METHODES

MEHARI 2010

Présentation générale

Janvier 2010

Espace Méthodes

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

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

Remerciements

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

Jean-Philippe	Jouas	Responsable de l'Espace Méthodes Responsable du Groupe de Travail Principes, Mécanismes et Bases de connaissances de Méhari
Jean-Louis	Roule	Responsable du Groupe de Travail Documentation de Méhari
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

1. Introduction

MEHARI a été conçue et est en constant développement pour aider les RSSI[1] dans leur tâche de gestion et de pilotage de la sécurité de l'information et des systèmes d'information. Cette présentation générale leur est ainsi destinée, mais elle s'adresse également aux auditeurs, aux DSI[2] ou aux Gestionnaires de risques (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 détaillée de Méhari, à savoir :

- La présentation des principes fondamentaux et spécifications fonctionnelles de MEHARI,
- Des guides d'utilisation, pour l'analyse des enjeux, le diagnostic des services de sécurité et l'analyse et le traitement des risques,
- Le manuel de référence des services de sécurité,
- Des bases de connaissance.

L'objectif premier de MEHARI est de fournir une méthode d'analyse[3] et de gestion des risques et, plus particulièrement pour le domaine de la sécurité de l'information, une méthode conforme aux exigences de la norme ISO/IEC 27005:2008, avec l'ensemble des outils et moyens requis pour sa mise en œuvre[4].

A cet objectif premier s'ajoutent deux objectifs complémentaires :

Permettre une analyse directe et individualisée de situations de risque décrites par des scénarios de risque.

Fournir une gamme complète d'outils adaptée à la gestion à court, moyen et long terme, de la sécurité, quelle que soit la maturité de l'organisme en matière de sécurité et quelques soient les types d'actions envisagés.

Compte tenu de ces objectifs, MEHARI propose un ensemble méthodologique cohérent, faisant appel à des bases de connaissance adaptées, et capable d'accompagner les responsables d'entreprise ou d'organisme et les responsables de la sécurité dans leurs différentes démarches et actions, ainsi que les acteurs impliqués dans la gestion des risques.

Un positionnement de MEHARI vis-à-vis des normes de la série ISO/IEC 27000 est abordé en fin de document.

---

1 RSSI : Responsable de la Sécurité des Systèmes d'Information ou, RSI : Responsable de la Sécurité de l'Information

2 DSI : Directeur des Systèmes d'Information

3 Appréciation des risques au sens de l'ISO/IEC 27005

4 Ces outils et moyens requis, en complément de la norme, sont décrits et justifiés dans le document « Méhari 2010 – Principes fondamentaux et spécifications fonctionnelles »

2. Utilisations de MEHARI

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

En fait, compte tenu du deuxième objectif cité plus haut, MEHARI et ses bases de connaissance sont bâties pour permettre une analyse précise de situations de risque, quand cela sera jugé nécessaire, ces situations de risque étant alors décrites par des scénarios de risque.

Ceci étant, la gestion de la sécurité est une fonction ou une activité qui évolue au cours du temps et les actions correspondantes 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 une « référence » 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, ainsi que le demande la norme ISO/IEC 27001 qui traite des Systèmes de Gestion de la Sécurité de l'Information (SMSI[5]). Ceci étant, cela n'est pas toujours le cas et il existe bien d'autres voies, dont l'alignement sur un « Référentiel » (ou standard), que ce Référentiel soit interne, professionnel ou interprofessionnel.

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 une analyse directe et individualisée des risques, sont utilisables indépendamment les uns des autres, à tous les stades de développement de la sécurité, dans différents modes de gestion de la sécurité, et garantissent une cohérence d'ensemble des décisions.

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

---

5 En anglais "Information Security Management System" ou ISMS, acronyme français : SMSI

2.1. *L'analyse (ou appréciation) des risques*

L'analyse de risque est citée dans beaucoup d'ouvrages sur la sécurité, et notamment dans les normes ISO/IEC de la série 27000, comme devant être la base de l'expression des besoins de sécurité, mais la plupart, sinon tous, sont silencieux quant à la méthode à employer.

MEHARI propose, depuis plus de 15 ans, une approche structurée du risque[6] 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.

Précisons simplement qu'une analyse des enjeux est nécessaire pour déterminer la gravité maximale des conséquences d'une situation de risque, ce qui est typiquement un facteur structurel, alors que des diagnostics de sécurité sont nécessaires pour évaluer les facteurs de réduction de risque.

MEHARI permet d'évaluer, qualitativement et quantitativement, ces facteurs et de porter, en conséquence, un jugement sur le niveau de risque. MEHARI s'appuie, pour cela, sur des outils (critères d'appréciation, méthodes de calcul, etc.) et des bases de connaissances (en particulier pour les diagnostics de sécurité) qui s'avèrent indispensables en complément du cadre minimum proposé par la norme ISO 27005.

2.1.1 L'analyse systématique des situations de risque

Pour répondre à la question « A quels risques l'organisme est-il exposé et ces risques sont-ils acceptables ? », une approche structurée 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 de réaliser 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.

Cette démarche s'appuie sur une base de connaissances de situations de risques et sur des mécanismes d'évaluation des facteurs caractérisant chaque risque et permettant d'en apprécier le niveau. La méthode fournit, en outre, des aides pour définir les plans de traitement adaptés.

Le processus d'appréciation des risques peut être soutenu :

Soit par un ensemble de fonctions de la base de connaissances (Microsoft Excel) permettant d'intégrer les résultats des divers modules de MEHARI (classification des actifs résultant de l'analyse des enjeux, diagnostics de sécurité, en particulier). Ces fonctions permettent d'évaluer les niveaux de risques actuels et de proposer des mesures additionnelles pour réduire la gravité des scénarios.

Soit par un outil logiciel (tel que RISICARE)[7] qui offre une assistance plus évoluée et plus complète et permet simulations, visualisations et optimisations.

---

6 Le détail du modèle de risque est donné dans le document *« Principes fondamentaux et spécifications fonctionnelles de MEHARI »*.

7 RISICARE édité par la société BUC S.A.

2.1.2 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.

En effet, dans certains modes de pilotage de la sécurité, pour lesquels la gestion des risques n'est pas la base principale, tels que le pilotage par les diagnostics de sécurité ou par des référentiels de sécurité, il se trouvera souvent des cas particuliers où les règles décidées ne pourront s'appliquer. Il sera fort utile alors de pouvoir s'appuyer sur une analyse ponctuelle de risque pour décider de la conduite à tenir.

2.1.3 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.

2.2. Les diagnostics de sécurité

La méthode intègre des questionnaires de diagnostic approfondi des mesures de sécurité[8], effectivement en place, questionnaires permettant d'évaluer le niveau de qualité des mécanismes et solutions mis en place pour réduire les risques.

2.2.1 Le diagnostic de sécurité, élément d'une analyse des risques

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 et fiable.

Une des forces de MEHARI, comme méthode d'analyse et de traitement des risques, est certainement que tant l'analyse du niveau de risque actuel que les prévisions de niveau de risque futur s'appuient sur une base de diagnostic expert de la qualité des mesures de sécurité, actuellement en place ou décidées.

2.2.2 Les plans de sécurité basés sur un diagnostic de sécurité

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

Le processus de pilotage 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.

Les questionnaires de diagnostic de MEHARI peuvent être utilisés à cette fin.

L'utilisation d'une analyse préalable des enjeux est alors préconisée, faisant ainsi la liaison avec cet autre module de MEHARI, présenté plus loin dans ce document. L'analyse des enjeux permettra notamment de fixer les objectifs de qualité des services de sécurité, voire de ne sélectionner que les services pertinents à auditer dans le cadre du diagnostic.

[8] Les mesures sont groupées par sous-services, eux-mêmes fédérés dans des services puis dans des domaines de sécurité

2.2.3 La base de connaissances comme support d'élaboration d'un référentiel de sécurité

Le module de diagnostic 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 » 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 de sécurité

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.

2.2.4 Les domaines couverts par le module 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 questionnaires 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.

2.2.5 Vue d'ensemble sur le module de diagnostic

Ce qu'il faut retenir en synthèse, sur les questionnaires 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.

2.3. *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 intègre un module d'analyse des enjeux, décrit dans le *« Guide de l'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 des actifs 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 des actifs

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

Une telle classification consiste à définir, pour chaque type d'information et pour chaque actif du système d'information, et pour chacun des critères de classification, classiquement la Disponibilité, l'Intégrité et la Confidentialité (mais éventuellement pour aussi d'autres critères, tels que la traçabilité ou la valeur probatoire), des indicateurs représentatifs de la gravité d'une atteinte à ce critère pour cette information ou cet actif.

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

2.3.1 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.

C'est une autre force de MEHARI que de présenter une méthode rigoureuse pour évaluer ces enjeux et classifier les actifs, sans se fier au « ressenti » des utilisateurs et de fournir des livrables objectifs et rationnels.

2.3.2 L'analyse des enjeux, support de tout plan d'action ou schéma directeur

Ceci étant, 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 immanquablement 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.

Ce module peut ainsi être utilisé en dehors de l'analyse des risques.

2.3.3 La classification, élément essentiel d'une politique de sécurité

Nous avons déjà évoqué les référentiels ou politiques de sécurité et ce mode de pilotage 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 actifs du système d'information.

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

2.3.4 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.

2.4. *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, Gestionnaires de risques, auditeurs, DSI, ..) dans l'accomplissement de leurs responsabilités.

3. MEHARI et les normes ISO/IEC de la série 27000

La question est souvent posée du positionnement de MEHARI vis-à-vis des normes internationales et en particulier celles de la série ISO/IEC 27000[9].

Il s'agit seulement ici d'aborder le positionnement de MEHARI vis-à-vis de ces normes, en termes d'objectifs et de compatibilité, et, plus particulièrement en ce qui concerne les normes ISO/IEC 27001, 27002 et 27005.

3.1. *Objectifs respectifs des normes ISO/IEC 27001, 27002, 27005 et de MEHARI*

3.1.1 Objectifs de la norme ISO/IEC 27002:2005

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 27002:2005, 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 27002 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 gestion 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 point de vue de la sécurité de l'information, de partenaires ou de prestataires.

---

9 en particulier ISO/IEC 27001:2005, 27002:2005 et 27005:2008)

3.1.2 Objectifs de l'ISO/IEC 27001:2005

L'objectif de l'ISO/IEC 27001 est clairement présenté comme celui de « fournir un modèle pour **établir et gérer un système de gestion (management) de la sécurité de l'information (SMSI)** 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 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 au sein du processus récursif du modèle (PDCA[10] – Planifier, Déployer, Contrôler, Améliorer) défini pour réaliser le SMSI.

Par ailleurs, les recommandations ou les *« meilleures pratiques »* pouvant être sélectionnées pour réduire les risques sont « alignées sur celles listées dans ISO/IEC 27002:2005 », dont la liste de points de contrôle est fournie en annexe.

Le fondement de **l'évaluation du système de gestion de la sécurité de l'information** 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 pilotage 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 l'ISO/IEC 27005:2008

Les objectifs de cette norme ne sont pas de constituer une méthode complète de gestion de risque mais de fixer un cadre minimum et d'imposer des exigences, tant pour le processus à suivre, que pour l'identification des menaces et des vulnérabilités permettant d'estimer les risques et d'en évaluer le niveau puis de pouvoir sélectionner le mode de traitement ainsi que les plans et les éléments (dont les mesures de sécurité et les indicateurs) destinés à améliorer la situation.

Il ne s'agit donc pas d'un ensemble méthodologique complet et autosuffisant – il est même précisé que le choix d'une méthode doit être fait – mais d'un cadre permettant d'éviter le choix de méthodologies trop simplistes et/ou trop éloignées de la notion de gestion de risque voulue par les normalisateurs.

3.1.4 Objectifs de MEHARI

MEHARI se présente comme un ensemble cohérent, complet et autosuffisant d'outils et de méthodes de gestion et de pilotage de la sécurité, fondés sur une analyse précise des risques. Les aspects fondamentaux de MEHARI que sont le modèle de risque (qualitatif et quantitatif), la prise en compte, dans ce modèle d'une évaluation quantitative de l'efficacité des services de sécurité mis en œuvre ou projetés, les possibilités d'évaluation et de simulation des effets des mesures envisagées sur les niveaux de risques résiduels sont des compléments indispensables à l'utilisation des normes de la série ISO 27000 et, en particulier à celle de l'ISO/IEC 27005.

---

[10] PDCA, en anglais : Plan, Do, Check, Act

3.1.5 Analyse comparée des objectifs de MEHARI et des normes ISO/IEC 27002 et ISO/IEC 27001

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

— MEHARI vise à donner des outils et des méthodes pour sélectionner les mesures de sécurité les plus pertinentes, techniquement et économiquement, pour une entreprise donnée, et pour évaluer les risques résiduels encourus une fois ces mesures mises en place, 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.

Au sein de l'ensemble MEHARI, le ***Manuel de référence des services de sécurité*** qui donne des éléments détaillés pouvant être utilisés pour bâtir un référentiel de sécurité peut être comparé à la norme ISO/IEC 27002 . 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 27002 car, bien qu'elles ne poursuivent pas les mêmes objectifs, il est possible de représenter facilement (si cela est souhaité) les résultats obtenus à l'issue de la démarche MEHARI en indicateurs de conformité de l'organisation aux objectifs de contrôle figurant dans ISO 27002.

MEHARI permet de répondre à la demande des deux normes (ISO 27001 et 27002) de s'appuyer sur une analyse de risques pour définir les mesures à mettre en œuvre.

3.2.1 Compatibilité avec ISO/IEC 27002 :2005

Les « contrôles » standards ou « bonnes pratiques » de l'ISO sont majoritairement des mesures générales (organisationnelles et comportementales) alors que MEHARI, tout en intégrant ces mesures, met prioritairement l'accent sur des mesures dont on puisse garantir l'efficacité pour réduire les vulnérabilités.

Malgré cette différence, il existe, dans MEHARI, des tables de correspondance qui permettent de fournir des résultats sous forme d'indicateurs alignés sur le découpage de la norme ISO/IEC 27002:2005, 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/IEC 27001

Il est aisé d'intégrer MEHARI dans les processus PDCA (Planifier – Déployer – Contrôler – Améliorer) définis par l'ISO/IEC 27001, principalement dans la phase 'Planifier' (§4.2.1) dont MEHARI couvre complètement la description des tâches permettant d'établir les bases du SMSI.

Pour la phase 'Déployer' (§4.2.2), destinée à implémenter et administrer le SMSI, 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 'Contrôler' (§4.2.3), MEHARI fournit les éléments permettant de déterminer les risques résiduels à partir de l'évaluation (ou audit) des services de sécurité 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 'Améliorer' (§4.2.4), MEHARI appelle implicitement au contrôle et à l'amélioration continus 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.

3.2.3 Compatibilité avec la norme ISO/IEC 27005:2008

Le cadre fixé par la norme ISO s'applique strictement à la façon dont MEHARI permet de gérer les risques, en particulier pour :

Le processus d'analyse, d'évaluation et de traitement de risque (repris d'ISO 13335),

L'identification des actifs primaires (ou primordiaux) et de support ainsi que les niveaux de classification (ou de valorisation) attachés, suite à l'analyse des enjeux,

L'identification des menaces et la détermination de leur niveau (exposition naturelle), pour laquelle MEHARI est plus précis dans la description des scénarios de risque,

L'identification et la valorisation de l'efficacité des mesures de sécurité existantes, destinées à réduire les vulnérabilités contextuelles,

La prise en compte de ces éléments pour indiquer le niveau de gravité des scénarios de risque sur une échelle à 4 niveaux,

La sélectivité dans le choix des mesures de sécurité à intégrer dans les plans de réduction des risques.

Ainsi la méthode MEHARI, non seulement s'intègre facilement dans une démarche de SMSI, telle que décrite dans ISO 27001, mais aussi satisfait entièrement les exigences dictées par ISO 27005 pour une telle méthode.

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