MEHARI

Process Reference Model

DOCUMENT HISTORY

Version	Modification	Date	Author
V00_00		23.02.2006	CSI
V00_01			

DIFFUSION

Organisation	Name	Diffusion mode
CLUSSIL – GT ANARISK	Membres présents	Electronique

Table of contents

1 Introduction

1.1 Mehari

Reference: « Mehari V3: principes et mécanismes»

Selon le CLUSIF (Club de la sécurité des systèmes d'information français) , toutes les parties impliquées dans la sécurité de l'information s'accordent pour reconnaître que les risques des délits informatiques sont aujourd'hui plus sérieux que jamais, ceci notamment en raison de la convergence d'un certain nombre de tendances propices à l'augmentation des délits informatiques, telles que le développement de l'informatique répartie et mobile, l'essor d'Internet pour les communications professionnelles, le développement de la culture informatique, des outils de piratage de plus en plus perfectionnés, etc. Dans la mesure où cette situation devrait se poursuivre dans un avenir prévisible, les entreprises s'en trouveront encore plus menacées.

Développée par le CLUSIF (et initialement issue du croisement de MELISA et de MARION), MEHARI (MEthode Harmonisée d'Analyse de RIsques) est une méthode d'analyse et de management des risques liés au système d'information. Elle permet, par une analyse rigoureuse et une évaluation quantitative des facteurs de risque propres à chaque situation, de concilier les objectifs stratégiques et les nouveaux modes de fonctionnement de l'entreprise avec une politique de maintien des risques à un niveau convenu. Elle est mise en œuvre par de nombreuses entreprises (PME/PMI et grandes entreprises) en France, Belgique, Suisse, au Luxembourg et au Quebec.

MEHARI apporte donc un modèle de gestion du risque et une démarche modulable. Dans l'optique d'une analyse des risques, au sens de l'identification de toutes les situations de risque et de la volonté de s'attaquer à tous les risques inacceptables, le domaine couvert pas MEHARI ne s'arrête pas aux systèmes informatiques. Les modules de diagnostic couvrent ainsi, outre les systèmes d'information et de communication, l'organisation générale, la protection générale des sites, l'environnement de travail des utilisateurs et les aspects réglementaires et juridiques.

2 Process Reference Model

2.1 PRM Liste des processus

processus PRIMAIRES
de risque opérationnel

Analyse des enjeux et classification des ressources (AECR)

Diagnostic de l'état des services de sécurité (DESS)

Recherche des situations de risque (RSR)

Analyse des situations de risque (ASR)

Gestion des risques de projets de développement (GRPD)

Réalisation d'un plan d'action (RPA)
RPA.1 Réalisation d'un plan d'action basé sur l'analyse de risque
RPA.2. Réalisation d'un plan d'action basé sur l'audit

3 Description des processus et indicateurs de performance

3.1 Avant-propos

3.2 AECR Analyse des enjeux et classification des ressources

Process ID	**AECR**
Process Name	**Analyse des enjeux et classification des ressources**
Process Purpose	L'objectif de l'analyse des enjeux et classification des ressources est d'identifier les dysfonctionnements potentiels et la gravité de leurs conséquences. [ref. 5.1.1] NOTE 1 : Dans le domaine de la sécurité, les enjeux sont vus comme des conséquences d'événements venant perturber le fonctionnement voulu de l'entreprise ou de l'organisme. NOTE 2 : L'analyse des enjeux doit : • identifier les activités majeures de l'entité et leurs finalités; • déterminer les dysfonctionnements qui peuvent être redoutés; • évaluer le niveau de gravité de ceux-ci, activité par activité. NOTE 3 : La classification des ressources doit : • identifier les ressources intervenant dans les activités de l'entité; • pour chacune d'elles, déterminer la manière dont elle peut conduire à un dysfonctionnement préalablement identifié ainsi que la gravité qui en résulterait.
Process Outcomes	Comme résultat d'une réalisation de l'analyse des enjeux et classification des ressources, on obtiendra : 1. une échelle de valeurs des dysfonctionnements, qui rassemble en un document unique l'ensemble des types de dysfonctionnements et les seuils de criticité correspondants; [ref. 5.2.2.5] 2. une classification des ressources avec, pour chacun des critères principaux (confidentialité, intégrité, disponibilité), le niveau de gravité d'un dysfonctionnement de la ressource selon ce critère; [ref. 5.2.3.3]

3.3 DESS Diagnostic de l'état des services de sécurité

Process ID	**DESS**
Process Name	**Diagnostic de l'état des services de sécurité**
Process Purpose	L'objectif du diagnostic de l'état des services de sécurité est de répertorier les services de sécurité existants dans l'entité et d'évaluer le niveau de qualité de chacun d'eux. [ref. 6.1] NOTE 1 : Préalablement, il est nécessaire de déterminer un schéma d'audit qui fait la distinction entre des domaines de solutions différents, devant faire l'objet d'analyses séparées. NOTE 2 : Chaque service de sécurité identifié doit être évalué en tenant compte de son efficacité, de sa robustesse et de sa mise sous contrôle.
Process Outcomes	Comme livrables du diagnostic de l'état des services de sécurité, on obtiendra : 1. une liste des services de sécurité présents dans l'entité; [ref. 6.2.5] 2. un schéma d'audit déterminant les variantes d'audit à effectuer selon les domaines de solutions considérés; [ref. 6.4.1] 3. une évaluation détaillée de l'état des services ainsi identifiés. [refs. 6.3, 6.4.2]

3.4 RSR Recherche des situations de risque

Process ID	**RSR**
Process Name	**Recherche des situations de risque**
Process Purpose	L'objectif de la recherche des situations de risque est de détecter et de sélectionner les situations de risque auxquelles l'entité se trouve exposée. NOTE 1 : Deux approches complémentaires devraient être utilisées concurremment : • L'approche directe à partir de l'échelle de valeurs des dysfonctionnements [voir AECR] • La recherche systématique à partir d'une base de connaissance
Process Outcomes	Comme résultat de la recherche des situations de risque, on obtiendra : 1. liste des risques à soumettre à une analyse plus détaillée; [ref. 8]

3.5 ASR Analyse des situations de risque

Process ID	**ASR**
Process Name	**Analyse des situations de risque**
Process Purpose	L'objectif de l'analyse des situations de risque est de quantifier une notion de danger auquel l'entité est exposée.
Process Outcomes	Comme résultat d'une analyse des situations de risque, on obtiendra : 1. une évaluation de la potentialité de scénarios de risque ; [ref. 7.3.1] NOTE 1 : L'évaluation de la potentialité comprend l'évaluation de l'exposition naturelle [ref. 7.3.1.1], ainsi que l'évaluation des facteurs de dissuasion et prévention [refs. 7.3.1.2, 7.3.1.3]. 2. une évaluation de l'impact de scénarios de risque ; [ref. 7.3.2] NOTE 1 : L'évaluation de l'impact comprend l'évaluation de l'impact intrinsèque [ref. 7.3.2.1], ainsi que l'évaluation des facteurs de protection [ref. 7.3.2.2], palliation [ref. 7.3.2.3] et récupération [ref. 7.3.2.4] 3. une évaluation globale du risque; [ref. 7.3.3]

3.6 GRPD Gestion des risques de projets de développement

Process ID	**GRPD**
Process Name	**Gestion des risques de projets de développement**
Process Purpose	L'objectif de la gestion des risques de projets de développement est de réaliser un plan de sécurité spécifique au projet de développement.
Process Outcomes	Comme résultat de la gestion des risques de projets de développement, on obtiendra : 1. une échelle de valeurs des dysfonctionnements, qui rassemble en un document unique l'ensemble des types de dysfonctionnements et les seuils de criticité correspondants; [ref. 9.3.4] NOTE 1 : voir processus AECR 2. une analyse de risques des scénarios définis par les responsables du projet; [ref. 9.3.5] NOTE 1 : voir processus ASR 3. un relevé des besoins de sécurité par activité [refs. 9.3.1, 9.3.6] 4. le plan d'action de sécurité du projet [ref. 9.3.6]

3.7 RPA Réalisation d'un plan d'action

3.7.1 RPA.1 Réalisation d'un plan d'action basé sur l'analyse de risque

Process ID	**RPA.1**
Process Name	**Réalisation d'un plan d'action basé sur l'analyse de risque**
Process Purpose	L'objectif de la réalisation d'un plan d'action basé sur l'analyse de risque est de définir, déployer et mettre en oeuvre ou renforcer des services de sécurité en s'appuyant sur une analyse organisée et méthodique des risques.
Process Outcomes	Comme résultat de la réalisation d'un plan d'action basé sur l'analyse de risque, on obtiendra : 1. une politique de sécurité [ref. 9.1.1.1] ; 2. les objectifs de sécurité [ref. 9.1.1.2] ; 3. un paramétrage de la métrique de risque [ref. 9.1.1.2] ; 4. la charte de management [ref. 9.1.1.3] ; 5. le plan opérationnel de sécurité par entité [ref. 9.1.2] ; NOTE 1 : ce produit comprend les éléments suivants : - analyse des enjeux et classification des ressources [voir AECR] - diagnostic de l'état de la sécurité [voir DESS] - identification et évaluation des risques encourus par l'entité [voir RSR et ASR] - expression des besoins d'amélioration des niveaux de sécurité

3.7.2 RPA.2 Réalisation d'un plan d'action basé sur l'audit

Process ID	**RPA.2**
Process Name	**Réalisation d'un plan d'action basé sur l'audit**
Process Purpose	L'objectif de la réalisation d'un plan d'action basé sur l'audit est de définir, déployer et mettre en oeuvre ou renforcer des services de sécurité directement à partir d'un audit de sécurité.
Process Outcomes	Comme résultat de la réalisation d'un plan d'action basé sur l'audit, on obtiendra : 1. le plan d'action de sécurité [ref. 9.2.4] ; NOTE 1 : ce produit comprend les éléments suivants : - analyse des enjeux et classification des ressources [voir AECR] - diagnostic de l'état de la sécurité [voir DESS] - identification et évaluation des risques encourus par l'entité [voir RSR et ASR] - expression des besoins d'amélioration des niveaux de sécurité;