

METHODES



MEHARI 2010

Évolutions par rapport aux versions précédentes

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

Ce document décrit les évolutions de MEHARI version 2010 par rapport à la précédente version (MEHARI 2007).

L'axe général d'évolution est la mise en conformité avec l'ISO/IEC 27005 : 2008, accompagnée d'une volonté de clarification des principes et de positionnement clair de MEHARI comme méthode de gestion de risques.

1. Positionnement de MEHARI

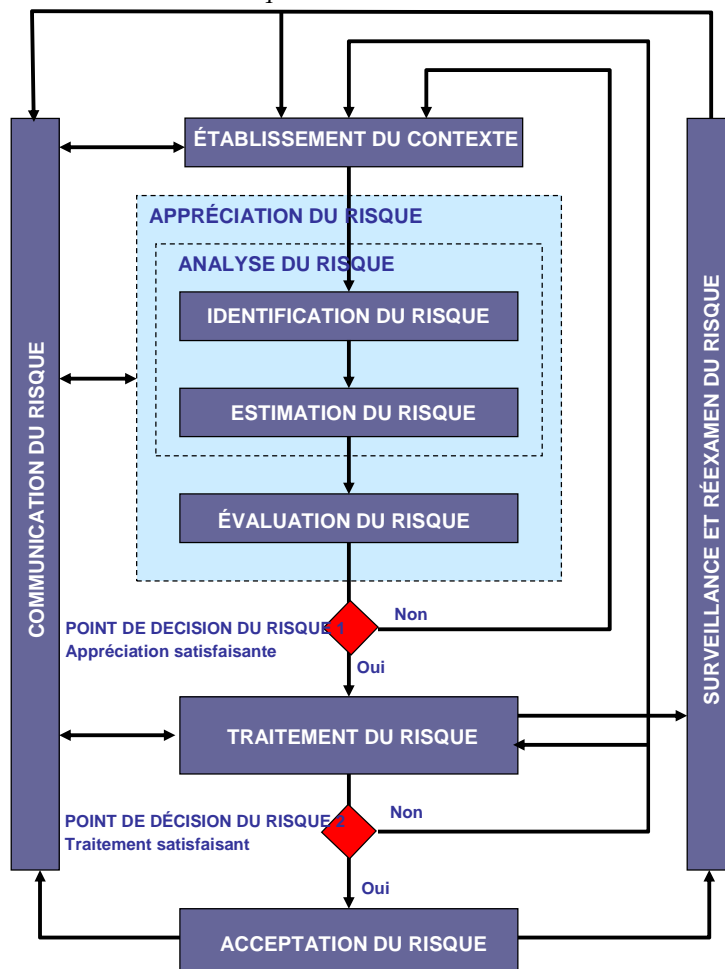
MEHARI a toujours été conçu comme une méthode permettant de gérer les risques de l'entreprise ou de toute sorte d'organisme, mais aussi comme une boîte à outils générale utilisable par des RSSI pour gérer la sécurité de l'information.

Tout en gardant cet objectif généraliste, MEHARI 2010 se positionne clairement comme étant une méthode d'analyse et de gestion de situations de risques, situations décrites par des scénarios de risque.

La capacité à gérer directement et de manière individualisée des situations de risque est ainsi établie comme un principe fondateur de la méthode et cela a des conséquences directes que nous décrirons dans ce document.

2. Mise en conformité avec la norme ISO/IEC 27005

Le schéma général présenté par la norme ISO/IEC 27005 et rappelé ci-dessous, est repris de la norme précédente ISO 13335 qui avait servi de référence à MEHARI dès l'origine.



Itération finale, première itération ou itérations ultérieures

Ensuite le cadre de description du risque par l'ensemble actif, vulnérabilité(s) et menace doit être pris en compte

Les points ci-dessus ont diverses conséquences, intégrées dans MEHARI 2010 et décrites ci-dessous.

2.1 Traitement des mesures de récupération et de transfert du risque

Pour se conformer totalement à la norme, il a été décidé de reporter le transfert du risque dans le traitement des risques.

Les mesures de récupération disparaissent donc des formules de réduction du risque.

Les questions relatives aux assurances sont cependant conservées et traitées en mesures générales.

Les grilles de décision ont été adaptées en conséquence : l'impact résiduel est déduit directement de l'impact intrinsèque et de l'efficacité des mesures de confinement (plutôt que de protection : voir plus loin) et palliatives (le STATUS-RI disparaît donc lui aussi).

2.2 La description des actifs

La définition des actifs donnée par l'ISO/IEC 27005 (par 8.2.1.2) est la suivante :

« Un actif désigne tout élément ayant de la valeur pour l'organisme et nécessitant par conséquent une protection. Concernant l'identification des actifs, il convient de garder à l'esprit qu'un système d'information ne comprend pas uniquement du matériel et des logiciels. »

L'annexe B de la norme précise :

« Afin de procéder à l'évaluation des actifs, il est nécessaire pour un organisme d'identifier ses actifs (à un niveau de détail approprié). Il est possible de distinguer deux types d'actifs :

- *les actifs primordiaux :*
 - *processus et activités métier,*
 - *informations ;*
- *les actifs en support (sur lesquels reposent les actifs primordiaux du domaine d'application) de tous les types :*
 - *matériel,*
 - *logiciels,*
 - *réseau,*
 - *personnel,*
 - *site,*
 - *structure de l'organisme. »*

La décomposition citée par la norme n'étant que proposée (il est possible de ...), MEHARI a choisi de distinguer comme **actifs primaires** (plutôt que primordiaux, mot qui véhicule une connotation d'importance) :

- Les services (par ailleurs cités comme types d'actifs dans l'ISO 27000),
- Les données,
- Les processus de management ou de gestion.

Ces items répondent bien à l'idée forte de la norme de s'attacher en priorité aux fondamentaux de l'organisme, mais répondent mieux à l'idée des **besoins** qu'il faut protéger.

L'activité métier est un point d'entrée mais non un besoin. Par contre les services nécessaires à l'exercice de l'activité sont bien des besoins, de même que les données (et leur historique) qui sont nécessaires à la mise en œuvre des services.

L'introduction à ce niveau des processus de management vise à pouvoir gérer les non conformités à des réglementations, lois ou cadres imposés.

Il est bien sûr nécessaire de décrire ensuite la matérialisation de ces actifs primaires, sans laquelle il ne serait pas possible d'aborder les vulnérabilités.

MEHARI 2010 introduit ici la notion d'**actifs secondaires** (ou de support)

Il s'agit ici de décrire toutes les contingences dont peuvent dépendre les actifs primaires (en particulier de service) mais aussi toutes les formes que peuvent revêtir ces actifs (en particulier pour les données).

On notera, en particulier, que l'appel à la notion de contingence permet de faire apparaître des aspects qui pourraient rester dans l'ombre tels que des moyens d'accès aux services (comptes utilisateurs), des moyens d'accès aux données (clés de déchiffrement), des prestations extérieures, etc.

On notera également que ces options permettent de mettre en évidence des différences telles que des données vivantes, des données d'archive ou des données publiées sur des sites Internet.

Partant de ces définitions, les tableaux de description des actifs et de leur classification sont donc modifiés dans la version 2010.

2.3 La description des vulnérabilités

La notion de vulnérabilité, est définie ainsi dans la norme ISO/IEC 27000 :

« **Faible dans un *actif* ou dans une *mesure de sécurité* qui peut être exploitée par une *menace* »**

Cette définition comporte deux aspects forts différents :

- celui de caractéristique intrinsèque d'un actif qui peut être exploitée par une menace
- celui de faiblesse dans un dispositif de sécurité

Or, si l'on cherche à identifier de nouveaux risques (ou simplement tous les risques auxquels l'organisme est confronté), ce qui est une étape importante de la démarche d'analyse et de gestion des risques, partir des faiblesses des dispositifs de sécurité suppose que l'on connaisse ces dispositifs ce qui n'est pas forcément le cas pour de nouveaux risques.

Par contre, la notion de vulnérabilité, en ne retenant que son premier sens, peut être très utile, si ce n'est nécessaire, et est déjà utilisée sans être mise en avant, dans les travaux passés ayant servi à développer et décrire les scénarios de risque.

Afin qu'il n'y ait plus d'ambiguïtés, MEHARI introduit, avec la version 2010, deux définitions différentes des vulnérabilités :

- Une « **vulnérabilité intrinsèque** » est une caractéristique intrinsèque d'un actif pouvant être exploitée par une menace.
- Une « **vulnérabilité contextuelle** » est une faiblesse dans un dispositif de sécurité pouvant être exploitée par une menace.

L'identification des risques s'appuie exclusivement sur la notion de vulnérabilité intrinsèque, alors que les vulnérabilités contextuelles ont un rôle dans l'appréciation des risques.

La base de connaissances de MEHARI 2010 a été créée en s'appuyant sur ces définitions et la base de scénarios décrit précisément la vulnérabilité intrinsèque exploitée pour chaque scénario.

2.4 La description des menaces

La notion de menace elle-même méritait d'être précisée.

MEHARI 2010 introduit donc de manière formelle les éléments qui la constituent à savoir :

- Un événement déclencheur,
- Des circonstances de survenance comprenant divers aspects :
 - Lieu de survenance,
 - Période ou époque de survenance,
 - Phase ou étape dans un processus,
- Type d'acteur.

Ces éléments étaient, de tout temps, présents dans les scénarios de risque MEHARI, mais ils n'étaient pas aussi formalisés et n'étaient mentionnés que dans le libellé des scénarios. Ils sont désormais clairement indiqués dans des colonnes spécifiques de la base de scénarios.

On notera que ces divers aspects sont souvent des points clés pour évaluer la probabilité de survenance d'un scénario de risque et que leur présence renforce l'objectif d'apprécier individuellement des situations de risque et leur niveau de risque.

Nota : le tableau d'exposition naturelle se trouve désormais reporté dans un onglet de la base de connaissances intitulé « Evénements types », le tableau portant le nom de « Tableau des événements : types et exposition naturelle »

2.5 Identification et description des scénarios de risque

La description des scénarios de risque devient ainsi, avec MEHARI 2010, très structurée et précise :

- Un type d'actif primaire (qui correspond à un élément du tableau d'impact intrinsèque) précisé par :
- Une « **vulnérabilité intrinsèque** » décrite par :
 - un type d'actif secondaire,
 - un type de dommage,
- Un type de menace décrit par :
 - un événement déclencheur,
 - des circonstances de lieux, de temps ou de processus,
 - un type d'acteur.
- Un libellé permettant de comprendre le scénario par une description globale.

3. Évolutions dans certains processus d'analyse

Les retours d'expérience et les remarques de praticiens de la méthode ont amené un certain nombre d'évolutions décrites ci-dessous.

3.1 *Évolution des mesures de limitation directe d'impact*

Ces mesures, appelées mesures de protection jusqu'ici, recouvrent deux types de mécanismes :

- Des mécanismes tendant à interrompre des sinistres évolutifs (incendie, propagation d'erreur, etc.) par des mesures de détection puis de réaction,
- Des mécanismes de limitation d'impact de scénarios évolutifs ou non, par des mesures de fragmentation, de limitation de degrés de liberté de certaines variables, etc.

Par ailleurs, dans ce deuxième cas, et pour des scénarios qui n'auraient pas de mesures palliatives possibles, les grilles de décision précédentes présentaient quelques difficultés.

Afin de tenir compte de ces observations, les évolutions suivantes ont été apportées, à partir de la version 2010 :

- **Les mesures de protection sont désormais appelées mesures de confinement (ce qui regroupe les divers aspects cités plus haut).**
- **Les scénarios auparavant déclarés non évolutifs deviennent des scénarios non confinables.**
- **Une grille supplémentaire destinée aux scénarios confinables, sans mesures palliatives, a été élaborée.**

3.2 *Distinction entre données individuellement sensibles et ensembles de données*

La distinction entre données isolées et ensembles de données n'était faite que pour les écrans applicatifs ou les données en transit, et essentiellement pour la confidentialité. Or il apparaît que la classification même des données peut faire apparaître une différence d'impact, tous critères confondus, entre une atteinte à une ou quelques données isolées ou à un ensemble de données.

Les données individuellement sensibles sont donc considérées, à partir de la version 2010, comme une classe d'actifs primaires spécifique (D06).

Elles font donc l'objet d'une classification et apparaissent dans les tableaux correspondants (T1 et Tableau d'impact intrinsèque).

3.3 *Traitement des scénarios de confidentialité dits « évolutifs »*

La base de connaissances précédente contenait un certain nombre de scénarios d'atteinte à la confidentialité dits « évolutifs » (*copie répétée de fichiers par ...*), avec des possibilités de mesures de confinement permettant de réduire l'impact. Le problème signalé est que rien ne permet de dire si l'impact intrinsèque de la divulgation du fichier de données (dans cet exemple) a été évalué pour une copie répétée ou pour une simple divulgation unique (du moins si l'on fait une évaluation de l'impact intrinsèque à partir d'une classification).

Il a été donc jugé plus prudent de modifier les scénarios correspondants pour parler de copie de fichier (sans notion de répétition) et de les considérer comme non évolutifs (quitte à laisser la

possibilité de revenir sur ce point, ce qui suppose que l'on conserve les mesures de confinement pouvant être efficaces, tout en déclarant par défaut le scénario non évolutif ou non confinable).

Les scénarios d'atteinte à la confidentialité sont, a priori, considérés comme non confinables.

3.4 Traitement des scénarios d'intégrité

Quand on analyse des scénarios d'atteinte à l'intégrité, on traite, en pratique, plusieurs types de scénarios :

- Les scénarios d'atteinte à l'intégrité d'une base de données ou de fichiers, pour lesquels, une fois le défaut d'intégrité détecté, les mesures palliatives consistent à réparer les fichiers ou bases endommagées pour pouvoir redémarrer sur des bases saines. Ces scénarios peuvent être évolutifs (confinables) ou non.
- Les scénarios de type fraude pour lesquels il n'y a guère de mesures palliatives et qui, le plus souvent, ne sont pas évolutifs (l'impact maximum est atteint dès l'action consommée) mais pour lesquels il existe des mesures de limitation d'impact direct (contrôles permanents, seuils de détection, etc.) qui font qu'ils doivent être considérés comme confinables.
- Certains scénarios d'erreurs ou d'accident ayant le même type de conséquences qu'une fraude, c'est-à-dire un impact limitable ou confinable, sans mesures palliatives possibles.

Les premiers sont, en fait, très proches des scénarios d'atteinte à la disponibilité ; la cause initiale est bien un défaut d'intégrité mais dès que ceci est connu, on se trouve ramené à un problème de disponibilité.

Ces scénarios sont intitulés « Pollution massive de données » et sont dorénavant traités comme des scénarios d'atteinte à la disponibilité.

Par contre, pour les scénarios d'atteinte à l'intégrité de type fraude ou équivalent (deuxième et troisième type cités ci-dessus), on considère que le défaut d'intégrité n'est pas connu et qu'il n'y a pas de service pertinent en mesure palliative susceptible de réduire l'impact. Par contre des mesures de confinement restent possibles.

Les scénarios d'atteinte à l'intégrité sont considérés comme confinables mais ne font pas appel, en standard, à des mesures palliatives.

La grille d'évaluation de l'impact pour les scénarios d'intégrité est maintenue (pour les cas où des mesures palliatives existeraient) et alignée sur la grille des scénarios confinables.

Les scénarios d'atteinte frauduleuse à l'intégrité de données individuellement sensibles peuvent ainsi s'adresser aux données de type D06 et non D01 ou D02 alors que les scénarios de pollution de bases de données continueront à référencer les données D01.

3.5 Scénarios de dégradation de performances

La notion de dégradation de performances était difficile à apprécier en termes d'impact.

Les scénarios de « dégradation de performances » sont remplacés par « blocage résultant de surcharges ».

4. Évolution de la base de connaissances

4.1 Évolution de la base de scénarios

La base de scénario a fait l'objet d'une reprise complète par une analyse exhaustive (autant que faire se peut) des combinaisons possibles de types d'actifs, primaires et secondaires, types de vulnérabilités et types de menaces (voir § 2.5).

Le nombre de scénarios de la nouvelle base est ainsi proche de 800.

Chaque scénario explicite chaque élément caractéristique.

4.2 Évolution de la base de questionnaires d'audit

Les questionnaires d'audit ont été repris avec trois objectifs :

- Eclater les questions qui paraissaient multiples et pouvaient présenter des ambiguïtés.
- Faire apparaître en face de chaque question des indications relatives au type de question et à son niveau d'expertise (en particulier pour pouvoir bâtir des questionnaires différents selon le niveau d'avancement et de maturité en sécurité de l'entité).
- Éviter les termes pouvant être mal interprétés ou mal compris au Québec.
- Revoir les pondérations des questions

De nouveaux domaines ont également été créés :

- Domaine spécifique à la gestion du parc des équipements des utilisateurs.
- Domaine spécifique à l'exploitation des télécommunications.
- Domaine des non conformités de processus de management (en remplacement de l'ancien domaine juridique).
- Domaine du système de management de la sécurité de l'information (SMSI).

La nouvelle base d'audit comprend ainsi :

- 14 domaines
- Environ 300 services de sécurité

Remarque : Quelques pondérations ayant été revues, les résultats de diagnostics effectués avec une base précédente peuvent être différents de ceux réalisés avec la base 2010.

4.3 Fonctions de calcul incorporées dans la base de connaissances

Des fonctions de calcul et de simulation ont été incorporées (base Excel) :

- Calcul de la qualité des services de sécurité,
- Calcul des facteurs de réduction de risques (en fonction de la qualité des services de sécurité),
- Calcul de la gravité intrinsèque et résiduelle des scénarios,
- Possibilité de simuler des sélections de plans d'action de sécurité et de voir l'effet de ces sélections sur les niveaux de gravité résiduelle (projetée) des scénarios.



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