METHODES

MEHARI 2010

Guide de la démarche d'analyse et de traitement des risques

Version 2 : Avril 2011

Espace Méthodes

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11, rue de Mogador, 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

Date	Calendrier des révisions
Janvier 2010	Origine (avec Mehari 2010 V1)
Avril 2011	version 2 ; prenant en compte les aménagements apportés par Mehari 2010 V2 mis en ligne en novembre 2010 et clarifiant les corrélations avec la norme ISO/IEC 27001:2005

Sommaire

Remerciements

Le CLUSIF tient à remercier ici les membres de l'espace méthodes qui ont rendu possible la réalisation de ce document.

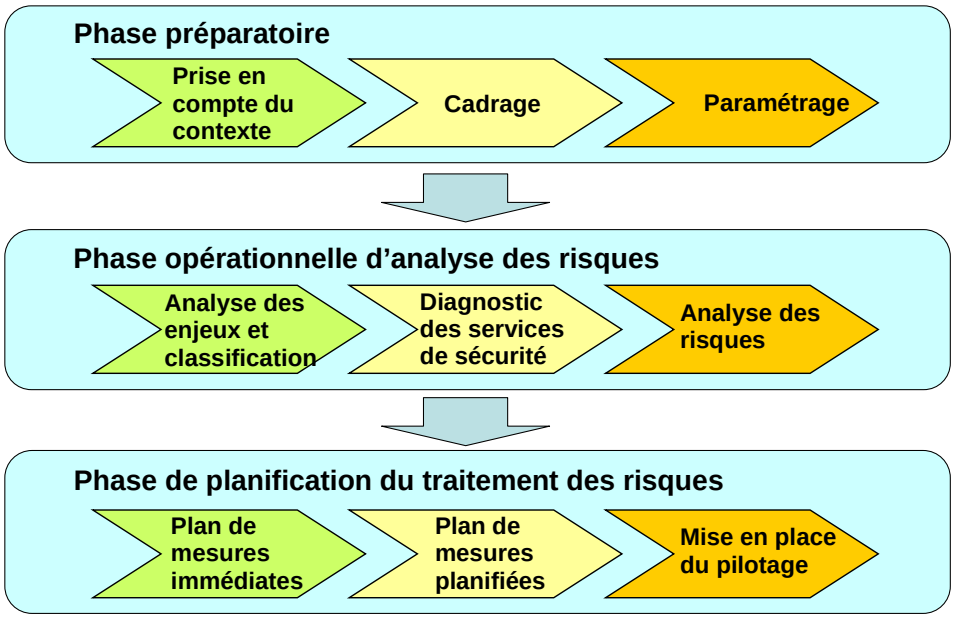
Introduction

Ce guide présente l'ensemble de la démarche d'analyse et de traitement des risques de Méhari et en détaille les différentes étapes.

Il est basé sur l'utilisation de la base de connaissances de Méhari 2010.

Présentation générale de l'ensemble de la démarche

La démarche Méhari comprend trois phases, conformément au schéma ci-dessous.



Nous décrivons, dans les chapitres et paragraphes suivants chacune de ces phases.

Conformité avec la norme ISO/IEC 27001:2005

Il est à noter que la démarche d'analyse et de traitement des risques utilisée par Mehari est complète et conforme au processus d'amélioration continue présenté par la norme ISO/IEC 27001:2005 ; par ailleurs, Mehari répond aux recommandations de la norme ISO/IEC 27005:2008.

La description des étapes faite dans ce guide peut être rapprochée de celle figurant dans la norme ISO/IEC 27003 mais elle est réalisée de manière plus concrète et utilisable directement par l'organisme dans le cadre de sa gestion des risques ou de son SMSI en s'appuyant sur Mehari.

Par ailleurs, les bases de connaissance contiennent un domaine "14 Msi" qui, dans le cas d'un système de management de la sécurité, permet de diagnostiquer si sa réalisation est satisfaisante.

Comme le fichier base de connaissance, chargé depuis le site du CLUSIF, ne peut décrire à l'avance les actions effectivement réalisées et les responsabilités lors de l'analyse et du traitement des risques, certains des livrables définis dans ce document peuvent contribuer à la création d'un dossier propre aux activités et aux engagements pris lors de l'analyse de risque et enregistrer l'appropriation de la méthode réalisée par l'organisme qui met en œuvre la méthode.

1. Phase préparatoire

La phase préparatoire comprend elle-même trois étapes principales, qu'il est préférable de mener successivement, sans que cela soit absolument nécessaire.

Ces étapes sont :

1.1 La prise en compte du contexte

- 1.1.1 Contexte stratégique
- 1.1.2 Contexte technique
- 1.1.3 Contexte organisationnel

1.2 Le cadrage de la mission d'analyse et de traitement des risques

- 1.2.1 Périmètre technique
- 1.2.2 Périmètre organisationnel
- 1.2.3 Structure de pilotage de la mission

1.3 La fixation des principaux paramètres de l'analyse des risques

- 1.3.1 Grille d'acceptabilité des risques
- 1.3.2 Grille des Expositions Naturelles
- 1.3.3 Grilles d'appréciation des risques

1.1 La prise en compte du contexte

1.1.1 Prise en compte du contexte stratégique

Objectifs

Formaliser un certain nombre de points qui méritent d'être éclaircis et pris en compte pour l'analyse et le traitement des risques.

Les points suivants devraient être abordés :

- Le positionnement stratégique de l'entité sur son marché (pour les entreprises commerciales) ou de l'organisation dans son contexte politique (pour les entreprises ou services publics) :
  - Position sur le marché (dominante ou non)
  - Caractère concurrentiel de l'activité
  - Criticité des services fournis
  - Médiatisation des événements et incidents de fonctionnement
  - Etc.
- Les contraintes pesant sur le fonctionnement et l'organisation de l'entité
  - Contraintes légales
  - Contraintes réglementaires
  - Les normes à respecter
- La politique de sécurité de l'information
  - Objectifs de sécurité (s'ils existent)
  - Rôle de l'analyse et du traitement des risques dans la politique de sécurité
  - Donneur d'ordre de l'analyse et du traitement des risques
  - Support de la Direction

Conditions préalables

Il importe, pour démarrer cette tâche que la mission d'analyse et de traitement des risques ait été précisée par un ordre de mission.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Les responsables d'activité
- La Direction générale
- La Direction juridique (contraintes légales)
- Le RSSI

Livrable

Le livrable est constitué d'un document de synthèse reprenant les divers points cités en objectifs.

Processus – conseils de mise en œuvre

Le processus comprend les éléments suivants :

- Recueil des divers éléments disponibles sur les aspects cités en objectifs
- Établissement d'une synthèse
- Validation en Comité de Direction ou directement auprès de la Direction Générale

1.1.2 Prise en compte du contexte technique

Objectifs

Formaliser et recueillir un certain nombre de données et renseignements techniques qui seront nécessaires pour l'analyse et le traitement des risques.

Les points suivants devraient être traités :

- L'architecture du système d'information
  - Architecture des réseaux
  - Architecture systèmes
  - Architecture applicative
  - Cartographie d'ensemble.
- Plans (ou risques) d'évolutions techniques à court, moyen et long terme
  - Plans d'évolutions
  - Pérennité des solutions opérationnelles
- Fournisseurs et prestataires externes critiques
  - Fournisseurs de services opérationnels (fournisseurs d'accès, services réseaux, infogérance, etc.)
  - Fournisseurs de logiciels
  - Prestataires de services occasionnels (maintenance, assistance, etc.)

Conditions préalables

Existence préalable d'une cartographie ou, a minima, d'un inventaire à jour des équipements, systèmes et applications informatiques

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques, ou un membre de son équipe.

Sont parties prenantes :

- La DSI (Direction des Systèmes d'Information)
- La Direction des réseaux (si différente de la DSI)

Livrable

Le livrable est constitué d'une cartographie synthétique et de listes annexes (équipements, applications, etc.).

Processus – conseils de mise en œuvre

Le processus comprend les éléments suivants :

- Recueil des divers éléments techniques disponibles.
- Établissement d'une synthèse
- Validation auprès de la DSI

1.1.3 Prise en compte du contexte organisationnel

Objectifs

Formaliser et recueillir un certain nombre de données et renseignements relatifs à l'organisation de l'entité qui seront nécessaires pour l'analyse et le traitement des risques.

Les points suivants devraient être traités :

- L'organigramme complet de l'entité
  - Rattachements hiérarchiques
  - Liens et rattachements fonctionnels
- Répartition des responsabilités en ce qui concerne la sécurité
  - Notes et descriptions de fonction
  - Répartition des responsabilités entre responsable de site, responsables d'activités, DSI et RSSI
- Structures de pilotage
  - Processus de proposition et de validation des plans d'action
  - Composition et modes de fonctionnement des structures de pilotage

Conditions préalables

Existence préalable d'un organigramme complet et détaillé et de notes de définition de fonction.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques, ou un membre de son équipe.

Sont parties prenantes :

- La DRH (Direction des Ressources Humaines) ou la Direction de l'organisation (si elle existe)
- La Direction Financière et Administrative
- Le RSSI

Livrable

Le livrable est constitué d'une note de synthèse sur l'organisation et les responsabilités, en ce qui concerne la sécurité de l'information et la mise en place des plans d'action éventuellement nécessaires.

Processus – conseils de mise en œuvre

Le processus comprend les éléments suivants :

- Recueil des divers éléments organisationnels disponibles.
- Établissement d'une synthèse
- Validation auprès de la Direction Générale

1.2 Le cadrage de la mission d'analyse et de traitement des risques

1.2.1 Le périmètre technique de l'analyse et du traitement des risques

Objectifs

Formaliser les limites techniques de l'analyse et du traitement des risques pour la mission en cours de lancement.

Les points suivants devraient être traités :

- Périmètre géographique
  - Sites et localisations
  - Pays éventuellement
- Systèmes d'information concernés
  - Systèmes d'information généraux
  - Exclusion ou non des systèmes de gestion de processus industriels
  - Exclusion ou non des systèmes de conception assistée
  - Etc.
- Types de supports d'information concernés
  - Médias informatiques
  - Médias papiers
  - Voix et supports audio

Conditions préalables

Existence préalable de la synthèse sur la cartographie du système d'information.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- La Direction Générale ou le donneur d'ordre
- Le RSSI

Livrable

Le livrable est constitué d'une note de synthèse sur le périmètre technique de la mission d'analyse et de traitement des risques.

Processus – conseils de mise en œuvre

Le processus comprend les éléments suivants :

- Recueil des diverses options et des choix du donneur d'ordre.
- Établissement d'une synthèse
- Validation auprès de la Direction Générale

1.2.2 Le périmètre organisationnel de l'analyse et du traitement des risques

Objectifs

Formaliser les limites organisationnelles de l'analyse et du traitement des risques pour la mission en cours de lancement.

Les points suivants devraient être traités :

- Périmètre d'activité
  - Activités concernées
  - Filiales, Départements ou Services éventuellement
- Types de risques inclus dans la mission
  - Tous les risques liés à l'information
  - Limitation à un ou plusieurs types de risques (divulgation d'information, fraude, par exemple)

Conditions préalables

Existence préalable de la synthèse sur l'organisation de l'entité.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- La Direction Générale ou le donneur d'ordre
- Le RSSI

Livrable

Le livrable est constitué d'une note de synthèse sur le périmètre organisationnel de la mission d'analyse et de traitement des risques.

Processus – conseils de mise en œuvre

Le processus comprend les éléments suivants :

- Recueil des diverses options et des choix du donneur d'ordre.
- Établissement d'une synthèse
- Validation auprès de la Direction Générale

1.2.3 La structure de pilotage de la mission

Objectifs

Formaliser la structure de pilotage de la mission et les relations entre l'équipe d'animation de l'analyse et du traitement des risques avec le donneur d'ordre et la Direction Générale.

Les points suivants devraient être traités :

- Structure et fonctionnement du Comité de Pilotage de la mission
  - Membres participants
  - Fréquence de réunion
- Supports et modes de validation des livrables

Conditions préalables

Existence préalable de la synthèse sur l'organisation de l'entité.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- La Direction Générale ou le donneur d'ordre
- Le RSSI

Livrable

Le livrable est constitué d'une note de synthèse sur la structure de pilotage de la mission d'analyse et du traitement des risques. Une réunion de lancement, avec le Comité de Pilotage, devrait être organisée.

Processus – conseils de mise en œuvre

Le processus comprend les éléments suivants :

- Recueil des diverses options et des choix du donneur d'ordre.
- Établissement d'une synthèse
- Validation auprès de la Direction Générale

1.3 La fixation des paramètres techniques de l'analyse des risques

Les paramètres à fixer avant l'analyse de risques proprement dite sont :

- La grille d'acceptabilité des risques
- La grille des potentialités intrinsèques ou grille d'expositions naturelles
- Les grilles d'appréciation des risques

1.3.1 La détermination de la grille d'acceptabilité des risques

Objectifs

Formaliser la grille d'acceptabilité des risques qui servira à déterminer si un scénario de risque donné est acceptable ou non.

Cette grille est présentée et introduite dans *« MEHARI 2010 - Principes fondamentaux et spécifications fonctionnelles »*.

Conditions préalables

Existence préalable de la synthèse sur la structure de pilotage de l'analyse et du traitement des risques.

En outre, le Comité de pilotage, qui est une partie prenante essentielle de cette tâche, doit avoir, au préalable, bien compris le modèle de risque Méhari.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- La Direction Générale ou le donneur d'ordre
- Le comité de pilotage de la mission
- Le RSSI

Livrable

Le livrable est constitué de la grille d'acceptabilité des risques et de la terminologie associée à chaque catégorie de risque, applicable à l'organisme.

Processus – conseils de mise en œuvre

Le processus comprend les éléments suivants :

- Élaboration d'un projet de grille d'acceptabilité des risques.
- Validation auprès de la Direction Générale

Nota : le livrable est constitué à partir de la grille générale proposée dans la base de connaissances Méhari, feuille « Gravité ». La validation par la Direction Générale est nécessaire.

1.3.2 La détermination de la grille des expositions naturelles

Objectifs

Formaliser la grille des expositions naturelles ou grille des potentialités intrinsèques qui servira à déterminer la potentialité intrinsèque des scénarios de risque de la base de connaissances.

Cette grille est présentée et introduite dans le « *guide de l'analyse et du traitement des risques* » et dans le document « *Méhari 2010 – Principes fondamentaux et spécifications fonctionnelles* ».

Conditions préalables

Le Comité de pilotage, qui est une partie prenante essentielle de cette tâche, doit avoir, au préalable, bien compris le modèle de risque Méhari.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Le comité de pilotage de la mission
- Le RSSI
- Les services généraux, les responsables métiers, la DRH, la DSI selon les types d'événements considérés.

Livrable

Le livrable est constitué de la grille des expositions naturelles retenue par l'organisme.

Nota : cette grille est très sensible à des variations de l'environnement interne comme externe et devra être reconsidérée en conséquence.

Processus – conseils de mise en œuvre

Le processus comprend les éléments suivants :

- Élaboration d'un projet de grille des Expositions Naturelles.
- Validation auprès du Comité de Pilotage

Nota : le livrable est constitué à partir de la grille générale des Expositions Naturelles proposée dans la base de connaissances Méhari (feuille « Expo ») et donnée, à titre d'exemple, dans le document : « *Méhari 2010 Guide de l'analyse et du traitement des risques* ». La validation par le Comité de Pilotage est nécessaire.

1.3.3 La détermination des grilles d'appréciation des Potentialités et Impacts résiduels

Objectifs

Formaliser les grilles permettant d'apprécier (d'évaluer) la potentialité et l'impact résiduels en fonction de la potentialité et de l'impact intrinsèques et des facteurs de réduction de risque de chaque scénario de la base de connaissances.

Ces grilles sont présentées et introduite dans le « *guide de l'analyse et du traitement des risques* » et dans le document « *Méhari 2010 – Principes fondamentaux et spécifications fonctionnelles* ».

Conditions préalables

Le Comité de pilotage, qui est une partie prenante essentielle de cette tâche, doit avoir, au préalable, bien compris le modèle de risque Méhari.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Le comité de pilotage de la mission
- Le RSSI

Livrable

Le livrable est constitué des grilles d'appréciation des risques.

Processus – conseils de mise en œuvre

Le processus comprend les éléments suivants :

- Élaboration de projets de grilles (3 pour l'appréciation de la potentialité résiduelle et 4 pour celle de l'impact résiduel).
- Validation auprès du Comité de Pilotage

Nota : le résultat peut être constitué des grilles générales proposées dans la base de connaissances Méhari (feuille Grilles_IP) et données, à titre d'exemple, dans le document : « *Méhari 2010 Guide de l'analyse et du traitement des risques* ». La validation par le Comité de Pilotage est souhaitable.

2. Phase opérationnelle d'analyse des risques

La phase d'analyse des risques comprend elle-même trois étapes principales.

Ces étapes sont :

2.1 L'analyse des enjeux et la classification des actifs

2.1.1 Échelle de valeur des dysfonctionnements

Objectifs

Formaliser les enjeux de chaque activité de l'entité, enjeux de sécurité qui seront utilisés pour classifier les actifs.

La finalité et les objectifs de l'échelle de valeur des dysfonctionnements sont décrits dans le Guide « *Méhari 2010 – Analyse des enjeux et classification des actifs* ».

L'échelle de valeur des dysfonctionnements permet de mettre en évidence, pour chaque activité :

- Les dysfonctionnements redoutés
- Les critères qualitatifs ou quantitatifs permettant d'apprécier le niveau d'impact résultant de ces dysfonctionnements, selon une échelle à 4 niveaux.

Conditions préalables

Il importe, pour démarrer cette tâche, que la mission d'analyse des enjeux ait été précisée par un ordre de mission.

Il est souhaitable que cette tâche débute par une réunion de lancement en précisant le déroulement et les attentes de la Direction.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Les responsables d'activité
- La Direction générale
- Le RSSI

Livrable

Le livrable est constitué de l'échelle de valeur des dysfonctionnements.

Processus – conseils de mise en œuvre

Le processus, qui est largement décrit dans le "*guide de l'analyse des enjeux et de la classification*", comprend les éléments suivants :

- Réunion de lancement
- Réunions avec les responsables d'activité permettant de mettre en évidence les dysfonctionnements potentiels et les critères d'appréciation de leur gravité
- Synthèse par activité
- Synthèse pour l'ensemble de l'entité
- Validation en Comité de Direction ou directement auprès de la Direction Générale

2.1.2 Classification des actifs

Objectifs

Déterminer la sensibilité de chaque classe d'actifs, sous forme d'une classification.

Les classes d'actifs utilisées par la base de connaissances de Méhari 2010 sont des regroupements, par domaine d'activité, des types d'actifs primaires tels que définis dans le document « *Méhari 2010 – Principes fondamentaux et spécifications fonctionnelles* ».

La classification est à faire avec un niveau de 1 à 4 pour les critères de Disponibilité, d'Intégrité, de Confidentialité et d'Efficience exigée.

La classification a pour objectif de remplir les tableaux de classification T1, T2 et T3 de la base de connaissance ainsi qu'indiqué dans le document « *Méhari 2010 – Guide de l'analyse des enjeux et de la classification* ». Chaque cellule de ce tableau devra ainsi indiquer le degré maximal de gravité que pourrait représenter le dommage subi suite à la perte de disponibilité, d'intégrité ou de confidentialité pour ce type d'actif ou pour le non respect de l'exigence d'efficience vis à vis d'une loi ou d'une réglementation, pour l'activité concernée (précisée sur chaque ligne des tableaux).

Conditions préalables

Il est fortement souhaitable, voire indispensable, que l'échelle de valeur des dysfonctionnements ait été déterminée au préalable. Une classification directe des actifs peut introduire des biais préjudiciables à l'analyse des risques.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Les responsables d'activité
- La DSI
- Le RSSI
- La Direction juridique (pour le tableau T3)

Livrables

Les livrables sont constitués des tableaux de classification T1, T2 et T3.

Processus – conseils de mise en œuvre

Le processus, qui est décrit dans le *« guide de l'analyse des enjeux et de la classification »,* comprend les éléments suivants :

- Indication, dans les tableaux T1 et T2, des processus correspondant aux divers domaines d'activité pris en compte lors de l'élaboration de l'échelle de valeur des dysfonctionnements.
  Remplissage de ces 2 tableaux, par domaine d'activité, et cellule par cellule :

  Chaque cellule ou case du tableau représentant le niveau du dommage subi suite à la perte de disponibilité, d'intégrité ou de confidentialité) par un type d'actif (indiqué en tête de colonne), pour une activité donnée (précisée sur chaque ligne du tableau), on recherchera :

  - Si ce dommage peut conduire à un ou plusieurs dysfonctionnements indiqués dans l'échelle de valeur des dysfonctionnements.
  - Si tel est le cas, quel niveau d'impact maximal peut être atteint et ce niveau constituera alors la classification à reporter dans la cellule du tableau

- Si tel n'est pas le cas, un 1 (plus faible niveau d'impact) sera reporté dans la cellule du tableau

- Indication dans le tableau T3, qui comporte une colonne pour chaque exigence indiquée en tête de colonne (E pour Efficience), du niveau d'impact qu'aurait une non-conformité pour chacun des processus métier et transversaux cités. Ceci est à faire avec les responsables d'activité assistés de la Direction Juridique et de la Direction de la Communication
- Remplissage, sur le même principe, des lignes des 3 tableaux correspondant à la prise en compte des processus transversaux s'ajoutant aux processus propres à chaque activité métier (qui peuvent indiquer un impact plus important que la synthèse des besoins de chaque activité métier)
- Validation en Comité de Direction

2.1.3 Tableau d'impact intrinsèque

Objectifs

Le tableau d'impact intrinsèque, qui sera utilisé pour apprécier les risques de la base de connaissances, est rempli par les automatismes de la méthode.

La base de connaissances des scénarios de risque de Méhari (voir le « *guide d'analyse et de traitement des risques* » de Méhari) contient des scénarios (plus de 800 dans la base 2010) qui font explicitement référence à un type d'actif et, pour leur appréciation, à un impact intrinsèque qui dépend du type d'actif.

Le tableau qui contient les valeurs des impacts intrinsèques des scénarios de la base de connaissances est le tableau d'impact intrinsèque.

Conditions préalables

Il est nécessaire d'avoir au préalable rempli les tableaux de classification T1, T2 et T3 (voir paragraphe précédent).

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques ou un membre de son équipe.

Sont parties prenantes :

- Les responsables d'activité
- La Direction juridique
- La Direction de la communication
- Le RSSI

Livrables

Le livrable est constitué du tableau d'impact intrinsèque (onglet « Classif » de la base).

Processus – conseils de mise en œuvre

L'option de base, décrite ci-dessous consiste à remplir le tableau d'impact intrinsèque standard. Le processus comprend les éléments suivants :

- Pour les deux premières parties du tableau d'impact intrinsèque (actifs de type services ou données), chaque ligne du tableau d'impact intrinsèque correspond à un type d'actif et comporte jusqu'à 3 valeurs d'impact (pour D, I et C) à remplir. Chaque valeur correspond au maximum d'une des colonnes de l'un des tableaux T1 ou T2 (la colonne ayant le même type de dommage pour le même type d'actif). Les automatismes de calcul de Mehari 2010 permettent d'effectuer automatiquement les opérations de remplissage du tableau d'impact intrinsèque en reportant la valeur maximum de chaque colonne à partir de T1 et T2.
- Pour la dernière partie, qui ne comporte qu'une colonne (E pour Efficience), le même mode de calcul est réalisé automatiquement à partir du tableau T3.
- Validation en Comité de Direction

2.2 Le diagnostic de la qualité des services de sécurité

2.2.1 Établissement du schéma d'audit

Objectifs

Les services de sécurité sont des fonctions dont la matérialisation, l'implémentation, peuvent revêtir des formes variées dans la même entité, que l'on doit considérer alors comme autant de variantes d'un même service nécessitant des diagnostics différenciés.

L'objectif de cette étape est d'identifier les **variantes** pour lesquelles il convient de faire des diagnostics séparés.

Conditions préalables

Il est nécessaire d'avoir au préalable une bonne connaissance du contexte technique et organisationnel (étapes 1.1.2 et 1.1.3)

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques ou un membre de son équipe.

Sont parties prenantes :

- Le donneur d'ordre
- Le responsable des services généraux
- La DSI
- Le RSSI

Livrables

Le livrable est constitué du schéma d'audit qui comprend le nombre de variantes par domaine de diagnostic.

Processus – conseils de mise en œuvre

Les considérations relatives au schéma d'audit et les conseils d'élaboration du schéma sont décrits dans le document : « *Méhari 2010 – Guide du diagnostic de l'état des services de sécurité* ».

Le processus comprend les éléments suivants :

- Analyse, pour chaque domaine du nombre de variantes nécessaires.
- Validation du schéma d'audit complet avec l'animateur de la mission d'analyse de risques

2.2.2 Diagnostic de la qualité des services de sécurité

Objectifs

Dresser un état de la qualité de chaque variante de service de sécurité. Ce diagnostic d'ensemble sera utilisé pour évaluer les facteurs de réduction de risque lors des étapes d'analyse et d'appréciation des risques.

Conditions préalables

Il est nécessaire d'avoir au préalable une bonne connaissance du contexte technique et organisationnel (étapes 1.1.2 et 1.1.3) et d'avoir établi le schéma d'audit.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Les responsables de domaines techniques (services généraux, Systèmes d'information, Réseaux, Télécommunication, Parc de microordinateurs, Sécurité applicative, développements applicatifs, etc.) ou de domaines de management (Juridique, Organisation, etc.)
- La DSI
- Le RSSI

Livrables

Le livrable est constitué de fichiers de diagnostics (un par domaine de diagnostic et par variante de domaine), selon la base de connaissances de Méhari qui comprend 14 domaines de diagnostic (version 2010).

La feuille Services de la base de connaissance est automatiquement constituée par les résultats des diagnostics pour chaque variante et par sous-service de sécurité.

Ces fichiers peuvent être accompagnés de synthèses aux fins de communication (synthèses graphiques, en particulier).

Processus – conseils de mise en œuvre

Les conseils relatifs au processus de diagnostic sont donnés dans le document : « *Méhari 2010 – Guide du diagnostic de l'état des services de sécurité* ».

Le processus comprend les éléments suivants :

- Diagnostic de chaque variante de domaine de diagnostic avec le responsable concerné.
- Corrections et adaptations éventuelles avec les responsables de domaines
- Établissement de synthèses
- Validation en Comité de Direction

2.3 L'appréciation des risques

2.3.1 Sélection des scénarios de risque

Objectifs

Faire une sélection de scénarios de risques parmi les 800 figurant dans la base de connaissance afin de limiter l'analyse aux situations pouvant s'avérer critiques

Conditions préalables

Il est nécessaire d'avoir effectué au préalable les étapes de la phase préparatoire et la classification des actifs.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Les responsables d'activité
- Le RSSI

Livrables

Le livrable est constitué d'une fiche de synthèse résumant les options prises et d'une liste de scénarios à analyser en détail (il est possible de soustraire des scénarios en forçant la valeur 0 dans la colonne « sélection directe » de la feuille de calcul « Scénarios » de la base de connaissances Méhari 2010).

Processus – conseils de mise en œuvre

Les indications relatives à la sélection de scénarios sont données dans le document : « *Méhari 2010 – Guide de l'analyse et du traitement des risques* ».

Le processus comprend les éléments suivants :

- Détermination d'une stratégie de sélection :
  - Scénarios dont l'impact intrinsèque est supérieur à une limite (3, par exemple)
  - Scénarios dont la gravité intrinsèque est supérieure à une limite (idem)
  - Sélection touchant des types d'actifs particuliers
- Validation en Comité de Direction
- Sélection effective des scénarios dans la base

2.3.2 Estimation des risques

Objectifs

Dresser un bilan de la gravité des scénarios de risques sélectionnés, en fonction des facteurs de réduction de risque découlant de l'état des services de sécurité.

Conditions préalables

Il est nécessaire d'avoir au préalable effectué l'ensemble des étapes précédemment décrites.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Est partie prenante :

- Le RSSI

Livrables

Le livrable principal est constitué par la base de connaissances Méhari complétée, remplie et finalisée.

Cette base contient des synthèses, par type d'actif et par type d'événements

Des présentations complémentaires peuvent y être ajoutées, montrant, par exemple une cartographie des risques (dans un plan I, P) ou toute autre forme de représentation synthétique.

Processus – conseils de mise en œuvre

Les conseils relatifs au processus d'estimation des risques sont donnés sont données dans le document : « *Méhari 2010 – Guide de l'analyse et du traitement des risques* ».

Le processus comprend les éléments suivants :

- Incorporation automatique dans la feuille scénarios, par les formules de la méthode, des résultats des diagnostics de l'état des services de sécurité.
- Possibilité de visualiser rapidement les conséquences de valeurs différentes pour l'Impact intrinsèque (obtenu en 2.1.3) et/ou l'exposition naturelle (obtenue en 1.3.2), en forçant d'autres valeurs dans les colonnes I décidé et P décidée de la feuille scénarios.
- Analyse des scénarios et corrections éventuelles des facteurs de réduction de risques si des anomalies sont mises en évidence
- Établissement de synthèses
- Présentation en Comité de Direction

3. Phase de planification et de traitement des risques

La phase de planification et de traitement des risques comprend elle-même trois étapes principales.

Ces étapes sont :

3.1 La planification des actions immédiates

3.1.1 Sélection des risques à traiter en priorité absolue

3.1.2 Choix des mesures à mettre en œuvre immédiatement

3.2 La planification des mesures à décider dans le cadre courant

3.2.1 Stratégie de traitement et priorités

3.2.2 Choix des mesures et planification

3.3 La mise en place du pilotage du traitement des risques

3.3.1 Organisation du pilotage

3.3.2 Indicateurs et tableau de bord

3.1 La planification des actions immédiates

3.1.1 Sélection des risques à traiter en priorité absolue

Objectifs

Faire une sélection de scénarios de risques devant être traités en priorité et en dehors du cycle de décision habituel.

Le critère de choix à prendre en compte est essentiellement le niveau de gravité le plus élevé (niveau 4), mais d'autres critères peuvent être décidés.

Conditions préalables

Il est nécessaire d'avoir effectué au préalable les étapes de la phase d'analyse des risques.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Les responsables d'activité
- Le RSSI

Livrables

Le livrable est constitué d'une fiche récapitulant les risques intolérables à traiter en priorité.

Processus – conseils de mise en œuvre

Les indications relatives à la sélection de scénarios sont données dans le document : « *Méhari 2010 – Guide de l'analyse et du traitement des risques* ».

Le processus comprend les éléments suivants :

- Détermination d'une stratégie de sélection :
  - Scénarios dont la gravité intrinsèque atteint le niveau maximal (4)
  - Autres critères éventuels retenus
- Validation auprès des Responsables d'activité
- Sélection effective des scénarios dans la base

3.1.2 Choix des mesures à mettre en œuvre immédiatement

Objectifs

Proposer à la Direction Générale des actions immédiates pour réduire les risques considérés comme intolérables. L'objectif n'est pas forcément de rendre directement acceptables les risques résiduels mais au moins de les faire passer du stade d'intolérable (gravité de niveau 4) au stade d'inadmissible (niveau 3) quitte à gérer, dans une phase ultérieure, leur passage du niveau 3 à un niveau inférieur.

Conditions préalables

Il est nécessaire d'avoir effectué au préalable les étapes de la phase d'analyse des risques.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Les responsables d'activité
- Le RSSI
- La Direction Générale

Livrables

Le livrable est constitué de plans d'action : un plan par risque intolérable à réduire.

Processus – conseils de mise en œuvre

Pour ces risques très critiques, l'essentiel est de pouvoir agir rapidement.

Le processus comprend les éléments suivants :

- Détermination d'une stratégie d'action :
  - Transfert ou Acceptation (signifiés par la lettre T ou A dans la colonne (Scén. Accepté ou transféré) de la feuille Scénarios). La gravité des scénarios correspondants devenant automatiquement nulle.
  - Évitement (par des mesures organisationnelles)
  - Réduction (par des mesures techniques ou organisationnelles)
- Choix de mesures rapides à mettre en œuvre.
- Planification et chiffrement des dépenses à engager
- Validation préliminaire avec les Responsables d'activité
- Validation en Comité de Direction ou auprès de la Direction Générale

3.2 La planification des actions à décider dans le cadre courant

3.2.1 Stratégie de traitement et priorités

Objectifs

Faire un choix dans les stratégies de traitement possibles, et les critères à prendre en compte pour fixer des priorités, en considérant que l'on ne pourra généralement pas s'attaquer à tous les risques inadmissibles simultanément.

Au-delà d'un premier niveau de sélection lié à la gravité des risques (on considère en priorité les risques de niveau 3), les aspects à considérer peuvent être :

- La rapidité de mise en œuvre (permettant d'obtenir rapidement des résultats et de motiver l'encadrement)
- L'optimisation des coûts
- L'optimisation des délais
- L'optimisation des moyens humains nécessaires à la mise en œuvre des plans d'action
- L'impact (favorable ou défavorable) sur les utilisateurs
- Le choix de thèmes particuliers (secours, sauvegardes, contrôle d'accès, etc.) pour leur impact sur la sensibilisation des utilisateurs,
- Etc.

Conditions préalables

Il est nécessaire d'avoir effectué au préalable les étapes de la phase d'analyse des risques.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Les responsables d'activité
- La DSI
- Le RSSI

Livrables

Le livrable est constitué d'une fiche récapitulant la stratégie de traitement et les priorités.

Processus – conseils de mise en œuvre

Le processus comprend les éléments suivants :

- Évaluation des avantages et inconvénients de chaque option
- Débat et arbitrage préliminaire avec les responsables d'activité, et les acteurs concernés
- Validation en Comité de Direction

3.2.2 Choix des mesures et planification

Objectifs

Proposer au Comité de Direction des plans d'action (généralement pluriannuels) pour réduire ou éviter les risques considérés comme inadmissibles (niveau 3).

L'objectif n'est pas forcément de s'attaquer simultanément à tous les risques inadmissibles mais d'avoir un plan d'ensemble, éventuellement sur plusieurs années, en fonction des priorités précédemment décidées.

Conditions préalables

Il est nécessaire d'avoir effectué au préalable les étapes de la phase d'analyse des risques.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Les responsables d'activité
- La DSI
- Le RSSI
- La Direction Générale

Livrables

Le livrable est constitué de plans d'action, généralement regroupés par projets.

Processus – conseils de mise en œuvre

Pour ces risques inadmissibles, l'essentiel est de pouvoir décider, selon le cycle habituel de décision, les actions à engager..

Le processus comprend les éléments suivants :

- Choix de mesures à mettre en œuvre (lors du déroulement de ce processus, plusieurs démarches sont possibles : voir le guide de l'analyse et du traitement des risques).
- Planification et chiffrement des dépenses à engager
- Présentation des objectifs en terme de risques et d'évolution des risques dans le temps
- Validation préliminaire avec les Responsables d'activité et la DSI
- Validation en Comité de Direction (selon le cycle habituel d'arbitrage)

3.3 La mise en place du pilotage du traitement des risques

3.3.1 Organisation du pilotage

Objectifs

Mettre en place l'organisation de suivi et de pilotage du traitement des risques et, notamment :

- Les membres du Comité de pilotage
- Sa présidence
- La fréquence des réunions de pilotage
- Les missions du Comité

Conditions préalables

Il est nécessaire d'avoir effectué au préalable les étapes de la phase de planification puis de déploiement.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Les responsables d'activité
- La DSI
- Le RSSI

Livrables

Le livrable est constitué d'une fiche récapitulant l'organisation du pilotage du traitement des risques.

Processus – conseils de mise en œuvre

Le processus comprend les éléments suivants :

- Proposition d'organisation élaborée par le responsable de la mission, avec le RSSI
- Choix des membres du Comité
- Validation en Comité de Direction

3.3.2 Choix des Indicateurs et du tableau de bord

Objectifs

Proposer au Comité de Pilotage un ensemble d'indicateurs et un tableau de bord permettant de :

- Vérifier le déploiement des mesures décidées et l'avancement des projets
- Vérifier l'évolution des niveaux de risques
- Décider des actions correctrices nécessaires

Conditions préalables

Il est nécessaire d'avoir défini au préalable les missions du Comité de pilotage et sa composition.

Acteurs et parties prenantes

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Les responsables d'activité
- La DSI
- Le RSSI

Livrables

Le livrable est constitué d'un projet de tableau de bord et de la liste des indicateurs qui seront utilisés.

Processus – conseils de mise en œuvre

Les indicateurs devraient être choisis de manière à permettre tant un suivi à court terme (avancement, difficultés rencontrées, suivi du budget, etc.) qu'une vision globale et à moyen et long terme (nombre de situations de risques par niveau, prévisions pluriannuelles, etc.)

Le processus comprend les éléments suivants :

- Choix des indicateurs.
- Définition du tableau de bord.
- Validation préliminaire avec les Responsables d'activité et la DSI
- Validation en Comité de Direction

Annexe A

Table de correspondance Mehari 2010 - ISO/IEC 27001:2005

Objectifs :

- Rappeler la liste de contrôle des activités de l'analyse de risque Mehari.
- Pouvoir suivre ainsi la progression des étapes de l'analyse de risque.
- Mettre cette liste en regard des activités requises pour implémenter un SMSI

Démarche Mehari 2010		**ISO/IEC 27001**	
N°	**Etape**	**§**	**PDCA**
1	Phase préparatoire		
1.1	Prise en compte du contexte		
1.1.1	Contexte stratégique	4.2.1.b	P
1.1.2	Contexte technique	4.2.1.a	P
1.1.3	Contexte organisationnel	4.2.1.c	P
1.2	Cadrage de la mission		
1.2.1	Périmètre technique	4.2.1.a	P
1.2.2	Périmètre organisationnel	4.2.1.a	P
1.2.3	Structure de pilotage	5.1	
1.3	Fixation des paramètres techniques		
1.3.1	Grille d'acceptabilité des risques	4.2.1.e	P
1.3.2	Grille des expositions naturelles	4.2.1.d	P
1.3.3	Grille des potentialités et des impacts résiduels	4.2.1.e	P
2	Phase opérationnelle		
2.1	Analyse des enjeux et classification des actifs		
2.1.1	Echelle de valeur des dysfonctionnements	4.2.1.e	P
2.1.2	Classification des actifs	4.2.1.d	P
2.1.3	Tableau d'impact intrinsèque	4.2.1.e	P
2.2	Diagnostic de la qualité des services de sécurité		
2.2.1	Etablissement du schéma d'audit	Absent	C
2.2.2	Diagnostic de la qualité des services de sécurité	4.2.3.e	C
2.3	Appréciation des risques		
2.3.1	Sélection des scénarios de risque	Absent	P
2.3.2	Estimation des risques	4.2.1.d	P
3	Phase de planification et de traitement des risques		
3.1	Planification des actions immédiates		
3.1.1	Sélection des risques à traiter en priorité absolue	Absent	P
3.1.2	Choix des mesures à mettre en œuvre immédiatement	4.2.1.f, 4.2.1.g	P
3.2	Planification des mesures à décider dans le		

Démarche Mehari 2010		ISO/IEC 27001	
N°	**Etape**	**§**	**PDCA**
	cadre courant		
3.2.1	Stratégie de traitement et priorités	4.2.1.f, 4.2.2 partiel	P, D
3.2.2	Choix des mesures et planification	4.2.1.g, 4.2.1.i, 4.2.2 partiel	P, D
3.3	Mise en place du pilotage du traitement des risques		
3.3.1	Organisation du pilotage	4.2.3 partiel	C
3.3.2	Indicateurs et tableau de bord	4.2.4 partiel	A

Par ailleurs, les éléments du SMSI concernant la documentation (§ 4.3 de la norme ISO 27001) et les responsabilités du management (§ 5 de la norme) sont abordés dans chacune des étapes de Mehari (en particulier lors de la phase d'analyse et lors du diagnostic des services de sécurité)

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Téléchargez les productions du CLUSIF sur

www.clusif.asso.fr