CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

MEHARI 2010
Une méthode de gestion de risques conforme à la norme ISO 27005

Comment dépasser les objectifs a minima de la norme pour permettre une véritable gestion des risques

Sommaire

Gérer ses risques

- Gérer ses risques : pourquoi ?
- Gérer ses risques : comment ?
  - Les concepts fondamentaux de l'ISO 27005 et les questions ouvertes
  - La nécessité d'un modèle de risque en complément des concepts de l'ISO 27005

Gérer les risques : pourquoi ?

Objectifs cités dans la norme ISO/IEC 27005 :

En introduction , au chapitre 1 – Domaine d'application :

- La présente Norme internationale … est conçue pour aider à la mise en place de la sécurité de l'information basée sur une approche de gestion de risque.

Gérer les risques : pourquoi ?

Objectifs cités dans la norme ISO/IEC 27005 :

Dans les considérations générales (par 7.1) :

- Il est essentiel de déterminer l'objectif de la gestion du risque en sécurité de l'information puisqu'il influence l'ensemble du processus … L'objectif peut être :
  - une réponse aux exigences d'un SMSI,
  - la conformité avec la loi et la preuve de la mise en œuvre du devoir de précaution,
  - la préparation d'un plan de continuité de l'activité,
  - la préparation d'un plan de réponse aux incidents,
  - la description des exigences en matière de sécurité de l'information pour un produit, un service ou un mécanisme

Gérer les risques : pourquoi ?

Objectifs réaffirmés de MEHARI avec la version 2010 :

Les objectifs fondamentaux d'une gestion … des risques auxquels l'entreprise ou l'organisation est exposée, sont :

- Identifier tous les risques auxquels l'entreprise est exposée.
- Quantifier le niveau de chaque risque.
- Prendre, pour chaque risque considéré comme inadmissible, des mesures pour que le niveau de ce risque soit ramené à un niveau acceptable.
- …

Gérer les risques : pourquoi ?

Objectifs réaffirmés de MEHARI avec la version 2010 :

Les objectifs fondamentaux d'une gestion … des risques auxquels l'entreprise ou l'organisation est exposée, sont :

- …
- Mettre en place, comme outil de pilotage, un suivi permanent des risques et de leur niveau.
- S'assurer que chaque risque, pris individuellement, est bien pris en charge et a fait l'objet d'une décision d'acceptation, de réduction, d'évitement ou de transfert.

Gérer les risques : comment ?

L'objectif de MEHARI de gestion directe, et individualisée si nécessaire, des risques nécessite des spécifications particulières et complémentaires, pour :

- L'identification des risques
- L'estimation des risques
- La gestion des risques

L'identification des risques

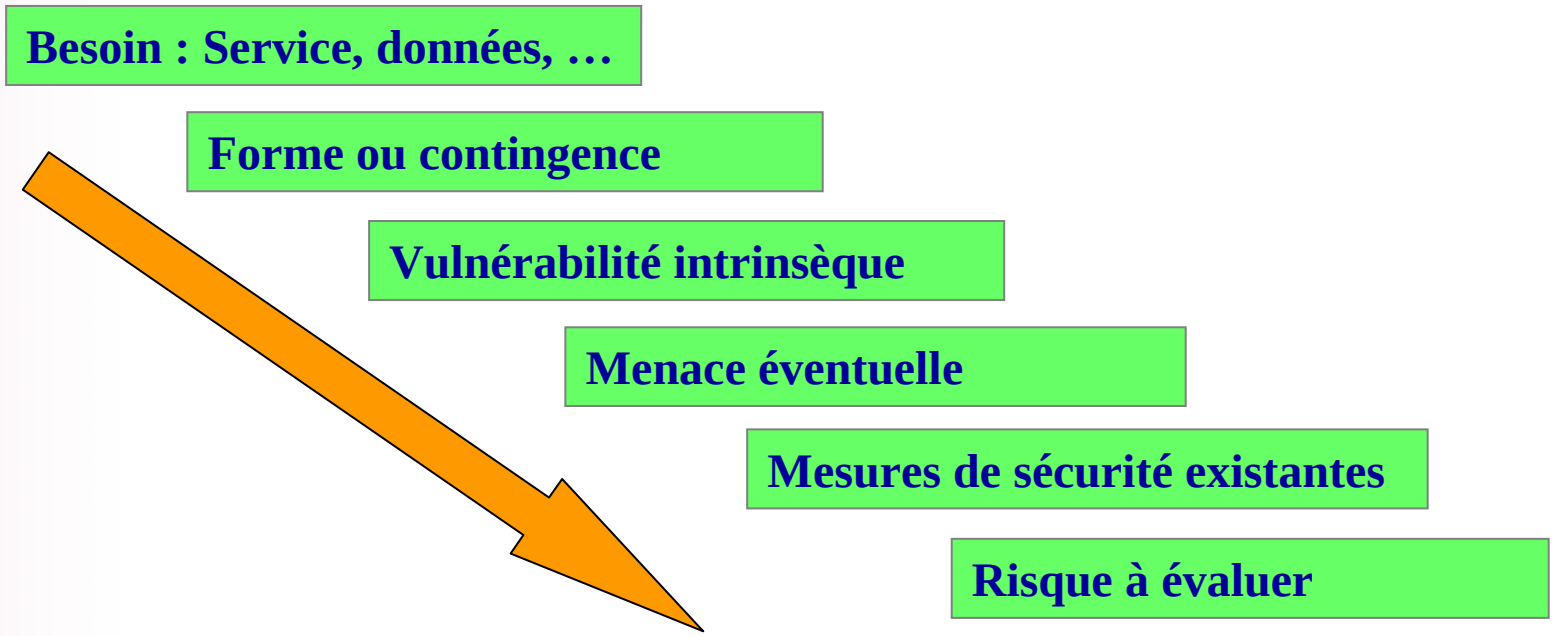
Les étapes prévues par la norme ISO 27005 sont :

- L'identification des actifs
- L'identification des menaces
- L'identification des mesures de sécurité existantes
- L'identification des vulnérabilités
- L'identification des conséquences

… et la norme précise, en introduction, que ces activités peuvent être effectuées dans un ordre différent selon la méthodologie appliquée.

L'identification des risques

MEHARI 2010 précise le processus d'identification des risques selon le schéma suivant :



L'identification des risques

Définitions complémentaires nécessaires :

Les actifs

Pour garantir que tous les risques seront identifiés, MEHARI 2010 part de la notion de « besoin de l'activité ».

Ce besoin peut revêtir trois formes :

- Un besoin de services
- Un besoin d'informations (ou données) nécessaires à l'accomplissement des services
- Un besoin de conformité (des processus et comportements) à un référentiel (éthique, réglementaire, légal, etc.)

La recherche exhaustive de ces besoins permet d'identifier les actifs « primaires » de l'entreprise ou de l'organisme

L'identification des risques

Définitions complémentaires nécessaires

Les actifs

Pour garantir que tous les risques seront identifiés, MEHARI 2010 précise comment ces besoins ou actifs primaires se matérialisent :

- Sous quelles formes ou sur quels supports
- En dépendant de quelles contingences

La recherche exhaustive de ces matérialisations permet d'identifier les actifs « secondaires » pour chaque type d'actif primaire

L'identification des risques

Définitions complémentaires nécessaires

Les vulnérabilités

La définition donnée à ce terme par l'ISO 27000 est la suivante :

« Faille dans un **actif** ou dans une **mesure de sécurité** qui peut être exploitée par une **menace** ».

Les deux aspects de cette définition sont de nature totalement différente.

L'identification des risques

Définitions complémentaires nécessaires

Les vulnérabilités

Pour garantir que tous les risques seront identifiés, MEHARI 2010 précise ces deux notions :

- **Vulnérabilité intrinsèque** : caractéristique intrinsèque d'un actif pouvant être le point d'application d'une menace
- **Vulnérabilité contextuelle** : faille dans un dispositif de sécurité pouvant être exploitée par une menace

L'identification des risques doit s'appuyer sur la recherche des vulnérabilités intrinsèques

L'identification des risques

Définitions complémentaires nécessaires

Les menaces

Pour pouvoir estimer les risques, la description de la menace doit comprendre tous ses éléments caractéristiques.

MEHARI 2010 précise ce que doit comprendre cette description :

- **L'événement déclencheur** et son caractère volontaire ou accidentel
- **L'acteur** déclenchant cet événement
- **Les circonstances** dans lesquelles survient cet événement

L'estimation des risques

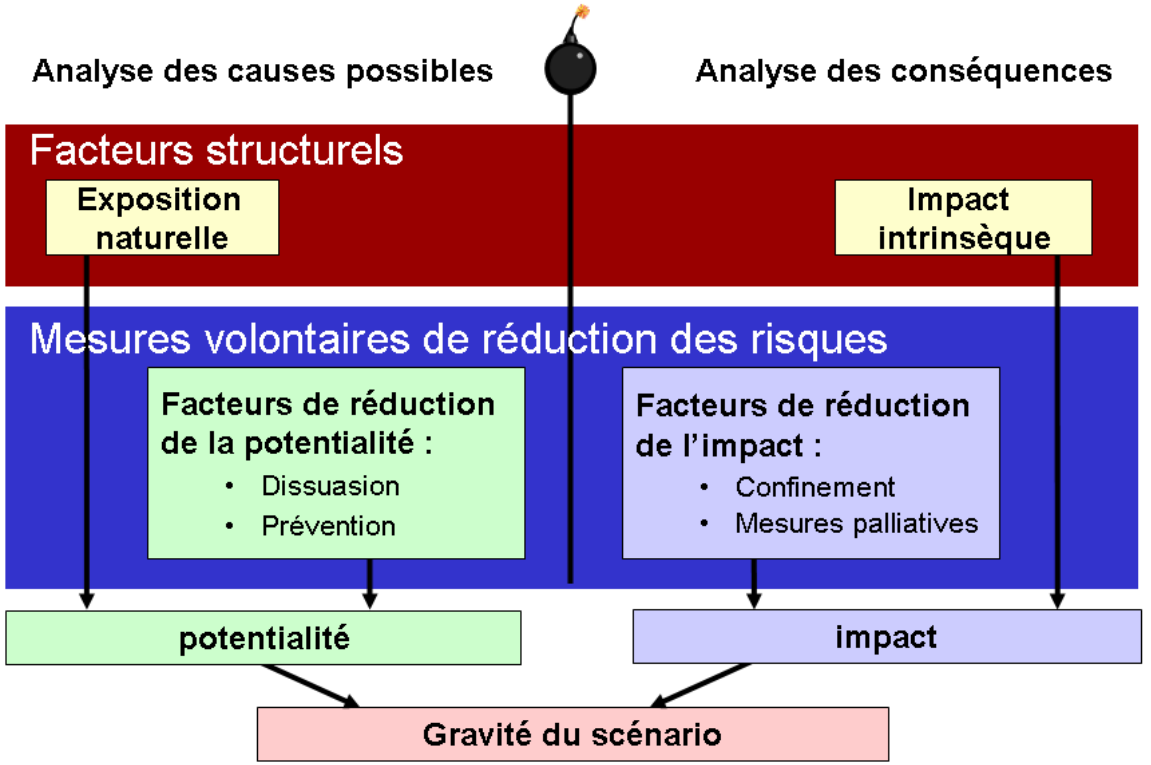
L'estimation des risques nécessite un modèle de risque et ce modèle doit être adapté à l'objectif fixé pour la gestion des risques.

Les objectifs de MEHARI (en tant que méthode de gestion de risques) imposent un modèle qui tienne compte :

- **Des facteurs structurels** liés à l'activité et au contexte de l'entreprise
- **Des mesures de sécurité mises en œuvre**
- **De la qualité de ces mesures**

L'estimation des risques

Le modèle de risque MEHARI est conforme depuis l'origine à cette spécification et n'évolue que très peu (sauf transfert du risque reporté en phase de traitement).



La gestion des risques

La gestion directe et individualisée des risques doit s'appuyer sur le modèle de risque et impose en outre que l'on sache fixer des objectifs en termes de :

- Services de sécurité à améliorer
- Niveaux de qualité cibles pour ces services

et que l'on sache mesurer l'atteinte des objectifs.

Ceci est difficilement envisageable sans une base de connaissance comprenant une base d'audit des services de sécurité.

L'ensemble des considérations développées à partir des objectifs complémentaires fixés (par MEHARI) pour la gestion des risques conduit à des principes fondamentaux et des spécifications fonctionnelles.

Ces principes et spécifications sont documentés et justifiés dans la version 2010 de MEHARI.

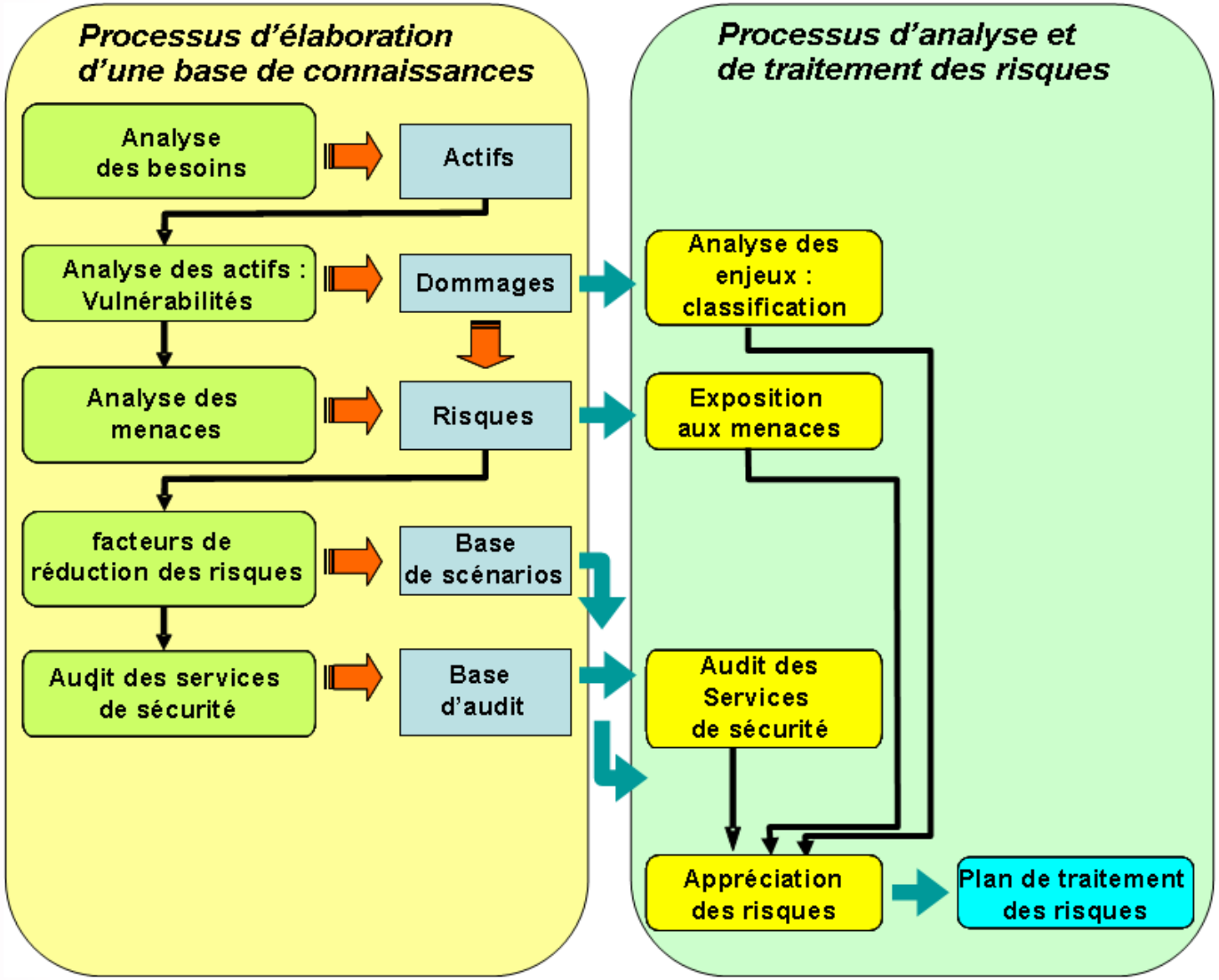
Sommaire

- Gérer ses risques avec la norme ISO 27005 et MEHARI 2010
- Les bases de connaissances de MEHARI 2010
- Modèles et fonctions de calcul
- Synthèse des nouveautés de MEHARI 2010
- Distribution Open Source de MEHARI

Les bases de connaissance de Méhari

- Base de situations de risque : une opportunité
- Base de services de sécurité : une nécessité
- Base de connaissance pour l'appréciation des situations de risque : une nécessité
- Conditions de création et de maintien d'une base de connaissance

Le processus de gestion des risques



Le développement d'une base de situations de risques

La gestion des risques comprend, de fait, une partie d'identification des risques qui correspond au développement d'une base décrivant des situations de risques (ou scénarios de risques).

Dès lors l'organisation systématique et systémique d'un tel développement est, pour le moins, une opportunité.

Le développement d'une base de connaissance de services de sécurité

La nécessité de faire référence aux mesures de sécurité pour estimer les risques renforce le besoin d'une base de connaissance des services de sécurité.

La nécessité de pouvoir évaluer la qualité des services de sécurité, selon plusieurs critères, exige clairement une base de connaissance d'analyse des services de sécurité.

Une base de connaissance pour l'appréciation des scénarios de risque

Quand la gravité d'une situation de risque peut être réduite par l'effet de plusieurs services de sécurité, parfois nombreux, un modèle de risque, même complet et performant, n'est pas suffisant :

- Les mécanismes d'appréciation des risques en fonction de la qualité de nombreux services de sécurité pertinents ne peuvent s'inventer au cas par cas
- La mise en commun des expertises et le recul dans la réflexion sont des garanties de qualité
- Le retour d'expérience ne peut être efficace que sur une base partagée

Une base de connaissance pour l'appréciation des scénarios de risque

Le nombre de situations de risques et le nombre de services de sécurité font qu'une base de connaissance de scénarios de risques n'est pas seulement un gage de qualité : c'est une nécessité.

Cela implique :

- L'explicitation des principes de construction
- Une structure d'accueil pour le développement et l'enrichissement permanent de la base

Le CLUSIF et les bases de connaissances de gestion de risques

Le CLUSIF a développé une compétence et de l'expérience dans le développement de base de connaissance de gestion de risque.

Cette compétence s'est accrue avec MEHARI 2010

Elle fera l'objet d'un guide du développement de base de connaissance de gestion de risque pour des contextes spécifiques ou la gestion d'autres risques que ceux liés aux systèmes d'information.

Ce n'est pas un hasard, c'est une nécessité

Sommaire

- Gérer ses risques avec la norme ISO 27005 et MEHARI 2010
- Les bases de connaissances de MEHARI 2010
- Modèles et fonctions de calcul
- Synthèse des nouveautés de MEHARI 2010
- Distribution Open Source de MEHARI

Des fonctions de calcul nécessaires

Le modèle de risque impose un minimum de fonctions de calcul pour estimer les niveaux de risque :

- Niveaux de qualité des services de sécurité
- Facteurs de réduction de risques
- Effets combinés de plusieurs services et de plusieurs facteurs
- Estimation des paramètres du risque
- Estimation de la gravité du risque

Une confiance raisonnée

Les mécanismes de calcul peuvent donner une fausse impression de précision :

- Certains paramètres, nécessaires pour les calculs, sont des estimations et non des mesures scientifiques
- Les formules elles-mêmes sont raisonnables et rationnelles mais ne sont pas « démontrables »

Il reste que, comme tout processus d'analyse, les modèles de calcul permettent de décomposer un problème complexe en problèmes élémentaires plus simples.

Ce sont des supports au raisonnement et des aides à la décision

Une confiance raisonnée

La confiance dans les modèles repose également sur un principe de prudence adopté lors de la construction des bases de connaissance :

- Prise en compte de la robustesse et de la mise sous contrôle (ou permanence) dans l'évaluation de la qualité d'un service de sécurité.
- Prise en compte des services de sécurité si et seulement si on peut garantir qu'ils auront une effet.
- Prudence dans les grilles de décision

La mise en pratique

Les automatismes de calcul restent des aides essentielles, si ce n'est indispensables, pour :

- Faire une présélection de plans d'action susceptibles de réduire les risques
- Mettre en évidence les risques non réduits par les actions décidées
- Simuler l'effet des mesures décidées sur les niveaux de risques résiduels
- Piloter la sécurité de l'information par la gestion des risques

Ces automatismes sont incorporés dans les bases au format Excel ou OpenOffice

Exemples de feuilles de calcul Excel

Feuille de calcul de la qualité des services de sécurité avec mention des variantes de schéma d'audit

SERVICES ET SOUS-SERVICES DE SECURITE											
DOMAINES				Prise en compte objectifs :					1,0	
	SERVICES										
		SOUS-SERVICES	Thème					Min	Obj	Fin
01	Organisation de la sécurité (01 Org)			V1	V2	V3	V4			
02	Sécurité des sites (02 Sit)			V1	V2	V3	V4			
	A - Contrôle d'accès physique au site et aux bâtiments									
	02A01	Gestion des droits d'accès au site ou à l'immeuble	B1	2,0	2,0			2,0		2,0
	02A02	Gestion des autorisations d'accès au site ou à l'immeuble	B1	2,8	2,8			3,0		3,0
	02A03	Contrôle d'accès au site ou à l'immeuble	B1	0,3	1,5			0,0		1,0
	02A04	Détection des intrusions sur le site ou dans l'immeuble	B1	0,0	0,0			0,0		1,0
	02A05	Accès aux zones de transfert (livraison ou chargement) ou aux zones accessibles au public	B1	X	0,0			0,0		1,0

Exemples de feuilles de calcul Excel

Feuille de synthèse des risques par famille d'actifs et niveaux de gravité

Panorama des gravités de scénarios		Disponibilité					Intégrité					Confidentialité				
Actifs de type Données et informations		Gr. 1	Gr. 2	Gr. 3	Gr. 4		Gr. 1	Gr. 2	Gr. 3	Gr. 4		Gr. 1	Gr. 2	Gr. 3	Gr. 4	
Données et informations																
D01	Fichiers de données ou bases de données applicatives	0	38	0	0	>	0	0	16	0	>	20	0	0	0	>
D02	Fichiers bureautiques partagés	0	23	0	0	>	0	9	0	0	>	0	0	18	0	>
D03	Fichiers bureautiques personnels (gérés dans environnement personnel)	0	26	0	0	>	0	7	0	0	>	0	0	17	0	>
D04	Informations écrites ou imprimées détenues par les utilisateurs, archives personnelles	0	0	10	0	>						0	0	12	0	>
D05	Listings ou états imprimés des applications informatiques											7	0	0	0	>
D06	Données échangées, écrans applicatifs, données individuellement sensibles	6	0	0	0	>	0	14	0	0	>	14	0	0	0	>
D07	Courrier électronique	9	0	0	0	>	3	0	0	0	>	0	0	4	0	>
D08	Courrier postal et télécopies	14	0	0	0	>	0	1	0	0	>	0	7	0	0	>
D09	Archives patrimoniales ou documentaires	10	0	0	0	>						4	0	0	0	>
D10	Archives informatiques	18	0	0	0	>	5	0	0	0	>	3	0	0	0	>
D11	Données et informations publiées sur des sites publics ou internes	23	0	0	0	>	9	0	0	0	>					
Actifs de type Services																
Services généraux communs																
G01	Environnement de travail des utilisateurs	0	0	3	1	>										
G02	Services de télécommunication (voix, télécopies, visioconférence, etc.)	18	0	0	0	>	6	0	0	0	>					
Services informatiques et télécom																
R01	Service du réseau étendu	27	0	0	0	>	5	0	0	0	>					
R02	Service du réseau local	0	0	19	8	>	5	0	0	0	>					
S01	Services applicatifs	0	46	12	6	>	0	18	0	0	>	16	0	0	0	>
S02	Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)	61	0	0	0	>	0	0	9	0	>					
S03	Equipements mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)	12	0	0	0	>										
S04	Services systèmes communs : messagerie, archivage, impression, édition, etc.	62	0	0	0	>	9	0	0	0	>					
S05	Services de publication d'informations sur un site web interne ou public	62	0	0	0	>	18	0	0	0	>					

Exemples de feuilles de calcul Excel

Feuille de sélection de plans de traitement

Elaboration de plans d'action						Pour évaluer les scénarios par leur gravité intrinsèque (et donc ne pas prendre en compte les services de sécurité), mettre un 0 dans la cellule ci-contre ➔ Pour évaluer les scénarios par leur gravité résiduelle (et donc prendre en compte les services de sécurité), mettre un 1 dans la cellule ci-contre ➔						1
						Pour prendre en compte les services retenus comme projets ou dans les plans d'action, en plus des services de sécurité actuels, dans l'évaluation des scénarios, mettre un 1 dans la cellule ci-contre ➔						1
Famille de scénarios	Nombre de scénarios					Mesures à améliorer	Type de plan	Décision	Services à améliorer	Niveau actuel	Niveau cible	Services à améliorer	Niveau actuel
	Gr 1	Gr 2	Gr 3	Gr 4	Tot								
R02-D	Indisponibilité du service du réseau local												
	0	0	19	8	27	Dissuasion : Plan de type A			03B06	1	3	06C02	1
						Prévention : Plan de type A			02A01	2	4	02A02	3
						Prévention : Plan de type A			03A01	1	4	03A02	1
						Prévention : Plan de type A			05D01	1	4	06A02	1
						Confinement : Plan de type A			02A04	0	4	03B04	1
						Palliation : **Plan de type E**			01C02	0	3	01E01	2
						Palliation : Plan de type A			03A02	1	3	03A06	1

Exemples de feuilles de calcul Excel

Feuille d'analyse et de décision sur scénarios individuels

LIBELLÉ	Sélection directe	Type AEM	Type DICL	Impact Intrins.	Exposition	Grav. Intrins.	Dissuasion	Prévention	Confinement	Palliation	Confinable	I décidé	P décidée	I calculé	P calculé	Gravité calc.	Scén. accepté ou transféré
Effacement accidentel de fichiers de données applicatives, suite à un incident d'exploitation	1	A	D	2	3	**2**	1	2	2	3	0	4		2	3	4	T
Effacement par erreur de fichiers de données applicatives, par un utilisateur autorisé légitime, se connectant depuis le réseau interne	1	E	D	2	3	**2**	1	1	1	3	0		4	2	3	3	A
Effacement par erreur de fichiers de données applicatives, par un utilisateur autorisé illégitime, se connectant depuis le réseau interne	1	E	D	2	3	**2**	1	1	1	3	0			2	3	2	

Sommaire

- Gérer ses risques avec la norme ISO 27005 et MEHARI 2010
- Les bases de connaissances de MEHARI 2010
- Modèles et fonctions de calcul
- Synthèse des nouveautés de MEHARI 2010
- Distribution Open Source de MEHARI

Évolution des scénarios de risque

Description des actifs primaires:

Données, services, processus

Processus de classification des actifs revu pour Mehari 2010

Structuration et description des scénarios

actif + dommage : vulnérabilité,

événement, circonstances, acteur : menace

regroupement par familles : par actif et type de dommage

Outils de sélection des scénarios

Évolution de la base des services de sécurité

Domaines de sécurité :

Nouveaux : Environnement de travail, Archives, SMSI, Télécom

Visualisation de variantes d'audit

Classification des mesures : efficacité, robustesse, contrôle

➔ audit adapté à la maturité de l'organisation

Évolution du modèle de risque

Évaluation des risques

mesures de récupération (assurance) traitées en transfert de risque (alignement sur l'ISO 27005

➔ simplification du traitement

Évolution des aides à la gestion des risques

Synthèse des risques par niveau de gravité

- par famille d'actifs
- par type de menace

Plans de traitement

- plans avec degré d'efficacité
- aides à la sélection de projets planifiés (avec date d'achèvement)

Sommaire

- Gérer ses risques avec la norme ISO 27005 et MEHARI 2010
- Les bases de connaissances de MEHARI 2010
- Modèles et fonctions de calcul
- Synthèse des nouveautés de MEHARI 2010
- Distribution Open Source de MEHARI

Pourquoi distribuer en Open source?

1 + CLUSIF = association sans but lucratif!

2 + lourdeur du mécanisme de livraison précédent

Quelles conséquences pour l'image de Mehari ?

3 + C'est maintenant une méthode reconnue

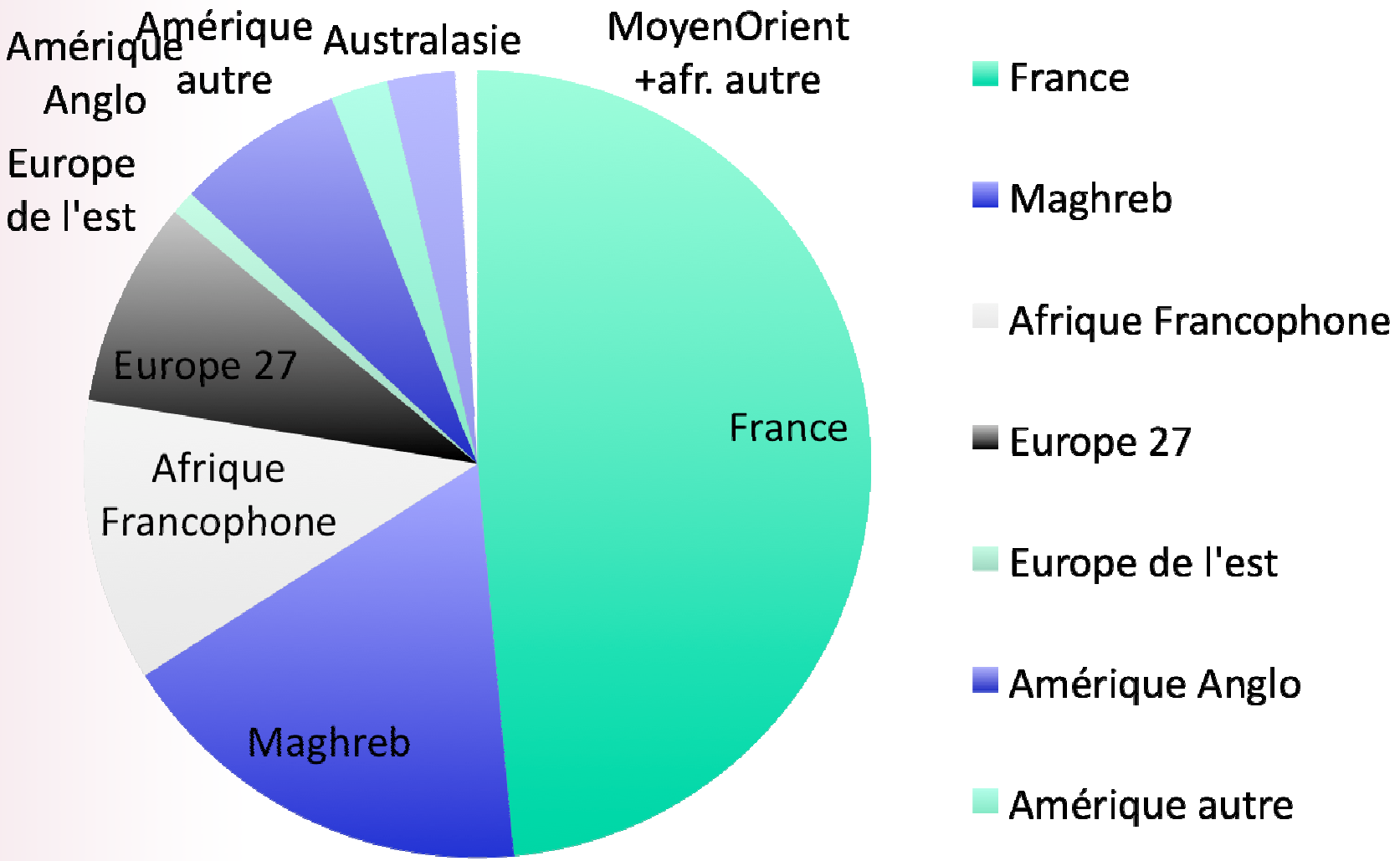
30.000 chargements,

statut international : 150+ pays en 4 ans

4 + traductions bénévoles : espagnol, allemand, italien, ...

5 + besoin de répondre aux demandes : www.mehari.info

6 + image renforcée du CLUSIF hors de France



chargements des bases 2007 (partiel)

Commentaires sur les chargements

Multiplication par 100 par rapport aux versions précédentes.

Demandes de création de CLUSI (Burkina, Tunisie, Maroc)

Chargements des **bases en anglais**/en français : 19 %

Formateurs Mehari locaux (Côte d'Ivoire, Tunisie?)

Notoriété du CLUSIF hors hexagone.

Nombreux contacts avec plusieurs pays (Europe ou autre)

Merci de votre attention