MEHARI-Expert permettent d'effectuer cette sélection. Pour ces bases, il est également possible d'effectuer une sélection directe des scénarios.

Mise en pratique avec les bases de connaissance MEHARI-Standard et MEHARI-Expert

En pratique :

- Les types d'actifs peuvent être sélectionnés directement dans la feuille « Classif » (dans la colonne sélection)
- Les types d'événements peuvent être sélectionnés, de même, dans la feuille « Expo »
- Les types de dommages peuvent être sélectionnés dans la feuille « Dommages »
- Les scénarios peuvent être sélectionnés ou désélectionnés dans la feuille « Scénarios »

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 - Principes fondamentaux et spécifications fonctionnelles » :*

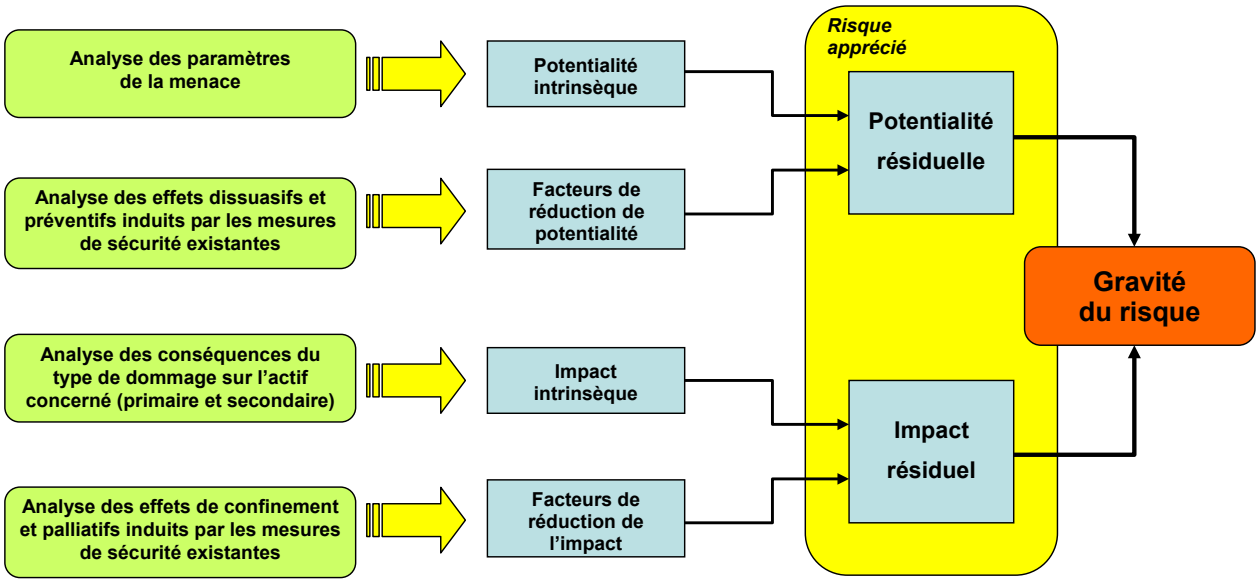

Figure 3 : Le processus d'estimation d'un risque

Les bases de connaissances de MEHARI offrent diverses assistances 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, confinement 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 – 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).

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 – Principes fondamentaux et spécifications fonctionnelles »* et qui sont rappelées en annexe.

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 les bases de connaissance MEHARI

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 :

- Sélectionner la feuille « Expo »
- 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 ou plusieurs actifs cibles de ce scénario. Chaque scénario indique clairement les types d'actif primaire et le type d'actif secondaire (voir « *MEHARI – 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, par exemple, 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'« efficience », 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 maximum de criticité ou de gravité résultant de la perte de disponibilité, d'intégrité, de confidentialité, ou de non-conformité selon le type de scénario, des types 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 scénarios de la base de connaissances. La démarche de classification est décrite dans le document *« MEHARI - Principes fondamentaux et Spécifications fonctionnelles »* et dans le « *Guide de l'analyse des enjeux et de la classification »*.

2.2.2.1Le tableau d'impact intrinsèque

La démarche d'évaluation des impacts intrinsèques peut donc être organisée et permet de remplir un tableau d'impact intrinsèque.

En pratique, ce tableau est repris automatiquement à partir de tableaux préliminaires, T1 et T2 pour MEHARI-Standard, T1, T2 et T3 pour MEHARI-Expert qu'il convient de remplir manuellement.

Le remplissage de ces tableaux s'effectue en transcrivant (par une valeur de 1 à 4) le niveau de conséquence maximale d'une atteinte à la disponibilité, l'intégrité ou la confidentialité de chaque type de données ou de services, pour un domaine d'activité.

Le détail de la démarche de remplissage des tableaux Ti est fourni dans le *« Guide de l'analyse des enjeux et de la classification ».*

Le tableau d'impact intrinsèque constitue une synthèse servant à définir le niveau d'impact intrinsèque de chaque scénario des bases de connaissances de MEHARI.

2.2.2.2 L'évaluation de l'impact intrinsèque des scénarios

L'évaluation de l'impact intrinsèque maximum 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, C ou E).

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 notée :

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 identifiant[2], 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 = 6B01

EFF-PREV = MAX (4B04; MIN(4B01;4B02;4B03))

La première formule signifie que l'efficacité (proposée) des mesures palliatives est directement fonction du service 6B01 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 4B04 et de la fonction représentant le minimum des services 4B01, 4B02, 4B03

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

[2] 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. 6B01)

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 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.

Les bases de connaissances de MEHARI fournissent 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 les bases sous Excel retiennent, pour le calcul des facteurs de réduction de risque, le minimum des valeurs obtenues pour chaque variante de service de sécurité.

Mise en pratique avec les bases de connaissance MEHARI

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 confinement 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 est conseillé 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 plutôt 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).

La base standard contient une valeur prédéfinie pour le caractère confinable des scénarios. Il est possible de modifier ce choix et de déclarer chaque scénario comme confinable ou non confinable

2.2.4 Évaluation de la potentialité et de l'impact résiduels

2.2.4.1Évaluation 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 Efficience

Ces grilles standards peuvent également être modifiées, si besoin est.

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.

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 les bases de connaissance MEHARI

En pratique, les valeurs calculées de la Potentialité et de l'Impact résiduels (après prise en compte des services de sécurité) sont indiquées 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 des scénarios de risque

La gravité de chaque scénario sera déduite des évaluations de leur Potentialité et de leur 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 – 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.

2.4 Panorama des risques

MEHARI propose un panorama des risques selon plusieurs visions :

Ces panoramas se trouvent dans les feuilles Risk%actif et Risk%event et dépendent en outre, pour MEHARI-Standard, d'une option de sélection :

- Panorama des risques intrinsèques, c'est-à-dire sans tenir compte des mesures de sécurité déjà en place et donc sans tenir compte de l'audit des services de sécurité
- Panorama des risques actuels tenant compte des services de sécurité déjà en place et de leur qualité telle qu'elle résulte de l'audit effectué
- Panorama des risques à terme, tenant compte des mesures (projets) prévues
- Panorama des risques à une date donnée tenant compte des projets planifiés (nouvelles mesures ou améliorations de services existants) achevés à cette date.

Deux modes de présentation globale des risques sont proposées : l'une globale, l'autre par domaine de scénarios de risques, ainsi que représenté ci-dessous.

Panorama des risques

résultant de l'option définie ci-dessus

Impact				
4	0	6	5	0
3	0	37	58	0
2	0	17	27	0
1	1	21	33	0
	1	2	3	4
				Potentialité

Panorama des gravités de scénarios

		Disponibilité					Intégrité					Confidentialité				
Actifs immatériels		N. 1	N. 2	N. 3	N. 4		N. 1	N. 2	N. 3	N. 4		N. 1	N. 2	N. 3	N. 4	
FIC	Fichiers de données ou de programmes, configurations des systèmes	3	16	4	0	>	1	0	18	0	>	8	0	12	0	>
DIT	Données isolées, messages ou données en transit	7	0	0	0	>	1	11	0	0	>	10	0	0	0	>
COU	Courriels	6	0	0	0	>	0	0	3	0	>	0	0	3	0	>
SIC	Services informatiques et de communication	0	3	2	1	>	2	0	8	0	>					
Actifs matériels																
ENV	Environnement de travail des utilisateurs	0	0	2	1	>										
IIR	Infrastructure informatique et réseaux	4	6	3	3	>										
EQU	Equipements mis à la disposition des utilisateurs (PC, imprimantes, périphériques, etc.)	4	0	0	0	>										
MED	Media supports de données ou de programmes	0	8	10	0	>	1	0	6	0	>	4	0	11	0	>
DOC	Documents écrits ou imprimés	0	0	11	0	>						0	0	8	0	>
Processus de management		Efficience														
ELC	Non conformité à la loi ou aux réglementations	4	0	0	0	>										
	Nombre de scénaios par niveaux de gravité :	28	33	32	5		5	11	35	0		22	0	34	0	

Nombre total de scénarios, hors scénarios évités, transférés ou acceptés : 205

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 :

- 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 structurelles ou organisationnelles
- Transférer le risque, essentiellement par l'assurance
- Accepter le risque tel quel

En pratique, il est rationnel d'organiser le travail de manière structurée et de commencer par la mise en place de mesures propres à réduire le maximum de risques à un niveau acceptable, puis s'il en reste quelques-uns dont la réduction s'avère difficile ou trop onéreuse, d'analyser s'il est possible de les éviter ou de les transférer ou enfin s'il faut les accepter.

Pour la réduction des risques, MEHARI propose de travailler par « Plans d'action » ou par « projets », sélectionnés et décidés selon des processus qui peuvent varier d'une version de base de connaissances à l'autre.

Un projet ou un plan comprend un ou plusieurs services de sécurité, avec pour les services inclus dans le projet, un objectif cible de qualité (comprenant l'efficacité du service, sa robustesse et sa mise sous contrôle).

Il s'agit généralement d'un ensemble de services qu'il est cohérent de traiter ensemble, tel que, par exemple :

- La gestion des supports amovibles, la sécurité physique des médias et la sécurité des médias en transit
- La sécurité des équipements de servitude, la continuité de la fourniture de l'énergie et la sûreté de fonctionnement des éléments d'architecture
- La sûreté de fonctionnement des éléments de l'architecture externalisée et la sauvegarde des données externalisées

La planification de la réduction des risques consiste ainsi à :

- Sélectionner ou présélectionner un ensemble de plans ou de projets décrits dans la base de connaissances
- Vérifier qu'avec la mise en place de ces plans ou projets les risques à réduire sont bien ramenés à un niveau acceptable
- Décider quels projets seront engagés et les budgéter
- Planifier ces projets en déterminant une date de début et une date de fin

Le détail des aides fournies par les différentes versions de MEHARI dans ce processus est fourni dans des documents séparés et spécifiques de chaque base de connaissances.

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 :
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 2 :
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 3 :
Grilles d'évaluation standards

Grilles d'élaboration des STATUS-P

1. Scénarios de type Accident

EXPO = 1

DISS	1	2	3	4
4				
3				
2				
1	1	1	1	1
	P	R	E	V

EXPO = 2

DISS	1	2	3	4
4				
3				
2				
1	2	2	2	1
	P	R	E	V

EXPO = 3

DISS	1	2	3	4
4				
3				
2				
1	3	3	2	1
	P	R	E	V

EXPO = 4

DISS	1	2	3	4
4				
3				
2				
1	4	4	2	1
	P	R	E	V

2. Scénarios de type Erreur

EXPO = 1

DISS	1	2	3	4
4				
3				
2				
1	1	1	1	1
	P	R	E	V

EXPO = 2

DISS	1	2	3	4
4				
3				
2				
1	2	2	2	1
	P	R	E	V

EXPO = 3

DISS	1	2	3	4
4				
3				
2				
1	3	3	2	1
	P	R	E	V

EXPO = 4

DISS	1	2	3	4
4				
3				
2				
1	4	4	2	1
	P	R	E	V

3. Scénarios de type action Volontaire

EXPO = 1

DISS	1	2	3	4
4	1	1	1	1
3	1	1	1	1
2	1	1	1	1
1	1	1	1	1
	P	R	E	V

EXPO = 2

DISS	1	2	3	4
4	1	1	1	1
3	2	2	1	1
2	2	2	2	1
1	2	2	2	1
	P	R	E	V

EXPO = 3

DISS	1	2	3	4
4	2	2	1	1
3	2	2	1	1
2	3	3	2	1
1	3	3	2	1
	P	R	E	V

EXPO = 4

DISS	1	2	3	4
4	2	2	2	1
3	3	3	2	2
2	4	4	3	2
1	4	4	3	2
	P	R	E	V

Grilles d'élaboration des STATUS-I

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
		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
		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
		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
		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
		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
		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
		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
		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			
		1			
		P	A	L	L

		II = 2			
C	4	2			
O	3	2			
N	2	2			
F	1	2			
		1			
		P	A	L	L

		II = 3			
C	4	2			
O	3	2			
N	2	3			
F	1	3			
		1			
		P	A	L	L

		II = 4			
C	4	2			
O	3	2			
N	2	3			
F	1	4			
		1			
		P	A	L	L

4. Scénarios de type Efficience

		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
		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
		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
		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
		1	2	3	4
		P	A	L	L

Tour Eria
5 rue Bellini
92821 Puteaux cedex
✆ + 33 1 53 25 08 80
clusif@clusif.fr

Téléchargez les bases de connaissances et la documentation de Méhari sur

https://clusif.fr/