



# MEHARI 2007

## Présentation générale

## *Remerciements*

Le CLUSIF remercie Jean-Philippe Jouas et Jean-Louis Roule qui ont bien voulu rédiger ce document présentant l'utilisation de MEHARI pour le management de la sécurité et en autoriser la publication par le CLUSIF.

# 1. Introduction

MEHARI a été initialement conçu et est en constant développement pour aider les RSSI<sup>1</sup> dans leur tâche de management de la sécurité de l'information et des systèmes d'information. Cette présentation générale leur est ainsi principalement destinée, mais elle s'adresse également aux auditeurs ou aux Risk Managers qui partagent, dans une large mesure, les mêmes préoccupations.

Cette présentation vise principalement à décrire les utilisations que l'on peut faire de MEHARI, étant entendu qu'une description plus complète de la méthode et de ses outils est fournie dans la documentation du CLUSIF, à savoir :

- La présentation des principes et mécanismes de MEHARI,
- Trois guides d'utilisation, respectivement pour l'analyse des enjeux, le diagnostic des services de sécurité et l'analyse des risques,
- Des manuels de référence (services de sécurité et scénarios de risque) et des bases de connaissance.

L'objectif de MEHARI est donc de fournir une gamme d'outils adaptée au management de la sécurité. Or, celui-ci se concrétise par un ensemble d'actions qui ont, chacune, des objectifs particuliers.

Parmi les actes de management citons :

- L'élaboration de plans de sécurité, ou de schémas directeurs.
- La mise en place de règles ou politiques de sécurité, que nous regrouperons sous l'appellation de « Référentiel de Sécurité ».
- La conduite de diagnostics, rapides ou approfondis sur l'état de la sécurité.
- L'évaluation et le management des risques
- La gestion de la sécurité dans la conduite de projets de développement.
- La sensibilisation et la formation à la sécurité.
- Le pilotage de la sécurité et le contrôle des actions décidées.

Ces différents actes de management et leurs variantes ne sont pas exclusifs, mais au contraire des actions pouvant être menées simultanément ou successivement, par des entités distinctes ou par la même entité, en fonction de besoins ponctuels ou permanents, indépendamment ou comme parties d'un programme d'ensemble.

En outre, les mêmes actes de management peuvent être conduits différemment selon :

- la maturité de l'entreprise et de son personnel en termes de sécurité,
- la volonté d'impliquer plus ou moins fortement les managers opérationnels dans les prises de décision concernant la sécurité de l'information,
- la culture de l'entreprise : hiérarchique et « technocratique » (il existe des règlements et ils sont appliqués) ou, au contraire, décentralisée et responsabilisante.

---

<sup>1</sup> RSSI : Responsable de la Sécurité des Systèmes d'Information

Dans ces conditions, il importe de trouver dans un ensemble méthodologique les outils adaptés à chaque situation et que ces outils soient cohérents et reliés les uns aux autres de sorte qu'ils se complètent sans duplication excessive de tâches et de charges.

MEHARI propose cet ensemble méthodologique cohérent, faisant appel à des bases de connaissance adaptées, et capable d'accompagner les responsables d'entreprise et les responsables de la sécurité dans leurs différentes démarches et actions, ainsi que les acteurs impliqués dans la réduction des risques.

L'objet principal de cette présentation est de décrire les utilisations que l'on peut faire de MEHARI. Le positionnement de MEHARI vis-à-vis des normes internationales est abordé en fin de document.

# 2. Utilisations de MEHARI

MEHARI est, avant tout, une méthode d'analyse et de management de risques.

En fait, cela veut dire que MEHARI et l'ensemble de ses bases de connaissance sont bâtis pour permettre une analyse précise des risques, quand cela sera jugé nécessaire, sans pour autant imposer l'analyse de risque comme une politique majeure de management.

En effet, le management de la sécurité est une fonction ou une activité qui évolue au cours du temps et les actes de management ne sont pas de même nature selon que l'entreprise n'a encore rien fait dans ce domaine ou, au contraire, qu'elle a déjà accompli des efforts substantiels.

Lors des premiers pas dans une démarche de sécurité, il sera sans doute bon de faire un bilan de l'état de la sécurité et de comparer ce bilan à un « norme » pour mettre en évidence le fossé à combler.

Ensuite, ce bilan fait et la décision prise de mettre en place une démarche sécuritaire, des actions concrètes devront être décidées. Ces décisions, qui seront le plus souvent regroupées dans des plans, schémas directeurs, référentiels ou politiques de sécurité, devront être prises dans le cadre d'une approche structurée. Une telle approche peut être basée sur une analyse des risques, ou inclure des concepts de risques, mais cela n'est pas obligatoire et il existe bien d'autres voies, dont l'alignement sur une « norme », que cette norme soit interne, professionnelle ou interprofessionnelle.

Il reste que, dès ce stade, et sans véritablement parler d'analyse de risque, la question des enjeux de la sécurité se pose. Bien souvent, en effet, quelle que soit la manière dont la décision a été préparée, le décideur ultime qui doit allouer le budget correspondant aura cette question : « est-ce bien nécessaire ? ». Sans analyse préliminaire des enjeux et sans consensus sur ce point, beaucoup de projets de sécurité sont abandonnés ou repoussés.

Souvent plus tard, mais parfois dès l'origine d'une démarche de sécurité, la question se pose du niveau de risque auquel est exposé l'entreprise ou l'organisme, et cette question se pose en ces termes : « A-t-on identifié tous les risques auxquels l'organisme est exposé et a-t-on l'assurance que leur niveau est acceptable ? ». Cette question peut, en outre, être posée dans toute sa généralité ou dans le cadre limité d'un nouveau projet. Il faudra alors utiliser une méthode d'analyse des risques.

Le principe sur lequel est fondé MEHARI est que les outils nécessaires, à chaque étape du développement de la sécurité, doivent être cohérents, c'est-à-dire que les résultats acquis à un stade donné doivent pouvoir être réutilisés ultérieurement.

Les différents outils et modules de l'ensemble méthodologique MEHARI, conçus pour pouvoir supporter l'analyse des risques, sont utilisables indépendamment les uns des autres, à tous les stades de développement de la sécurité, dans différents modes de management, et garantissent une cohérence d'ensemble des décisions.

Ces différents modules et outils, qui sont décrits brièvement ci-dessous, comprennent des modules de diagnostic de l'état de la sécurité, un module d'analyse des enjeux et une méthode d'analyse de risques avec des outils associés.

## 2.1. *Les diagnostics de sécurité*

Il existe deux modules de diagnostic dans l'ensemble MEHARI :

- Un module de diagnostic rapide<sup>2</sup>

---

<sup>2</sup> Ce module est en cours de développement.

## — Un module de diagnostic approfondi

Dans l'un et l'autre cas l'objectif est d'évaluer un niveau de sécurité. En pratique, le diagnostic portera sur l'état de services de sécurité. Il est clair que si le diagnostic est rapide la précision sera moindre et que si le diagnostic est approfondi, on peut attendre un résultat plus fiable.

Le premier module est utilisable lors d'une première approche, pour mettre en évidence les faiblesses majeures. Les services de sécurité abordés sont les mêmes que ceux du diagnostic approfondi, mais les questions visent à savoir si la fonction de sécurité a été mise en place, sans chercher à vérifier si elle présente des points faibles. En ce sens, les points faibles mis en évidence le sont certainement, alors que les points forts éventuels ne peuvent être garantis.

Le module de diagnostic approfondi recherche, de surcroît, toutes les faiblesses possibles de chaque service de sécurité. Il constitue une base d'expertise, pouvant être le support d'une analyse de risque.

La cohérence de ces deux modules permet de partir du premier et d'approfondir, à tout moment, tel ou tel point pour lequel on voudrait une meilleure assurance.

Ces modules de diagnostic peuvent être utilisés de diverses manières.

### ***2.1.1 Le diagnostic de sécurité, élément d'une analyse des risques***

MEHARI propose une méthode structurée d'analyse des risques qui sera présentée plus loin.

Disons simplement, à ce niveau, que le modèle de risque prend en compte des « facteurs de réduction de risque », précisément concrétisés par des services de sécurité.

Le diagnostic approfondi de ces services sera donc, lors de l'analyse des risques, un élément important d'assurance que les services remplissent bien leur rôle, ce qui est essentiel pour qu'une analyse de risque soit crédible.

### ***2.1.2 Les plans de sécurité basés sur un diagnostic de sécurité***

Une démarche relativement répandue consiste à bâtir des plans d'action directement à partir d'un diagnostic de l'état de la sécurité.

Le processus de management de la sécurité par le diagnostic de l'état des services de sécurité est extrêmement simple : on déclenche un diagnostic et on décide d'améliorer tous les services qui n'ont pas un niveau de qualité suffisant.

L'utilisation d'une analyse préalable des enjeux est également prévue, faisant ainsi la liaison avec cet autre module de MEHARI, présenté plus loin dans ce document.

Les différentes étapes et les conseils de mise en œuvre relatifs à ce type de management sont décrits dans le guide du diagnostic des services de sécurité.

### ***2.1.3 Le support des bases de connaissance pour élaborer un référentiel de sécurité***

Le module de diagnostic approfondi s'appuie, en pratique, sur une base de connaissance des services de sécurité (appelée Manuel de référence des services de sécurité) qui décrit, pour chaque service, la finalité (ce qu'il fait), à quoi il sert (ce contre quoi il lutte), les mécanismes et solutions supports du service et les éléments à prendre en compte pour évaluer la qualité du service.

Cette base d'expertise, sans doute unique en son genre, peut être employée directement pour bâtir un référentiel de sécurité (parfois aussi appelé politiques de sécurité) qui contiendra et décrira l'ensemble des règles et instructions de sécurité à respecter dans l'entreprise ou l'organisme.

Cette démarche est souvent employée dans des organismes ou entreprises ayant un grand nombre d'entités autonomes ou de sites. Il peut s'agir d'entreprises multinationales ayant de nombreuses

filiales, mais aussi, tout simplement, d'entreprises moyennes, voire petites, ayant de nombreuses agences ou représentations régionales. Il est en effet difficile, dans de tels cas, de multiplier les diagnostics ou les analyses de risque.

#### Élaboration du référentiel

Les questionnaires de diagnostic, mais surtout le manuel de référence des services de sécurité avec les explications qu'il contient, seront une bonne base de travail pour que les responsables de la sécurité décident de ce qui devra être appliqué dans l'entreprise.

#### La gestion des dérogations

La mise en place d'un corpus de règles, par le biais d'un référentiel, se heurte souvent à des difficultés d'applications locales et il faut savoir gérer les dérogations.

Le fait d'employer une base de connaissance cohérente avec des moyens et une méthode d'analyse de risque permet alors de gérer les difficultés locales en traitant les demandes de dérogations par une analyse de risques ciblée sur la difficulté mise en évidence.

### ***2.1.4 Les domaines couverts par les modules de diagnostic***

Dans l'optique d'une analyse des risques, au sens de l'identification de toutes les situations de risque et de la volonté de s'attaquer à tous les risques inacceptables, le domaine couvert par MEHARI ne s'arrête pas aux systèmes informatiques.

Les modules de diagnostic couvrent ainsi, outre les systèmes d'information et de communication, l'organisation générale, la protection générale des sites, l'environnement de travail des utilisateurs et les aspects réglementaires et juridiques.

### ***2.1.5 Vue d'ensemble sur les modules de diagnostic***

Ce qu'il faut retenir en synthèse, sur les modules de diagnostic, est qu'ils offrent une vision large et cohérente de la sécurité, utilisable dans différentes approches, avec une progressivité dans la profondeur d'analyse permettant de les utiliser à tous les stades de maturité de la sécurité dans l'entreprise.

## ***2.2. L'analyse des enjeux***

Quelles que soient les orientations ou la politique, en matière de sécurité, il y a un principe sur lequel tous les dirigeants s'accordent, c'est celui de la juste proportion entre les moyens investis dans la sécurité et la hauteur des enjeux de cette même sécurité.

C'est dire qu'avoir une juste connaissance des enjeux de la sécurité est fondamental et que l'analyse des enjeux mérite un très haut degré de priorité et une méthode d'évaluation rigoureuse.

L'objectif de l'analyse des enjeux est de répondre à cette double question :

« Que peut-on redouter et, si cela devait arriver, serait-ce grave ? »

C'est dire que dans le domaine de la sécurité, les enjeux sont vus comme des conséquences d'événements venant perturber le fonctionnement voulu de l'entreprise ou de l'organisme.

MEHARI propose un module d'analyse des enjeux, décrit dans le guide « *Analyse des enjeux et de la classification* », qui débouche sur deux types de résultats :

- Une échelle de valeurs des dysfonctionnements
- Une classification des informations et ressources du système d'information

#### Échelle de valeur des dysfonctionnements

La recherche des dysfonctionnements dans les processus opérationnels ou des événements que l'on peut redouter est une démarche qui s'exerce à partir des activités de l'entreprise. Une telle démarche

débouche sur:

- Une description des types de dysfonctionnements redoutés
- Une définition des paramètres qui influent sur la gravité de chaque dysfonctionnement
- L'évaluation des seuils de criticité de ces paramètres qui font passer la gravité des dysfonctionnements d'un niveau à un autre

Cet ensemble de résultats constitue une échelle de valeur des dysfonctionnements.

Classification des informations et ressources

Il est d'usage, dans le domaine de la sécurité des systèmes d'information, de parler de la classification des informations et de la classification des ressources du système d'information.

Une telle classification consiste à définir, pour chaque type d'information et pour chaque ressource du système d'information, et pour chacun des critères de classification, classiquement la Disponibilité, l'Intégrité et la Confidentialité, des indicateurs représentatifs de la gravité d'une atteinte à ce critère pour cette information ou cette ressource.

La classification des informations et ressources est la traduction, pour les systèmes d'information, de l'échelle de valeur des dysfonctionnements, définie précédemment, en indicateurs de sensibilité associés aux ressources du système d'information.

Expression des enjeux de la sécurité

L'échelle de valeurs des dysfonctionnements et la classification sont deux manières distinctes d'exprimer les enjeux de la sécurité.

La première est plus détaillée et fournit plus de renseignements pour des responsables de sécurité, la seconde est plus globale et plus utile à la communication sur le degré de sensibilité, avec une perte de précision.

### ***2.2.1 L'analyse des enjeux, base de l'analyse des risques***

Il est clair que ce module est un élément clé de l'analyse des risques et que sans consensus sur les conséquences des dysfonctionnements potentiels, tout jugement sur un niveau de risque est impossible.

### ***2.2.2 L'analyse des enjeux, support de tout plan d'action ou schéma directeur***

Comme nous l'avons indiqué en introduction, l'analyse des enjeux est très souvent nécessaire pour la mise en œuvre de tout plan de sécurité. En effet, quelle que soit la démarche suivie, il y aura un moment où il faudra allouer des moyens pour mettre en œuvre les plans d'action et inmanquablement la question sera posée du bien fondé d'un tel investissement.

Les moyens que l'on est disposé à octroyer à la sécurité sont, comme pour l'assurance, directement fonctions de l'importance du risque et, s'il n'y a pas de consensus sur les enjeux des dysfonctionnements redoutés, il y a fort à craindre que les budgets ne soient pas accordés.

### ***2.2.3 La classification, élément essentiel d'une politique de sécurité***

Nous avons déjà évoqué les référentiels ou politiques de sécurité et ce mode de management de la sécurité.

En pratique, les entreprises qui gèrent la sécurité par un corpus de règles sont amenées à différencier, dans les règles elles-mêmes, les actions à mener en fonction de la sensibilité des informations traitées. La manière usuelle de le faire est de se référer à une classification des informations et des ressources du système d'information.

Le module d'analyse des enjeux de MEHARI permet alors d'effectuer cette classification.

## ***2.2.4 L'analyse des enjeux, base de plans de sécurité***

Le processus même d'analyse des enjeux, qui met bien entendu à contribution les responsables opérationnels, engendre, très souvent, un besoin d'actions immédiates.

L'expérience prouve que quand on a rencontré des responsables opérationnels à un haut niveau de responsabilité dans l'entreprise, indépendamment d'ailleurs de la taille de l'entreprise, et qu'ils se sont exprimés sur ce qu'ils estimaient être des dysfonctionnements graves, cela a fait naître chez eux des besoins de sécurité dont ils n'avaient pas conscience et auxquels il faut répondre rapidement.

On peut alors bâtir directement des plans d'action, par une approche directe et légère basée sur la rencontre de deux expertises : celle du métier, par les responsables opérationnels et celle des solutions de sécurité par les responsables de la sécurité.

## ***2.3. L'analyse des risques***

L'analyse de risque est citée dans beaucoup d'ouvrages sur la sécurité, comme devant être le moteur de la sécurité, mais la plupart sinon tous sont silencieux quant à la méthode à employer.

MEHARI propose, depuis plus de 10 ans, une approche structurée du risque<sup>3</sup> qui repose sur quelques éléments simples.

Pour ne retenir que l'essentiel, une situation de risque peut être caractérisée par divers facteurs :

- Des facteurs structurels qui ne dépendent pas des mesures de sécurité, mais du métier de l'entreprise, de son environnement et de son contexte.
- Des facteurs de réduction de risque qui sont, eux, directement fonction des mesures de sécurité mises en place.

MEHARI permet d'évaluer, qualitativement et quantitativement, ces facteurs et de porter, en conséquence, un jugement sur le niveau de risque.

Précisons simplement que l'analyse des enjeux sera prise en compte pour déterminer la gravité maximale des conséquences d'une situation de risque, ce qui est typiquement un facteur structurel, alors que les diagnostics de sécurité seront pris en compte pour évaluer les facteurs de réduction de risque.

### ***2.3.1 L'analyse de risque, méthode d'élaboration d'un schéma directeur***

La mise en évidence de facteurs de réduction de risque, eux-mêmes fonction de mesures de sécurité, offre une base méthodologique pour élaborer un plan de sécurité ou schéma directeur.

Sur cette base, MEHARI propose et structure une démarche organisée qui conduit à l'élaboration de plans de sécurité.

Cette démarche s'appuie sur une base de connaissance de situations de risques et sur des automatismes d'évaluation des facteurs de réduction de risque. Elle est soutenue par un outil logiciel<sup>4</sup> qui décharge l'utilisateur de toutes les tâches de calcul et permet simulations et optimisations.

Dans cette utilisation de MEHARI, l'accent est porté sur l'optimisation globale des mesures de sécurité dans l'optique d'une réduction des risques.

---

<sup>3</sup> Le détail du modèle de risque est donné dans le document « *Principes et mécanismes de MEHARI* », disponible sur le site du Clusif.

<sup>4</sup> RISICARE édité par la société BUC S.A.

### ***2.3.2 L'analyse systématique des situations de risque***

Sur la même base méthodologique, une approche sensiblement différente consiste à identifier toutes les situations de risque potentielles, à analyser individuellement les plus critiques, puis à décider des actions à mener afin de les ramener à un niveau acceptable.

MEHARI permet également cette approche et les bases de connaissance ont été développées afin de répondre à cet objectif.

Dans cette utilisation de MEHARI, l'accent est porté sur l'assurance que chaque situation de risque critique a été prise en compte et est bien couverte par un plan d'action.

### ***2.3.3 L'analyse ponctuelle de situations de risque***

Les mêmes outils peuvent être utilisés ponctuellement dans le cadre d'autres modes de pilotage de la sécurité.

Dans les cas que nous avons évoqués, de pilotage par les diagnostics de sécurité ou par des référentiels de sécurité, il se trouvera toujours des cas particuliers où les règles décidées ne pourront s'appliquer. Il est fort utile alors de pouvoir s'appuyer sur une analyse ponctuelle de risque pour décider de la conduite à tenir.

### ***2.3.4 L'analyse des risques liés à de nouveaux projets***

Le modèle et les mécanismes d'analyse de risque peuvent enfin être utilisés dans le cadre de la gestion de projets, pour en analyser les risques et décider en conséquence des mesures à prendre.

## ***2.4. Vue d'ensemble sur les utilisations de MEHARI***

Il est clair que l'orientation majeure de MEHARI est l'analyse et la réduction des risques et que ses bases de connaissance, ses mécanismes et les outils support ont été construits dans ce but.

Il est clair aussi, dans l'esprit des concepteurs de cet ensemble méthodologique, que l'appel à une méthode structurée d'analyse et de réduction de risque peut être, selon les entreprises :

- une méthode de travail permanente, principale et structurante,
- une méthode de travail permanente employée concurremment avec d'autres méthodes de pilotage de la sécurité,
- un mode de travail occasionnel venant en complément d'autres méthodes de pilotage.

Dans cet esprit, ce que MEHARI apporte est un ensemble de concepts et d'outils permettant de recourir à l'analyse de risque quand cela sera jugé utile ou nécessaire.

MEHARI est diffusé par le CLUSIF, sous forme de fichiers téléchargeables contenant les bases de connaissances ainsi que des manuels permettant de mieux appréhender les différents modules (enjeux –risques -vulnérabilités), afin d'aider les responsables de la sécurité de l'information (RSSI, Risk Manager, auditeurs, DSI, ..) dans leurs démarches de management.

# 3. MEHARI et les normes

La question est souvent posée du positionnement de MEHARI vis-à-vis des normes internationales et en particulier ISO 13335, ISO17799<sup>5</sup> et ISO/IEC 27001<sup>6</sup>.

Il ne s'agit pas de comparer MEHARI et les divers outils méthodologiques créés autour de normes, mais seulement d'aborder le positionnement de MEHARI vis-à-vis de normes de l'ISO, en termes d'objectifs et de compatibilité.

En ce qui concerne la norme ISO 13335, celle-ci contient un modèle de management de risque auquel MEHARI se réfère et avec lequel MEHARI est totalement compatible. MEHARI propose une méthode et des outils tels que la norme le réclame.

Nous abordons donc plus particulièrement ci-dessous le positionnement de MEHARI vis-à-vis de l'ISO 17799 et de l'ISO/IEC 27001.

## 3.1. *Objectifs respectifs de l'ISO 17799, de l'ISO/IEC 27001 et de MEHARI*

### 3.1.1 *Objectifs de la norme ISO/IEC 17799:2005*

Cette norme indique qu'une organisation doit identifier ses exigences de sécurité en partant de trois sources principales :

- l'analyse de risques,
- les exigences légales, statutaires, réglementaires ou contractuelles,
- l'ensemble des principes, objectifs et exigences relatives au traitement de l'information que l'organisation a développé pour supporter ses opérations.

Partant de là, les points de contrôle peuvent être choisis et implémentés selon la liste fournie dans la partie « *code des pratiques pour le management de la sécurité de l'information* » de la norme ou provenir de tout autre ensemble de points de contrôle (§4.2).

*Note : Dans le « Scope » de la version 17799:2005, il est précisé que la norme fournit des « guidelines and general principles for initiating, implementing, maintaining and improving information security management », ce qui indique que la norme ISO peut être « regardée comme un point de départ », mais l'ISO/IEC 27001 indique (§1.2) que toute exclusion doit être justifiée et qu'il est cependant possible d'ajouter des objectifs de contrôle (Annexe A - A.1)*

La norme ISO 17799 fournit donc un recueil de lignes directrices dont les entreprises devraient (*should*) tirer parti, en précisant que ce recueil n'est pas exhaustif et que des mesures complémentaires peuvent être nécessaires, mais aucune méthodologie n'est indiquée pour élaborer le système complet de management de la sécurité.

Par contre, chaque partie du guide des meilleures pratiques comprend des introductions et des commentaires sur les objectifs poursuivis qui peuvent constituer une aide appréciable.

Note : La norme ISO indique également dans son « Scope » qu'il peut être utilisé « **to help build confidence in inter-organizational activities** ». Ceci n'est pas un hasard et met en lumière **un objectif essentiel des promoteurs de la norme qui est l'évaluation, voire la certification**, du

---

<sup>5</sup> dans sa version ISO/IEC 17799:2005(E)

<sup>6</sup> dans sa version ISO/IEC 27001-2005

point de vue de la sécurité de l'information, **de partenaires ou de prestataires**.

### ***3.1.2 Objectifs de l'ISO/IEC 27001***

L'objectif de l'ISO/IEC 27001 est clairement présenté comme celui de « fournir un modèle pour **établir et gérer un système de gestion de la sécurité de l'information (ISMS)** d'une organisation » et « **d'être utilisé** soit en interne soit par des tiers, y compris **des organismes de certification** ».

Cet objectif d'évaluation et de certification conduit à mettre fortement l'accent sur des aspects de formalisation (documentation et enregistrement des décisions, déclaration d'applicabilité, registres, etc.) et sur les contrôles (revues, audits, etc.). A ce titre, il s'agit d'une approche très orientée qualité.

Il reste que le fond de la démarche de sécurité présentée implique de réaliser au préalable une analyse des enjeux puis des risques auxquels l'entreprise ou l'organisation est exposée et à sélectionner les mesures adéquates pour réduire ces risques à un niveau acceptable (§4.2.1).

ISO/IEC 27001 indique qu'une méthode d'analyse de risque doit être utilisée, mais elle ne fait pas partie de la norme et rien n'est proposé, sinon de l'intégrer dans le processus récursif du modèle (PDCA – Plan, Do, Check, Act) défini pour réaliser l'ISMS

Par ailleurs, les recommandations ou les « *meilleures pratiques* » pouvant être sélectionnées pour réduire les risques sont « alignées sur celles listées dans ISO/IEC 17799:2005 », dont la liste de points de contrôle est fournie en annexe.

Le fondement de **l'évaluation du système de management de la sécurité** selon l'ISO/IEC 27001 n'est pas de savoir ou de vérifier si les décisions prises sont pertinentes et si elles reflètent bien les besoins de l'entreprise, mais de vérifier qu'une fois ces décisions prises, le système de management est bien tel que l'on pourra avoir une certaine assurance qu'elles seront appliquées (« on » désignant un auditeur ou un certificateur).

### ***3.1.3 Objectifs de MEHARI***

MEHARI se présente comme un ensemble cohérent d'outils et de méthodes de management de la sécurité, fondés sur l'analyse des risques. Les deux aspects fondamentaux de MEHARI que sont le modèle de risque (qualitatif et quantitatif) et les modèles de management de la sécurité basés sur l'analyse de risque n'ont pas d'équivalent ni dans l'ISO/IEC 27001 ni dans l'ISO 17799.

### ***3.1.4 Analyse comparée des objectifs de MEHARI et des normes ISO 17799 et ISO/IEC 27001***

Les objectifs de MEHARI d'une part et des normes ISO ci-dessus mentionnées d'autre part sont radicalement différents :

- MEHARI vise à donner des outils et des méthodes pour sélectionner les mesures de sécurité les plus pertinentes pour une entreprise donnée, ce qui n'est absolument pas le point de vue des deux normes ISO.
- Les deux normes ISO fournissent un ensemble de bonnes pratiques, certainement utiles mais pas forcément adaptées aux enjeux de l'organisation, et un moyen de jugement de la maturité, au plan de la sécurité de l'information, d'entités internes autonomes ou de partenaires.

Le seul point de l'ensemble MEHARI qui pourrait être comparé à l'ISO 17799 (et à l'annexe A de l'ISO/IEC 27001) est le ***Manuel de référence des services de sécurité***<sup>7</sup> qui donne effectivement

---

<sup>7</sup> Ce manuel est disponible sur le site du Clusif.

des éléments détaillés pouvant être utilisés pour bâtir un référentiel de sécurité. Concernant cet aspect, il est clair que la couverture des services de MEHARI est plus vaste que celle de l'ISO et couvre des aspects essentiels de la sécurité en dehors des systèmes informatiques proprement dits.

## **3.2. *Compatibilité de ces approches***

L'approche de MEHARI est, en réalité, totalement conciliable avec celle de l'ISO 17799 car, bien qu'elles ne poursuivent pas les mêmes objectifs, il est possible de représenter facilement (si cela est nécessaire) les résultats obtenus à l'issue de la démarche MEHARI en indicateurs ISO 17799.

MEHARI permet de répondre à la demande des deux normes de s'appuyer sur une analyse de risques pour définir les mesures à mettre en œuvre.

### **3.2.1 *Compatibilité avec ISO 17799***

Les « contrôles » standards ou « bonnes pratiques » de l'ISO sont majoritairement des mesures générales (organisationnelles et comportementales) alors que MEHARI met prioritairement l'accent sur des mesures techniques dont on puisse garantir l'efficacité. Les résultats, en termes de management de la sécurité, seront donc radicalement différents avec ces deux approches.

Malgré cette différence, il existe, dans MEHARI, particulièrement avec la version 2007, des tables de correspondance qui permettent de fournir des résultats de points de contrôle sous forme d'indicateurs alignés sur le découpage de la norme ISO 17799:2005, pour ceux qui ont un besoin particulier de fournir des preuves de conformité à cette norme.

Il est bon de rappeler ici que les questionnaires d'audit de MEHARI sont conçus et découpés afin de réaliser efficacement l'analyse des vulnérabilités auprès des responsables opérationnels concernés et d'en déduire la capacité de chacun des services de sécurité à réduire les risques.

### **3.2.2 *Compatibilité avec ISO 27001***

Il est aisé d'intégrer MEHARI dans les processus définis par l'ISO/IEC 27001, principalement dans la phase 'PLAN' (§4.2.1) dont MEHARI couvre complètement la description des tâches permettant d'établir les bases de l'ISMS.

Pour la phase 'DO' (§4.2.2), destinée à implémenter et administrer l'ISMS, MEHARI apporte des éléments initiaux utiles tels que l'établissement des plans de traitement des risques, avec des priorités directement liées à la classification des risques et des indicateurs de progrès au cours de leur réalisation.

Pour la phase 'CHECK' (§4.2.3), MEHARI fournit les éléments permettant de déterminer les risques résiduels et les améliorations introduites dans les mesures de sécurité. Par ailleurs, toute modification de l'environnement (enjeux, menaces, solutions et organisation) peut être réévaluée aisément par des audits plus ciblés s'appuyant sur les résultats de l'audit initial réalisé par MEHARI afin de réviser les plans de sécurité au fil du temps.

Pour la phase 'ACT' (§4.2.4), MEHARI appelle implicitement au contrôle et à l'amélioration continue de la sécurité afin d'assurer la tenue des objectifs de réduction des risques. Dans ces trois phases, MEHARI n'est pas au cœur des processus mais contribue à leur réalisation et à l'assurance de leur efficacité.