Pratique recommandée en sécurité de l'information

PR-064

Guide d'utilisation de la méthode d'analyse de risque en sécurité de l'information MEHARI et l'outil RISICARE

Guide d’utilisation de la méthode d’analyse de risque en sécurité de l’information MEHARI et l’outil RISICARE

Cette publication a été réalisée par
le Sous-secrétariat du dirigeant principal de l'information
et produite par la Direction des communications du Secrétariat du Conseil du trésor.

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
Secrétariat du Conseil du trésor
5e étage, secteur 500
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca
www.tresor.gouv.qc.ca

Dépôt légal – 2014
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-71122-3

Table des matières

Liste des sigles et acronymes

ASIQ : Association de la sécurité de l'information du Québec

CLUSIF : Club de la Sécurité de l'Information français

COSI : Conseiller organisationnel de la sécurité de l'information

DIC(E) : Disponibilité, intégrité et confidentialité (efficience)

IEC : *International Electrotechnical Commission* (Commission électrotechnique internationale)

ISO : *International Standard Organisation* (Organisation internationale de normalisation)

MEHARI : Méthode Harmonisée de Risques Informatiques (marque déposée du CLUSIF)

PRP : Protection des renseignements personnels

RAIPRP : Responsable de l'accès à l'information et de la protection des renseignements personnels

ROSI : Responsable organisationnel de la sécurité de l'information

SOA : *Statement of applicability* (déclaration d'applicabilité). SOA est un document qui identifie les contrôles (mesures) qui ont été choisis et donne les raisons de leur applicabilité. Ce document est fonction de l'évaluation des risques et du plan de traitement des risques.

Remerciements

Le Secrétariat du Conseil du trésor remercie l'équipe de réalisation et le groupe de travail interministériel pour leur participation et le travail accompli.

Équipe de réalisation

Mohamed Darabid, coordonnateur
Lyonel Vallès, chargé de projet
Socheat Sonn, conseiller
Secrétariat du Conseil du trésor

Notes à l'intention du lecteur

Note 1 :	Pour ne pas alourdir le texte, le masculin est utilisé comme générique dans le présent document.
Note 2 :	Le terme « organisme public » ou « organisme » désigne un ministère ou un organisme, qu'il soit budgétaire ou autre que budgétaire, ainsi que tout organisme du réseau de l'éducation, du réseau de l'enseignement supérieur ou du réseau de la santé et des services sociaux. [Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement].
Note 3 :	Bien que les éléments du présent guide soient applicables à la plupart des organismes publics, il convient pour chaque organisme public de les adapter à son contexte et aux risques qui lui sont propres.
Note 4 :	Certains termes ou acronymes sont définis à leur première apparition dans le texte. Ces définitions sont également présentées à l'annexe.

Sommaire exécutif

Le présent guide est un document synthèse sur la méthodologie MEHARI[1] d'analyse de risques[2] de sécurité et son outil de mise en œuvre RISICARE. Il a été élaboré en prenant appui sur la norme ISO/IEC 27005[3] et sur le cadre de gestion des risques et des incidents à portée gouvernementale.

Avant d'aborder l'aspect pratique d'une démarche d'analyse de risques au moyen de la méthode MEHARI et de son outil RISICARE, le guide la positionne dans le cadre d'une démarche de gestion globale de sécurité de l'information, consacrée par la norme ISO/IEC 27001 portant sur la mise en place d'un système de gestion de la sécurité de l'information (SGSI). Il présente par la suite un bref portrait de la méthode MEHARI, de ses concepts et de ses différentes étapes, à savoir :

- ✓ Étape 1 : La préparation;
- ✓ Étape 2 : La classification[4];
- ✓ Étape 3 : L'évaluation et l'analyse des mesures de sécurité[5];
- ✓ Étape 4 : L'élaboration des plans de sécurité;
- ✓ Étape 5 : Le pilotage[6] et le contrôle des plans.

Le présent guide décrit également les différentes déclinaisons (variantes) de la méthode MEHARI (MEHARI Expert, MEHARI Pro et MEHARI Manager), avant de présenter l'outil d'analyse de risques RISICARE et sa base de connaissances RISIBASE.

Il est à noter que le présent guide n'est ni un support de formation, ni un manuel d'utilisation de MEHARI ou de RISICARE. Il ne prétend en aucune façon remplacer ces outils indispensables à la réalisation d'un exercice d'analyse de risques.

1. MEHARI : Méthode harmonisée d'analyse des risques développée par le Club de la sécurité de l'information français (CLUSIF). Référence : http://www.clusif.asso.fr/
2. Risque : Exprime le fait qu'un événement puisse empêcher de maintenir ou d'atteindre les objectifs d'une organisation ou d'une activité dans les conditions fixées ou encore de satisfaire une finalité programmée.
3. ISO/IEC : International Standard Organisation (Organisation internationale de normalisation) / International Electrotechnical Commission (Commission électrotechnique internationale).
4. Classification ou catégorisation : Processus d'assignation d'une valeur à certaines caractéristiques d'une information, lesquelles définissent le degré de sensibilité de cette information et, conséquemment, la protection à lui accorder.
5. Mesure ou mécanisme de sécurité : Manière concrète de mettre en œuvre un service de sécurité.
6. Pilotage : Le pilotage de la gestion des risques est identique à tout pilotage de projet. Il est réalisé à l'aide d'outils tels que les tableaux de bord et indicateurs, la reddition de compte, l'évaluation périodique et les décisions d'actions de correction.

1. Introduction

La gestion des risques de sécurité de l'information constitue une composante de plus en plus importante de la gouvernance des organisations, tant privées que publiques. En effet, la concrétisation d'un risque peut sérieusement mettre en péril la crédibilité de l'organisation et la continuité de ses activités. Dans le cas des organismes publics, cela peut contribuer à affecter l'image de marque du gouvernement et la confiance des citoyens envers les institutions publiques.

L'analyse des risques, étape déterminante de la gestion des risques de sécurité de l'information, permet notamment aux entreprises et organismes publics (OP) :

- ✓ de connaître les scénarios de risques[7] qui les menacent;
- ✓ de déterminer clairement les actifs informationnels[8] à protéger;
- ✓ d'évaluer et de renforcer les mesures de sécurité en place;
- ✓ d'appuyer la prise de décision quant aux mécanismes de sécurité appropriés à mettre en œuvre et à la définition du plan global de sécurité de l'organisme;
- ✓ de soutenir les activités de gestion et le processus[9] de planification budgétaire en matière de sécurité de l'information.

Ainsi, le présent guide sert de référence aux organismes publics dans le cadre de leur démarche de réalisation d'une analyse de risques. Il présente sommairement la méthode MEHARI et sa base de connaissances, ainsi que le logiciel RISICARE, un outil d'utilisation de la méthode MEHARI.

La documentation et la base de connaissances de MEHARI sont disponibles en libre téléchargement à partir du site du CLUSIF[10]. L'outil RISICARE est disponible au Secrétariat du Conseil du trésor. Les organismes publics qui désirent l'utiliser peuvent en faire la demande à l'adresse suivante : http://www.securite.gouv.qc.ca[11] en se rendant à la section « Méthode d'analyse des risques en SI ».

MEHARI et RISICARE présentent un très grand intérêt pour les organismes publics dans le cadre de leur démarche d'analyse de risques. Bien que leur utilisation soit recommandée, la décision de les adopter relève d'un choix de gestion de la part des organismes publics.

1.1 Contexte

Dans sa démarche de mise en œuvre d'une gouvernance forte et intégrée de la sécurité de l'information gouvernementale, le dirigeant principal de l'information (DPI) place la gestion des risques de sécurité de l'information au cœur de ses priorités. En effet, l'augmentation continuelle des menaces et des risques de sécurité de l'information exige que des actions soient posées afin d'assurer une meilleure gestion des

7. Scénario de risque : Description d'un événement adverse ou d'un dysfonctionnement et de la manière dont celui-ci peut survenir.
8. Actif informationnel : Une information, quels que soient son canal de communication (téléphone analogique ou numérique, télégraphe, télécopie, voix, etc.) ou son support (papier, pellicule photographique ou cinématographique, ruban magnétique, support électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitué par une organisation.
9. Processus : Regroupement d'événements d'affaires, agencés selon une logique de création de valeur, exécutés dans le but de livrer un résultat.
10. CLUSIF : Club de la sécurité de l'information français, www.clusif.asso.fr.
11. Seuls les organismes publics dont le budget est voté, en totalité ou en partie, par l'Assemblée nationale ou dont le personnel est nommé et rémunéré selon la Loi sur la fonction publique (chapitre F3.1.1) auront accès au contenu de ce site et pourront s'y inscrire.

risques de sécurité de l'information, tant sur le plan gouvernemental qu'à l'échelle des organismes publics.

C'est ainsi que la nouvelle directive sur la sécurité de l'information gouvernementale, adoptée en janvier 2014, énonce de nouvelles obligations favorisant l'évolution des organismes publics vers un niveau de maturité adéquat en matière de sécurité de l'information. Parmi ces obligations, citons, notamment, la conformité des organismes publics aux bonnes pratiques de sécurité de l'information, dont la mise en œuvre d'un processus officiel de gestion des risques de sécurité de l'information.

Pour aider les organismes publics à se conformer à cette obligation, un guide intitulé « Guide de mise en place d'un processus de gestion de la sécurité de l'information » est mis à leur disposition. Celui-ci, se basant sur la norme ISO/IEC 27005, décrit la démarche de mise en place d'un tel processus, tout en laissant une certaine neutralité à l'égard des moyens (méthodes et outils) qui pourraient en faciliter la conception et la mise en œuvre.

En revanche, le présent guide met l'accent sur la méthode MEHARI et l'outil RISICARE, largement utilisés par les organismes publics en tant que moyens de mise en œuvre d'un processus de gestion des risques de sécurité de l'information. Il a été élaboré en remplacement d'une version datée de juillet 2006, en vue, notamment, de tenir compte du nouveau cadre de gouvernance de la sécurité de l'information[12], de nouvelles pratiques gouvernementales tel le guide de catégorisation de l'information et de l'évolution de la méthode MEHARI.

1.2 Objectif

Le présent document pourra guider les organismes publics dans la réalisation d'une analyse de risques à l'aide de la méthode MEHARI. Il fournit, à cet égard, une description synthèse des étapes d'utilisation de la méthode et de RISICARE, outil de mise en application de la méthode.

1.3 Champ d'application et portée

Le présent guide s'applique à l'information gouvernementale consignée dans un document[13] au sens de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1). L'information visée est celle qu'un organisme public détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

Il est à l'usage des organismes publics visés par l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03).

12. Le nouveau cadre de gouvernance, adopté en janvier 2014, est constitué de la directive sur la sécurité de l'information gouvernementale, du cadre gouvernemental de gestion de la sécurité de l'information, du cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information et de l'approche stratégique triennale 2014-2017 en sécurité de l'information.
13. Document : Un ensemble « constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles.
[...] est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite. »

1.4 Public cible

Le présent guide est à l'usage de tout intervenant appelé à réaliser une analyse de risques de sécurité de l'information, celle-ci pouvant être exhaustive et porter sur l'ensemble des actifs et services de sécurité[14] de l'information, ou être restreinte à quelques-uns de ces actifs et services. Parmi ces intervenants, on peut citer :

- ✓ le responsable organisationnel de la sécurité de l'information (ROSI);
- ✓ le conseiller organisationnel en sécurité de l'information (COSI);
- ✓ le conseiller en gestion de la sécurité de l'information (coordonnateur de la sécurité de l'information, adjoint au ROSI, etc.);
- ✓ les spécialistes en gestion des risques de sécurité de l'information;
- ✓ tout intervenant dans un domaine connexe à la sécurité de l'information, appelé à en évaluer les risques et à proposer les mesures de sécurité afférentes (responsable de la continuité des services, responsable des accès, etc.).

1.5 Cadre légal, normatif et administratif

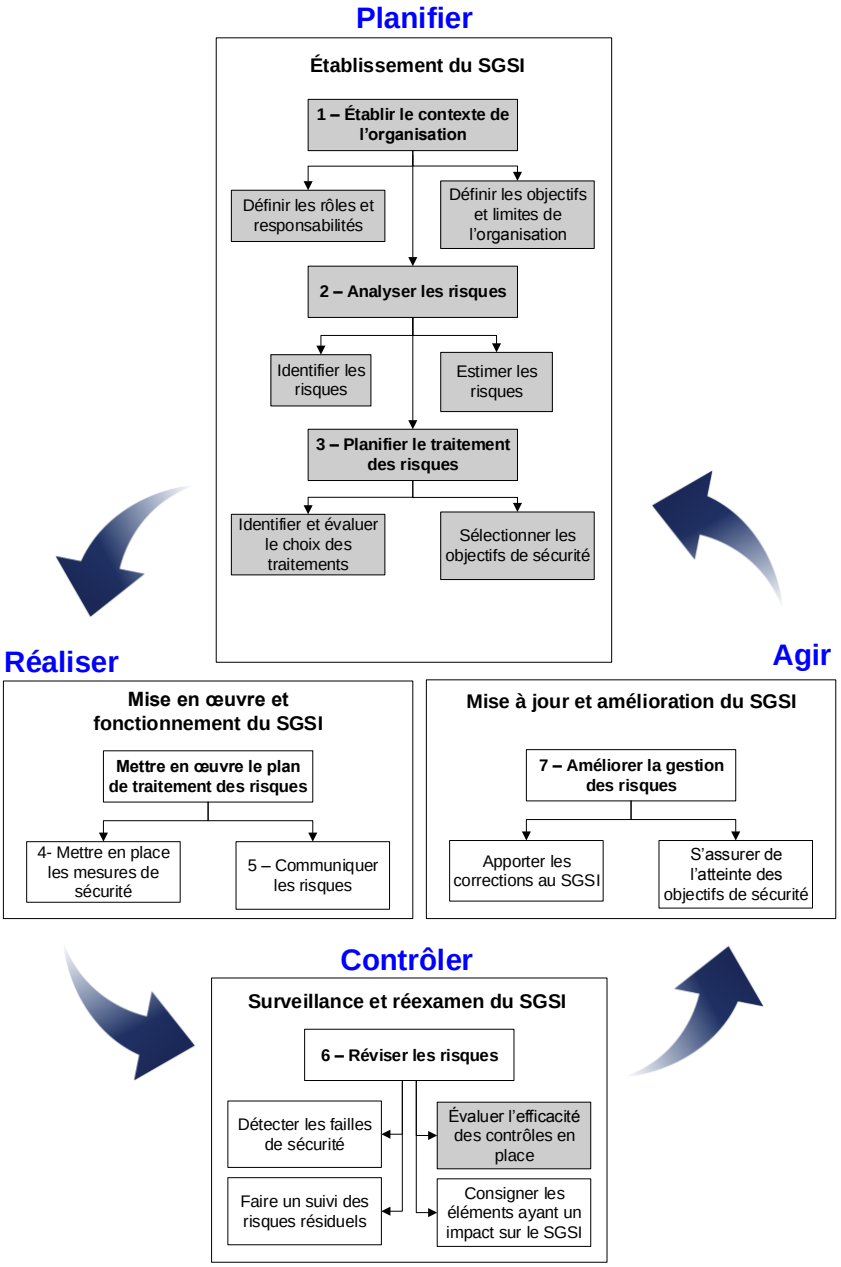
Le présent guide de soutien aux organismes publics dans le cadre de leur démarche d'analyse de risques s'inscrit dans un cadre légal, normatif et administratif comprenant des lois, des directives, des pratiques gouvernementales, des normes internationales et des standards de l'industrie. Les principaux éléments constitutifs de ce cadre sont présentés à l'Annexe II – Cadre légal, normatif et administratif.

14. Service de sécurité : Réponse possible à un besoin précis de sécurité. Il est assuré par un ou un ensemble de mécanismes ou de mesures de sécurité.

2. Positionnement des étapes de la méthode MEHARI

Conforme à la norme ISO/IEC 27005 portant sur la gestion des risques de sécurité de l'information, la méthode MEHARI se décline en plusieurs étapes, qui se positionnent transversalement dans le système de gestion de la sécurité de l'information (SGSI), comme le préconise la norme ISO/IEC 27001. Ces étapes sont illustrées en gris dans la figure 1, présentée ci-dessous.

Figure 1 – Positionnement des étapes de la méthode MEHARI dans le SGSI



3. Évolution de la méthode MEHARI

Le présent chapitre traite des principaux changements de la méthode MEHARI 2010, par rapport à la précédente version de 2007. Ces changements visent essentiellement à aligner la méthode sur la norme ISO/IEC 27005[15] portant sur la gestion du risque en sécurité de l'information. Ces changements concernent principalement la récupération et le transfert du risque, la description des actifs et la description des vulnérabilités.

Comme le préconise la norme ISO/IEC 27005, MEHARI 2010 place le *transfert des risques* dans l'étape de traitement des risques. Toujours selon cette même norme, les mesures concernant l'acceptation du risque (récupération du risque), présentes dans la version 2007, ne font pas partie des mesures de réduction du risque dans la version 2010.

De plus, MEHARI 2010 s'aligne sur la définition d'un actif, préconisée par la norme ISO/IEC 27005, selon laquelle « Un actif désigne tout élément ayant de la valeur pour l'organisme et nécessitant, par conséquent, une protection […] ». Toujours selon la définition, il convient de garder à l'esprit qu'un système d'information[16] ne comprend pas uniquement du matériel et des logiciels[17]. Il peut comprendre des processus, des activités, de l'information, du personnel, des sites, etc.

Pour la description des vulnérabilités, MEHARI 2010 se base sur la définition énoncée dans la norme ISO/IEC 27000[18] selon laquelle une vulnérabilité est « une faille dans un actif ou dans une mesure de sécurité pouvant être exploitée par une menace ». Sur cette base et pour qu'il n'y ait pas d'ambigüité, MEHARI 2010 introduit deux déclinaisons de cette définition. La première concerne une vulnérabilité intrinsèque[19], qui est la caractéristique intrinsèque d'un actif pouvant être exploitée par une menace. La seconde définit une vulnérabilité contextuelle comme étant une faiblesse dans un dispositif de sécurité pouvant être exploitée par une menace.

L'évolution de MEHARI 2010 porte également sur la description des menaces ainsi que sur l'identification et la description des scénarios de risques. Pour la description d'une menace, MEHARI 2010 introduit, de manière formelle, les éléments qui la constituent : un événement déclencheur, des circonstances de survenance et un type d'acteur. Quant à la description des scénarios de risques, elle devient très structurée et précise un type d'actif primaire, une vulnérabilité intrinsèque, un type de menace et un libellé permettant de comprendre le scénario au moyen d'une description globale.

On observe également d'autres changements dans certains processus d'analyse et dans la base de connaissances.

Pour obtenir de plus amples renseignements concernant l'évolution de la méthode MEHARI, le lecteur pourra consulter le document du CLUSIF intitulé « MEHARI 2010 : Évolutions par rapport aux versions précédentes »[20].

15. Norme ISO/IEC 27005 : Gestion du risque en sécurité de l'information.
16. Système d'information : Système constitué de l'équipement, des procédures, des logiciels, des applications, des ressources humaines, ainsi que des données qui sont traitées, et dont le but est de fournir de l'information afin de soutenir une fonction d'affaires.
17. Voir la norme ISO/IEC 27005, partie 8.2.1.2.
18. Norme ISO/IEC 27000, Systèmes de gestion de la sécurité de l'information- Vue d'ensemble et vocabulaire.
19. Intrinsèque : En l'absence de toute mesure de sécurité.
20. http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Evolutions.pdf

4. La méthode MEHARI

Le présent chapitre décrit les concepts de base de la méthode, ses limites, les scénarios de risques en matière de protection des renseignements personnels (PRP), la base de connaissances afférente, les étapes de la démarche et ses différentes déclinaisons.

4.1 Concepts de base

Les concepts de base de la méthode se traduisent par ses objectifs fondamentaux, par un ensemble de principes et de spécifications fonctionnelles et par un plan global lui permettant de se conformer à la norme ISO/IEC 27005, portant sur la gestion des risques de sécurité de l'information.

4.1.1 Objectifs fondamentaux

Les objectifs fondamentaux de la méthode MEHARI[21] sont les suivants :

- ✓ identifier tous les risques auxquels l'organisation est exposée;
- ✓ quantifier le niveau de chaque risque, sur le plan de l'impact (importance des dommages), de celui de la potentialité (probabilité d'apparition d'un événement) et sur celui de la gravité[22];
- ✓ prendre, pour chaque risque admissible, des mesures pour que le niveau de risque soit ramené à un seuil acceptable;
- ✓ mettre en place un processus de suivi permanent des risques et de leur niveau de gravité;
- ✓ s'assurer que chaque risque, considéré individuellement, est bien pris en charge et qu'il a fait l'objet d'une décision de traitement telle que l'acceptation, la réduction, l'évitement ou le transfert du risque.

4.1.2 Principes et spécifications fonctionnelles

La méthode se base sur des principes et spécifications fonctionnelles[23], qui peuvent se résumer comme suit :

- ✓ Les risques sont identifiés et décrits par des scénarios élaborés à l'aide d'un nombre d'éléments précis (actif concerné, vulnérabilité intrinsèque de cet actif et la menace sur l'actif);

21. Cf. le document « MEHARI 2010 : Principes fondamentaux et spécifications fonctionnelles, janvier 2010 ». http://www.clusiq.org/documents/MEHARI/pdf/MEHARI-2010-Principes-Specifications.pdf
22. Gravité : Exprime l'effet conjugué de la potentialité (probabilité) qu'un scénario de risque se matérialise et de l'importance de ses conséquences (impact).
23. Cf. le document « MEHARI 2010 : Guide de l'analyse et du traitement des risques, janvier 2010 ». http://www.clusiq.org/documents/MEHARI/pdf/MEHARI-2010-Anarisk.pdf

- ✓ Chaque scénario de risque peut être évalué (quantitativement ou qualitativement); cette évaluation prend en compte :
  - l'impact intrinsèque du scénario de risque, lequel reflète le niveau de conséquence du scénario, s'il se réalise en l'absence de toute mesure de sécurité (p. ex. faible impact sur l'organisation, en cas de perte d'un document interne peu confidentiel, même si ce dernier n'est pas protégé);
  - la potentialité intrinsèque du scénario (ou exposition naturelle), qui reflète le niveau de probabilité de survenance du scénario en l'absence de toute mesure de sécurité (p. ex. forte probabilité de contamination par un virus, avant l'utilisation d'un antivirus);
  - des facteurs de réduction de risques, différenciés par leur type d'effet[24] sur l'impact ou la potentialité, facteurs qui dépendent des mesures de sécurité et de la qualité de ces mesures (p. ex. existence d'une mesure de dissuasion).
- ✓ Le processus d'évaluation de chaque scénario de risque permet de sélectionner des mesures de sécurité et des objectifs de qualité[25] pour ces mesures, de sorte que le risque puisse être maintenu à un niveau acceptable.

4.1.3 Plan global de la méthode

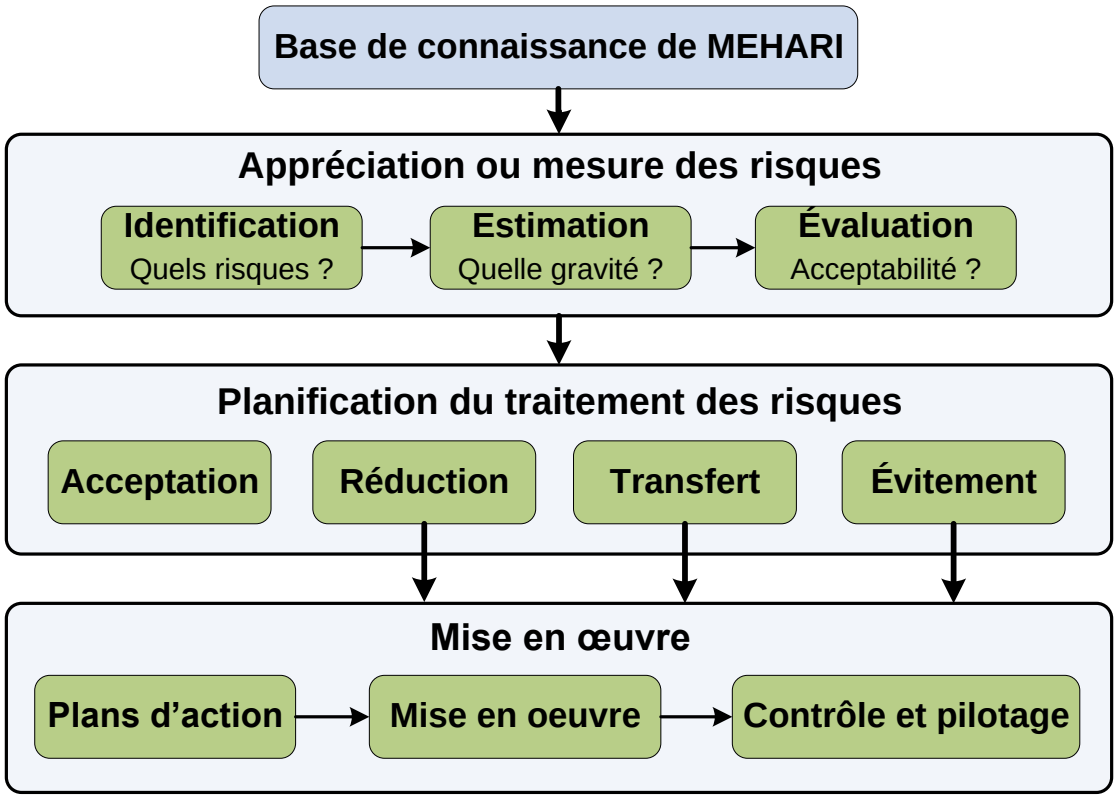
Afin d'atteindre les objectifs décrits au point 4.1.1, la méthode MEHARI préconise un plan global permettant de se conformer aux étapes et processus décrits dans la norme ISO/IEC 27005. Ce plan comprend :

- ✓ l'appréciation ou la mesure des risques;
- ✓ la planification du traitement des risques;
- ✓ la mise en œuvre du traitement et du contrôle des risques.

24. Les facteurs de réduction ont quatre types d'effet : dissuasif et préventif sur la potentialité, palliatif et de confinement sur l'impact.
25. La qualité d'une mesure est déterminée par trois critères, soit son efficacité, sa robustesse et sa mise sous contrôle (vérification).

Ce plan est schématisé comme suit :

Figure 2 - Plan global de la démarche MEHARI



Le plan global est appuyé par des outils permettant non seulement de prendre en compte, entre autres, les concepts de base, les grilles et les formules de calcul, mais également de disposer d'une base de connaissances intégrant une liste exhaustive de risques et de mesures associées. Parmi ces outils, RISICARE, accompagné d'une gestion de la base de connaissances appelée RISIBASE, offre une assistance évoluée et complète, permettant de réaliser des simulations, des visualisations et des optimisations. À titre d'exemple, RISICARE permet de simuler l'état final du niveau de sécurité global, lorsque l'on applique tel ou tel jeu de mesures de sécurité, en réponse à des scénarios de risques évalués.

RISICARE et RISIBASE sont présentés en détail au chapitre 0 du présent guide.

4.2 Limites de la méthode

La méthode MEHARI permet d'identifier les risques liés aux technologies de l'information, sous forme de scénarios de risques. Bien que les procédés administratifs, sans lesquels un mécanisme de sécurité ne peut être efficace, soient également évalués, la méthode MEHARI n'est pas un outil destiné à évaluer les processus administratifs.

Si l'on décide d'utiliser la méthode MEHARI pour analyser les risques liés à des processus administratifs, seuls seront évalués les aspects liés aux technologies de l'information qui soutiennent ces processus administratifs. Pour obtenir une évaluation complète, il sera nécessaire d'utiliser d'autres méthodes ou d'adapter certaines séries de questions et de résultats fournis par RISICARE. Ce travail peut demander des efforts importants si le processus administratif est complexe.

4.3 Scénarios de risques en matière de PRP

Si la protection des renseignements personnels[26] (PRP) et la sécurité de l'information sont étroitement liées, certains risques sont propres à la PRP. Ainsi, le domaine juridique et réglementaire des bases de connaissances MEHARI aborde la PRP du seul point de vue de la sécurité de l'information. Afin de pallier cette lacune, un groupe de travail interministériel, piloté par le ministère du Conseil exécutif, a développé des services de sécurité et des scénarios de risques afin de traiter des principes et des règles législatives liés à la PRP[27], soit :

- ✓ la collecte de renseignements personnels;
- ✓ leur accessibilité par la personne concernée;
- ✓ leur accessibilité par le personnel concerné;
- ✓ leur rectification;
- ✓ leur utilisation à l'interne (traitement);
- ✓ leur communication;
- ✓ leur détention et leur conservation;
- ✓ leur archivage et leur destruction.

Les scénarios de risques de PRP intégrés à la base de connaissances de MEHARI, classés dans la famille « Non-conformité à la législation et à la règlementation – Règlementation des renseignements personnels », sont les suivants :

- ✓ la collecte non nécessaire;
- ✓ la communication non autorisée;
- ✓ l'utilisation illicite de renseignements personnels;
- ✓ l'accès par une personne autorisée (habilitation reconnue), mais illégitime (accès non nécessaire);
- ✓ l'accès par une personne non autorisée (habilitation non reconnue);
- ✓ la détention au-delà de la limite prévue au calendrier de conservation;
- ✓ la non-destruction d'un renseignement personnel dont l'objet est accompli;
- ✓ le refus d'une demande d'accès ou d'une demande de rectification concernant un renseignement personnel.

26. Renseignement personnel : Renseignement qui concerne une personne physique et qui permet de l'identifier, à l'exception des renseignements qui ont un caractère public en vertu de la loi. Les renseignements personnels sont confidentiels, sauf dans les cas d'exception prévus par la loi.
27. On peut lire le détail des travaux du groupe de travail piloté par le ministère du Conseil exécutif dans le document « Développement de scénarios d'analyse de risques en matière de protection des renseignements personnels (PRP) intégrés à la méthodologie MEHARI », daté du 19 juin 2006.

4.4 La base de connaissances de MEHARI

La base de connaissances de la méthode MEHARI contient des données, des règles et des formules qui permettent d'en faciliter la mise en œuvre.

4.4.1 Présentation de la base de connaissances

La base de connaissances est distribuée par le CLUSIF (version 2-14 de mars 2012)[28]. Elle se présente sous la forme de feuilles de calcul[29] de plusieurs types :

- ✓ Des feuilles générales de **mise en œuvre** :

  Elles contiennent des données sur l'outil (paramètre d'affichage et description des feuilles du classeur, description du contexte de réalisation, éléments sur la navigation dans l'outil et licence d'utilisation de l'outil);

- ✓ Quatre feuilles relatives aux résultats de l'analyse des enjeux et de la classification des actifs :

  Elles contiennent les données d'identification de la typologie des actifs en présence ainsi que leur classification selon les critères de sécurité DIC(E)[30];

- ✓ Des feuilles relatives au **diagnostic**[31] des services de sécurité :

  Elles contiennent tous les questionnaires d'audit[32] permettant d'évaluer les mesures de sécurité existantes, les récapitulatifs des résultats des diagnostics, par service et par « thème » de sécurité, ainsi que les résultats des diagnostics selon la classification IS0/IEC 27001/27002 et la déclaration d'applicabilité (SOA[33]) propre à la démarche ISO;

- ✓ Des feuilles relatives à l'**évaluation** des risques :

  Elles donnent de l'information sur l'exposition naturelle aux menaces des différents événements, les scénarios de risques (en fonction des types d'actifs, de leurs vulnérabilités et des menaces), les récapitulatifs des gravités des scénarios (par types d'actifs et par types d'événements);

- ✓ Des feuilles relatives à la préparation de **plans d'action** :

  Elles contiennent le récapitulatif des scénarios par famille et les plans d'action possibles, le récapitulatif des objectifs issus des plans d'action et leur regroupement en projets;

- ✓ Quatre feuilles d'éléments permanents et de **paramétrage** de la méthode : Elles portent sur les vulnérabilités types, la grille de calcul des gravités (ou grille d'aversion) et des facteurs de

28. La base de connaissances est également accessible en utilisant l'outil RISIBASE de RISICARE (Cf. le chapitre 5.).
29. Le classeur de la base de connaissances du CLUSIF est compatible avec les formats Microsoft Excel et Open Office (version 3.1 ou plus récente).
30. DIC(E) : Disponibilité, intégrité, confidentialité, efficience (la notion d'efficience est introduite par la méthode MEHARI).
31. Diagnostic : Cf. Audit à la note suivante.
32. Audit : Opération de diagnostic qui analyse de façon exhaustive et globale le fonctionnement d'un centre, d'un service informatique ou d'un processus, afin de mesurer l'adéquation entre les ressources matérielles et humaines mises en œuvre, les besoins de l'entreprise, les objectifs recherchés et les résultats attendus.
33. SOA : Statement of applicability (déclaration d'applicabilité). SOA est un document qui identifie les contrôles (mesures) qui ont été choisis et qui donne les raisons de leur applicabilité. Ce document est fonction de l'évaluation des risques et du plan de traitement des risques.

réduction des gravités, les correspondances entre les services de MEHARI 2010 et ceux de MEHARI 2007 et, en dernier lieu, des codes de libellés des scénarios (feuille masquée[34]).

Pour obtenir plus de détails sur la base de connaissances et son utilisation dans le classeur du CLUSIF, le lecteur pourra consulter le document téléchargeable intitulé « **MEHARI 2010 : Bases de connaissances** », sur le site du CLUSIF[35].

Pour obtenir plus de détails sur la base de connaissances de l'outil RISIBASE et sur son utilisation, le lecteur pourra consulter le manuel d'utilisation du logiciel RISICARE (module RISIBASE).

4.4.2 Modifications de la base de connaissances MEHARI

Lors de l'utilisation des feuilles de la base de connaissances, il est conseillé de ne pas changer les noms des feuilles de calcul, car celles-ci sont également utilisées par les fonctions de calcul servant à la mise à jour des données.

Par contre, il est permis d'ajouter des feuilles supplémentaires dans le classeur. Il est également possible de changer le nom du classeur.

Il est également à noter que les feuilles sont protégées, à l'exception des cellules utilisées pour la saisie. **Il est fortement déconseillé de retirer la protection des feuilles du classeur CLUSIF.**

De plus, les liens entre les différents éléments de la base de connaissances sont très complexes. **Il est donc fortement recommandé de ne pas modifier la base de connaissances**.

4.5 Démarche préconisée

La démarche d'analyse de risques préconisée par la méthode MEHARI se décline en cinq étapes, soit la préparation, la classification, l'évaluation et l'analyse des mesures de sécurité, l'élaboration des plans de sécurité et, en dernier lieu, le pilotage et le contrôle des plans.

4.5.1 Étape 1 – Préparation

Cette étape de la démarche permet de situer le contexte de l'étude, d'opérer un cadrage des travaux et de procéder à d'éventuels paramétrages d'outils.

Définition du contexte

Cette activité consiste à situer le contexte de l'analyse de risques, sur les plans stratégique, opérationnel et organisationnel. Elle permet de préciser et de formaliser les aspects comme :

- ✓ le contexte politique de l'organisation;
- ✓ le cadre légal et réglementaire;
- ✓ les politiques de sécurité de l'information;
- ✓ les architectures informationnelles;
- ✓ les plans en lien avec les ressources informationnelles;

34. Bien qu'il soit recommandé de ne pas changer les données de la base de connaissances, on peut accéder à cette feuille en consultant le manuel « MEHARI 2010 : Base de connaissances, mars 2012 ».
35. http://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=METHODES ou à l'aide du logiciel Microsoft Excel.

- ✓ les fournisseurs de prestations critiques (p. ex. les impartiteurs, etc.);
- ✓ les organigrammes des unités visées de l'organisation;
- ✓ les registres d'autorité en matière de sécurité de l'information;
- ✓ les comités et les structures de pilotage de la sécurité de l'information;
- ✓ etc.

Définition du cadre de l'analyse de risques

Cette activité consiste à préciser et à formaliser le cadre de l'analyse (portée technique, portée organisationnelle et cadre de pilotage) et, en particulier, les points suivants :

- ✓ le périmètre géographique (sites, locaux, etc.);
- ✓ les systèmes visés par l'étude;
- ✓ les supports d'information visés;
- ✓ les activités et les domaines analysés (processus);
- ✓ les interlocuteurs;
- ✓ le cadre de pilotage et de gestion de l'analyse de risques;
- ✓ etc.

Définition des paramètres

Cette activité consiste à définir les paramètres techniques de l'analyse de risques, notamment :

- ✓ la grille d'acceptabilité des risques;
- ✓ la grille des potentialités intrinsèques (ou grille d'expositions naturelles);
- ✓ les grilles d'appréciation des risques résiduels.

4.5.2 Étape 2 – Classification[36]

Cette étape a pour but d'identifier les actifs dont la valeur sur le plan de la DIC(E) représente un enjeu d'importance pour l'organisation et qui, de ce fait, doivent être considérés dans le cadre de l'analyse de risques. Pour réaliser cette étape, le lecteur pourra consulter le « Guide de catégorisation de l'information » de septembre 2013.

La démarche de classification ou de catégorisation constitue donc la première étape de l'analyse de risques et en fournit les intrants. À titre d'exemple, les actifs informationnels pour lesquels un niveau d'impact « élevé » ou « très élevé », sur le plan de la DIC(E), a été attribué pourraient faire l'objet de l'analyse de risques et seraient considérés à l'étape de préparation du schéma d'audit.

Lorsque la catégorisation des actifs informationnels est déjà réalisée dans un organisme public, celui-ci pourra en utiliser les résultats comme intrant pour son analyse de risques. Il pourra également, au besoin, confirmer ces résultats dans le cadre d'un atelier de travail.

36. Bien qu'il soit recommandé de ne pas changer les données de la base de connaissances, on peut accéder à cette feuille en consultant le manuel « MEHARI 2010 : Base de connaissances, mars 2012 ».

4.5.3 Étape 3 – Évaluation et analyse des mesures de sécurité

Cette étape a pour but de diagnostiquer les mesures de sécurité en place, afin de déterminer les mesures additionnelles nécessaires pour réduire les risques qui auront été calculés.

Préparation et élaboration du schéma d'audit

Idéalement, il faudrait identifier, analyser et évaluer toutes les mesures et solutions de sécurité mises en place dans l'organisation. Cette méthode demanderait des efforts importants et ne permettrait pas de cibler l'essentiel. C'est pourquoi les services de sécurité (ou mesures) de MEHARI ont été regroupés en 14 domaines, abordés du point de vue de la sécurité :

1 - Organisation de la sécurité

2 - Sécurité des sites et bâtiments

3 - Sécurité des locaux

4 - Réseau étendu intersites

5 - Réseau local

6 - Exploitation des réseaux

7 - Sécurité des systèmes et de leur architecture

8 - Production informatique

9 - Sécurité applicative

10 - Sécurité des projets et développements applicatifs

11 - Postes de travail utilisateurs

12 - Exploitation des télécommunications

13 - Processus de management

14 - Management de la sécurité de l'information

En situant les actifs informationnels jugés critiques dans leur contexte technologique, le schéma d'audit permet de déterminer, pour chacun d'eux, les domaines de sécurité et les composantes technologiques qui seront examinés lors de l'évaluation des mesures en place.

La décomposition ainsi faite dans le schéma d'audit définit le niveau de granularité de l'étude. Il convient de préciser qu'un niveau de granularité trop fin augmente la quantité d'efforts nécessaires à l'analyse, sans augmenter nécessairement la qualité des résultats obtenus.

Évaluation des mesures en place

Cette activité correspond à celle du diagnostic (audit) des mesures de sécurité existantes au sein de l'organisation. Pour ce faire, la méthode MEHARI propose 14 questionnaires correspondant aux 14 domaines de sécurité précédemment mentionnés.

Adaptation des questionnaires

La méthode MEHARI est une méthode d'analyse de risques élaborée par un groupe d'étude français, le CLUSIF. Les logiciels RISIBASE et RISICARE sont également des logiciels conçus en France. Dans ce contexte, les expressions employées ne sont pas toujours couramment utilisées au Québec. Il peut s'avérer nécessaire, pour en faciliter la compréhension, de faire certaines adaptations, notamment en ce qui a trait aux questionnaires d'audit fournis par le CLUSIF.

Il est cependant suggéré de ne pas procéder à l'adaptation des questionnaires, en raison des travaux qui devraient être entrepris pour chaque changement de version des logiciels.

Par contre, certaines sections, comme celles concernant les assurances, ne s'appliquent pas dans un contexte gouvernemental. On pourra donc ignorer et considérer comme étant sans objet les questions correspondantes.

Gestion des questionnaires

Après avoir procédé à la définition du schéma d'audit, il y a lieu de réaliser l'évaluation des services et sous-services de sécurité[37] en place, à l'aide des questionnaires disponibles (p. ex. l'outil RISICARE). On pourra, par exemple, générer les questionnaires, en exportant, à l'aide de RISICARE, les questions en format CSV[38].

Les réponses aux questions se présentent sous la forme de « OUI/NON ». Lorsqu'une question ne s'applique pas dans le contexte de l'organisation, il suffit d'y répondre « SO » (sans objet).

Une question sans objet n'affectera pas les calculs effectués par l'outil (logiciel RISICARE); les mesures de sécurité afférentes ne seront tout simplement pas proposées au moment de la création du plan d'action.

Réflexion sur la gestion des questionnaires

Certaines difficultés peuvent se présenter, lorsque les réponses immédiates ne sont pas clairement OUI ou NON, comme, par exemple :

- ✓ OUI en général, mais il y a certaines exceptions;
- ✓ OUI en théorie, mais, en pratique, ce n'est pas certain ou ce n'est pas appliqué partout;
- ✓ OUI partiellement à x %;
- ✓ OUI, mais c'est en cours de déploiement;
- ✓ OUI, c'est prévu, mais ce n'est pas encore en place;
- ✓ Etc.

On peut gérer ces situations de la manière suivante :

- ✓ noter les réponses exactes dans l'espace « Commentaires » des questionnaires en format papier et dans l'espace prévu à cet effet, sous l'onglet **Audit** de RISICARE;
- ✓ prendre position. La position conservatrice est de répondre NON à toutes ces questions pour ne pas influencer les résultats de l'audit;
- ✓ être conscient que des résultats trop alarmistes peuvent démotiver les utilisateurs et diminuer la crédibilité des résultats;
- ✓ on peut raisonnablement répondre OUI, chaque fois que le processus de correction et de réaction au problème est en cours, et NON, dans les autres cas.

En résumé, il est important de :

- ✓ déterminer une ligne directrice, la documenter et l'appliquer de manière uniforme, tout au long du processus;
- ✓ prendre en compte, pour la pondération et l'évaluation des services, une approche sécuritaire (généralement en répondant NON) et revoir la réponse au moment de l'analyse des résultats.

37. Sous-service de sécurité : Service contribuant à atteindre la finalité à laquelle doit répondre le service de sécurité auquel il participe.
38. Les détails concernant les exportations des questionnaires sont disponibles dans le « Manuel d'utilisation de RISICARE ».

Il est également important de noter que les bases de connaissances de MEHARI ont été conçues de façon à ce que les automatismes de calcul ne considèrent pas un scénario de risque comme étant de peu d'importance et qu'ils l'éliminent, alors qu'il est d'un niveau de gravité élevé. C'est pourquoi il est nécessaire de mettre son expérience à profit avant de déterminer quelle position adopter face aux réponses qui ne sont pas franchement OUI ou NON.

Impact intrinsèque des scénarios

La détermination de l'impact intrinsèque des scénarios est l'évaluation des conséquences de l'occurrence (ou la survenance) du risque, indépendamment de toute mesure de sécurité.

Un actif informationnel est associé à chaque scénario (un scénario est défini par l'association d'un actif, d'une vulnérabilité et d'une menace) inscrit dans la base de connaissances de MEHARI. Donc, la détermination de l'impact intrinsèque d'un scénario revient simplement à déterminer l'impact associé à l'actif visé par ledit scénario, en utilisant les résultats de la classification.

Évaluation du degré d'exposition

L'un des facteurs d'influence sur le niveau de gravité d'un scénario de risque est l'exposition naturelle aux menaces de l'actif visé. Celle-ci intervient dans le calcul de la potentialité finale d'un scénario de risque. Cette potentialité finale sera la potentialité intrinsèque diminuée de l'influence des facteurs de réduction (mesures de sécurité).

La détermination de l'exposition naturelle (ou potentialité intrinsèque) est réalisée grâce à l'événement associé au scénario de risque, lequel peut être regroupé selon les types suivants : accident, malveillance, acte volontaire non malveillant, erreur.

Choix des scénarios

À la suite de l'évaluation des mesures de sécurité existantes, la méthode MEHARI propose une liste de scénarios de risques avec une évaluation de leur gravité. Cette évaluation tient compte du diagnostic des mesures, effectué précédemment. La gravité sera d'autant plus basse que les mesures de sécurité auront été diagnostiquées comme étant efficaces.

Rappelons que la gravité des scénarios est déterminée à l'aide de la potentialité et de l'impact, à partir de la grille d'aversion (ou grille de calcul de la gravité du risque), évoquée lors de la présentation de la base de connaissances, introduite au point 4.4.1.

Au cours de la phase de choix des scénarios, le niveau de gravité permettra de déterminer les scénarios de risques à retenir. À titre d'exemple, les scénarios de faible gravité pourront être éliminés.

Afin d'alléger l'étude, l'outil RISICARE propose également de définir d'autres critères permettant de procéder à un filtrage et de ne retenir que les scénarios véritablement utiles à l'analyse de risques.

4.5.4 Étape 4 – Élaboration des plans de sécurité

Cette étape est celle de la définition des plans d'action et des mesures de sécurité à mettre en place.

Choix des mesures

L'outil (RISICARE) permet de faire un choix parmi des mesures proposées contribuant à réduire les risques retenus. Ces mesures sont principalement de trois types :

- ✓ les mesures indispensables (pour les risques les plus graves);
- ✓ les mesures d'équilibrage (pour les risques relativement faibles);

- ✓ les mesures à maintenir (pour les risques faibles, dus à la présence de mesures existantes efficaces).

Ces mesures peuvent avoir un caractère général ayant un effet assez peu perceptible sur le niveau des risques à traiter comme :

- ✓ le contrôle de la circulation des visiteurs;
- ✓ la classification (catégorisation) des ressources;
- ✓ la mise en place d'un processus de gestion des incidents;
- ✓ la définition d'un processus de gestion documentaire;
- ✓ etc.

Elles peuvent également avoir un caractère plus précis ayant un effet direct et perceptible sur le niveau des risques à traiter. Ces mesures sont proposées par ordre d'importance en matière de réduction des risques à traiter.

Définition des plans

Les outils (RISICARE) permettent de définir plusieurs plans comprenant différents projets. Citons, à cet égard :

- ✓ Le plan global de sécurité (ou plan de gestion des risques), qui porte sur la vision globale, la recherche de cohérence et les orientations à long terme de l'organisme.
- ✓ Le plan opérationnel de sécurité de l'organisation, qui est la consolidation des plans opérationnels de chacune des unités administratives.
- ✓ Les plans opérationnels de l'organisation, qui sont établis pour chacune des unités administratives visées et qui permettent de concrétiser les choix de solutions adaptées aux différents contextes, aux méthodes de travail et aux technologies.

a) Plan de gestion des risques

Le plan global de sécurité (ou plan de gestion des risques) porte sur la vision globale, la recherche de cohérence et les orientations à long terme de l'organisme. Rappelons que la rédaction d'un tel plan répond à deux impératifs :

- ✓ définir une stratégie de sécurité dont les objectifs sont conformes aux enjeux de l'organisme;
- ✓ garantir la cohérence des actions en matière de sécurité, au sein de chaque unité administrative de l'organisme.

Certaines activités du plan de gestion des risques doivent être réalisées au niveau global de l'organisme (niveau transverse), afin d'assurer une bonne cohérence et une meilleure efficacité. Il s'agit, notamment, de :

- ✓ la mise en place d'une politique de sécurité;
- ✓ la mise en place d'un processus de gestion des incidents de sécurité de l'information;
- ✓ l'élaboration et la diffusion d'un programme de sensibilisation en matière de sécurité de l'information;
- ✓ la catégorisation (classification) des actifs informationnels;

- ✓ la gestion de métriques comme les seuils d'impact, la grille d'aversion, etc.;
- ✓ etc.

b) Plans opérationnels de sécurité

Les plans opérationnels se rapportent aux unités administratives visées. Ils sont déduits directement du diagnostic et traduisent le choix de solutions adaptées à différents contextes, aux méthodes de travail et aux technologies.

Le plan opérationnel est donc élaboré à partir des besoins de services de sécurité et des priorités fixées en fonction du coefficient d'influence de la mesure sur l'atténuation de la gravité des scénarios.

c) Plan opérationnel de l'organisation

Ce plan est la version consolidée de tous les plans opérationnels des unités administratives. Il permet, entre autres, de déterminer l'impact des mesures retenues sur les activités des unités administratives visées. Il permet également d'assurer le suivi de la mise en œuvre des actions retenues au sein de l'organisation.

4.5.5 Étape 5 – Pilotage et contrôle des plans

Une fois l'analyse de risques réalisée, il est important d'assurer le suivi des plans de traitement des risques. À cet effet, un comité de pilotage doit être constitué. Les personnes susceptibles de contribuer à ce comité sont, notamment, les détenteurs de l'information[39], le ROSI ou le COSI[40], le responsable de la gestion des TI[41], le RAIPRP[42], le RVI[43], etc.

Pour assurer un meilleur suivi de la mise en œuvre des plans de traitement des risques, la constitution de tableaux de bord et d'indicateurs de mesure[44] permettra de :

- ✓ vérifier l'état de la réalisation des plans;
- ✓ suivre l'évolution des niveaux de risques (contrôle régulier des mesures);
- ✓ corriger les écarts éventuels.

4.5.6 Mise en œuvre de la démarche

On peut envisager de mettre sur pied une ou plusieurs équipes de travail pour la réalisation de l'analyse de risques, dans le cadre d'un ou de plusieurs projets. Le nombre d'équipes à former dépend, entre autres, du contexte organisationnel, de la complexité et de l'ampleur du ou des projets. La mise en œuvre de la démarche sera identique à celle de tout autre projet.

39. Détenteur de l'information : Un employé désigné par son organisme public, appartenant à la classe d'emploi de niveau cadre et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.
40. COSI : Conseiller organisationnel de la sécurité de l'information.
41. TI : Technologies de l'information.
42. RAIPRP : Responsable de l'accès à l'information et de la protection des renseignements personnels.
43. RVI : Responsable de la vérification interne.
44. À cet égard, le lecteur pourra consulter le document gouvernemental intitulé « ».

Équipe de projets et intervenants

L'équipe d'un projet de réalisation d'une analyse de risques pourrait être composée du chargé de projet, du COSI, du RVI, du RAIPRP ou de tout autre intervenant dans un domaine connexe[45].

À titre d'exemple, les tâches de cette équipe pourraient inclure les suivantes :

- ✓ planifier les activités et l'échéancier de travail;
- ✓ procéder à la collecte des renseignements requis;
- ✓ organiser les entrevues et ateliers de travail et y participer;
- ✓ produire les documents de travail;
- ✓ consolider et présenter les résultats.

Planification du projet et organisation du travail

Comme pour tout projet, la planification et l'organisation du travail sont déterminantes pour l'analyse de risques et devront être communiquées aux intervenants concernés.

4.6 Variantes de la méthode MEHARI

La méthode MEHARI a connu plusieurs évolutions. Elle est actuellement disponible en différentes versions (déclinaisons).

4.6.1 MEHARI Expert

Il s'agit de la version complète de la méthode, décrite tout au long du présent guide. Cette version est particulièrement utile pour les analyses de risques de grande envergure ou portant sur des domaines particulièrement critiques. Sa mise en œuvre requiert la participation de spécialistes de la gestion des risques de sécurité de l'information.

4.6.2 MEHARI Pro

Réalisée conjointement par l'ASIQ[46] et le CLUSIF[47], MEHARI Pro n'a pas encore été officiellement publiée, en date de la rédaction du présent guide. Elle constitue une version allégée de la méthode MEHARI Expert. Elle est généralement destinée aux petites et moyennes organisations, particulièrement lorsque l'analyse de risque porte sur :

- ✓ un nombre réduit de types d'actifs primaires, de services de sécurité, de questionnaires de diagnostic, etc.;
- ✓ des analyses de risques d'envergure moyenne;
- ✓ des domaines d'activité de criticité moyenne.

45. Cf., par exemple, les rôles et responsabilités définis dans le « guide de mise en place du PGRSI ».
46. ASIQ : Association de la sécurité de l'information du Québec.
47. Cf. le site du CLUSIF : https://www.clusif.asso.fr/fr/production/mehari/presentation.asp

L'approche actuelle de Méhari Pro présente les points forts suivants[48] :

- ✓ allègement et simplification de l'application de la méthode MEHARI Expert;
- ✓ maintien de la rigueur de l'approche méthodologique;
- ✓ exploitation de la richesse et de la cohérence de sa base de connaissances, laquelle est une extraction de celle de MEHARI Expert;
- ✓ prise en compte des niveaux d'efficacité d'une mesure de sécurité pour diminuer les risques (en effet, certaines mesures de sécurité apportent plus de valeur ajoutée);
- ✓ plus de facilité pour un non-spécialiste de bien analyser les situations et de proposer des mesures tenant compte de la maturité et de la capacité de l'organisation à mettre en œuvre les solutions proposées;
- ✓ plus de simplicité pour illustrer la progression en matière de gestion de risques de l'organisation.

4.6.3 MEHARI Manager

Il s'agit de la version la plus légère de la méthode MEHARI Expert. Elle permet de réaliser une analyse rapide des principales exigences de sécurité, particulièrement dans le cas de nouveaux projets, ou pour ajouter à une analyse complète, précédemment effectuée, un domaine d'activité qui n'était pas dans la portée d'origine.

La démarche permet, par exemple :

- ✓ d'effectuer une analyse dans le cadre d'un projet applicatif ou d'un nouveau système d'information;
- ✓ de travailler avec les directions métiers en utilisant une terminologie et une démarche immédiatement compréhensibles;
- ✓ de traiter des situations de risques précises, éventuellement non couvertes par MEHARI 2010.

La démarche MEHARI Manager peut compléter une démarche classique effectuée avec MEHARI 2010 qui aura permis d'identifier les besoins de sécurité les plus critiques, les menaces pesant sur l'organisation ainsi que l'état des mesures de sécurité. En effet, elle s'appuie sur le modèle de risque de MEHARI et utilise les mêmes éléments d'évaluation et de traitement du risque[49].

De façon générale, l'analyse et l'identification des risques se font sous forme d'entrevues avec les responsables des domaines d'activités pertinents, en remplissant des « fiches de risque » (description des risques, des menaces, des impacts, des mesures de réduction de risque, etc.).

48. Méhari Pro, Vue d'ensemble et principes directeurs, CLUSIQ
49. Tiré de : www.clusif.asso.fr

5. L'outil RISICARE

Le chapitre 5 est consacré à la description de l'outil logiciel RISICARE d'aide à la réalisation d'une analyse de risques de sécurité de l'information par la méthode MEHARI Expert.

5.1 Présentation de RISICARE

« RISICARE – Logiciel de gestion de risques » est, en fait, le regroupement de deux modules : RISICARE et RISIBASE. Ces deux modules fonctionnent sous l'environnement *Windows* et utilisent des composantes et des interfaces comme les arborescences, les menus déroulants, les pages à onglets, les fonctions d'aide, les fonctions « glisser-déplacer », les menus contextuels (*pop-up menus*), etc. Le logiciel décrit ci-dessous correspond à la version 7 de RISICARE 2010.

5.1.1 Le module RISICARE – Réalisation d'une analyse de risques

Le module RISICARE offre les fonctionnalités suivantes :

- ✓ la création, l'ouverture, l'enregistrement, l'impression et la fermeture d'une étude de risques;
- ✓ la gestion des grandes étapes de l'étude, sur :
  - la page pilotage;
  - la page Enjeux;
  - la page Schéma d'audit;
  - la page Résultat d'audit;
  - la page Graphiques;
  - la page Indicateurs;
  - la page Expo;
  - la page Risques;
  - la page Traitement des risques.
- ✓ la copie, l'importation et l'exportation de notes d'audit;
- ✓ l'exportation des données de l'analyse de risques dans le format CSV;
- ✓ etc.

5.1.2 Le module RISIBASE – Formatage des bases de connaissances

Le logiciel offre les fonctionnalités suivantes :

- ✓ la création, l'ouverture, l'enregistrement, l'impression et la fermeture d'une base de connaissances;
- ✓ le formatage de l'audit;
- ✓ le formatage des scénarios;

- ✓ le formatage des indicateurs;
- ✓ le tableau des actifs (saisie);
- ✓ l'exposition naturelle (saisie);
- ✓ la saisie des paramètres de base (critères d'impact, nature d'agression, status[50] I ou status RI, status P, grille d'aversion ou d'acceptabilité des risques, codes pour scénarios);
- ✓ l'exportation et l'importation en format CSV des données des questionnaires d'audit et des scénarios;
- ✓ etc.

5.2 Stratégie d'utilisation de RISICARE

Cette section décrit brièvement les fonctionnalités de l'outil RISICARE et de la base de connaissances RISIBASE.

5.2.1 Utilisation de RISICARE

Les fonctionnalités de RISICARE comprennent, entre autres, la classification des actifs informationnels, l'évaluation des mesures en place dans une organisation et son exposition aux risques, l'identification des scénarios de risques et le choix de mesures à mettre en place.

Classification

Sur la page des enjeux, RISICARE permet d'intégrer les résultats de la classification (catégorisation) par types de ressources, ou pour des ressources propres à l'organisme.

Évaluation des mesures de contrôle en place

RISICARE permet, à partir du schéma d'audit, de générer des questionnaires qui servent à évaluer la présence et l'efficacité des mesures de contrôle. À la suite de l'enregistrement des réponses aux questions, la page d'audit permet de compiler les résultats des questionnaires d'évaluation, afin d'obtenir un diagnostic de la sécurité en place. RISICARE propose les résultats sous forme de tableaux et de graphiques.

Évaluation du degré d'exposition

RISICARE permet de déterminer le degré d'exposition d'une organisation aux scénarios de risques[51] ou dysfonctionnements. L'un des facteurs d'influence sur le niveau de risque d'un organisme, face à un scénario de risque particulier, est son exposition naturelle à un événement[52]. Cette exposition peut varier d'un organisme à un autre.

50. Status : Le « status » est un indicateur spécifique de l'absence ou de la présence de mesures de sécurité par rapport à un facteur de risque et, dans ce dernier cas, de l'évaluation de leur « qualité », c'est-à-dire de leur « efficacité » et de leur « robustesse », autrement dit de leur expérience par rapport à un facteur de risque et pour un ensemble de cellules. Dans un premier temps, les « status » seront évalués par type de mesure, puis ils seront consolidés à un niveau global en « status RI », de Réduction d'Impact; puis en « status P » de Potentialité, qui permettront de déterminer la gravité d'un scénario donné.
51. Rappelons que le scénario est constitué par l'association d'un actif, d'une vulnérabilité et d'une menace.
52. Au sens MEHARI du terme, l'événement est l'une des composantes de la menace (en plus des circonstances et de l'acteur).

Les événements auxquels une organisation peut être exposée sont répertoriés dans les bases de connaissances de MEHARI, en quatre catégories, soit accident, malveillance, actes volontaires non malveillants, erreurs.

Identification des scénarios de risque

À la suite de l'évaluation des mesures de contrôle en place, RISICARE génère automatiquement les scénarios de risque et leur attribue une gravité.

Choix des mesures à mettre en place

RISICARE propose une série de mesures susceptibles d'atténuer les niveaux de risque, en agissant sur la potentialité ou l'impact des scénarios de risques proposés. Les mesures sont établies selon l'ordre décroissant de leur coefficient d'influence. Lorsque l'équipe en charge de l'analyse de risques choisit d'appliquer une mesure, RISICARE calcule de nouveau la gravité des scénarios de risques visés par la mesure. Il permet ainsi de faire des simulations de mesures et d'élaborer des variantes de plans d'action.

5.2.2 Utilisation de RISIBASE

L'outil RISIBASE permet de gérer les bases de connaissances de la méthode MEHARI. Il n'est pas utilisé lors de l'analyse de risques, puisque RISICARE intègre dans ses fichiers, lors de la création d'une étude, toutes les composantes de la méthode (questions, scénarios, paramètres, etc.). Il est utilisé lorsque l'on veut apporter des modifications aux bases de connaissances fournies avec la méthode MEHARI ou lorsqu'un organisme veut créer ses propres bases de connaissances.

RISIBASE contient l'ensemble des paramètres de la méthode MEHARI, tels que les paramètres de pondération des questions, la définition des scénarios avec les types de mesures, les tables de définition des « status P » et des « status RI » ainsi que la grille de tolérance au risque[53].

53. Les organismes publics et entreprises du gouvernement peuvent se procurer RISICARE auprès du Secrétariat du Conseil du trésor (cf. chapitre 1).

Annexe I – Définitions

Actif informationnel : Une information, quels que soient son canal de communication (téléphone analogique ou numérique, télégraphe, télécopie, voix, etc.) ou son support (papier, pellicule photographique ou cinématographique, ruban magnétique, support électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitué par une organisation.

Audit : Opération de diagnostic qui analyse, de façon exhaustive et globale, le fonctionnement d'un centre, d'un service informatique ou d'un processus, afin de mesurer l'adéquation entre les ressources matérielles et humaines mises en œuvre, les besoins de l'entreprise, les objectifs recherchés et les résultats attendus.

Cadre de pilotage : Cf. **Pilotage**.

Catégorisation ou classification : Processus d'assignation d'une valeur à certaines caractéristiques d'une information, lesquelles définissent le degré de sensibilité de cette information et, conséquemment, la protection à lui accorder.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes autorisées.

Détenteur de l'information : Un employé désigné par son organisme public, appartenant à la classe d'emploi de niveau cadre, et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.

Diagnostic : cf. **Audit**.

Disponibilité : Propriété d'une information ou d'une ressource informationnelle d'être accessible en temps voulu et de la manière requise par une personne autorisée.

Document : Selon la Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1), un document est un ensemble « constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles l'une de ces formes ou en un autre système de symboles.
[...] est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite. »

Gravité : Exprime l'effet conjugué de la potentialité (probabilité) qu'un scénario de risque se matérialise et de l'importance de ses conséquences (impact).

Impact : Importance des conséquences d'un scénario de risque.

Intégrité : Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni détruite sans autorisation. L'intégrité fait référence à l'exactitude et à l'état complet de l'information.

Intrinsèque : En l'absence de toute mesure de sécurité.

Pilotage : Le pilotage de la gestion des risques est identique à tout pilotage de projet. Il est réalisé à l'aide d'outils comme les tableaux de bord et les indicateurs, la reddition de compte, l'évaluation périodique et les décisions d'actions de correction.

Potentialité : Capacité ou probabilité qu'un événement adverse ou un scénario de risque se matérialise.

Mesure ou mécanisme de sécurité : Manière concrète de mettre en œuvre un service de sécurité.

Processus : Regroupement d'événements d'affaires, agencés selon une logique de création de valeur, exécutés dans le but de livrer un résultat.

Renseignement personnel : Renseignement qui concerne une personne physique et qui permet de l'identifier, à l'exception des renseignements qui ont un caractère public en vertu de la loi[54]. Les renseignements personnels sont confidentiels, sauf dans les cas d'exception prévus par la loi.

Risque : Exprime le fait qu'un événement puisse empêcher de maintenir ou d'atteindre les objectifs d'une organisation ou d'une activité dans les conditions fixées ou encore de satisfaire une finalité programmée.

Scénario de risque : Description d'un événement adverse ou d'un dysfonctionnement et de la manière dont celui-ci peut survenir.

Service de sécurité : Réponse possible à un besoin spécifique de sécurité. Il est assuré par un ou un ensemble de mécanismes ou de mesures de sécurité.

Sous-service de sécurité : Service contribuant à atteindre la finalité à laquelle doit répondre le service de sécurité auquel il participe.

Status : Le « status » est un indicateur spécifique de l'absence ou de la présence de mesures de sécurité par rapport à un facteur de risque et, dans ce dernier cas, de l'évaluation de leur « qualité », c'est-à-dire de leur « efficacité » et de leur « robustesse », autrement dit de leur expérience par rapport à un facteur de risque et pour un ensemble de cellules. Dans un premier temps, les « status » seront évalués par type de mesure, puis ils seront consolidés à un niveau global en « status RI », de **R**éduction d'**I**mpact, puis en « status P » de **P**otentialité, qui permettront de déterminer la gravité d'un scénario donné.

Système d'information : Système constitué de l'équipement, des procédures, des logiciels, des applications, des ressources humaines, ainsi que des données qui y sont traitées, et dont le but est de fournir de l'information afin de soutenir une fonction d'affaires.

54. L'article 57 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels prévoit, notamment, cinq cas d'exception où les renseignements ont un caractère public. Par exemple, l'alinéa 2 de l'article 57 indique que sont publics « le nom, le titre, la fonction, l'adresse et le numéro de téléphone du lieu de travail et la classification, y compris l'échelle de traitement rattachée à cette classification, d'un membre du personnel d'un organisme public » (sauf s'ils peuvent avoir pour effet de révéler le traitement de la personne). Il en est de même pour « le nom et l'adresse de l'établissement du titulaire d'un permis délivré par un organisme public et dont la détention est requise en vertu de la loi pour exercer une activité ou une profession ou pour exploiter un commerce » (alinéa 5 de l'article 575).

Annexe II – Cadre légal, normatif et administratif

Le présent document prend appui sur des fondements légaux, normatifs et administratifs tels que les lois, les directives, les normes, les pratiques et les standards gouvernementaux suivants :

- ✓ la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03);
- ✓ la Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1);
- ✓ la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1);
- ✓ la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- ✓ la Directive sur la sécurité de l'information gouvernementale;
- ✓ le cadre gouvernemental de gestion de la sécurité de l'information;
- ✓ le cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information;
- ✓ les pratiques gouvernementales en matière de sécurité de l'information;
- ✓ Les politiques et directives de sécurité de l'information propres à chaque organisme les lois sectorielles régissant la mission de chaque organisme.
- ✓ les normes internationales, notamment les normes ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 ET ISO/IEC 3100.

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique