M2 Miage

SMSI / analyse de risque

Damien Ploix
Université d'Evry Val d'Essonne

Plan

- Introduction
- La démarche SMSI
  - Établissement du contexte
  - Appréciation du risque
  - Traitement du risque
  - Gestion du risque
- Exemple d'analyse de risque

SMSI

- Définition du risque :

« *Le risque est mesuré en termes de combinaison entre la vraisemblance d'un événement et ses conséquences* »

Positionnement du SMSI

ISO 27001
Système de Management Sécurité Information

Activité

Application données

Serveurs

Réseaux LAN / MAN / WAN

Locaux - Humains

Pirates
Intelligence économique
SOX / BAL x / …
Pandémie

PCA

ISO 2700?
MCA

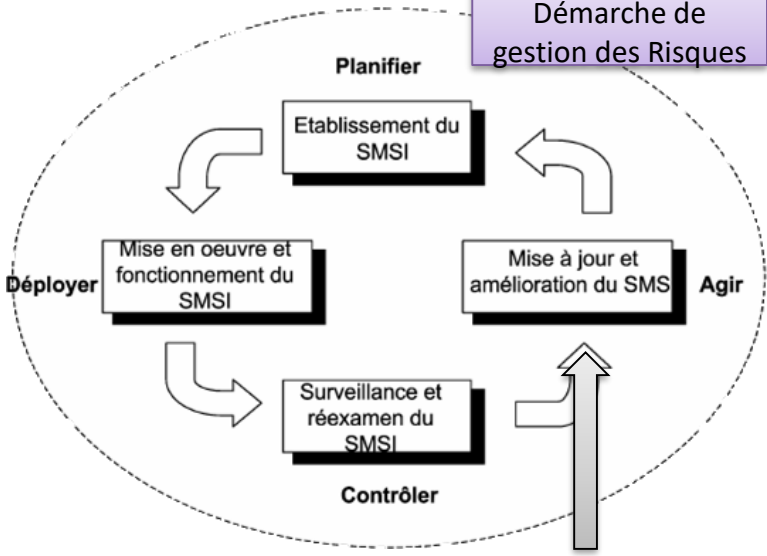
Mesure et analyse du risque

ISO 27005
Démarche d'analyse des Risques

ISO 27002
Mesures (17799)

ISO 27004 Indicateurs

ISO 27005
Démarche de gestion des Risques

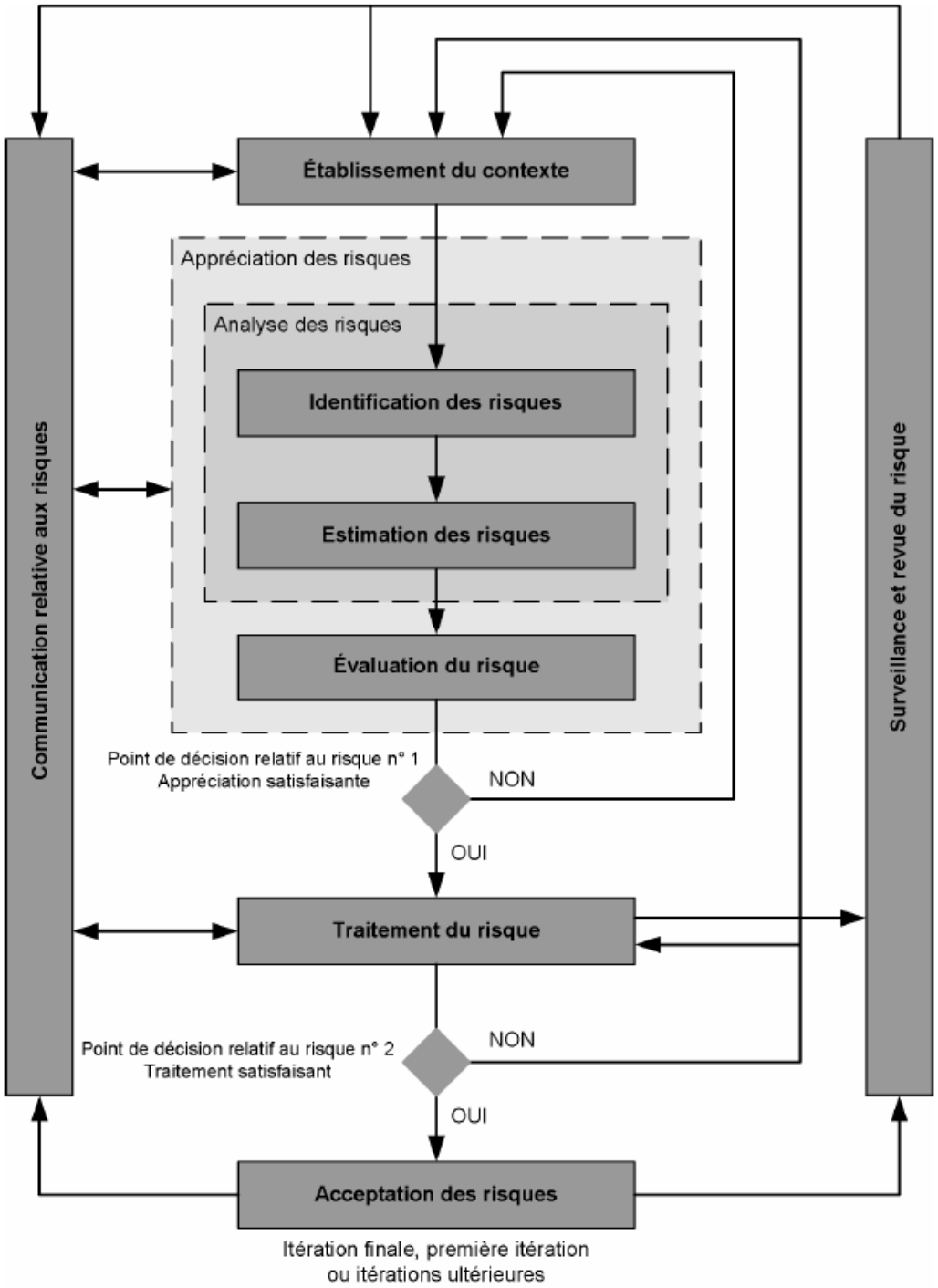


Plan

- Introduction
- La démarche SMSI
  - Établissement du contexte
  - Appréciation du risque
  - Traitement du risque
  - Gestion du risque
- Exemple d'analyse de risque

Démarches de la SSI

- ISO 27005 pose une démarche générale =>
- Des outils structurent la démarche et proposent des mesures (ISO 27002) et des indicateurs (ISO 27004)
  - Mehari
  - OSSTMM
  - …
  - *(+ de 200 outils existent)*



Processus du SMSI
(ISO 27005)

Processus SMSI	Processus de gestion des risques en sécurité de l'information
Planifier	Établissement du contexte Appréciation des risques Élaboration du plan de traitement des risques Acceptation des risques
Déployer	Mise en œuvre du plan de traitement des risques
Contrôler	Surveillance et revue continues des risques
Agir	Maintien et amélioration du processus de gestion des risques en sécurité de l'information

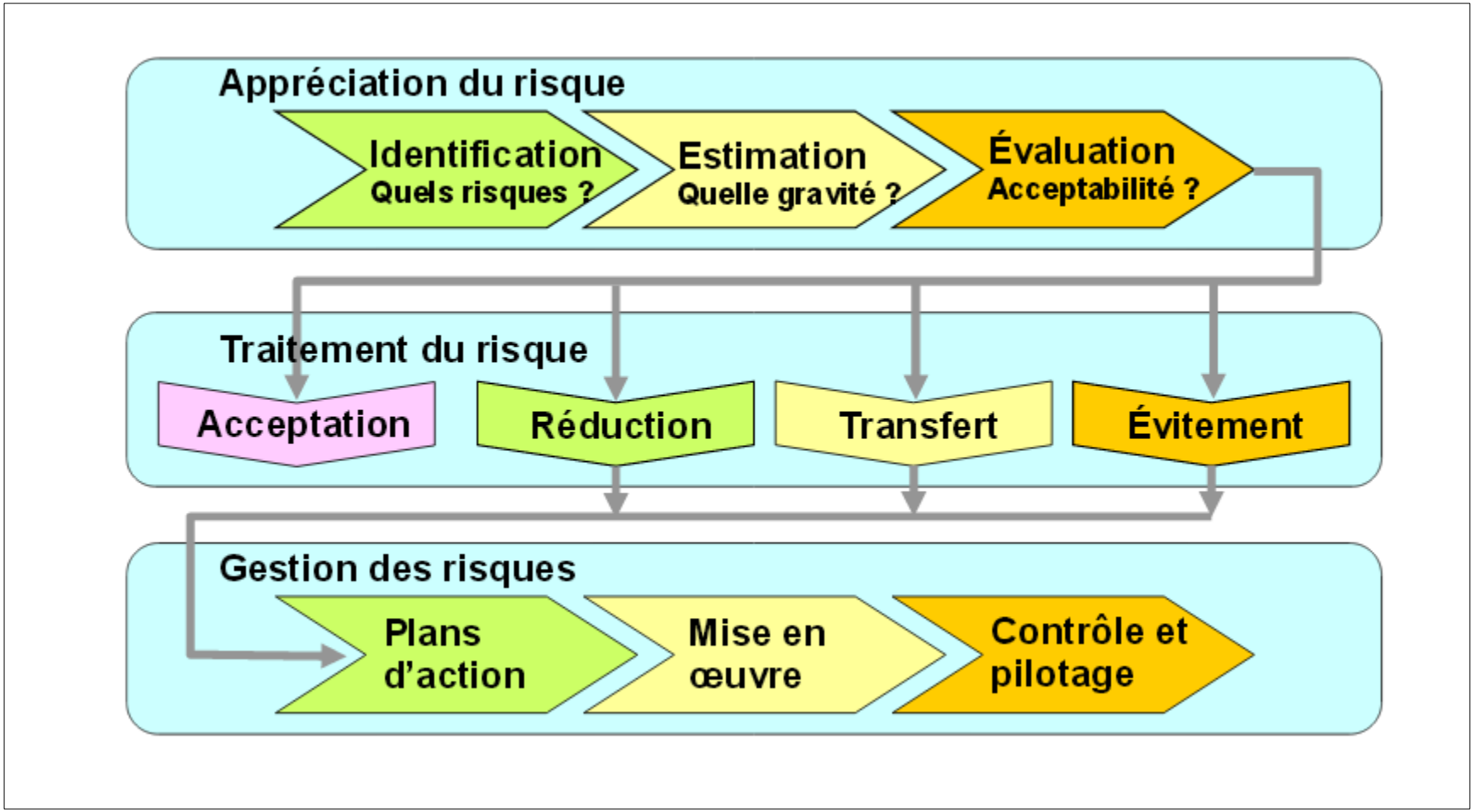
Un outil de gestion du risque : Mehari

- Redite L3 ?
  - L'attente est différente :
    - approche critique de la méthode
    - capacité à contextualiser
    - … un rappel n'est peut être pas inutile…
- Source : CLUSIF
- Représente une « instanciation » des normes ISO 27001 et 27005.

SMSI : du vocabulaire !

Terme	Définition
Enjeu de la sécurité	Conséquences d'un incident de sécurité sur les objectifs de l'organisme.
Impact	Conséquence, pour l'organisme concerné, de l'occurrence du risque considéré.
Impact intrinsèque	Conséquence, pour l'organisme concerné, de l'occurrence du risque considéré en l'absence de toute mesure de sécurité.
Menace	Description de l'ensemble des éléments conduisant à l'occurrence du risque incluant l'événement déclencheur et son caractère volontaire ou accidentel, l'acteur déclenchant cet événement et les circonstances dans lesquelles survient cet événement.
Potentialité	Probabilité de l'occurrence du risque considéré, dans le contexte l'organisme concerné ;
Potentialité intrinsèque	Probabilité de l'occurrence du risque considéré, dans le contexte l'organisme concerné, en l'absence de toute mesure de sécurité.
Scénario de risque	Description de l'ensemble des caractéristiques d'un risque, incluant l'actif concerné, la vulnérabilité intrinsèque de cet actif mise en cause et la menace conduisant à l'occurrence du risque.
Service de sécurité	Description d'une fonction de sécurité répondant à un besoin.
Vulnérabilité intrinsèque	Caractéristique intrinsèque d'un système, d'un objet ou d'un actif constituant un point d'application potentiel de menaces.
Vulnérabilité contextuelle	Défaut ou faille dans les dispositifs de sécurité pouvant être exploité par une menace pour atteindre un système, un objet ou un actif cible

Démarche globale



Plan

- Introduction
- La démarche SMSI
  - Établissement du contexte
  - Appréciation du risque
  - Traitement du risque
  - Gestion du risque
- Exemple d'analyse de risque

Établissement du contexte

- Déterminer les *actifs* :
  - Classification des *processus métier* « critiques »
  - Dans ces processus métier, identification des *activités*, *méthodes* et *outils.*
  - Les actifs représentent l'ensemble des composants du système d'information (outils) nécessaire à l'accomplissement des processus métiers critiques :
    - Poste de travail,
    - Serveurs centraux,
    - Mails,
    - Imprimante,
    - …

Exemple d'analyse de risque Enjeux/Besoins

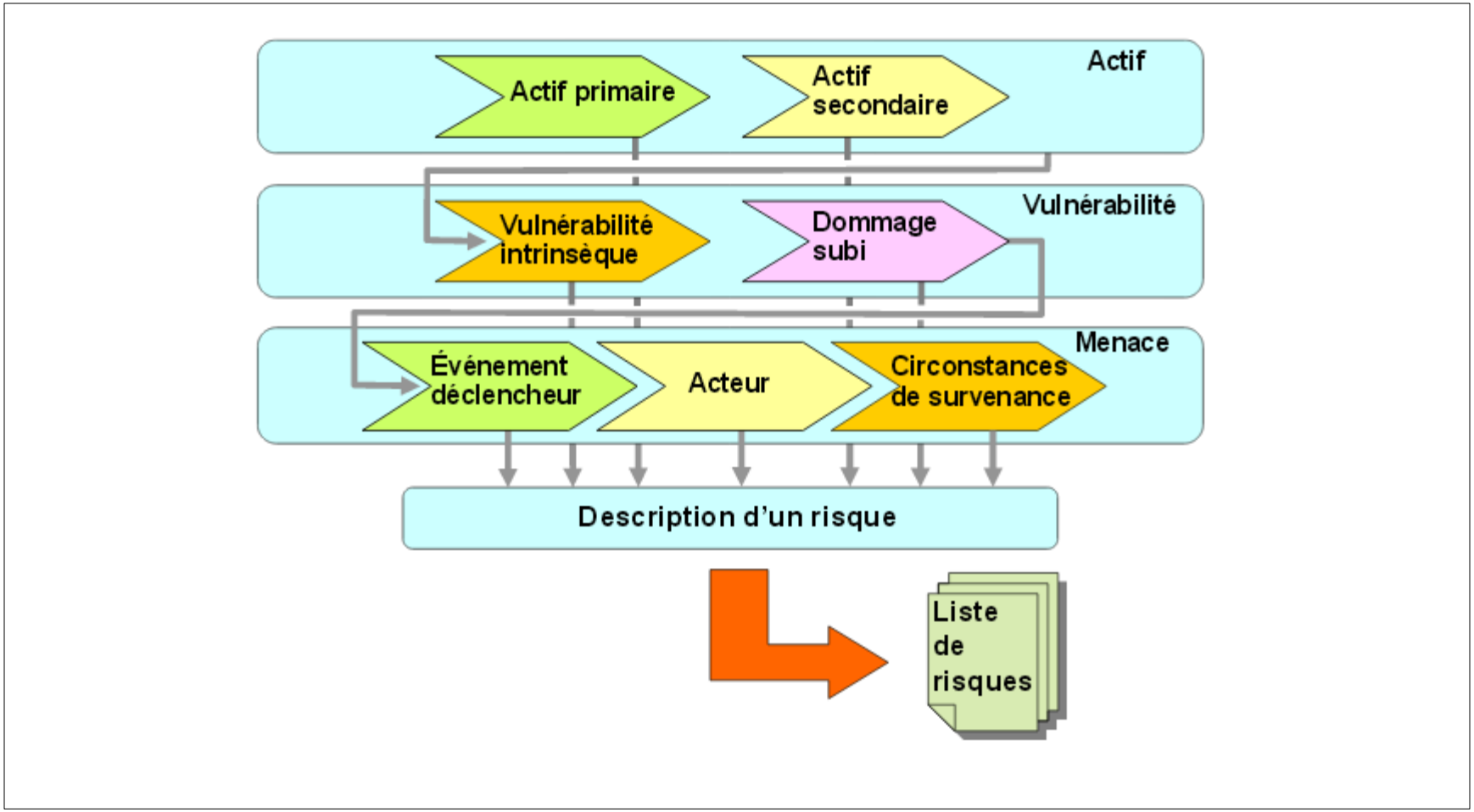
- Contexte de l'exemple (fictif) :
  - *« la PME AlphaCentoris assure deux activités. Pour un ensemble d'associations, elle administre leurs sites WordPress via une offre IaaS d'un fournisseur cloud. Pour des clients industriels, elle réalise le développement de site de communication interne. »*
- Processus à enjeu ?

Plan

- Introduction
- La démarche SMSI
  - Établissement du contexte
  - Appréciation du risque
  - Traitement du risque
  - Gestion du risque
- Exemple d'analyse de risque

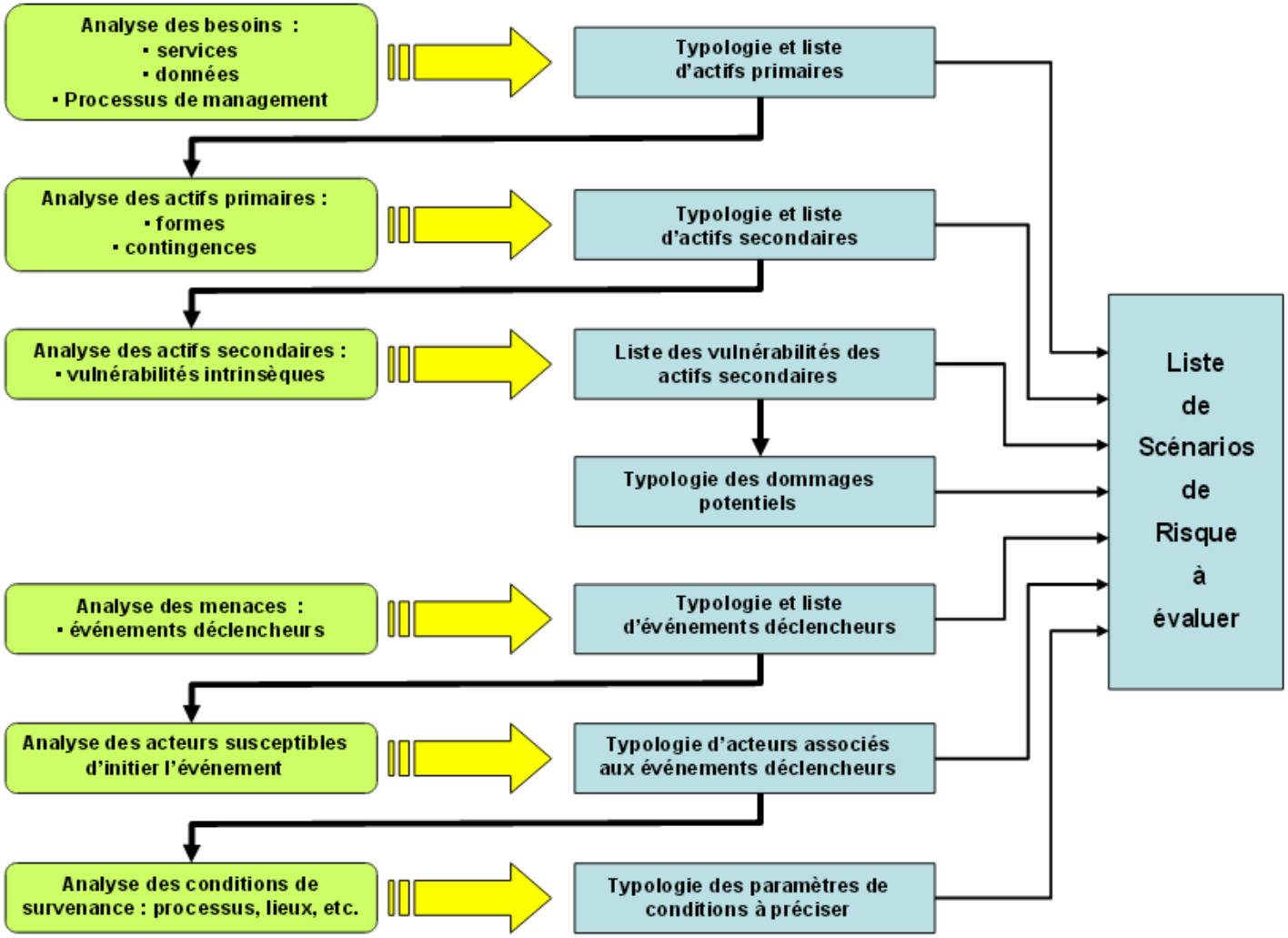
Appréciation du risque

Identification / estimation / évaluation



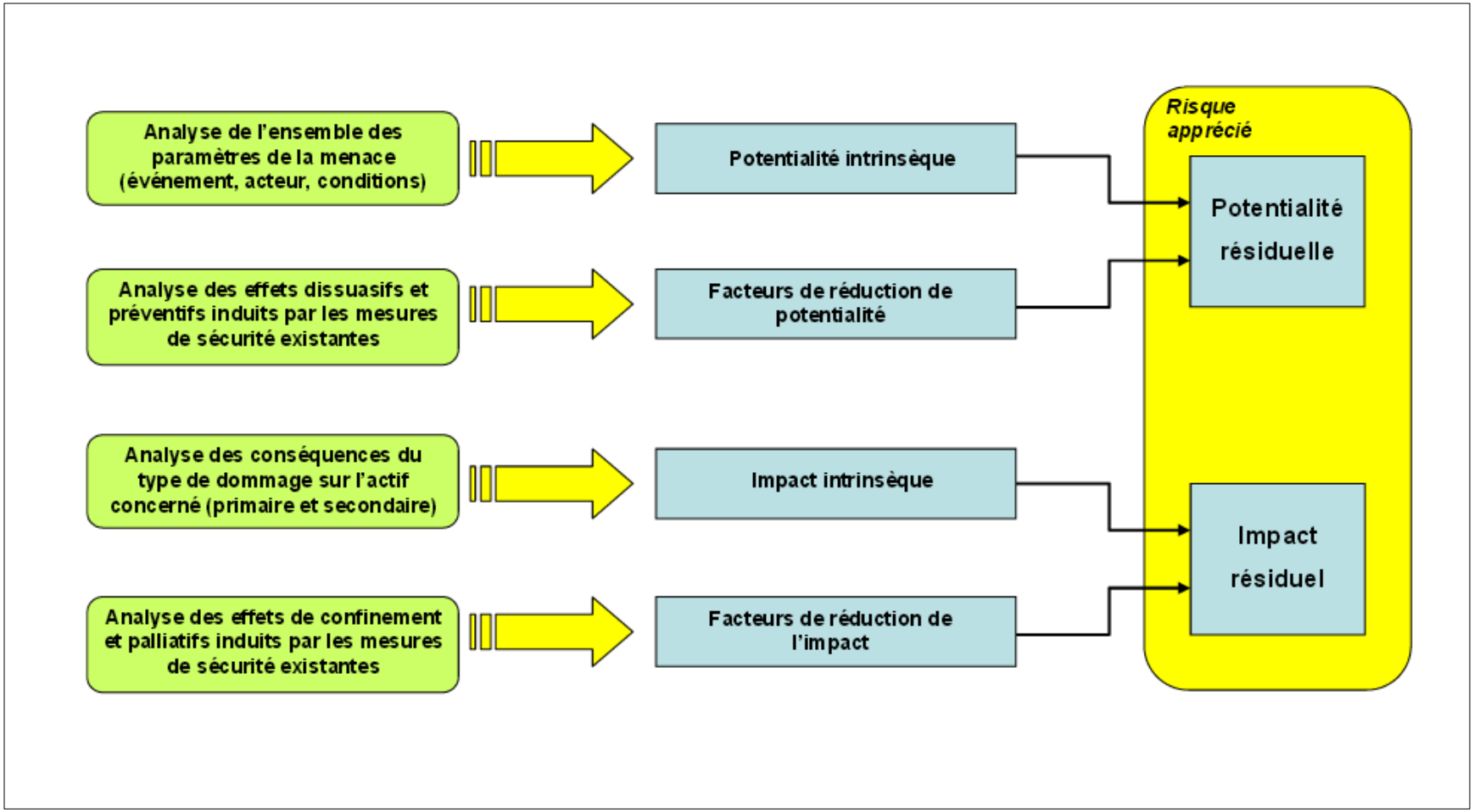
Appréciation du risque MEHARI

Identification des risques



Appréciation du risque MEHARI

Estimation des risques



Analyse de risque : Enjeux/Besoins

Tableau T1			CLASSIFICATION DES DONNÉES																	
Processus ou activités métier, Services communs	Fonction (descriptif)	Sélection si 1	Données applicatives (bases de données)			Données applicatives isolées, en transit Messages			Fichiers bureautiques partagés			Fichiers bureautiques personnels			Documents personnels		Archives informatiques		
			D	I	C	D	I	C	D	I	C	D	I	C	D	C	D	I	C
	Types d'actifs ->		D01	D01	D01	D06	D06	D06	D02	D02	D02	D03	D03	D03	D04	D04	D10	D10	D10
Processus métiers																				
Commerce Logistique		1	2	2	1	2	2										4	4	4
RH		1	2		2	2	2	2	2	2									
Finance		1	2	3	3	2	2	3		3	2						2	2	2
Hébergement		1	3	4	4	3	2	1	2	2	2						4	3	1
Développement		1	4	3	3	2	2	1	4	3	2	3	3	1	3	2	3	3	1
Classification pour l'ensemble			**4**	**4**	**4**	**3**	**2**	**3**	**4**	**3**	**2**	**3**	**3**	**1**	**3**	**2**	**4**	**4**	**4**
Classification des activités sélectionnées			**4**	**4**	**4**	**3**	**2**	**3**	**4**	**3**	**2**	**3**	**3**	**1**	**3**	**2**	**4**	**4**	**4**

Analyse de risque : enjeux/besoin

Tableau T2	CLASSIFICATION DES SERVICES																
Processus métier, application ou domaine applicatif **Services communs**	**Services du réseau étendu**		**Services du réseau local**		**Services applicatifs**			**Services bureautiques communs**		**Equipe-ments mis à la disposition des utilisateurs**	**Services systèmes Communs (Systèmes, périfs, etc.)**		**Services de publication sur site web**		**Services généraux environ-nement de travail**	**Services télécom**	
	D	**I**	**D**	**I**	**D**	**I**	**C**	**D**	**I**	**D**	**D**	**I**	**D**	**I**	**D**	**D**	**I**
Nom de colonne pour formules Classif	**R01**	**R01**	**R02**	**R02**	**S01**	**S01**	**S01**	**S02**	**S02**	**S03**	**S04**	**S04**	**S05**	**S05**	**G01**	**G02**	**G02**
Processus métiers																	
hébergement	**3**	**3**	**3**	**3**	**3**	**3**	**4**	1	1	2	2	2	**3**	**3**	1	2	2
développement	2	2	**3**	**3**	2	2	2	**3**	**3**	**4**	**3**	**3**	1	1	**3**	2	2
Classification pour le périmètre	3	3	3	3	3	3	4	3	3	4	3	3	3	3	3	2	2

Analyse de risque : exposition naturelle *(extrait)*

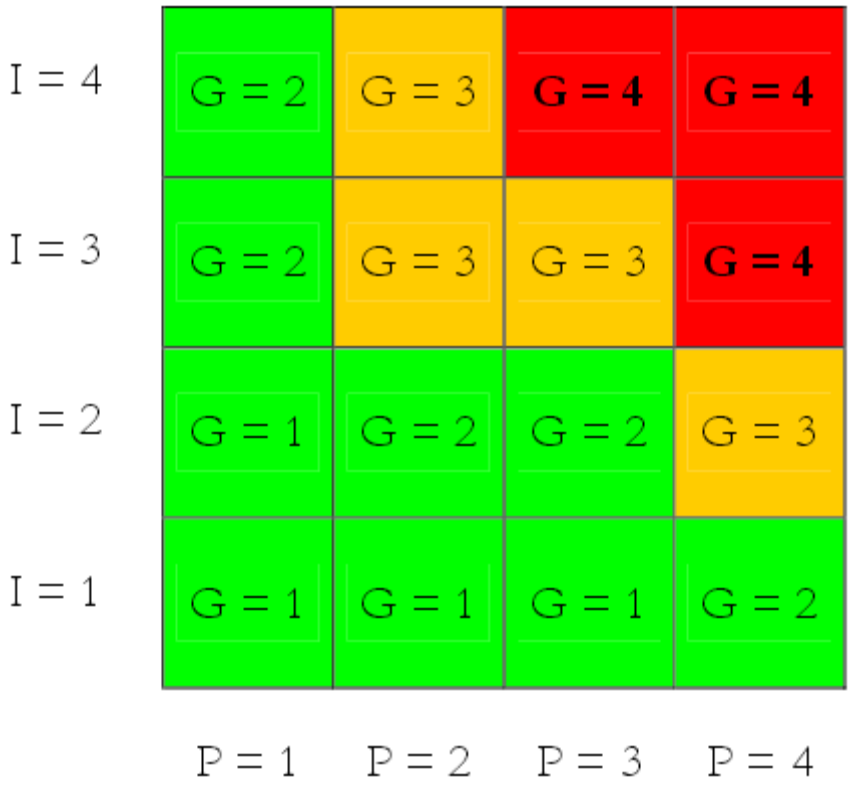
Type	***Événement***	***Code***	***Exposition naturelle standard CLUSIF***	***Exposition naturelle décidée***	***Exposition naturelle résultante***	***Sélection***
Erreur de conception	Bug bloquant dû à une erreur de conception ou d'écriture de programme (interne)	ER.L.Lin	3	3	3	1
Erreur matérielle ou de comportement du personnel	Perte ou oubli de document ou de media	ER.P.Peo	3	3	3	1
	Erreur de manipulation ou dans le suivi d'une procédure	ER.P.Pro	3	3	3	1
	Erreur de saisie ou de frappe	ER.P.Prs	3	3	3	1
Incident dû à l'environnement	Dégât dû au vieillissement	IC.E.Age	2	2	2	1
	Dégât des eaux	IC.E.De	3	1	1	0
	Dégât dû à la pollution	IC.E.Pol	2	1	1	0
	Surcharge électrique	IC.E.Se	2	3	3	1
Incident logique ou fonctionnel	Incident d'exploitation	IF.L.Exp	3	3	3	1
	Bug bloquant dans un logiciel système ou un progiciel	IF.L.Lsp	2	3	3	1
	Saturation bloquante pour cause externe (ver)	IF.L.Ver	3	3	3	1
	Virus	IF.L.Vir	4	4	4	1

Analyse de risque : impacts intrinsèques

Tableau d'Impact Intrinsèque					Sélection d'actifs
Actifs de type Données et informations		**D**	**I**	**C**	
Données et informations					
D01	Fichiers de données ou bases de données applicatives	4	4	4	1
D02	Fichiers bureautiques partagés	4	3	2	1
D03	Fichiers bureautiques personnels (gérés dans environnement personnel)	3	3	1	0
D04	Informations écrites ou imprimées détenues par les utilisateurs, archives personnelles	3		2	0
D05	Listings ou états imprimés des applications informatiques			1	0
D06	Données échangées, écrans applicatifs, données individuellement sensibles	3	2	1	0
D07	Courrier électronique	1	1	1	0
D08	Courrier postal et télécopies	1	1	1	0
D09	Archives patrimoniales ou documentaires	3		1	0
D10	Archives informatiques	4	3	1	1
D11	Données et informations publiées sur des sites publics ou internes	1	1	1	0
Actifs de type Services		**D**	**I**	**C**	
Services généraux communs					
G01	Environnement de travail des utilisateurs	3			1
G02	Services de télécommunication (voix, télécopies, visioconférence, etc.)	2	2		0
Services informatiques et réseaux					
R01	Service du réseau étendu	3	3		0
R02	Service du réseau local	3	3		0
S01	Services applicatifs	3	3	4	1
S02	Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)	3	3		0
S03	Equipements mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.) **Nota : Considérer ici la perte massive de ces services et non celle d'un seul utilisateur**	4			1
S04	Services systèmes communs : messagerie, archivage, impression, édition, etc.	3	3		0
S05	Services de publication d'informations sur un site web interne ou public.	3	3		0

Appréciation du risque MEHARI

Évaluation du risque



Analyse de risque : scénarios (1/2)

Panorama des gravités de scénarios		Disponibilité					Intégrité					Confidentialité				
Actifs de type Services																
Services informatiques et télécom																
R01	Service du réseau étendu	0	0	13	0	V	0	0	5	0	V					
R02	Service du réseau local	0	0	13	0	V	0	0	5	0	V					
S01	Services applicatifs	0	0	41	0	V	0	0	18	0	V	0	16	0	0	V
S02	Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)	0	0	0	0	V	0	0	0	0	V					
S03	Equipements mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)	0	0	0	6	V										
S04	Services systèmes communs : messagerie, archivage, impression, édition, etc.	0	0	0	0	V	0	0	0	0	V					
S05	Services de publication d'informations sur un site web interne ou public	0	0	0	0	V	0	0	0	0	V					

Analyse de risque : scénarios (1/2)

VULNÉRABILITÉ			LIBELLÉ	Sélection directe	Type AEM	Type DICL	Impact Intrinsèque	Exposition	Gravité Intrinsèque	Dissuasion	Prévention	Confinement	Palliation	Confinable (standard)	Confinabilité décidée	Impact décidé	Potentialité décidée	Impact calculé	Potentialité calculée	Gravité calculée	Scén. accepté ou transféré	Gravité pour plans
DIC	Actif	Type de																				
	support	dommage																				
de données applicatives																						
D	Fichier	Effacement	Effacement malveillant de fichiers de données applicatives, par un utilisateur autorisé légitime, se connectant depuis le réseau interne	1	M	D	4	3	**4**	1	1	1	1	0				4	3	4		4
D	Fichier	Effacement	Effacement malveillant de fichiers de données applicatives, par un utilisateur autorisé illégitime, se connectant depuis le réseau interne	1	M	D	4	3	**4**	1	1	1	1	0				4	3	4		4
D	Fichier	Effacement	Effacement malveillant de fichiers de données applicatives, par un utilisateur non autorisé, se connectant depuis le réseau interne	1	M	D	4	3	**4**	1	1	1	1	0				4	3	4		4
D	Fichier	Effacement	Effacement malveillant de fichiers de données applicatives, par un membre du personnel d'exploitation, se connectant depuis le réseau interne	1	M	D	4	3	**4**	1	1	1	1	0				4	3	4		4

Plan

- Introduction
- La démarche SMSI
  - Établissement du contexte
  - Appréciation du risque
  - Traitement du risque
  - Gestion du risque
- Exemple d'analyse de risque

Traitement du risque

- Via quatre *moyens :*
  - L'acceptation du risque,
  - La réduction du risque,
  - Le transfert du risque,
  - L'évitement du risque.

Traitement du risque

Acceptation du risque

- Un risque est acceptable si :
  - Il est ce niveau acceptable dans la grille d'aversion,
  - Du fait d'un contexte particulier dans la vie de l'entreprise qui voit *changer ses priorités*
  - Du fait du coût nécessaire pour y remédier
- Quel qu'en soit le motif, l'acceptation d'un risque est un acte lié à la gouvernance de la sécurité.

Traitement du risque
Réduction du risque

- Moyen de réduire un risque ?
  - En diminuer l'impact
  - En diminuer la probabilité
- Le travail s'oriente alors sur :
  - Les facteurs de réduction de risques (actions structurelles, organisationnelles, …) via l'identification des *services de sécurité* (cf 27002) impliqués dans le risque.
  - La définition d'une échelle de mesure du niveau de qualité des services de qualité ainsi qu'un niveau cible (contextuel)
  - Les mécanismes techniques et organisationnels envisageables pour la mise en œuvre du service
- Ou bien alors … prendre des mesures structurelles faisant disparaître le contexte « risqué » (déménagement si en zone inondable, …)

Traitement du risque

Transfert du risque

- Transférer le risque … sur un tiers :
  - En souscrivant à une assurance (transfert d'une partie des charges financières à un tiers)
  - Via le transfert de la charge sur un tiers (responsable) par une action en justice

Traitement du risque

Évitement du risque

- … si c’est trop risqué … on le fait pas …

Plan

- Introduction
- La démarche SMSI
  - Établissement du contexte
  - Appréciation du risque
  - Traitement du risque
  - Gestion du risque
- Exemple d'analyse de risque

Gestion du risque

- La gestion du risque se compose de :
  - La construction de plans d'actions,
  - La mise en œuvre des actions (des différents plans)
  - Le contrôle des effets et le pilotage des plans d'actions

Gestion du risque
Construction de plans d'actions

- Les plans d'actions viseront à :
  - Mettre en place les services de sécurités identifiés en objectifs de réduction des risques
  - Réaliser des mesures structurelles et organisationnelles visant à réduire certaines exposition au risque (transfert vers les tiers, évitement)
- À cette fin, ils devront procéder suivant les étapes :
  1. Prioriser les objectifs en terme de service de sécurité à mettre en œuvre,
  2. Établir les plans d'actions concrets de transformation permettant de mettre en place les services de sécurité selon le niveau cible,
  3. Établir les plans d'actions concerts pour les mesures structurelles ou organisationnelles d'évitement du risque,
  4. Définir la gouvernance nécessaire à sa mise en œuvre

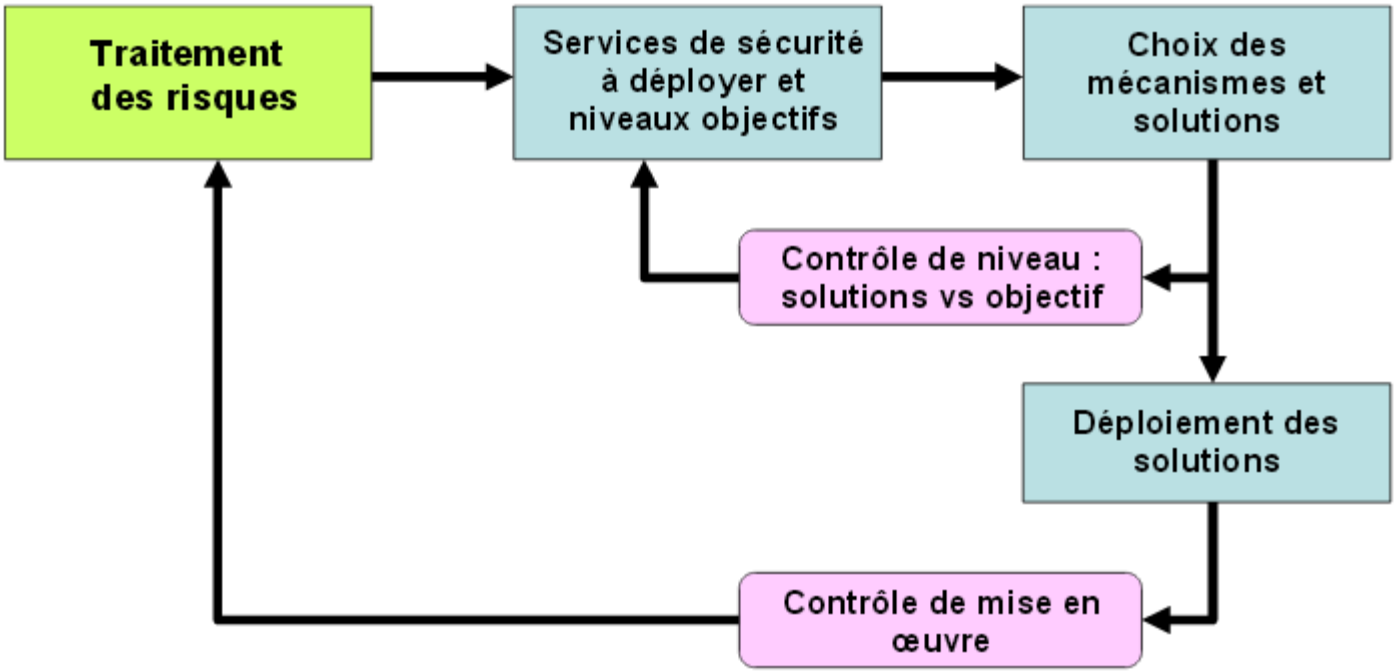
Traitement du risque : plan d'action

Gr 1	Gr 2	Gr 3	Gr 4	Tot	Mesures à améliorer	Type de plan	Décision	Services à améliorer	Niveau actuel	Niveau cible	Services à améliorer	Niveau actuel	Niveau cible	Services à améliorer	Niveau actuel	Niveau cible
Perte de données applicatives																
0	**1**	**0**	**7**	**8**	Dissuasion :	Plan de type A		07C01	1	3	07C02	1	3	08E02	1	3
					Dissuasion :	Plan de type A		03B06	1	3						
					Prévention :	Plan de type A		07A01	1	4	07A02	1	4	07A03	1	4
					Prévention :	Plan de type B		08A03	1	4	08A06	1	4	08C03	1	4
					Prévention :	Plan de type A		03A01	1	4	03A04	1	4	03B03	1	4
					Confinement :	Plan de type A		08E02	1	3	08E03	1	3			
					Palliation :	**Plan de type E**		08D05	1	3	08D09	1	3	09D02	1	3

Gestion du risque
Mise en œuvre des plans d'actions

- Ce sont des projets visant, le plus souvent, soit à ajouter des activités dans des processus en place, soit à modifier les modes de travail en place.
  - Attention à la conduite du changement !

Gestion du risque
Contrôle et pilotage



Vulnérabilités / plan d'action

pour le service « équipements mis à la disposition des utilisateurs »

Vulnérabilité sur les équipements mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)	**Mesures Dissuasive**	**Mesures Préventive**	**Mesures Palliative**
Effacement généralisé accidentel de configuration (programmes, codes, paramétrage, etc.) d'équipements mis à la disposition des utilisateurs, suite à un incident d'exploitation		11A01	11D03
Effacement généralisé, par erreur, de configurations (programmes, codes, paramétrage, etc.) d'équipements mis à la disposition des utilisateurs, par un membre du personnel d'exploitation			11D03
Effacement généralisé, par erreur, de configurations (programmes, codes, paramétrage, etc.) d'équipements mis à la disposition des utilisateurs, par un membre du personnel de maintenance			11D03
Effacement malveillant généralisé de configurations (programmes, codes, paramétrage, etc.) d'équipements mis à la disposition des utilisateurs, par un membre du personnel d'exploitation	min(11E02;11E03)		11D03
Indisponibilité massive d'équipements mis à la disposition des utilisateurs, due à un virus		11D06	max(01E03;11D07)
Indisponibilité temporaire accidentelle d'équipements mis à la disposition des utilisateurs, due à une panne d'équipement (Equipement partagé)			11D01

Scénario / plan d'action

- Mesure dissuasives :
  - 11E02 Authentification et contrôle d'accès des administrateurs
  - 11E03 Surveillance des actions d'administration du parc de postes utilisateurs
- Mesures préventives :
  - 11A01 Contrôle de l'installation de nouvelles versions sur les postes utilisateur
  - 11D06 Protection des postes de travail contre les virus
- Mesures palliatives :
  - 01E03 Plan de reprise de l'environnement de travail
  - 11D03 Plan de sauvegarde des données utilisateur
  - 11D07 Plan de reprise d'activité des postes utilisateur
  - 11D01 Organisation de la maintenance du matériel mis à la disposition du personnel

Authentification et contrôle d'accès des administrateurs

(T) La prise de contrôle d'un poste utilisateur nécessite-t-elle l'authentification de l'administrateur ?

(T) Le protocole d'authentification des administrateurs ou possesseurs de droits privilégiés est-il considéré comme "fort" ?
Un protocole d'authentification est considéré comme fort s'il n'est pas susceptible d'être mis en brèche par une observation ou une écoute de réseau, ni mis en défaut par des outils de spécialistes (en particulier des outils de craquage de mots de passe). Il s'agit de protocole s'appuyant généralement sur des procédés cryptologiques.

(T) A défaut, s'il s'agit de mots de passe, les règles imposées peuvent-elles être considérées comme très strictes ?
Des règles très strictes supposent des mots de passe non triviaux et testés comme tels avant acceptation, des mélanges de différents types de caractères avec une longueur importante (10 caractères ou +). Il est souhaitable que de telles règles soient élaborées en accord avec le RSSI.

(P) Y a-t-il un contrôle systématique des droits de l'administrateur, de son contexte et de l'adéquation de ces droits et du contexte avec l'accès demandé, en fonction de règles de contrôle d'accès formalisées ?

(P) Les paramètres de l'authentification sont-ils sous contrôle strict ?
Un contrôle strict requiert que la liste des personnes habilitées à changer les règles de définition des authentifiants, les authentifiants eux-mêmes, les règles de surveillance des tentatives de connexion, etc. soit très limitée, qu'il existe un contrôle d'accès renforcé pour procéder à ces modifications, que les modifications soient journalisées et auditées et qu'il existe un audit général au moins annuel de l'ensemble des paramètres de l'authentification.

(P) Les processus qui assurent l'authentification sont-ils sous contrôle strict ?
Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus de l'authentification.

(P) Existe-t-il un audit régulier des paramètres de sécurité de protection des profils et des droits ?

Surveillance des actions d'administration du parc de postes utilisateurs *(ISO 27002, « Surveillance »)*

(P) A-t-on fait une analyse approfondie des événements ou successions d'événements menés avec des droits d'administration sur le parc de postes utilisateurs et pouvant avoir un impact sur la sécurité ?

(T) Enregistre-t-on ces événements ainsi que tous les paramètres utiles à leur analyse ultérieure ?

(T) Existe-t-il un système permettant de détecter toute modification ou suppression d'un enregistrement passé et de déclencher une alerte immédiate auprès d'un responsable ?

(T/P) Existe-t-il une synthèse de ces enregistrements permettant à la hiérarchie de détecter des comportements anormaux ?

(T) Existe-t-il un système permettant de détecter toute modification des paramètres d'enregistrement et de déclencher une alerte immédiate auprès d'un responsable ?

(T) Toute inhibition du système d'enregistrement et de traitement des enregistrements d'actions menées sur les configurations du parc des postes utilisateurs déclenche-t-elle une alarme auprès d'un responsable ?

(T) Les enregistrements ou les synthèses sont-ils protégés contre toute altération ou destruction ?

(T) Les enregistrements ou les synthèses sont-ils conservés sur une longue durée ?

(P) Les procédures d'enregistrement des actions privilégiées sur le parc des postes utilisateurs et de traitement de ces enregistrements font-elles l'objet d'un audit régulier ?

Contrôle de l'installation de nouvelles versions sur les postes utilisateur
(ISO 27002, « Procédures et responsabilités liées à l'exploitation » et « Planification et acceptation du système »)

(P) Les décisions d'évolution de version des progiciels utilisateurs font-elles l'objet de procédures de contrôle (enregistrement, planning, approbation formelle, communication à l'ensemble des personnes concernées, etc.) ?

(P) Les nouvelles versions sont-elles testées sur sites pilotes avant généralisation à l'ensemble du parc ?

(P) Le déclenchement à distance de nouvelles installations sur les postes utilisateurs est-il réservé à une population limitée d'administrateurs spécifiques du parc bureautique ?

(T/P) Les paramétrages de sécurité et règles de configuration des postes utilisateurs font-ils l'objet d'une liste précise tenue à jour?

(P) Les paramétrages de sécurité et règles de configuration sont-ils contrôlés après toute évolution de configuration des postes utilisateurs ?

(P) L'impact éventuel des évolutions de configuration des postes utilisateurs sur les plans de continuité a-t-il été pris en compte ?

(P) L'ensemble des procédures de contrôle des configurations utilisateurs fait-il l'objet d'un audit régulier ?

Protection des postes de travail contre les virus

(ISO 27002, « Protection contre les codes malveillant et mobile »)

(P) A-t-on défini une politique afin de lutter contre les risques d'attaque par des codes malveillants (virus, chevaux de Troie, vers, etc.) : interdiction d'utiliser des logiciels non préalablement autorisés, mesures de protection lors de la récupération de fichiers via des réseaux externes, revues de logiciels installés ?

(T) Les postes de travail sont-ils pourvus de dispositifs de protection contre les virus et les codes malveillants ?

(T) Le produit anti-virus est-il régulièrement et automatiquement mis à jour ?
Avec internet, l'instantanéité de la menace oblige à un contrôle de disponibilité d'une mise à jour au minimum quotidiennement.

(T) Un analyse complète des fichiers du poste de travail est-elle régulièrement effectuée de façon automatique ?

(P) A-t-on défini les actions à mener par l'équipe d'assistance aux utilisateurs en cas d'attaque par des codes malveillants (alerte, actions de confinement, déclenchement de processus de gestion de crise, etc.) ?

(T/P) L'équipe d'assistance aux utilisateurs a-t-elle la possibilité d'effectuer à tout moment une analyse complète de l'ensemble du parc des postes utilisateurs ?

(T/P) A-t-on défini une politique et des mesures de protection pour lutter contre des codes exécutables (applets, contrôles activeX, etc.) non autorisés (blocage ou contrôle de l'environnement dans lequel ces codes s'exécutent, contrôle des ressources accessibles par les codes mobiles, authentification de l'émetteur, etc.) ?

(P) L'activation et la mise à jour des antivirus sur les postes utilisateurs font-elles l'objet d'un audit régulier ?

Plan de reprise de l’environnement de travail

(T) Existe-t-il des solutions de secours pour pallier l'indisponibilité de l'environnement de travail (indisponibilité des locaux, de l'alimentation en énergie, de la téléphonie, etc.) ?

(P) Ces solutions sont-elles décrites en détail dans des Plans de Reprise de l'Environnement de Travail (PRET) incluant les règles de déclenchement, les actions à mener, les priorités, les acteurs à mobiliser et leurs coordonnées ?
(T/P) Ces plans sont-ils testés au moins une fois par an ?

(T) Le cas de défaillance ou d'indisponibilité d'un moyen de secours a-t-il été envisagé et y a-t-il, pour chacun, une solution de secours de deuxième niveau ?

(T) Les solutions de secours sont-elles utilisables pour une durée illimitée ou, à défaut, est-il prévu une deuxième solution venant en remplacement de la première après un temps déterminé ?

(P) L'existence, la pertinence et la mise à jour des PRET font-elles l'objet d'un audit régulier ?

Plan de sauvegarde des données utilisateur

ISO 27002 « Code de bonne pratique pour la gestion de la sécurité de l'information », « Sauvegardes »

(P) A-t-on établi un plan de sauvegarde, couvrant l'ensemble des paramètres de configuration des postes utilisateurs ?

(T) Ce plan de sauvegarde est-il traduit en automatismes de production ?

(T/P) Teste-t-on régulièrement que les sauvegardes des paramètres de configuration des postes utilisateurs permettent effectivement de reconstituer l'environnement de travail des utilisateurs à partir de postes vierges ou d'une réinstallation complète, dans des temps compatibles avec les exigences des métiers ?

(T) Les automatismes de production assurant les sauvegardes des configurations utilisateurs sont-ils protégés par des mécanismes de haute sécurité contre toute modification illicite ou indue ?
Un tel mécanisme pourrait être un scellement électronique ou tout système de détection de modification équivalent.

(P) L'ensemble des procédures et plans de sauvegarde des logiciels fait-il l'objet d'un audit régulier ?

Plan de reprise d'activité des postes utilisateur

ISO 27002 « Code de bonne pratique pour la gestion de la sécurité de l'information », « Gestion du plan de continuité de l'activité »

(P) A-t-on identifié précisément les scénarios de sinistre pouvant affecter l'ensemble du parc des postes utilisateurs et analysé, pour chaque scénario, ses conséquences en termes de services rendus impossibles aux utilisateurs ?

(P) A-t-on défini, pour chaque scénario et en accord avec les utilisateurs, un échéancier des services minimum à assurer en fonction du temps ?

(T) Les services à assurer sont à considérer qualitativement et quantitativement (pourcentage du parc à remettre en opération)

(T) A-t-on défini et mis en place, en conséquence et pour faire face à chaque scénario retenu, une solution de secours respectant les demandes des utilisateurs ?

(T) Les ressources organisationnelles, techniques et humaines sont-elles suffisantes pour satisfaire les exigences de l'organisation ?
Il faudra veiller à introduire des moyens permettant de pallier à des défaillances en personnel .

(T/P) Les ressources organisationnelles et humaines sont-elles éduquées afin de pouvoir satisfaire les exigences de l'organisation ?
Il faudra veiller à former tous les acteurs concernés.

(P) Les solutions de continuité des services liés au parc de postes utilisateurs sont-elles décrites en détail dans des Plans de Reprise d'Activité (des postes utilisateurs) incluant les règles de déclenchement, les actions à mener, les priorités, les acteurs à mobiliser et leurs coordonnées ?

(P) Ces plans sont-ils testés au moins une fois par an ?

(T/P) Les tests effectués permettent-ils de garantir la capacité de la solution de secours à assurer, en pleine charge opérationnelle, les services minimum demandés par les utilisateurs ?
Les tests requis pour obtenir cette garantie reposent généralement sur des essais en vraie grandeur impliquant l'ensemble des utilisateurs et pour chaque variante de scénario. Les résultats des tests doivent être consignés et analysés afin d'améliorer les capacités de l'organisation à répondre aux situations envisagées.

(T/P) Si les solutions de secours incluent des livraisons de matériels, qui ne peuvent être déclenchées lors des tests, existe-t-il un contrat d'engagement de livraison des matériels de remplacement dans des délais fixés et prévus au plan de secours, par le constructeur ou un tiers (distributeur) ?

(P) L'existence, la pertinence et la mise à jour des plans de reprise d'activité des postes utilisateurs font-elles l'objet d'un audit régulier ?

(P) La mise à jour des procédures citées dans le plan de secours des postes utilisateurs font-elles l'objet d'un audit régulier ?

Organisation de la maintenance du matériel mis à la disposition du personnel
ISO 27002 « Sécurité du matériel »

(T) Tous les matériels sont-ils couverts par un contrat de maintenance (micro-ordinateurs, périphériques, etc.) ?

(T) Existe-t-il des contrats de maintenance particuliers pour tous les matériels demandant une forte disponibilité dont la réparation ou le remplacement ne pourrait s'effectuer dans des délais acceptables ?

(T) Ces contrats de maintenance prévoient-ils explicitement la mise à disposition d'un matériel équivalent ?

(T) Ces contrats prévoient-ils des engagements d'intervention dont la durée maximale est fixée au contrat et compatible avec les impératifs de disponibilité ?

(P) Les contrats de maintenance, le choix des prestataires et les procédures de maintenance associées font-ils l'objet d'un audit régulier ?

Résultat

- La mise en œuvre du plan d'action permet la réduction du risque

Panorama des gravités de scénarios	Disponibilité					Intégrité					Confidentialité				
Actifs de type Services															
Services informatiques et télécom															
R01 Service du réseau étendu	0	0	13	0	V	0	0	5	0	V					
R02 Service du réseau local	0	0	13	0	V	0	0	5	0	V					
S01 Services applicatifs	0	0	41	0	V	0	0	18	0	V	0	16	0	0	V
S02 Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)	0	0	0	0	V	0	0	0	0	V					
S03 Equipements mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)	6	0	0	0	V										
S04 Services systèmes communs : messagerie, archivage, impression, édition, etc.	0	0	0	0	V	0	0	0	0	V					
S05 Services de publication d'informations sur un site web interne ou public	0	0	0	0	V	0	0	0	0	V					

Exercice de mise en pratique

- Contexte métier :
  - L'entreprise AlphaBeta souhaite développer une application de payement en ligne utilisant un algorithme d'encryptage développé par le fondateur.
  - Le fond d'investissement JaiDesSioux demande à ce qu'une analyse de risque de sécurité soit réalisée préalablement à l'accord de financement.

Exercice de mise en pratique

- Cadrage de l'étude :
  - Le processus métier étudié est celui relatif au développement d'application
  - Les moyens techniques utilisés sont :
    - Trois serveurs (développement unitaire, recette, intégration) en local sur le site de développement,
    - Utilisation de Subversion sur un serveur autonome,
    - Partage des documents sur le serveur de fichiers centralisé,
    - Les développeurs utilisent des PC en mode pair programming,
  - Aucune activité de développement n'est réalisée via de la sous-traitance.
  - L'entreprise n'a pas fixé de politique de sécurité mais l'expertise de ses membres fait que l'ensemble des bonnes pratique de l'état de l'art sont mises en œuvre.

Précision du contexte

- Définition de l'activité étudiée
  - *Identification d'événements (métier) redoutés en vue de la définition de l'importance (relative) en terme de DIC des moyens nécessaires à sa réalisation.*
- Définition des moyens mis en œuvre pour la réaliser
  - *Clarification du périmètre de chaque élément de classification des données, des services et de la conformité aux lois et règlements.*

Analyse du risque intrinsèque

1. Établir les valeurs pour l'onglet « Expo » qualifiant les types et expositions naturelles de l'entreprise.
2. Classification des impacts de non-conformité :
    1. DIC des données sur le processus métier étudié (T1),
    2. DIC des services sur le processus métier étudié (T2),
    3. De l'efficience des processus de management sur les processus métier étudiés (T3).
3. Sélectionner les actifs du tableau d'impact intrinsèque (« Classif ») selon le niveau de criticité choisi.

Niveau de risque intrinsèque :

consultation des onglets Risk%actif et Risk%event

Analyse du niveau de risque actuel

- L'audit du niveau de risque actuel sera établi en fonction du niveau de risque intrinsèque à traiter en priorité (= 4) concernant l'intégrité.

1. Analyser les scénarios correspondant au risque relatif à l'intégrité sur les actifs (« Scénario ») :
   - Scénarii de l'identifiant de l'actif considéré + (I)ntégrité
   - Décision via la colonne « sélection directe » si le scénario correspond à la situation (1) ou pas (0).
2. Analyser les plans d'actions correspondant au risques relatifs à l'intégrité sur les actifs (« Plans_action ») :
   - Lister les services concernés
   - Se répartir l'audit de ces services et établir le niveau de risque actuel.

Permet la définition du niveau de risque actuel.

Établissement des plans d'action

1. Analyse des plans d'action après calcul du niveau de risque actuel et prioriser ceux dont le niveau est *très* inférieur au niveau cible (1 à 4).
2. Identification des actions correctrices à apporter aux services.

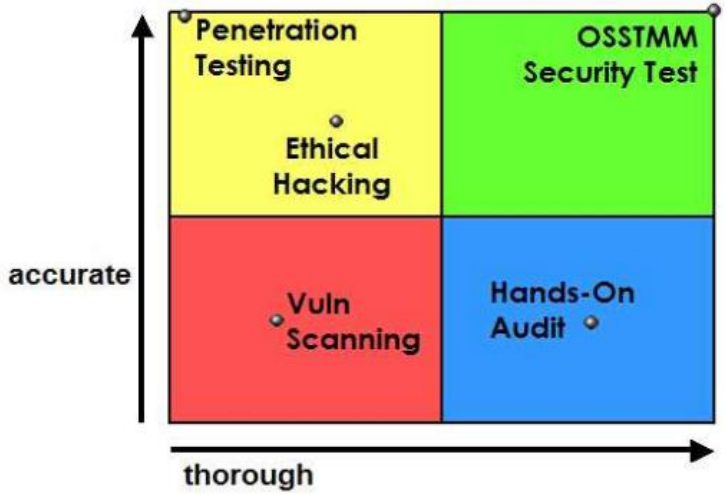
Plan

- Introduction
- La démarche SMSI
  - Établissement du contexte
  - Appréciation du risque
  - Traitement du risque
  - Gestion du risque
- Exemple d'analyse de risque
- OSSTMM

Appréciation du risque OSSTMM

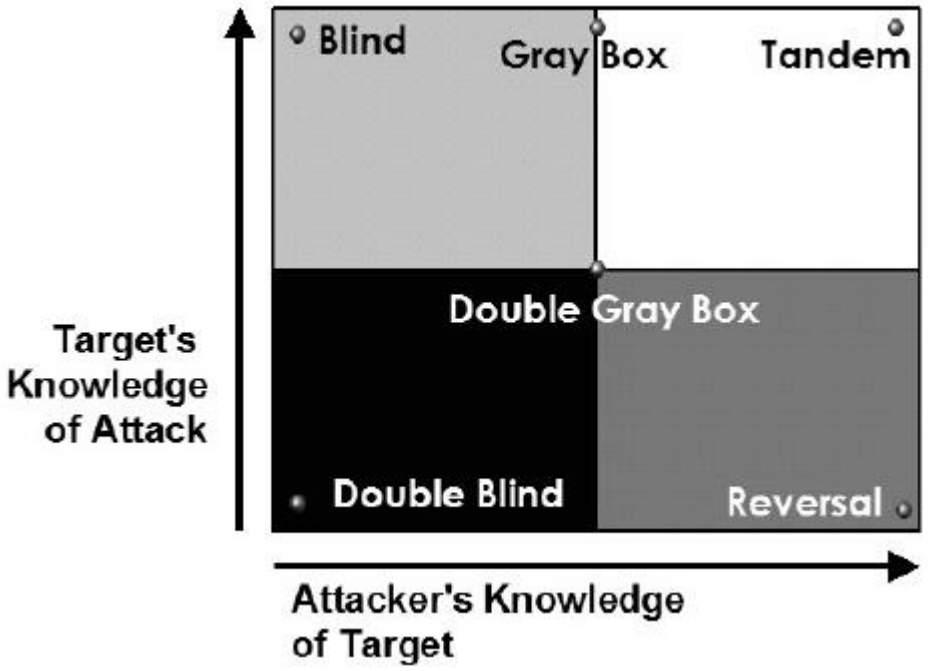
- Exemple de complément méthodologique à MEHARI dans l'organisation de tests et dans l'analyse de niveaux de sécurité. OSSTMM permet une mesure de la sécurité à un niveau opérationnel en garantissant :

  Un standard de mesure de la sécurité,
  Une méthodologie assurant une mesure cohérente et reproductible



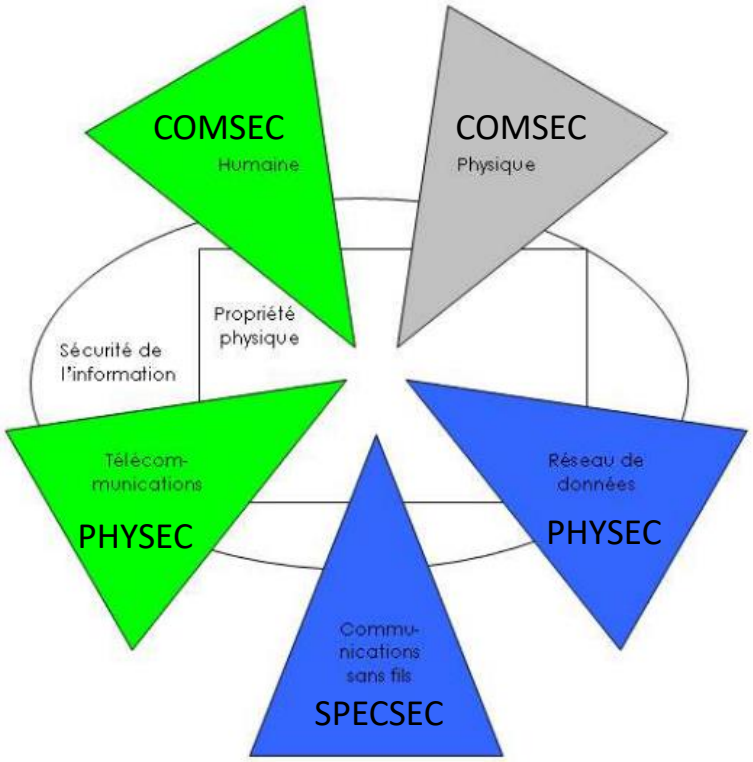
Appréciation du risque OSSTMM

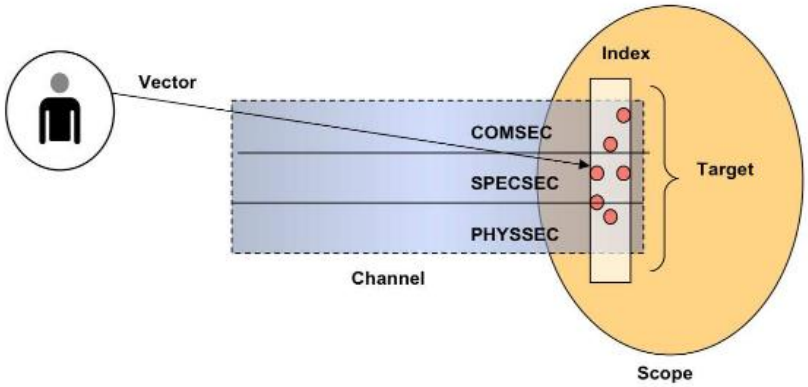
- Méthodologie utilisée pour les tests



Appréciation du risque OSSTMM

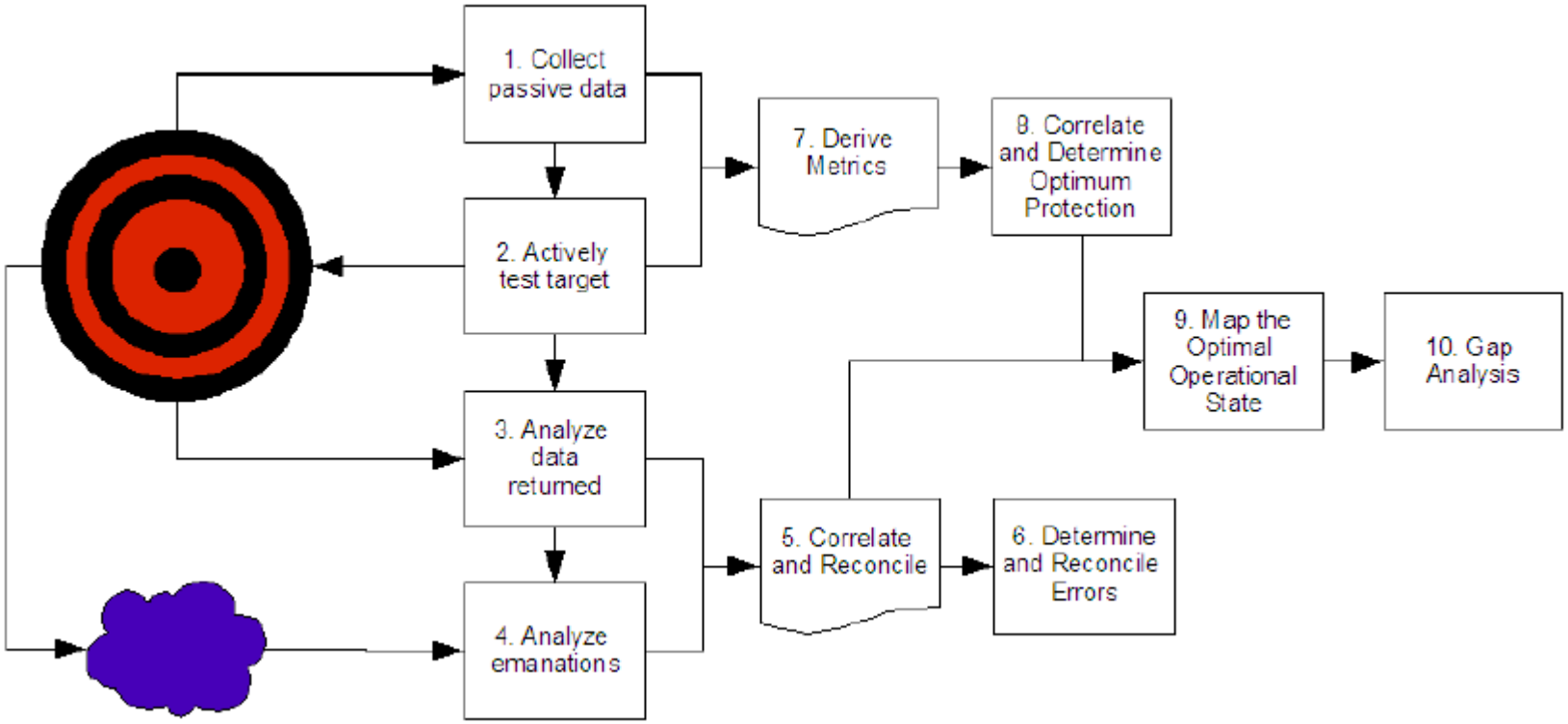
- Définition des types de tests





Appréciation du risque OSSTMM

- Mise en œuvre



Appréciation du risque OSSTMM

Grille d'analyse

Catégorie		Sécurité Opérationnelle	Limitation
Surface exposée		**Visibles**	**Exposition**
		Accédant	**Vulnérabilité**
		De confiance	
Contrôles	Classe A Interactives	**Identification/Authorisation**	**Faiblesses**
		Mitigation	
		Résilience	
		Assujettissement	
		Continuité	
	Classe B Processus	**Non-Répudiation**	**Sujet d'attention**
		Confidentialité	
		Protection des données	
		Intégrité	
		Alarmes	
			Anomalies

Correction exercice

Suite à la diffusion sur le darkweb de fichiers bureautiques personnels liés à l'activité de gestion de contenu du processus de développement il est décidé d'utiliser l'analyse de risque Mehari pour éviter que cela se reproduise. Une analyse de la l'évènement a été réalisée et **le personnel d'exploitation ainsi que celui de maintenance ont été mis hors de cause**.

Identifiez les scénarios correspondant à l'évènement et proposez un plan d'actions préventif sur la base des préconisations Méhari. Que pensez-vous des préconisations données ?

Acteur	LIBELLÉ	Sélection directe	Valeurs calculées (courant)			Risque Accepté (A) ou Transféré (T)	Gravité pour plans	Mesures (formules littérales)			
			Impact	Potentialité	Gravité			Dissuasives EFF-DISS	Préventives EFF-PREV	Confinement EFF-CONF	Palliatives EFF-PALL
	Divulgation, par erreur, de fichiers bureautiques personnels due à une erreur de procédure, lors de traitements utilisateurs	1	4	3	4		4		11C01		
E	Divulgation, par erreur, de fichiers bureautiques personnels due à une erreur de procédure, lors d'une opération de maintenance matérielle	1	4	3	4	A			max(11C01;11C03)		
Pna	Détournement de fichiers bureautiques personnels , par un membre du personnel non autorisé, se connectant directement au poste de travail, en l'absence de l'utilisateur	1	4	3	4		4		max(min(11B01;11E01);11C01)		
Pna	Détournement de fichiers bureautiques personnels , par un membre du personnel non autorisé, se connectant directement au poste de travail, en dehors des heures ouvrables	1	4	3	4		4		max(min(11B01;11E01);11C01)		
E	Détournement de fichiers bureautiques personnels , en exploitation, par un membre du personnel d'exploitation	1	4	3	4	A		min(11E02;11E03)	11C01		
M	Détournement de fichiers bureautiques personnels , lors d'une opération de maintenance, par un membre du personnel de maintenance	1	4	3	4	A			max(11C01;11C03)		
	Divulgation d'informations, par perte accidentelle, de media support de fichiers bureautiques personnels , en dehors de l'entreprise	1	4	3	4		4		11C01		
Per	Divulgation d'informations, par vol de media support de fichiers bureautiques personnels , dans les bureaux, par un membre du personnel de l'entreprise, en l'absence de l'utilisateur	1	4	2	3		3	02C05	max(min(02C01;02C02;02C03);11C02)		
Vis	Divulgation d'informations, par vol de media support de fichiers bureautiques personnels , dans les bureaux, par un visiteur, en l'absence de l'utilisateur	1	4	2	3		3	02C05	max(02C06;11C02)		
Per	Divulgation d'informations, par vol de media support de fichiers bureautiques personnels , dans les bureaux, par un membre du personnel de l'entreprise, en dehors des heures ouvrables	1	4	2	3		3	max(02C04;02C05)	max(min(02C01;02C02;02C03);11C02)		
Ser	Divulgation d'informations, par vol de media support de fichiers bureautiques personnels , dans les bureaux, par un membre du personnel de service, en dehors des heures ouvrables	1	4	2	3		3	02C05	11C02		
	Divulgation d'informations, par vol de media support de fichiers bureautiques personnels , en dehors de l'entreprise	1	4	2	3		3		11C02		
Per	Divulgation d'informations, par vol de PC portable contenant des fichiers bureautiques personnels , dans les bureaux, par un membre du personnel de l'entreprise, en l'absence de l'utilisateur	1	4	2	3		3	02C05	max(min(02C01;02C02;02C03;11B01);11C01)		
Vis	Divulgation d'informations, par vol de PC portable contenant des fichiers bureautiques personnels , dans les bureaux, par un visiteur, en l'absence de l'utilisateur	1	4	2	3		3	02C05	max(02C06;11B01;11C01)		
Per	Divulgation d'informations, par vol de PC portable contenant des fichiers bureautiques personnels , dans les bureaux, par un membre du personnel de l'entreprise, en dehors des heures ouvrables	1	4	2	3		3	max(02C04;02C05)	max(min(02C01;02C02;02C03;11B01);11C01)		
Ser	Divulgation d'informations, par vol de PC portable contenant des fichiers bureautiques personnels , dans les bureaux, par un membre du personnel de service, en dehors des heures ouvrables	1	4	2	3		3	02C05	max(11B01;11C01)		
	Divulgation d'informations, par vol de PC portable contenant des fichiers bureautiques personnels , en dehors de l'entreprise	1	4	2	3		3		max(11B01;11C01)		

Plan d’action

Prévention : **Plan de type E**		11C01	1	4	11C02	1	4

11C01	***Protection de la confidentialité des données contenues sur le poste de travail ou sur un serveur de données (disque logique pour le poste de travail)***
11C01-01	Les données sensibles contenues éventuellement sur le poste de travail ou sur un disque logique de données partagées hébergé sur un serveur de données sont-elles chiffrées ?
11C01-02	Les éléments du processus de chiffrement sont-ils fortement protégés contre toute altération, modification ou arrêt ?
11C01-03	Les postes de travail sont-ils équipés d'un système d'effacement empêchant effectivement de relire toute donnée effacée sur le disque local ou sur un disque partagé ?
11C01-04	Le poste de travail est-il équipé d'un système d'effacement réel et efficace des fichiers temporaires créés sur le disque local ou sur un disque partagé ?
11C01-05	Le processus ou les directives concernant le chiffrement des fichiers s'étend-il aux messages électroniques et à leurs pièces jointes ?
11C01-06	Le processus ou les directives concernant le chiffrement des fichiers s'étend-il aux informations contenues dans les carnets d'adresses électroniques ?
11C01-07	Les utilisateurs ont-ils reçu une formation à l'utilisation des moyens de chiffrement et d'effacement des informations à supprimer, leur indiquant, en particulier, les conditions à respecter pour que ce chiffrement ne puisse être contourné ?
11C01-08	Procède-t-on à des audits réguliers de l'utilisation des moyens de chiffrement et d'effacement par les utilisateurs ?
11C02	***Protection de la confidentialité des données de l'environnement de travail personnel stockées sur support amovible***
11C02-01	Les données sensibles stockées sur support amovible sont-elles chiffrées ?
11C02-02	Les éléments du processus de chiffrement sont-ils fortement protégés contre toute altération, modification ou inhibition ?
11C02-03	Le processus de chiffrement est-il appliqué quelque soit le type de support (disque externe, clé USB, PDA, etc.)

Question 2 : évolution de la criticité des listings

Processus ou activités métier, Services communs	Fonction (descriptif)	Sélection si 1	Données applicatives (bases de données)			Données applicatives isolées, en transit Messages			Fichiers bureautiques partagés			Fichiers bureautiques personnels			Documents personnels		Listings ou états imprimés	Courrier électronique		
			D	I	C	D	I	C	D	I	C	D	I	C	D	C	C	D	I	C
	Types d'actifs ->		D01	D01	D01	D06	D06	D06	D02	D02	D02	D03	D03	D03	D04	D04	D05	D07	D07	D07
Processus métiers																				
Développement	WebDesign	0	2	3	1	1	1	1	4	3	2	3	3	2	1	1	1	1	1	3
Développement	Contenu	1	4	4	4	1	3	4	1	1	1	3	3	4	1	1	4	2	3	4

Actifs de type Données et informations		**D**	**I**	**C**		
Données et informations						
D01	Fichiers de données ou bases de données applicatives	4	4	4	1	désigne la base XXX
D02	Fichiers bureautiques partagés	1	1	1	1	le serveur bureautique YYY
D03	Fichiers bureautiques personnels (gérés dans environnement personnel)	3	3	4	1	les données sur les postes de travail
D04	Informations écrites ou imprimées détenues par les utilisateurs, archives personnelles	1		1	0	
D05	Listings ou états imprimés des applications informatiques			4	1	**Archive des contenus sous forme de listing**
D06	Données échangées, écrans applicatifs, données individuellement sensibles	1	3	4	1	échange en cours d'élaboration (design & contenu)
D07	Courrier électronique	2	3	4	1	échange en cours d'élaboration (design & contenu)
D08	Courrier postal et télécopies	1	1	1	0	
D09	Archives patrimoniales ou documentaires	1		1	0	
D10	Archives informatiques	1	1	1	1	anciens modèls de design & photothèque
D11	Données et informations publiées sur des sites publics ou internes					

Scénarios & plan d'action

Acteur	LIBELLÉ	Sélection directe	Valeurs calculées (courant)			Risque Accepté (A) ou Transferé (T)	Gravité pour plans	Mesures (formules littérales)			
			Impact	Potentialité	Gravité			Dissuasives EFF-DISS	Préventives EFF-PREV	Confinement EFF-CONF	Palliatives EFF-PALL
E	Divulgation de listings ou d'états imprimés, par erreur ou perte accidentelle, lors de la diffusion, par un membre du personnel d'exploitation	1	4	3	4		4		08A07		
Pa	Vol de listings ou d'états imprimés, dans les locaux de l'exploitation, par un membre du personnel autorisé	1	4	2	3		3	03B06	08A07		
Ser	Vol de listings ou d'états imprimés, dans les locaux de l'exploitation, par un membre du personnel de service	1	4	2	3		3	03B06	08A07		
Pna	Vol de listings ou d'états imprimés, dans les locaux de l'exploitation, par un membre du personnel non autorisé	1	4	2	3		3	03B06	08A07		
Per	Vol de listings ou d'états imprimés, lors de la diffusion, par un membre du personnel de l'entreprise	1	4	2	3		3		08A07		
Vis	Vol de listings ou d'états imprimés, lors de la diffusion, par un visiteur	1	4	2	3		3		08A07		
	Vol de listings ou d'états imprimés, dans le circuit de ramassage des corbeilles à papiers	1	4	2	3		3		08A07		

D05-C	Divulgation de listings ou d'états imprimés						
	0	0	6	1	7	Dissuasion : Plan de type C	03B06
						Prévention : **Plan de type E**	08A07
						Confinement :	

Plan d'action 1 (08A07)

08A07	***Protection des états et rapports imprimés sensibles***
08A07-01	Tous les états et rapports sensibles sont-ils imprimés dans des locaux protégés contre des intrusions ?
08A07-02	Tous les états et rapports sensibles sont-ils protégés contre les risques de détournement d'état en cours d'élaboration ?
08A07-03	Tous les états et rapports sensibles sont-ils protégés contre les risques de détournement d'état en attente de diffusion ?
08A07-04	Les procédures de diffusion des états et rapports imprimés assurent-elles une protection contre les vols (casiers fermés à clé, conteneurs sécurisés pendant le transport) ?
08A07-05	Les procédures de diffusion des états et rapports imprimés assurent-elles une protection contre les consultations indiscrètes ?
08A07-06	Les procédures de diffusion des états et rapports imprimés prévoient-elles une authentification du destinataire avant remise des états et rapports ?
08A07-07	Les états et rapports imprimés sont-ils "marqués" anonymement à l'exclusion de toute classification ?
08A07-08	Ces mesures de protection sont-elles adaptées à la sensibilité maximale des informations (stockage intermédiaire en armoires fortes et remise en main propre pour les informations très sensibles) ?
08A07-09	Les états et rapports imprimés sensibles rebutés sont-ils détruits de manière sécurisée rendant impossible leur exploitation ?
08A07-10	L'ensemble des procédures de diffusion des états et rapports imprimés sensibles fait-il l'objet d'un audit régulier ?

Plan d'action 2 (03B06)

03B06	***Surveillance des locaux sensibles***
03B06-01	Pour les locaux sensibles, utilise-t-on un système complémentaire de vidéosurveillance cohérent et complet contrôlant tous les mouvements de personnes à l'intérieur des locaux sensibles et permettant de détecter des anomalies dans les comportements ?
03B06-02	L'équipe de surveillance est-elle dégagée de toute tâche opérationnelle et toute alarme est-elle immédiatement détectée et traitée en toute priorité ?
03B06-03	En cas d'alerte, l'équipe de surveillance a-t-elle la possibilité d'envoyer sans délai une équipe d'intervention pour vérifier l'alerte ou agir en conséquence ?
03B06-04	L'équipe de surveillance et d'intervention a-t-elle été dimensionnée en envisageant l'hypothèse d'alarmes multiples déclenchées volontairement ?
03B06-05	La surveillance des locaux est-elle également en service pendant le nettoyage des locaux sensibles ?
03B06-06	Existe-t-il un enregistrement de la vidéosurveillance, conservé sur une longue période ?
03B06-07	Le système de surveillance des locaux sensibles est-il lui-même sous contrôle (alarme en cas d'inhibition, auto-surveillance des caméras, etc.) ?
03B06-08	Les procédures de surveillance et les procédures de réaction aux comportements anormaux font-ils l'objet d'audits réguliers ?