CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

MEHARI 2010 : synthèse des nouveautés et des évolutions

La continuité dans le changement

Tout en conservant l'essentiel!

Le modèle de risque, les éléments et les quantifications

L'analyse des enjeux

Le diagnostic des services de sécurité

L'analyse par scénarios de risque

L'assistance offerte par les bases de connaissance :

- *** questionnaires d'audit professionnels**
- *** scénarios pour une gestion individuelle des risques**
- *** matrices de décision (Impact - Potentialité - Gravité)**

MEHARI est une méthode de gestion de risque rapide et solide

Cette version est enrichie!

Evolutions alignées sur la normalisation :

ISO/IEC 27005:2008 Information security risk management

Evolutions des traitements de la méthode :

Nouveaux domaines d'audit

Identification des scénarios

Plans d'amélioration et de suivi de la sécurité

Fonctions de calcul intégrées

Retours d'expérience de la distribution libre :

Outils d'aide pour les évaluations et traitements de risque

Documentation et Guides de mise en œuvre

ISO/IEC 27005:2008 ….

- expose les exigences pour choisir une méthodologie,
- confirme l'importance de la gestion continue des risques,
- reprend la démarche ISO 13335, comme MEHARI,
- cadre les étapes et les concepts

… et MEHARI

MEHARI 2010 est conforme aux exigences de ISO 27005 ++

- quantification des enjeux – menaces – vulnérabilités,
- diagnostic des mesures de sécurité,
- disponibilité des scénarios de situations de risque,
- optimisation des plans de réduction des risques.

MEHARI complète ISO 27005

- Approfondissement du traitement des risques
- Affirmation de l'intérêt de l'analyse individuelle des risques plutôt qu'une gestion globale et indirecte
- Scénarios et mesures de sécurité directement associés
- Groupement des mesures selon leur contribution: dissuasion – prévention – confinement – palliation
- Efficacité et rapidité de traitement
- Reproductivité des résultats

Evolutions de la méthode 1/4

Description des actifs primaires:

Données, services, processus

Processus de classification des actifs revu

Domaines de sécurité :

Nouveaux domaines : gestion du parc des postes de travail,

Télécommunications, législations, SMSI

Visualisation de variantes d'audit

classification des mesures : efficacité, robustesse, contrôle

➔ audit adapté à la maturité de l'organisation

Evolutions de la méthode 2/4

Structuration et description des scénarios

actif + dommage : vulnérabilité,

événement, circonstances, acteur : menace

regroupement par familles : par actif et type de dommage

Evaluation des risques

séparation des mesures de récupération (assurance)

➔simplification du traitement

Evolutions de la méthode 3/4

Plans de traitement

regroupement des scénarios par actif et dommage

visualisation des gravités

aides à la sélection de projets:

prioritisation facilitée

scénarios, services (niveau cible)

«besoin de service»

outillage de base pour les aides à la décision

Evolutions de la méthode 4/4

Déploiements

niveaux de qualité anticipés par projet

dates d'achèvement

Pilotage du traitement des risques

suivi des indicateurs de niveau des risques

Documentation et aides

Reprise de la documentation pour :

- **prendre en compte ISO 27005 (termes et concepts)**
- **améliorer l'utilisation de la méthode**

Tableur ou chiffrier (Excel, OpenOffice ensuite):

- **réarranger les feuilles en séquence**
- **introduire les automatismes de calcul (option)**

Documentation et base

		MEHARI 2007	2010
	Présentation générale *	✓	✓+27005
	Principes et …	Mécanismes	Spécifications
Guides	analyse des enjeux et de la classification	✓	✓+27005
Guides	diagnostic de l'état des services de sécurité	✓	✓
Guides	analyse et traitement des risques	✓	✓+plans
Guides	démarche d'analyse et de traitement des risques	--	✓
ZIP	**Base de connaissance Excel**	✓	✓+plans
ZIP	de la base de connaissances *		✓
Manuels de référence	des services de sécurité	✓	✓
Manuels de référence	des scénarios de risque (méthode globale)	✓	--
	Évolutions par rapport aux versions précédentes	✓	✓

Comment aider le CLUSIF?

ASSOCIATION SANS BUT LUCRATIF

1- en adhérant toujours plus nombreux,

2- en encourageant d'autres à adhérer,

3- en participant aux travaux sur Mehari,

pour améliorer la sécurité de votre information.

4- en faisant retour d'idées, d'améliorations, etc.

sur mehari.info

et, pourquoi pas ?

5- en devenant sponsor du CLUSIF.

Merci d'avance

CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Pour la gestion des risques, MEHARI utilise le modèle ISO 13335 et 27005