



MEHARI 2007

Sommaire

- 1. Introduction : vue d'ensemble de Méhari**
- 2. L'analyse des enjeux et la classification**
- 3. L'analyse de l'état des services de sécurité**
- 4. L'analyse des risques**
- 5. L'évaluation quantitative des risques**
- 6. Plans d'action et démarches**
- 7. Outils et support**
- 8. Personnalisation**
- 9. Domaines d'utilisation**



1. Introduction : Vue d'ensemble de Méhari



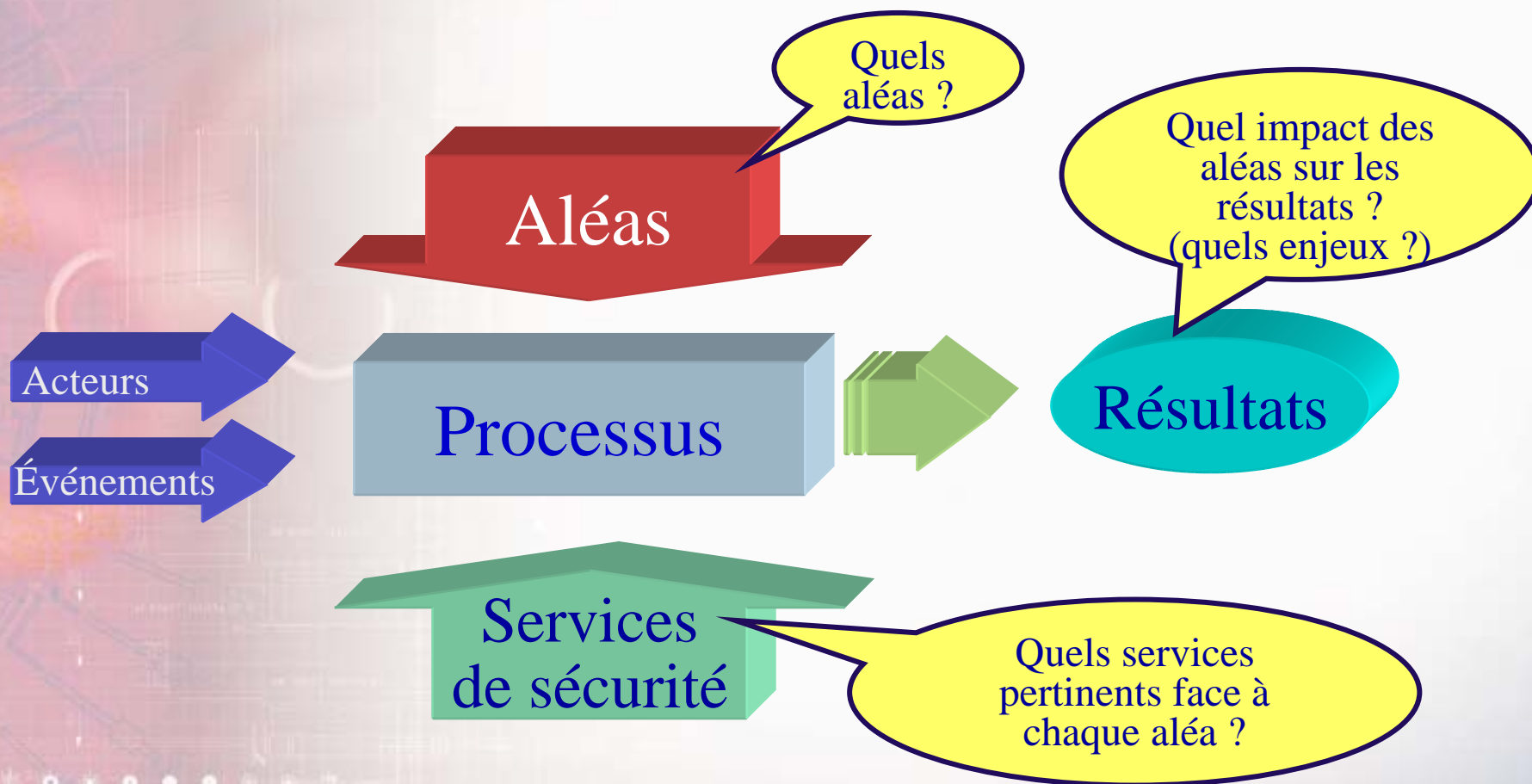
L'essentiel de Méhari

Méhari est un ensemble d'outils destinés au management des risques, c'est-à-dire :

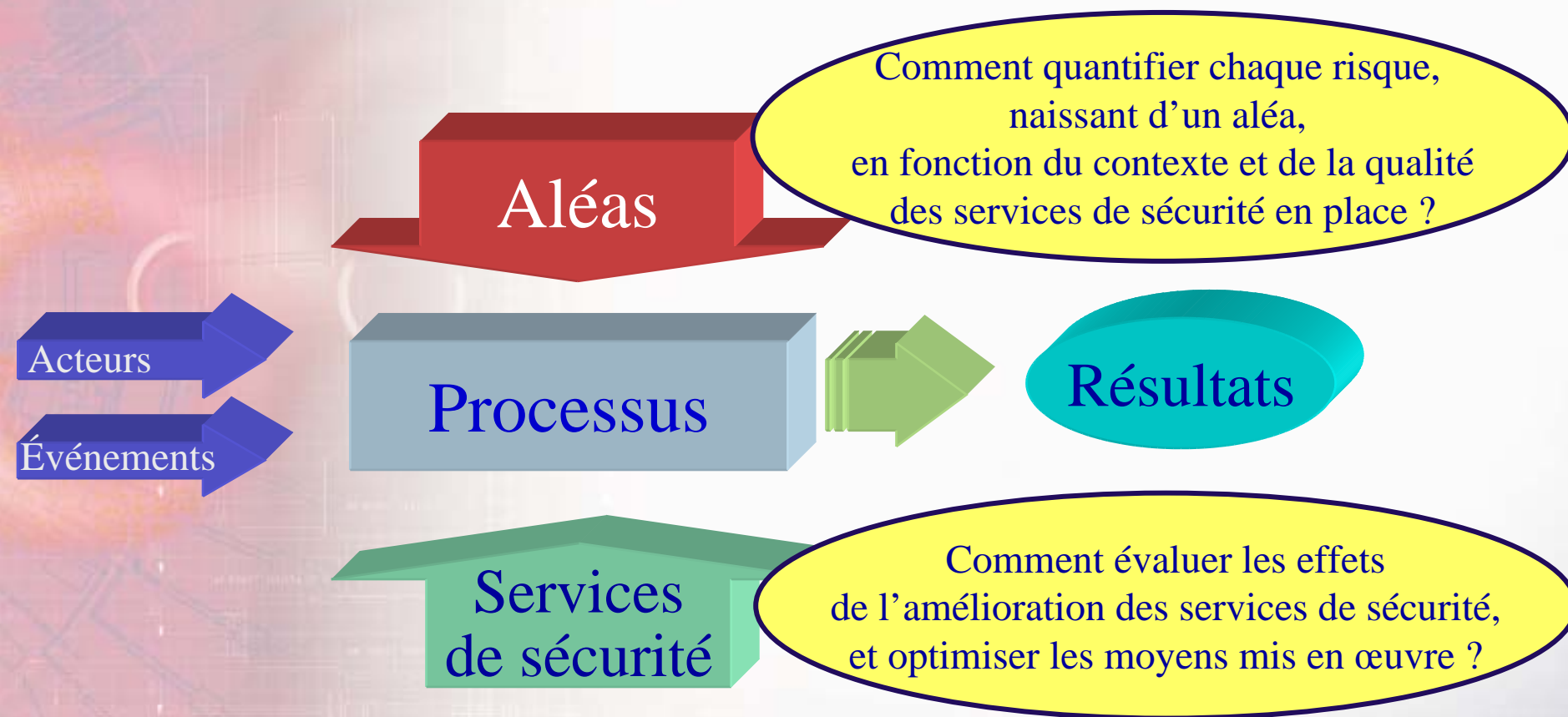
- L'identification des situations de risque
- L'analyse des facteurs influençant la nature et la gravité des risques
- L'évaluation quantitative du niveau de chaque risque
- L'identification des mesures de sécurité pouvant réduire les risques
- L'évaluation quantitative de l'effet de ces mesures et de leur qualité sur le niveau des risques
- L'optimisation du choix des mesures de sécurité



Modèle général de l'analyse de risque

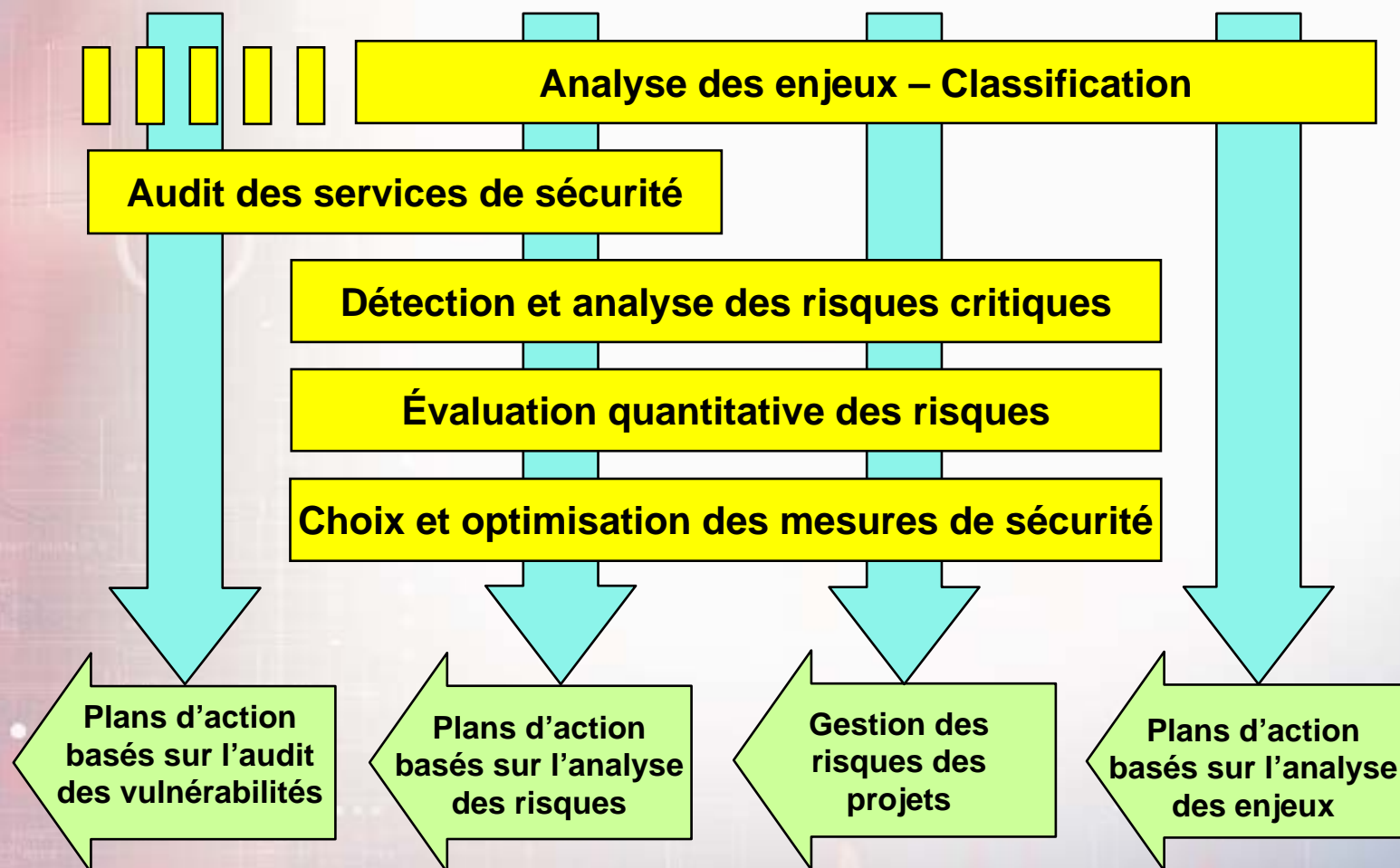


Modèle général de management des risques



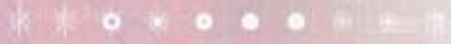
Vue d'ensemble de Méhari

Méhari propose un ensemble de modules indépendants pouvant être utilisés et associés de diverses manières et avec des objectifs variés





2. L'analyse des enjeux et la classification



L'analyse des enjeux de la sécurité

On appelle « analyse des enjeux de la sécurité » :

- La recherche des dysfonctionnements potentiels pouvant être créés par un défaut de sécurité
- L'évaluation de la gravité de ces dysfonctionnements

Cela revient à se poser, pour chaque activité de l'organisme, la double question suivante :

- Que pourrait-il arriver ?
- Si cela arrivait, serait-ce grave ?

L'analyse des enjeux de la sécurité

Pourquoi l'analyse des enjeux est-elle utile et, le plus souvent, nécessaire, voire essentielle ?

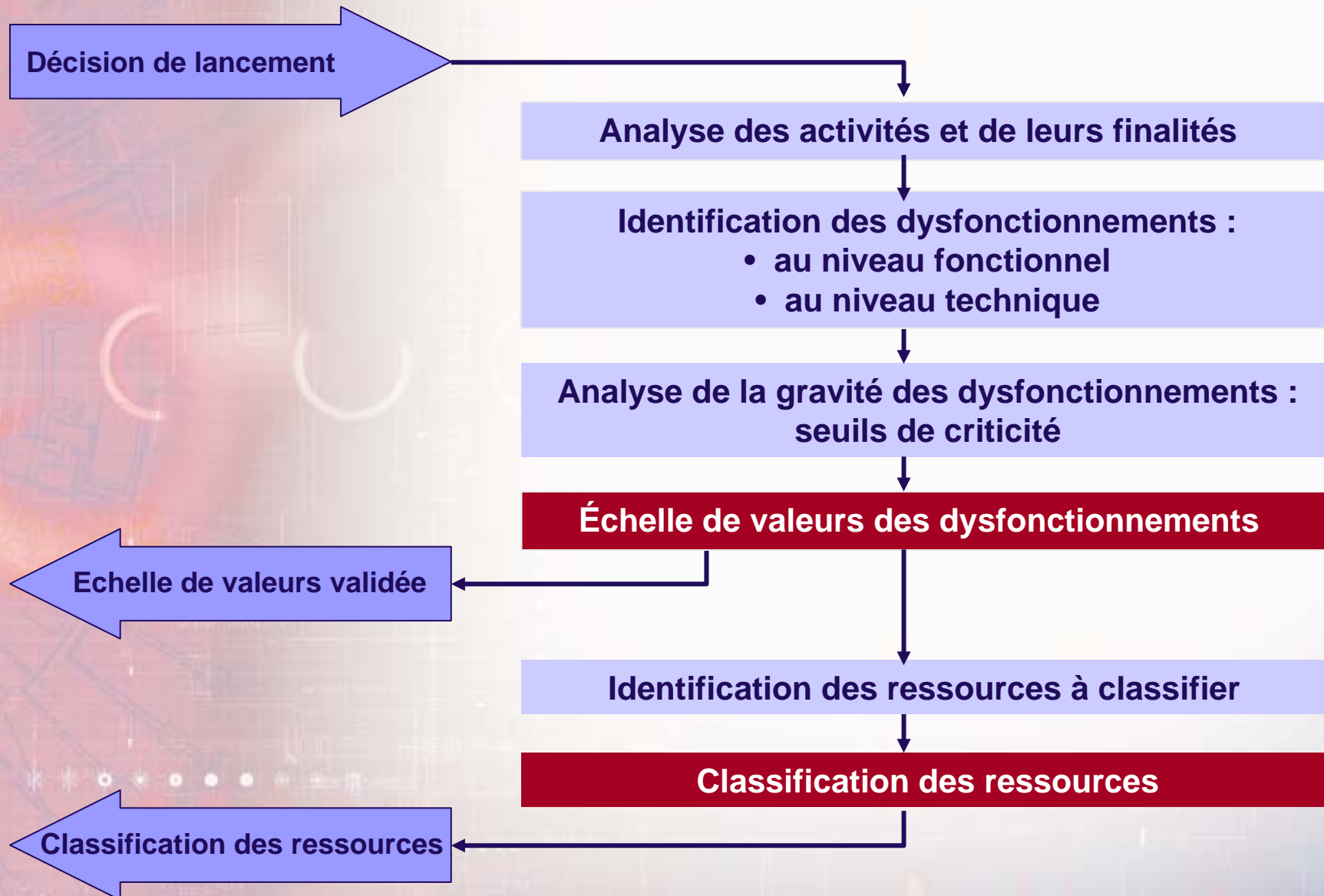
- Pour être sélectif dans les moyens à mettre en œuvre et ne pas engager de dépenses là où les enjeux sont faibles
- Pour éviter des contraintes inutiles aux utilisateurs
- Pour définir les priorités
- Pour répondre à l'inévitable question des dirigeants en face d'un budget de sécurité : « est-ce bien nécessaire ? »
- Pour permettre l'analyse des risques

L'analyse des enjeux de la sécurité

Cette analyse se traduit par :

- Une **échelle de valeurs des dysfonctionnements** (potentiels), document de référence centré sur les impacts « business »
- Une **classification** formelle des informations et ressources du système d'information

Processus d'analyse des enjeux



Processus d'analyse des enjeux

Le processus d'analyse des enjeux comprend des étapes clairement décrites dans le guide Méhari

1. Description des activités en termes de fonctionnalités et de résultats attendus
2. Identification et description des dysfonctionnements potentiels (techniques et/ou fonctionnels)
3. Détermination des seuils de criticité et des niveaux de gravité possibles des dysfonctionnements identifiés
4. Synthèse sous forme d'échelle de valeur des dysfonctionnements et **validation en Comité de Direction**
5. Identification des ressources à classifier et regroupement en domaines de ressources
6. Prise en compte de l'architecture, mise en évidence des liaisons entre ressources et dysfonctionnements potentiels et **classification formelle**

Processus d'analyse des enjeux

Conditions pratiques de l'élaboration de l'échelle de valeurs des dysfonctionnements

1. Une réunion de travail avec chaque responsable d'un domaine d'activité : 1 h à 1 h 15 par Dirigeant
2. Éventuellement des réunions complémentaires avec leurs collaborateurs directs (niveau N – 2)
3. Une synthèse par activité revue par le responsable
4. Une synthèse générale présentée, discutée et validée **en Comité de Direction**
5. Charges moyennes constatées :
 - 2 à 3 h par Dirigeant
 - 1 semaine pour l'animateur (intervenant externe ou RSSI)



Échelle de valeurs de dysfonctionnements

Exemple partiel

1. Pertes financières

<i>Type de dysfonctionnement</i>	<i>Niveau 1 Non significatif</i>	<i>Niveau 2 Important</i>	<i>Niveau 3 Très grave</i>	<i>Niveau 4 Vital</i>
Perte financière directe - fraude	Perte < 1 M€	Perte comprise entre 1 et 10 M€	Perte comprise entre 10 et 100 M€	Perte > 100 M€

2. Stratégie et opérations jouant sur le périmètre d'activité

<i>Type de dysfonctionnement</i>	<i>Niveau 1 Non significatif</i>	<i>Niveau 2 Important</i>	<i>Niveau 3 Très grave</i>	<i>Niveau 4 Vital</i>
Divulgence d'informations sur la stratégie	Informations sur la stratégie à court terme d'une zone limitée d'activité	Informations sur la stratégie à court terme globale d'une filiale	Plan stratégique à long terme d'une filiale	Plan stratégique à long terme de l'entreprise

Échelle de valeurs de dysfonctionnements

Exemple partiel

3. Optimisation de la production

<i>Type de dysfonctionnement</i>	<i>Niveau 1 Non significatif</i>	<i>Niveau 2 Important</i>	<i>Niveau 3 Très grave</i>	<i>Niveau 4 Vital</i>
Indisponibilité des moyens d'étude d'optimisation de la production	Indisponibilité durant moins d'une semaine	Indisponibilité durant plus d'une semaine		

4. Nouveaux produits, contrats et achats

<i>Type de dysfonctionnement</i>	<i>Niveau 1 Non significatif</i>	<i>Niveau 2 Important</i>	<i>Niveau 3 Très grave</i>	<i>Niveau 4 Vital</i>
Retards dans la mise en production	Retard inférieur à une semaine	Retards compris entre 1 et 4 semaines	Retard supérieur à 4 semaines	
Indisponibilité ou altération de la nomenclature produit	Indisponibilité de la nomenclature produit	Erreur ponctuelle dans la nomenclature produit	Pollution complète de la nomenclature produit	

Échelle de valeurs de dysfonctionnements

Exemple partiel

5. Rapports avec l'administration

<i>Type de dysfonctionnement</i>	<i>Niveau 1 Non significatif</i>	<i>Niveau 2 Important</i>	<i>Niveau 3 Très grave</i>	<i>Niveau 4 Vital</i>
Incapacité à envoyer à temps des informations contractuelles ou réglementaires		Incapacité à envoyer à temps les résultats annuels	Incapacité à envoyer à temps des infos touchant des concessions d'exploitation	

6. Gestion des ressources humaines

<i>Type de dysfonctionnement</i>	<i>Niveau 1 Non significatif</i>	<i>Niveau 2 Important</i>	<i>Niveau 3 Très grave</i>	<i>Niveau 4 Vital</i>
Perte de personnel clé (accident, départ volontaire, ...)		Perte de personnel clé dans un domaine d'expertise		
Divulgence de données personnelles (paye)	Divulgence ponctuelle d'information	Divulgence massive d'informations privées		

Processus d'analyse des enjeux

Conditions pratiques de l'élaboration de la classification formelle des informations et ressources du système d'information

1. Condition préalable : existence d'une cartographie des applications et bases de données
2. Quelques séances de travail avec la DSI et le RSSI pour tirer les conséquences de l'échelle de valeurs des dysfonctionnements en termes de classification
3. Une consolidation et une synthèse des résultats
4. Des conclusions présentées, discutées et validées **en Comité de Direction**
5. Charges moyennes constatées :
 - 1 h pour les membres du Comité de Direction
 - Quelques jours pour l'animateur (intervenant externe ou RSSI)

Tableaux de classification

Exemple partiel

Tableau T1

<i>Processus métiers</i> <i>Services applicatifs</i> <i>Services communs</i>	<i>Programmes</i> <i>Procédures</i>			<i>Données</i> <i>applicatives</i>			<i>Messages</i> <i>Données en</i> <i>transit</i>			<i>Fichiers</i> <i>bureautiques</i>			<i>Listings Docs</i> <i>imprimés</i>			<i>Courrier</i> <i>Mail</i> <i>Fax</i>		
	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C
Stratégie/plan	1	2	1	2	2	3	1	2	1	1	2	3	1	2	3	1	2	1
Finance/Trésorerie	2	2	1	2	2	1	2	2	1	2	2	1	1	2	1	2	2	1
Gestion/compta	2	2	1	3	2	1	2	2	1	2	2	1	1	2	1	2	2	1
Commercial	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Production	2	1	1	2	3	3	2	1	1	2	1	1	2	1	1	2	1	1
Recherche	1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1
Ressources humaines	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1
Support	2	1	1	2	2	1	2	1	1	2	1	1	2	1	1	2	1	1
Messagerie	2	1	1	2	1	2	2	1	1	2	1	1	2	1	1	2	1	1
Courrier	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	2	2
Téléphone	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	2
Archives	1	1	1	3	1	1	-	-	-	1	1	1	1	1	1	-	-	-
Administration IT	3	2	1	3	2	1	3	2	1	3	2	1	3	2	1	-	-	-
Help desk	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	-	-	-

Tableaux de classification

Exemple partiel

Suite Tableau T1

<i>Processus métiers</i> <i>Services applicatifs</i> <i>Services communs</i>	Prise en compte de l'architecture					
	<i>Serveurs applicatifs</i>	<i>Serveurs Bureautiques</i>	<i>Réseau Local</i>	<i>Réseau étendu</i>	<i>Équipements dédiés</i>	<i>Postes mobiles</i>
Stratégie/plan		X	X	X		
Finance/Trésorerie	X	X	X	X		
Gestion/compta	X		X	X		
Commercial		X	X			
Production		X			X	
Recherche		X	X			
Ressources humaines	X	X	X			
Support	X		X	X		X
Messagerie	X		X	X		
Courrier						
Téléphone			X			
Archives		X	X			
Administration IT	X	X	X			
Help desk	X		X			

Tableaux de classification

Exemple partiel

Tableau T2

Éléments D'architecture	Matériel Câblage		Fichiers de configuration			Programmes systèmes			Documents (maintenance Spécs)		
	D	I	D	I	C	D	I	C	D	I	C
Réseau local 1	2	2	2	2	2	1	2	1	1	1	1
Réseau local 2	2	2	2	2	1	1	2	1	1	1	1
Réseau étendu	2	2	3	2	3	2	2	1	1	1	1
Réseau téléphonique	1	1	1	2	2	1	2	1	1	1	1
Serveurs Finance	2	3	2	3	3	2	3	1	2	1	1
Serveurs Commercial	1	1	1	2	3	1	3	1	1	1	1
Serveurs Production	1	1	2	2	2	1	2	1	1	1	1
Serveurs RH	2	1	2	2	1	2	1	1	1	1	1
Serveurs Support	2	1	2	1	1	1	1	1	2	2	1
Serveurs Messagerie	2	1	2	1	2	2	1	1	1	1	1
Périphériques Production	1	1	-	-	-	2	2	1	2	2	1
Passerelle Internet	1	1	3	1	3	1	2	1	1	1	1
Serveurs DNS	3	2	1	2	1	1	1	1	1	1	1

Synthèse sur l'analyse des enjeux et la classification

L'échelle de valeurs est plus détaillée (sur les dysfonctionnements redoutés) et permet un jugement plus fin sur des mesures à prendre.

- L'échelle de valeurs ne dépend que des métiers de l'entreprise ou de l'organisme.
- C'est un document de stratégie essentiel

La classification permet de communiquer sur la sensibilité des ressources.

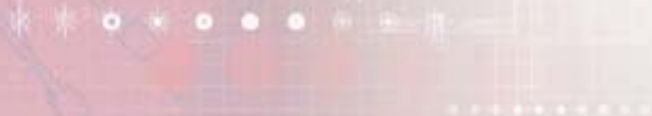
- C'est une information résumée.
- La classification dépend de l'architecture du système d'information.
- La classification selon la démarche proposée permet une entrée directe dans le tableau d'impact intrinsèque de l'analyse des risques Méhari.

Points clés de l'analyse des enjeux et la classification

Les niveaux les plus élevés du management (N et N-1) doivent impérativement être impliqués dans le processus d'élaboration de l'échelle de valeurs des dysfonctionnements

L'atteinte d'un consensus est essentielle

Les mesures de sécurité existantes ne doivent pas être prises en compte lors de ce processus



Points clés de l'analyse des enjeux et la classification

Les enjeux de la sécurité, pour une analyse de risque, peuvent être notablement différents du « besoin ressenti » ou du « degré d'utilité » :

- L'usage d'une technologie ou d'un service peut être ressenti comme essentiel par les utilisateurs sans pour autant que son indisponibilité provoque une catastrophe.
- Certaines lacunes peuvent être sans effet visible direct sur les résultats d'un processus et ne pas être considérées, par les utilisateurs opérationnels, comme critiques, alors qu'elles peuvent avoir des conséquences stratégiques très graves à long terme.



3. Le diagnostic de l'état des services de sécurité

Définition d'un service de sécurité

Un service de sécurité est une réponse à un besoin de sécurité :

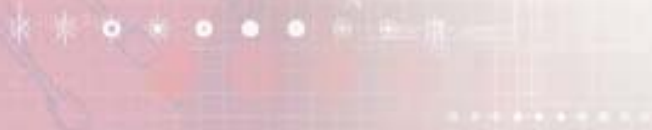
- décrite en termes génériques et fonctionnels décrivant leur finalité face à certains types de menaces.
- exprimée indépendamment des mécanismes et solutions concrètes permettant la réalisation effective de ce service.
- Pouvant éventuellement être composée de plusieurs services
- Exemple : Contrôle d'accès logique (aux serveurs et/ou applications) comprenant 4 sous-services :
 - ✚ "Établissement des profils d'accès"
 - ✚ "Gestion des autorisations d'accès et privilèges"
 - ✚ "Authentification de l'accédant"
 - ✚ "Filtrage des accès et gestion des associations"

Qualité d'un service de sécurité

On évaluera un service de sécurité en faisant une « mesure globale » de sa qualité.

Cette mesure globale évalue 3 paramètres :

- L'efficacité du service
- Sa robustesse
- Sa mise sous contrôle



Qualité d'un service de sécurité

Efficacité d'un service de sécurité

L'efficacité mesure la capacité du service à assurer effectivement la fonction demandée face à des « acteurs » ayant plus ou moins de « forces » :

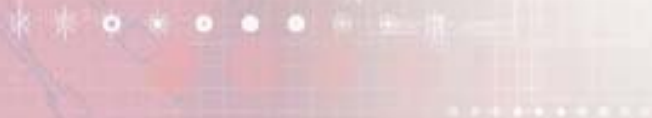
- compétences et moyens des acteurs humains plus ou moins importants (néophyte, professionnel, spécialiste, expert).
- Force ou sévérité d'un événement naturel (hauteur d'une crue, par exemple). En pratique cette force sera souvent évaluée en fonction du caractère plus ou moins exceptionnel de l'événement.

Qualité d'un service de sécurité

Robustesse d'un service de sécurité

La robustesse d'un service mesure sa capacité à résister aux actions ou événements se traduisant par le contournement ou l'inhibition du fonctionnement attendu :

- Interruption volontaire (arrêt) de l'équipement assurant le service
- Panne non détectée
- Contournement du contrôle par une voie détournée
- Altération des fonctionnalités



Qualité d'un service de sécurité

Mise sous contrôle d'un service de sécurité

La mise sous contrôle d'un service de sécurité mesure la capacité de l'organisme à garantir la permanence dans le temps des fonctions du service :

- Permanence des paramétrages décidés
- Application effective des procédures
- Maintien de la pertinence et de la cohérence

Qualité d'un service de sécurité

La base de connaissance de Méhari comprend un manuel de référence des services de sécurité qui décrit pour chaque service :

- L'objectif du service
- Les résultats attendus
- Les mesures, mécanismes et solutions mis en œuvre pour réaliser le service
- Les éléments pertinents pour juger de la qualité du service (sous les trois aspects d'efficacité, de robustesse et de mise sous contrôle)

La recherche systématique des critères de qualité des services conduit à une base de plus en plus experte ...

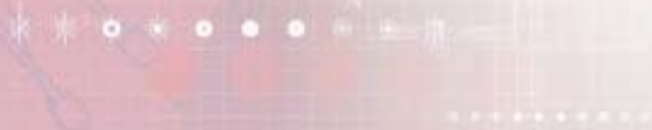
Mesure de la qualité d'un service de sécurité

La qualité d'un service de sécurité est évaluée sur une échelle numérique (de 1 à 4)

L'évaluation se fait grâce à des questionnaires d'audit et à une méthode de pondération des réponses à ces questionnaires

Une attitude de « prudence » est privilégiée :

Une surévaluation de la qualité d'un service de sécurité pourrait conduire à minimiser un risque et à ne pas le prendre en compte alors qu'il est critique.



Diagnostic de l'état des services de sécurité

Conditions pratiques du diagnostic

1. Les questionnaires sont découpés en domaine fonctionnels correspondant à des domaines de responsabilité :
 - il est ainsi aisé de définir les personnes à rencontrer
 - Les variantes peuvent facilement être identifiées
2. Des aides au diagnostic sont fournies dans le guide livré avec la méthode
3. Des outils de calcul et de synthèse graphique sont disponibles sur le marché
4. Charges moyennes constatées :
 - 2 à 3 h par responsable de domaine fonctionnel
 - 1 semaine pour l'animateur (intervenant externe ou RSSI) synthèse comprise

Liaison avec l'ISO 17799:2005

Certains auditeurs souhaitent pouvoir déduire d'un diagnostic Méhari, une évaluation de la conformité aux pratiques de l'ISO 17799:2005

La version 2007 permet l'élaboration de tels indicateurs par l'incorporation dans la base de connaissances de :

- Nouvelles questions adaptées aux pratiques recommandées par l'ISO 17799
- Formules de calcul du degré de conformité à chaque contrôle cité dans la norme ISO



4. L'analyse de risque

Concepts de base de l'analyse de risque

L'analyse de risque a pour objectif :

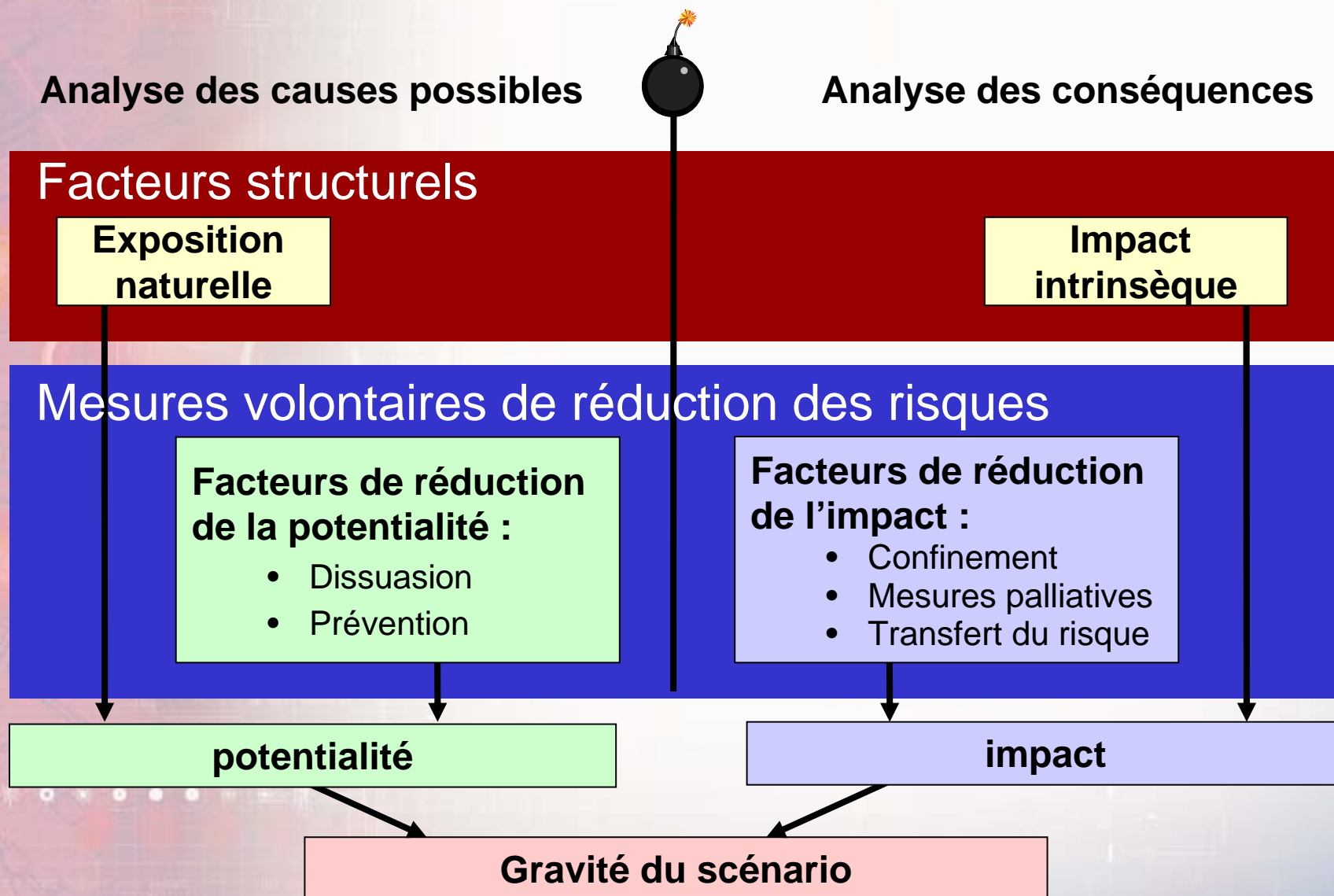
- De détecter des situations de risque
- D'analyser les divers facteurs caractéristiques de chaque situation de risque
- De porter un jugement global sur le caractère acceptable ou non de chaque situation

Concepts de base de l'analyse de risque

Pour analyser les risques, Méhari s'appuie sur un modèle de risque qui distingue :

- 2 facteurs structurels, indépendants de toute mesure de sécurité :
 - ✚ L'exposition naturelle ou potentialité intrinsèque
 - ✚ L'impact intrinsèque
- 2 facteurs de réduction de la potentialité
- 3 facteurs de réduction de l'impact

Modèle de risque Méhari

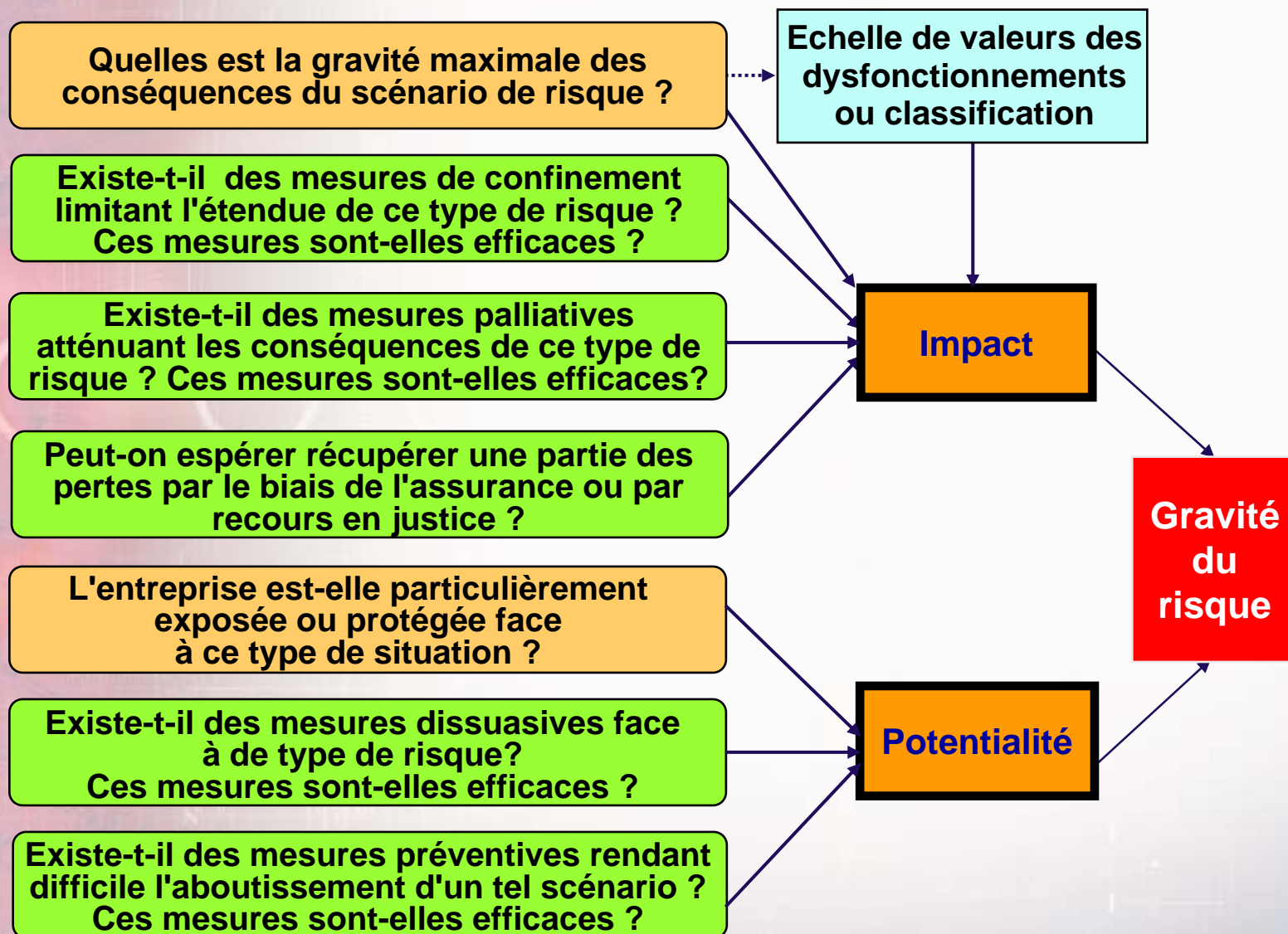


Analyse des risques avec Méhari

Pour identifier les situations de risque et analyser les risques correspondants, Méhari s'appuie sur une base de connaissance :

- 180 situations types y sont décrites par des fiches individuelles qui aident à évaluer globalement :
 - ✦ L'exposition naturelle de l'organisation à ce type de situation
 - ✦ L'impact intrinsèque, c'est-à-dire la gravité des conséquences de l'occurrence du risque en l'absence de toute mesure de sécurité
 - ✦ Les divers facteurs de réduction de la potentialité et de l'impact de ce risque
- Des grilles de décision permettent d'évaluer la potentialité, l'impact et, in fine, la gravité de chaque situation

Analyse d'une situation de risque



Analyse des situations de risque

L'analyse des situations de risque débouche sur deux résultats :

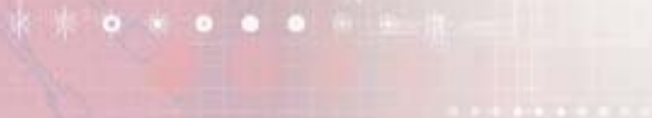
- La caractère acceptable ou non de chaque situation de risque
- La compréhension des facteurs qui rendent certaines situations inacceptables

Elle permet un premier niveau de décision sur les actions à mener

Analyse des situations de risque

Conditions pratiques d'une analyse globale

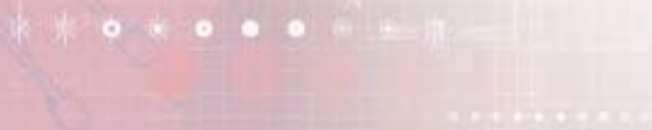
1. Les situations de risque sont facilement identifiées après une analyse des enjeux (limitée à l'échelle de valeurs)
2. Une analyse globale peut être menée directement avec les responsables opérationnels
3. Les décisions qui sont du ressort du management sont prises très rapidement et mises en œuvre sans délai
4. Les décisions qui sont du ressort de l'architecture des systèmes sont consolidées à un niveau plus central
5. Charges moyennes constatées :
 - 1 journée par domaine d'activité



Analyse des situations de risque

L'analyse globale des situations de risque peut être insuffisante pour un management hiérarchisé des risques (par niveaux)

Le management des risques réclame un niveau plus fin d'analyse : **l'évaluation quantitative des risques et des facteurs de risque**





5. L'évaluation quantitative des risques et des facteurs de risque

Évaluation quantitative d'une situation de risque

Méhari propose, pour chaque situation de risque, des mécanismes permettant une évaluation quantitative :

- De l'impact intrinsèque, en partant de la classification des ressources
- De la potentialité intrinsèque par l'intermédiaire d'un tableau personnalisable de l'exposition naturelle à une série d'événements types
- De chaque facteur de réduction de risque, en s'appuyant sur un diagnostic Méhari de la qualité des services de sécurité
- De l'impact et de la potentialité résultant des points précédents
- De la gravité résultante de la situation de risque

Évaluation de l'impact intrinsèque

Les situations de risque de la base de connaissance Méhari font référence à des types de ressources (environ 30) :

- types de données ou informations
- éléments d'architecture informatique et télécom
- éléments d'infrastructure générale
- situations dont il faut évaluer directement la gravité

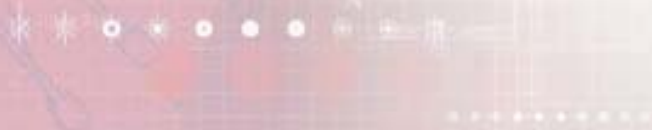
Méhari 2007 propose des mécanismes pour évaluer l'impact intrinsèque des scénarios impliquant ou touchant ces ressources, à partir des tableaux de classification

Évaluation de la potentialité intrinsèque

Méhari propose un tableau d'événements que l'on peut analyser globalement (environ 50) :

- accidents
- malveillances
- actes volontaires non malveillants
- erreurs

Méhari propose une exposition naturelle type ou potentialité intrinsèque type, pour chaque type d'événement, qui peut être utilisée pour les cas les plus courants



Évaluation des facteurs de réduction de risque

La qualité des services de sécurité peut être mesurée par un diagnostic

Méhari propose, pour chaque situation de risque, des mécanismes d'évaluation des facteurs de réduction de risque, en fonction de la mesure de la qualité des services de sécurité pertinents pour cette situation

Évaluation quantitative de la potentialité d'une situation de risque

L'évaluation de la potentialité sera faite en fonction de :

- l'exposition naturelle (potentialité intrinsèque)
- 2 facteurs de réduction de risque (dissuasion et prévention)

Méhari propose des grilles standard permettant d'automatiser cette évaluation

- Il s'agit en fait de fixer le raisonnement ou le type de décision dans une grille
- Les grilles sont différentes selon qu'il s'agit de scénario d'accident, d'erreur ou d'acte volontaire
- Les grilles sont personnalisables par l'organisation

Évaluation quantitative de l'impact d'une situation de risque

L'évaluation de l'impact sera faite en fonction de :

- L'impact intrinsèque
- 3 facteurs de réduction de risque (confinement, mesures palliatives et transfert de risque)

Méhari propose des grilles standard permettant d'automatiser cette évaluation

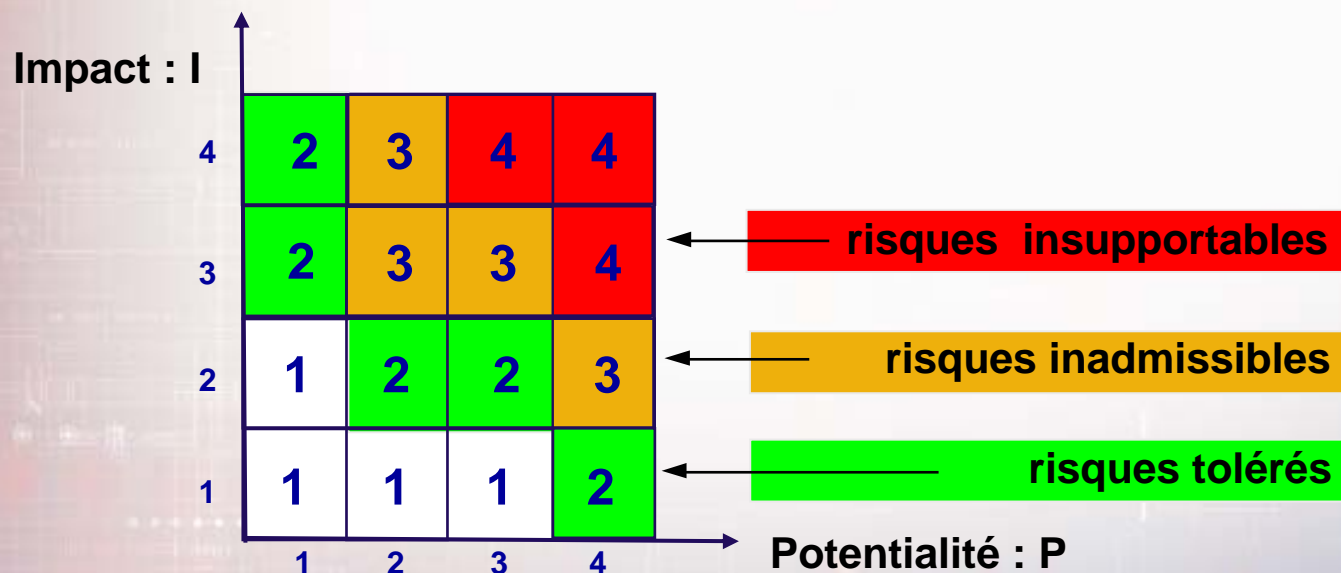
- Il s'agit en fait de fixer le raisonnement ou le type de décision dans une grille
- Les grilles sont différentes selon qu'il s'agit de scénario d'atteinte à la disponibilité, l'intégrité ou la confidentialité
- Les grilles sont personnalisables par l'organisation

Évaluation globale de la gravité d'un risque

La gravité du risque est le résultat d'une décision, fonction de l'impact et de la potentialité

Cette décision peut être traduite en termes **d'objectif de sécurité** ou **d'acceptabilité du risque** représentable sur une grille.

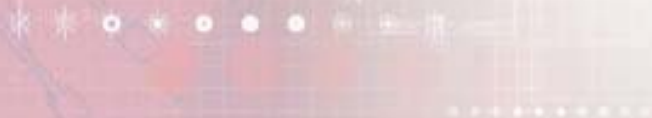
Un exemple de telle grille est donné ci-dessous.



Analyse quantitative des risques

Conditions pratiques d'une analyse quantitative détaillée des situations de risque

1. Les mécanismes de Méhari sont utilisables directement dans des cas simples.
2. Les outils existant sur le marché permettent d'aborder des situations complexes et d'optimiser le management de situations de risque nombreuses
3. Charges moyennes constatées :
 - 1 semaine pour une entité autonome moyenne





6. Plans d'action et démarches

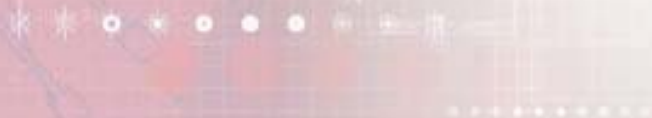


Introduction aux plans de sécurité

Les plans de sécurité sont la réponse à cette simple question : « que convient-il de faire ? »

Il y a plusieurs approches ou démarches possibles

Divers paramètres peuvent avoir une influence sur le choix le plus pertinent, à un moment donné



Introduction aux plans de sécurité

Les paramètres à prendre en compte pour déterminer la démarche la plus pertinente sont :

- La maturité de l'entreprise, dans le domaine de la sécurité
- Le choix des acteurs à impliquer dans les diverses décisions à prendre concernant les actions à mener :
 - ✦ Managers opérationnels
 - ✦ Staff technique
- Les domaines couverts par les plans de sécurité :
 - ✦ Infrastructure technique
 - ✦ Processus métiers
 - ✦ Pratiques courantes
- Le besoin de références nationales, internationales, ou spécifiques d'un domaine d'activité, etc.

Les plans de sécurité avec Méhari

Méhari est organisée en modules indépendants, de manière à permettre différentes démarches

La documentation Méhari en développe plusieurs :

- Plans de sécurité par entité, basés sur l'analyse et l'évaluation des risques (orientation technique)
- Plans de sécurité par secteur d'activité, basés sur l'analyse et l'évaluation des risques (démarche managériale)
- Plans de sécurité des projets
- Plans de sécurité basés sur l'audit des services de sécurité
- Management par directives et référentiel de sécurité
- Plans d'action déduits directement d'une analyse des enjeux



7. Outils et support



Outils logiciels

RISICARE est un logiciel proposé par BUC SA

- C'est un support parfaitement adapté à la méthode Méhari
- Les bases de connaissances peuvent être générées en dehors des bases standard
- Il permet l'utilisation de Méhari, y compris dans des situations très complexes
- Il est régulièrement mis à jour en fonction des évolutions de Méhari (version actuelle : V5)

D'autres logiciels sont en fin de développement

La documentation et les supports de MEHARI

La documentation de Méhari comprend :

- Une présentation générale, introduction à Méhari (en français, anglais, allemand, italien)
- Une présentation des principes et mécanismes (français et anglais)
- Un guide de l'analyse des enjeux et de la classification (nouveau 2007; en français et en anglais)
- Un guide du diagnostic des services de sécurité (français et anglais)
- Un guide de l'analyse des risques (français et anglais)

Cette documentation est en libre accès sur le site du Clusif

La documentation et les supports de MEHARI

La documentation de Méhari comprend :

- Un manuel de référence des services de sécurité (une fiche par service décrivant les objectifs, les mécanismes mis en œuvre et les critères de qualité du service), en français et bientôt en anglais (mi 2007)
- Un manuel de référence des scénarios de risque de la base de connaissance (une fiche par scénario décrivant le contexte et les facteurs influant sur les divers paramètres de risque), en français

Cette documentation est livrée avec les bases de connaissance



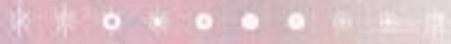
La documentation et les supports de MEHARI

Les « bases de connaissances », livrées sous forme de fichiers Excel

- Constituent une base puissante pour manager la sécurité
- Établissent des liens entre :
 - ✚ les enjeux
 - ✚ les ressources du SI
 - ✚ les menaces et les parades
- Contiennent des formules de calcul pour évaluer :
 - ✚ La qualité des services de sécurité audités,
 - ✚ La gravité des scénarios de risques de la base.



8. Personnalisation des bases de connaissance



Personnalisation des bases de connaissance

Les bases de connaissance peuvent être personnalisées :

1. par l'ajout de commentaires et d'aides à la décision

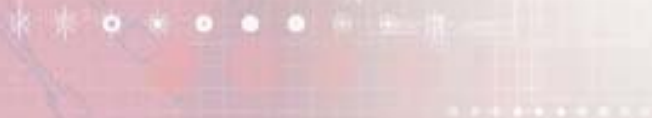
- C'est une fonction standard de Risicare qui permet d'ajouter :
 - ✚ des commentaires sur chaque domaine audité et pour chaque question des questionnaires (aide à la réponse, références internes, solutions standards, coûts induits, etc.)
 - ✚ Des commentaires sur chaque décision (exposition, impact intrinsèque, correction de facteurs de risque, etc.)
- C'est une possibilité naturelle avec les bases Excel fournies en support standard par le Clusif

Personnalisation des bases de connaissance

Les bases de connaissance peuvent être personnalisées :

2. Au niveau des services de sécurité

- C'est un concept standard de Méhari qui permet de préciser des variantes de services de sécurité en fonction des mécanismes employés (variantes définies par le schéma d'audit)
- Cette possibilité permet de définir différentes politiques de sécurité en fonction des contextes rencontrés (entités/filiales, localisations, types de systèmes, etc.)

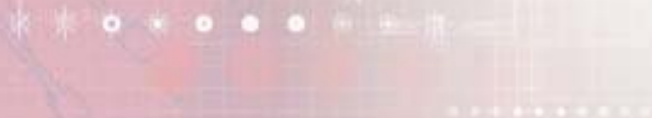


Personnalisation des bases de connaissance

Les bases de connaissance peuvent être personnalisées :

3. Au niveau des ressources impactées

- C'est un concept introduit depuis Méhari V3 qui permet de préciser des variantes de ressources impactées par des scénarios de risque (variantes définies par une décomposition cartographique)
- Cette possibilité permet de différencier des situations de risque en fonction de ressources ou d'actifs particulièrement sensibles et de définir des actions plus ciblées

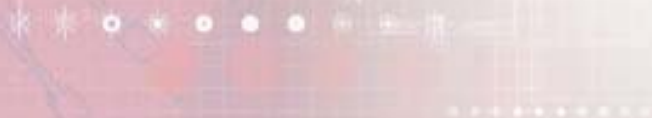


Personnalisation des bases de connaissance

Les bases de connaissance peuvent être personnalisées :

4. Création de nouveaux scénarios de risque

- La base Clusif est, par essence, « généraliste » et il est fréquent de vouloir créer des scénarios spécifiques en fonction des dysfonctionnements critiques identifiés
- Cette possibilité est totalement ouverte aux utilisateurs qui le souhaitent et est régulièrement pratiquée
- C'est ce que fait régulièrement l'Espace Méthodes du Clusif

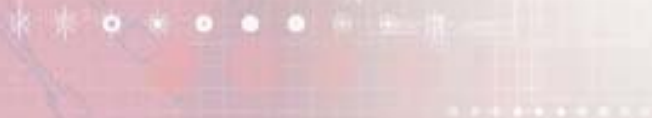


Personnalisation des bases de connaissance

Les bases de connaissance peuvent être personnalisées :

5. Création de nouveaux services de sécurité

- Un tel besoin peut naître de l'existence de services de sécurité spécifiques d'un métier (services mis en œuvre par une solution spécifique, exemple carte Vitale)
- Cette possibilité est bien sûr ouverte et ne présente pas de difficulté pour un spécialiste de la sécurité de telles solutions
- Cela conduit généralement à créer également de nouveaux scénarios de risque faisant appel à ces nouveaux services



Personnalisation des bases de connaissance

Les bases de connaissance peuvent être personnalisées :

7. Création de nouvelles bases de connaissance

- Le modèle de risque Méhari n'est pas spécifique des systèmes d'information et on peut donc envisager de créer des bases de connaissance radicalement différentes, par exemple pour :
 - ✚ Les risques de fraude ou de vol dans la grande distribution
 - ✚ Les risques industriels liés à une industrie spécifique
- Le facteur clé de succès est de pouvoir réunir un groupe d'experts du domaine concerné autour d'un expert de la méthode





9. Domaines d'utilisation



Domaines d'utilisation de Méhari

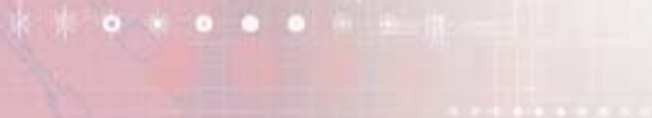
Les domaines d'utilisation de Méhari sont variés et sont indépendants :

- de la taille de l'entreprise ou de l'organisme :
Méhari a été utilisé avec succès aussi bien dans des grands groupes multinationaux que dans des PME
- du mode d'organisation et de management de l'entreprise
- du secteur d'activité

Domaines d'utilisation de Méhari

Méhari apparaît particulièrement bien adapté aux entreprises ayant une culture entrepreneuriale :

- Les entrepreneurs sont habitués à évaluer leurs risques et à prendre des décisions basées sur des évaluations de risques
- Cela fait longtemps que les discours sécuritaires basés sur les seules notions de « danger » ont montré leur inefficacité vis-à-vis de ces décideurs.
- Il est par contre nécessaire de leur apporter des outils d'évaluation et de discussion performants





Merci de votre attention