

# Formation Sécurité Organisationnelle et normes ISO 2700x

Animée par

**CGI** | Business Consulting

**Anthony AUGEREAU**

Directeur Consulting Services  
[CISSP, ISO 27001 Lead Implementor, ITIL]

E-mail : anthony.augereau@cgi.com



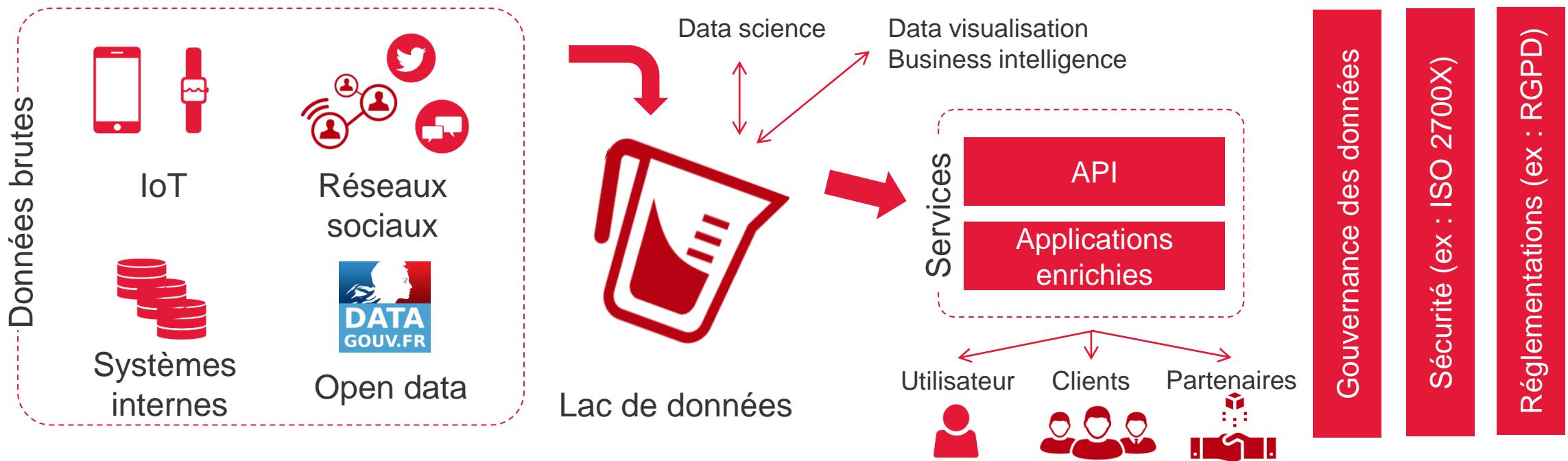
**CGI** | Business Consulting  
La force de l'engagement<sup>MD</sup>



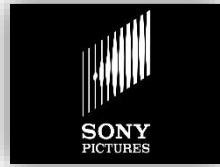
# Evolution du contexte

- Passage du Système d'information **centré sur les traitements** vers le SI **centré sur l'information** (Big Data/Data mining, Cloud Computing => KYC)
- **Prolifération des informations et des accès** (Mobilité, IoT)
- **Stratégie de transformation digitale** de l'entreprise (ex : dématérialisation des contrats)

Ex : Big data, vers une logique data-centric



# Evolution des menaces



Novembre 2014



Avril 2015



Octobre 2016



Mai & Juin 2017



Septembre 2017

Attaque contre Sony Pictures Entertainment  
**Vaste vol de données confidentielles**

Attaque contre TV5 Monde entraîne une **interruption de la diffusion dans le monde**. Les réseaux sociaux de la chaîne ont également été ciblés (surcoût estimé à 4,6M€).

Vaste attaque DDoS contre DynDNS Twitter, Netflix,... **inaccessibles mondialement**

"Wannacry" et "NotPetya" cryptolocker De nombreuses **entreprises et services publics impactés à travers 150 pays**. Un **industriel français impacté évalue à 250 M€ les conséquences financières** sur ses ventes

Fuite importante de données de l'entreprise Equifax. Elle a touchée pas moins de 145 millions d'Américains (presque la moitié de la population américaine)

- Des **transactions techniques**, donc **automatisables**
- D'**énormes quantités de flux d'information**, de transactions et de données
- Une **distance abolie** et des attaquants opérant depuis le monde entier
- Des attaques **asymétriques** : peu de gens avec peu de moyens peuvent provoquer en quelques heures des dégâts considérables, **pouvant survenir 24H sur 24, 7 jours sur 7**
- Des **fuites d'informations** qui se médiatisent
- Des **entreprises françaises** de plus en plus ciblées

# Evolution des menaces – en France



Janvier 2019

Attaque contre  
Altran



Avril 2019

Attaque contre  
Fleury Michon



Novembre 2019

Attaque contre le  
CHU de Rouen



Janvier 2020

Attaque contre  
Bouygues Construction



Octobre 2020

Attaque contre  
Sopra/Steria



Août 2023

Mairie de Betton  
(Bretagne)

**Rançongiciel**  
affectant ses  
opérations dans  
plusieurs pays  
européens (impact  
estimé à 20M€)  
#isolate #provider

**Rançongiciel**  
entraînant un arrêt total  
de l'activité pendant 3  
jours (et fonctionnement  
en mode dégradé  
pendant deux semaines)  
#supplychain

**Rançongiciel entraînant un**  
arrêt général des  
équipements (IT, ascenseurs,  
imagerie médicale, systèmes  
d'analyses), le report ou  
l'externalisation de certains  
soins  
#industrial #crisis

**Rançongiciel (Maze)**  
entraînant le blocage de  
237 terminaux et la  
divulgation d'informations  
sensibles suite au refus de  
paiement (activités en Asie,  
contrats, listes de clients,  
données professionnelles)  
#dataleak #repair

**Rançongiciel (Ryuk)**  
entraînant une  
compromission de  
l'AD et un  
ralentissement de  
l'activité (autres  
impacts en cours  
d'analyse)

**Rançongiciel**  
entraînant  
l'exfiltration de 2%  
des données de la  
ville (et diffusion sur  
le DarkWeb: avis  
d'imposition, RIB,  
factures...)

« **La meilleure défense** contre les cyber-attaquants **reste la défense**: la cybersécurité, c'est à 99% de la prévention, de la protection, mettre des barrières, comprendre ce qui se passe, détecter les attaques le plus tôt possible. Tout ramener à une capacité de réponse offensive, c'est une erreur. »

- Guillaume Poupard, Directeur Général de l'ANSSI

*Et cela continue (Mairies, Hôpitaux...): Mairies de Betton, Vincennes, Angers et Marseille, hôpital de Corbeil-Essonnes, CHU de Brest, etc.*

# Panorama des lois & réglementations

## Lois & Règlements (FR / EU)

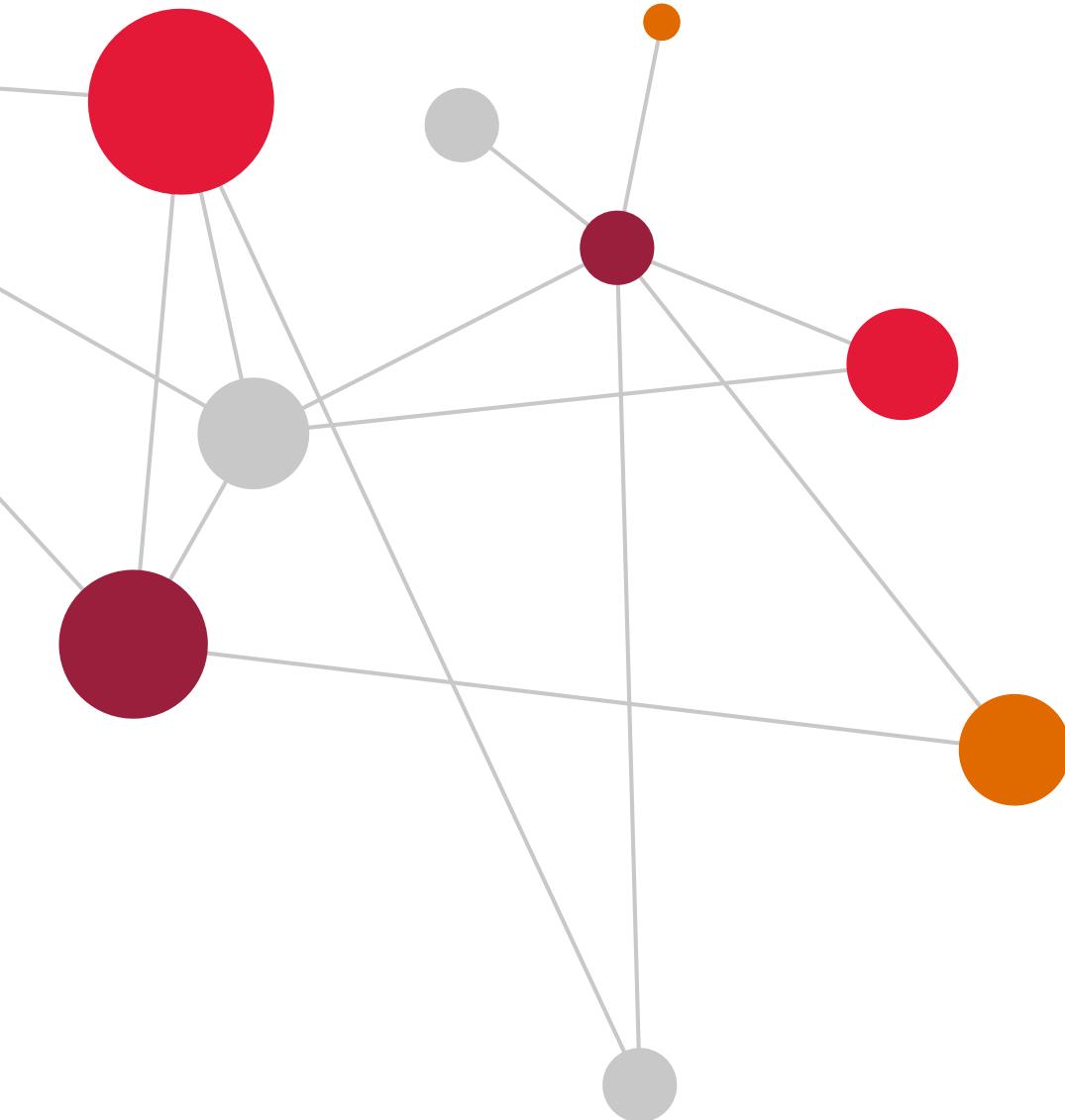


## Réglementations spécifiques (activité, secteur)



## Normes, standards et guides de bonnes pratiques



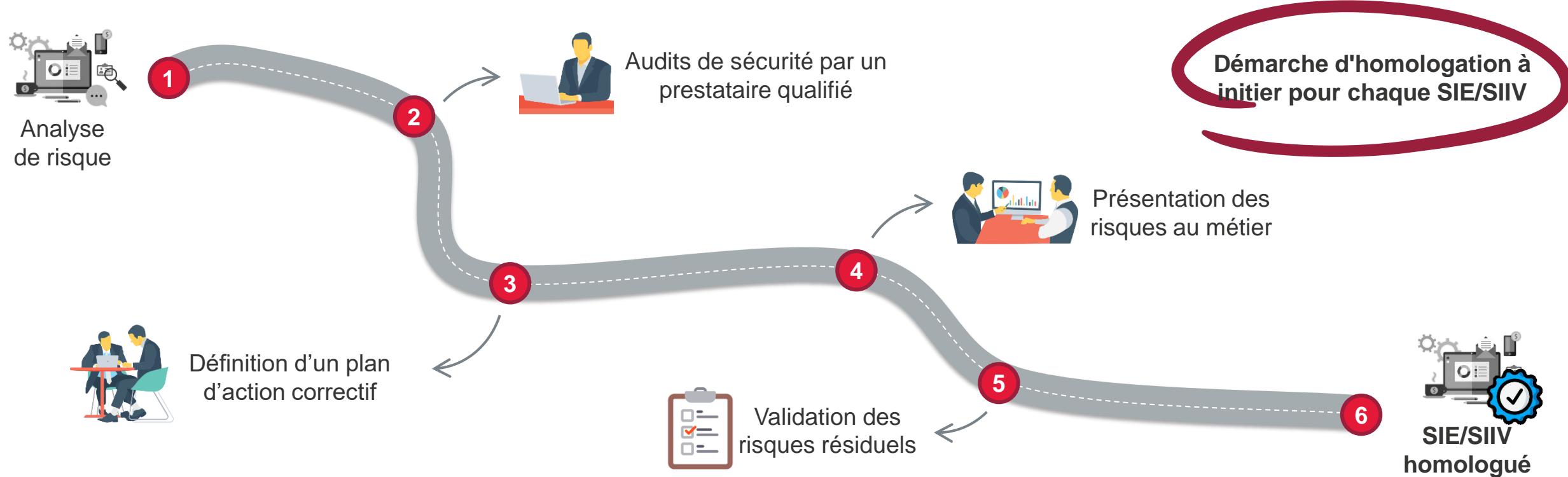


## LPM & Directive NIS

**Loi de Programmation Militaire (OIV:  
Opérateur d'Importance Vitale)**

**Directive Network and Information  
Security (OSE: Opérateurs de Services  
Essentiels)**





La démarche d'homologation est réalisée pour chaque SIE/SIIV et consiste en une démarche de gestion des risques avec **une évaluation théorique puis pratique** (via un audit de sécurité) du niveau de ces risques.

Ces risques doivent faire l'objet d'un **plan de traitement** pour être réduits à un niveau acceptable par le métier. Cette démarche permet également de traiter les potentielles non-conformités aux mesures ANSSI en évaluant le niveau de risques engendré.

# NIS – Liste des exigences par chapitre

Chapitre	Sous-chapitre	Num	Nom
Gouvernance de la sécurité des réseaux et systèmes d'information	Gouvernance de la sécurité des réseaux et systèmes d'information	1	Analyse de risque
		2	Politique de sécurité
		3	Homologation de sécurité
		4	Indicateurs
		5	Audits de la sécurité
		6	Cartographie
Protection des réseaux et systèmes d'information	Sécurité de l'architecture	7	Configuration
		8	Cloisonnement
		9	Accès distant
		10	Filtrage
	Sécurité de l'administration	11	Comptes d'administration
		12	Systèmes d'information d'administration
	Gestion des identités et des accès	13	Identification
		14	Authentification
		15	Droits d'accès
		16	Procédure de maintien en conditions de sécurité
Défense des réseaux et systèmes d'information	Sécurité physique et environnementale	17	Sécurité physique et environnementale
	Détection des incidents de sécurité	18	Détection
		19	Journalisation
		20	Corrélation et analyse de journaux
	Gestion des incidents de sécurité	21	Réponse aux incidents
		22	Traitements des alertes
Résilience des activités	Gestion de crises	23	Gestion de crises

# NIS / LPM référentiel d'exigences

Politique des systèmes d'information	Homologation sécurité	Cartographie	Maintien en condition en sécurité	MAITRISER RISQUES	MAITRISER SES SI
Elaboration et mise en œuvre d'une PSSI	Homologation obligatoire pour chaque SIE/SIIV, prononcée par l'opérateur, incluant un audit réalisé selon les critères définis par l'ANSSI	Mise à disposition de l'ANSSI d'une cartographie de chaque SIE/SIIV	Suivi et prise en compte des correctifs de sécurité. Gestion des mises à jour des SIE/SIIV	GERE LES INCIDENTS CYBER	PROTEGER LES SYSTEMES
Détection	Traitement des incidents	Traitement des alertes	Gestion de crise	Journalisation	Gestion des identités et des accès
Système de corrélation et d'analyse des journaux, exploité en s'appuyant sur les exigences d'un référentiel  Systèmes de détection qualifiées opérées par l'ANSSI	Mise en place d'une organisation de gestion des incidents de sécurité informatique  Traitement des incidents de sécurité en s'appuyant sur les exigences d'un référentiel	Communication à l'ANSSI d'un point de contact fonctionnel pouvant prendre connaissance à toute heure des signalements de l'ANSSI	Mise en œuvre d'une procédure de gestion de crise en cas d'attaques informatiques majeures	Mise en place d'un système de journalisation pour chaque SIE/SIIV	Identification par comptes individuels. Protection des éléments secrets d'authentification.  Gestion des autorisations selon le principe du moindre privilège.  Connaissance des comptes privilégiés et des droits associés
Administration	Défense en profondeur	Indicateurs			
Utilisation de comptes dédiés pour l'administration des SIE/SIIV. Mise en place de ressources matérielles et logicielles dédiées aux opérations d'administration.  Séparation entre les flux d'administration et les autres flux.	Cloisonnement Filtrage Contrôle strict des connexions distantes. Durcissement des éléments du SIE/SIIV.	Evaluation pour chaque SIIV d'indicateurs SSI et transmission annuelle à l'ANSSI d'un tableau de bord de suivi de ces indicateurs.			

# Les règles de la directive NIS

A l'échelle nationale, NIS 2 s'appliquera à des milliers d'entités appartenant à plus de dix-huit secteurs qui seront désormais régulés. Environ 600 types d'entités différentes seront concernés, parmi eux des administrations de toutes tailles et des entreprises allant des PME aux groupes du CAC40.

## Gouvernance

01. Analyse de risques
02. Politique de sécurité
03. Homologation de sécurité
04. Indicateurs de sécurité
05. Audits de la sécurité
06. Cartographie

## Protection

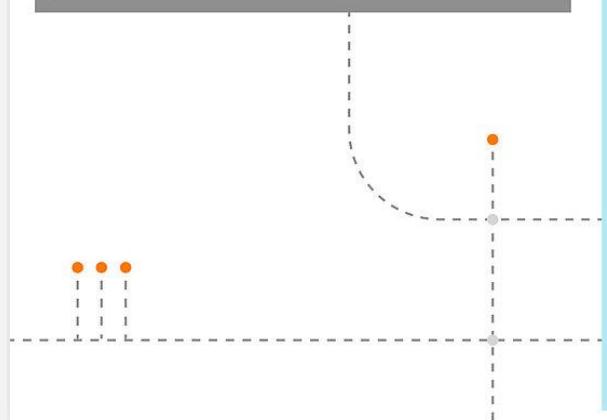
- Sécurité de l'architecture**
07. Configuration
  08. Cloisonnement
  09. Accès distant
  10. Filtrage
- Sécurité de l'administration**
11. Comptes d'administration
  12. SI d'administration
- Gestion des identités et des accès**
13. Identification
  14. Authentification
  15. Droits d'accès
- 
16. Maintien en conditions de sécurité
  17. Sécurité physique et environnemental

## Défense

- Détection des incidents**
18. Détection
  19. Journalisation
  20. Corrélation et analyse de journaux
- Gestion des incidents**
21. Réponse aux incidents
  22. Traitement des alertes

## Résilience

23. Gestion de crise



## #NISv2

Le secteur de la chimie se voit dorénavant directement concerné en tant qu'opérateur important et de très nombreuses entreprises entreront dans le champ d'application de la directive NIS2.

Les États membres disposeront d'un délai de vingt-et-un mois à compter de l'entrée en vigueur de la directive pour **transposer le texte dans leur droit national** (donc avant le 17 octobre 2024).

#*Elargissement du champ d'application*#*Renforcement du contrôle et des sanctions*

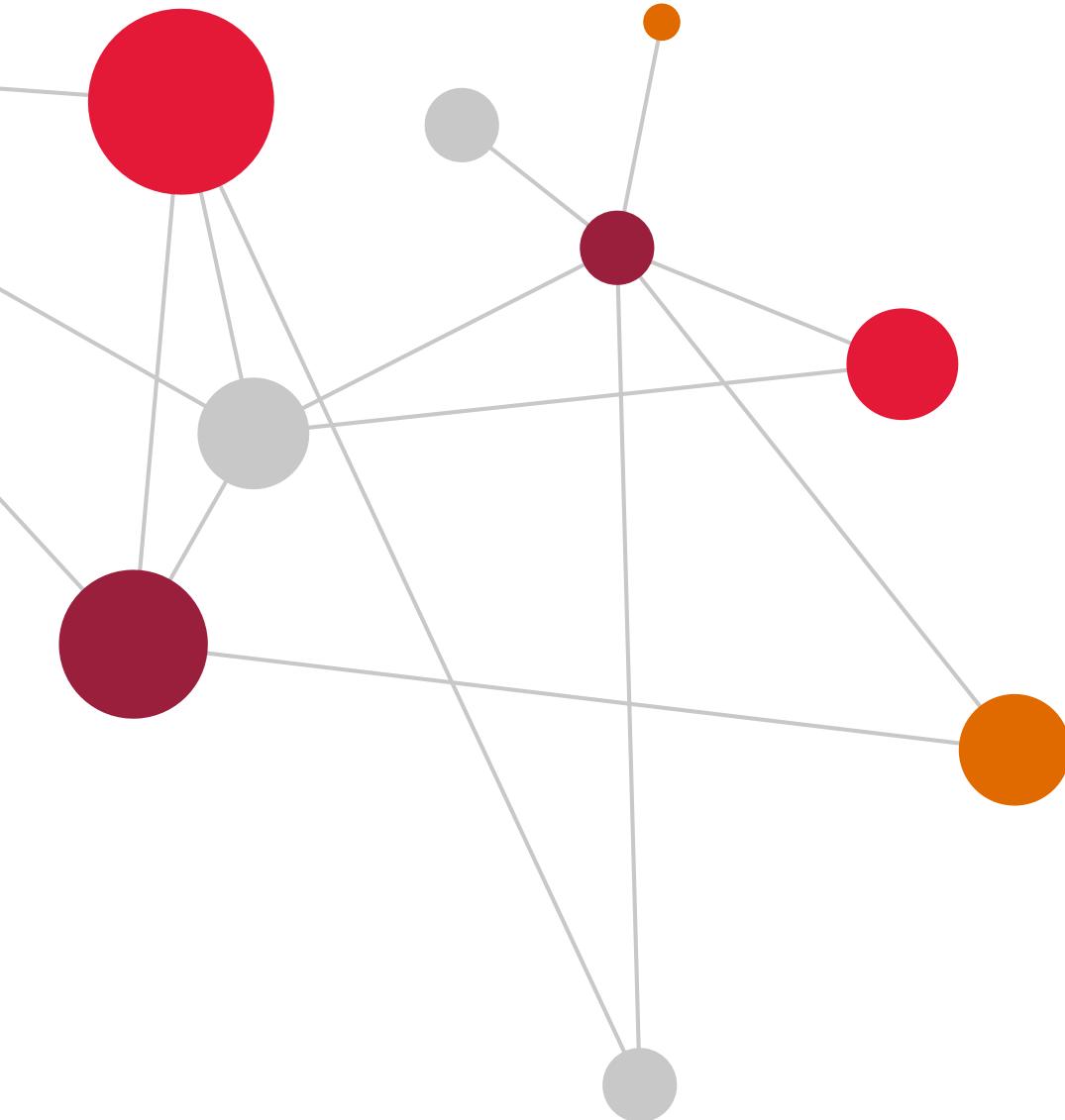
La directive NIS 2 élargit le champ d'application de l'actuelle directive NIS :

- en définissant de **nouveaux opérateurs de services essentiels** (OSE) ;
- en ajoutant un niveau d'opérateurs importants (OI) ;
- en intégrant les administrations publiques.

Concernant les opérateurs importants, **l'annexe II de la directive NIS 2 désigne en particulier les produits chimiques.**

Concernant les obligations pour les OSE et OI de notifier des incidents de sécurité le délai de notification est porté :

- **A 24h au plus tard** après avoir pris connaissance de l'incident si cet incident est causé par un acte illégal ou malveillant ou peut avoir des impacts transfrontaliers ;
- A 72h dans les autres cas



# RGPD

## Règlement Général sur la Protection des Données



# Présentation du RGPD

Le RGPD une évolution pas une révolution

**1978**

Loi informatique  
et  
Liberté

**1995**

Directive  
95/46/CE

**2004**

Révision de la  
LIL

**2011**  
LCEN

**2009**

Paquet  
Telecom

**2016**

Loi Lemaire  
&  
Adoption du  
RGPD

**2018**

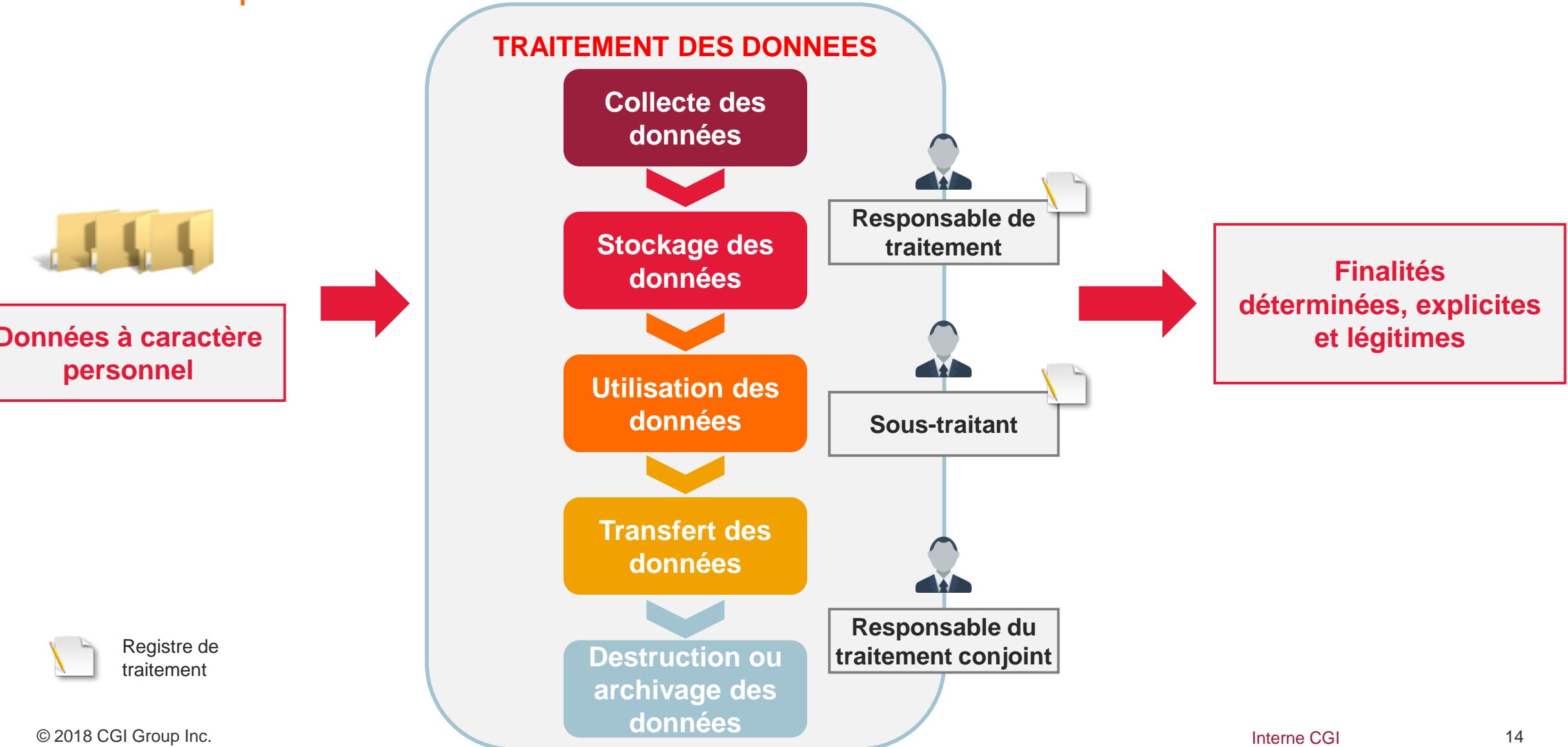
Entrée en  
application du  
RGPD



**88 pages**  
**173 considérants**  
**99 articles**  
**11 chapitres**

# Présentation du RGPD

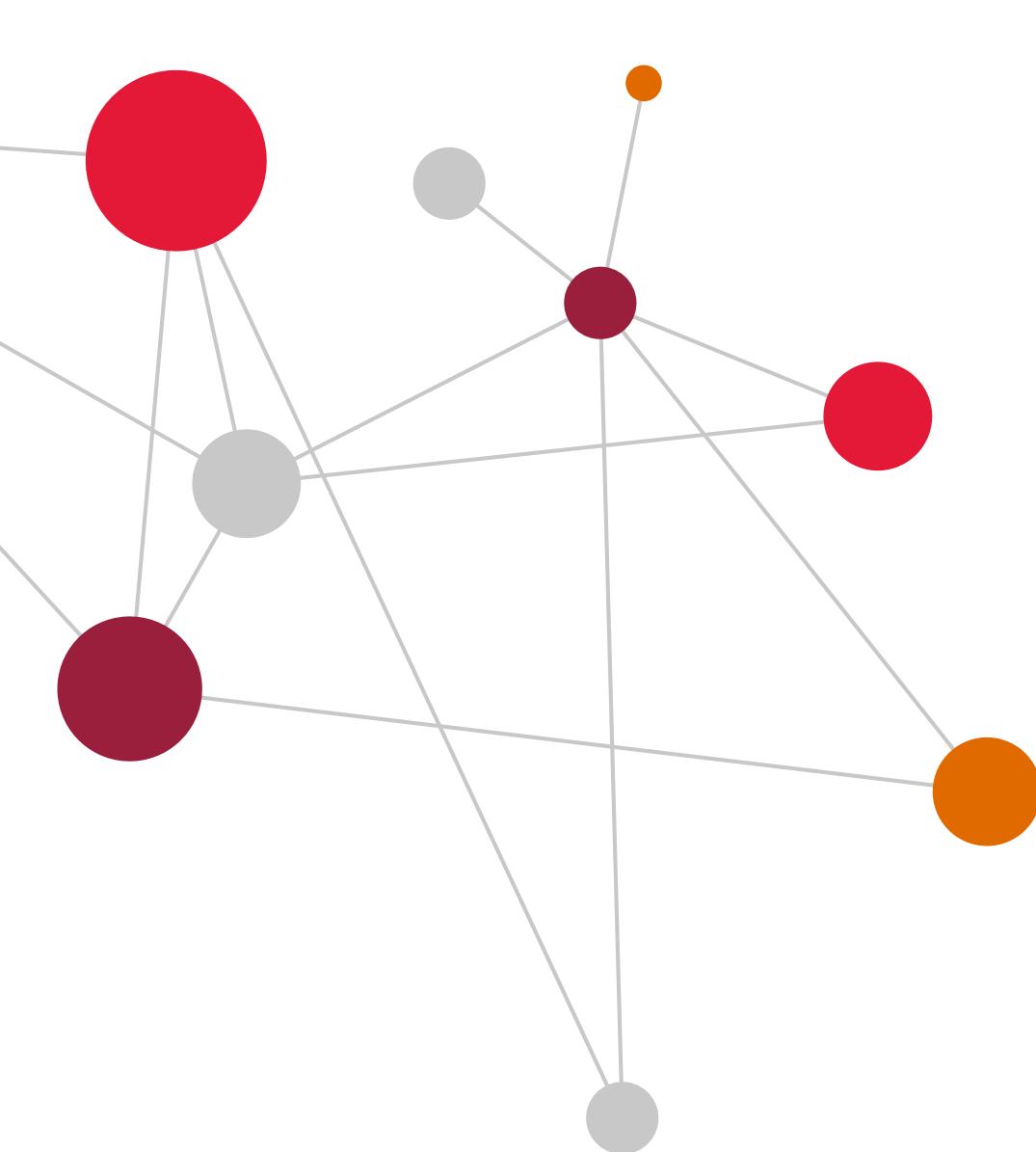
## Qu'est-ce qu'un traitement ?



# Présentation du RGPD

## Principes clés du RGPD





# PCI DSS

## Payment Card Industry Data Security Standard



## PCI DSS : Ca veut dire quoi ?

 Payment Card Industry Data Security Standard

 Standard de sécurité des données pour l'industrie des cartes de paiement

## PCI DSS : Ca sert à quoi ? A qui s'adresse le standard ?

- Fondé par les principaux fournisseurs de cartes internationaux (Visa, MasterCard, American Express, etc.), le standard PCI DSS liste l'**ensemble des exigences de sécurité applicables** aux SI qui collectent, stockent, traitent et sur lesquels transitent des données CB.
- PCI DSS s'adresse par conséquent aux (e-)commerçants, aux banques, aux prestataires de services de paiement (PSP), etc.

## PCI DSS : Quels sont les enjeux pour l'entreprise ?



> 6 thématiques > 12 conditions > des 100N exigences de sécurité

Thématiques	N°	Conditions
Création et gestion d'un réseau et d'un système sécurisés	1	Installer et gérer une configuration de pare-feu pour protéger les données de titulaires de carte
	2	Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur
Protection des données de titulaires de carte	3	Protéger les données de titulaires de carte stockées
	4	Crypter la transmission des données de titulaires de carte sur les réseaux publics ouverts
Gestion d'un programme de gestion des vulnérabilités	5	Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels ou programmes anti-virus
	6	Développer et maintenir des systèmes et applications sécurisés
Mise en œuvre de mesures de contrôle d'accès strictes	7	Restreindre l'accès aux données de titulaires de carte aux seuls individus qui doivent les connaître
	8	Identifier et authentifier l'accès à tous les composants de système
	9	Restreindre l'accès physique aux données de titulaire de carte
Surveillance et test réguliers des réseaux	10	Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaires de carte
	11	Tester régulièrement les processus et les systèmes de sécurité
Gestion d'une politique de sécurité des informations	12	Gérer une politique de sécurité des informations pour l'ensemble du personnel



TPE


 Solution  
Chiffrement  
P2PE

 Service  
monétique

## DORA

**Digital Operational Resilience Act  
(DORA)**

**Résilience opérationnelle  
numérique du secteur financier**



# Champ d'application de DORA en bref



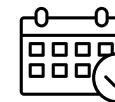
## A quoi s'applique DORA ?

- **Activités des entités financières :**
  - Gestion des risques liés aux technologies de l'information et de la communication (TIC) ;
  - Notification aux autorités compétentes des incidents majeurs liés à l'informatique ;
  - Tests de résilience opérationnelle numérique ;
  - Partage d'informations et de renseignements en rapport avec les cybermenaces et les cybervulnérabilités ;
  - Mesures destinées à garantir une gestion solide, par les entités financières, du risque lié aux tiers prestataires
- **Accords entre des tiers prestataires de services informatiques et des entités financières**
- **Supervision des tiers prestataires critiques de services informatiques lorsqu'ils fournissent des services à des entités financières**
- **Coopération entre les autorités compétentes, surveillance et exécution par les autorités compétentes**



## A quels acteurs s'applique DORA ?

- Etablissements de crédit
- Etablissements de paiement
- Etablissements de monnaie électronique
- Entreprises d'investissement
- Prestataires de services sur crypto-actifs, les émetteurs de crypto-actifs, les émetteurs de jetons
- Dépositaires centraux de titres
- Contreparties centrales
- Plateformes de négociation
- Sociétés de gestion
- Référentiels centraux
- Gestionnaires de fonds d'investissement alternatifs
- Sociétés de gestion
- Prestataires de services de communication de données
- Entreprises d'assurance, de réassurance, intermédiaires d'assurance et de réassurances, intermédiaires d'assurance à titre accessoire
- Institutions de retraite professionnelle
- Agences de notation de crédit
- Contrôleurs légaux des comptes / cabinets d'audit
- Administrateurs d'indices de référence d'importance critique
- Prestataires de services de financement participatif
- Référentiels des titrisations
- Tiers prestataires de services informatiques



## Quand s'appliquera DORA ?

Entrée en vigueur fin 2024 (estimation)



## Où s'applique DORA ?

Entités financières réglementées au niveau de l'Union

# Ecosystème institutionnel du projet DORA

## Entités européennes

Autorités européennes de surveillance (AES)



## Entités nationales



Les entités européennes sont en charge de l'**élaboration de normes techniques** de réglementations concernant :

- La mise en place et le suivi du cadre de gestion des risques informatiques
- La définition des critères de classification des incidents
- La réalisation de tests de pénétration
- La gestion des risques liés aux tiers prestataires de services informatiques
- Les accords contractuels entre une entité financière et un tiers prestataire de services informatiques

Les entités nationales assurent le **bon respect des normes et recommandations** localement et fournissent des **rapports détaillés aux autorités européennes**.

# Objectifs poursuivis par le projet DORA

Esprit du texte : **renforcer la résilience opérationnelle numérique des entités du secteur financier et assurantiel de l'Union européenne** en rationalisant et en améliorant les règles en vigueur et en introduisant de nouvelles exigences dans les domaines où il existe des lacunes.

Ce but est structuré en **3 objectifs généraux** comprenant **8 sous-objectifs spécifiques** :

**Réduire le risque de perturbation et d'instabilité financière**

1

- *Parer aux risques informatiques de manière plus intégrée et renforcer le niveau global de résilience numérique du secteur*
- *Veiller à ce que les entités financières évaluent l'efficacité de leurs mesures de prévention et de résilience et détectent les vulnérabilités*
- *Renforcer les garanties contractuelles avec les tiers fournisseurs services informatiques, y compris en ce qui concerne les règles d'externalisation*

**Réduire la charge administrative et accroître l'efficacité de la surveillance**

2

- *Rationaliser les notifications d'incidents et résoudre les problèmes de chevauchement des exigences en matière de notification*
- *Réduire la fragmentation du marché unique et favoriser la reconnaissance transfrontière des résultats des tests*
- *Permettre une supervision des activités des tiers prestataires critiques de services informatiques*

**Renforcer la protection des consommateurs et des investisseurs**

3

- *Permettre aux autorités de surveillance financière d'avoir accès aux informations sur les incidents*
- *Encourager l'échange de renseignements sur les menaces dans le secteur financier*

# 5 piliers du projet DORA

## 1.



### Gestion des risques informatiques (art. 4 à 14)

**Objectifs :** S'assurer du bon fonctionnement et mise à jour des mesures de contrôles

## 2.



### Gestion, classification et notification des incidents liés à l'informatique

**Objectifs :** Harmoniser et centraliser les notifications des incidents à des fins de transmission aux autorités

## 3.



### Test de Résilience opérationnelle numérique (art. 21 à 24)

**Objectifs :** Tester l'efficacité des dispositifs de gestion des risques et des mesures en place afin de limiter les effets sur les activités critiques et importantes

## 4.



### Gestion des risques liés aux tiers prestataires de services informatiques (art. 25 à 39)

**Objectifs :** Vérifier le niveau de contrôles suffisants de leurs tiers, tout particulièrement les PCI et mettre en place les mesures de surveillance requises

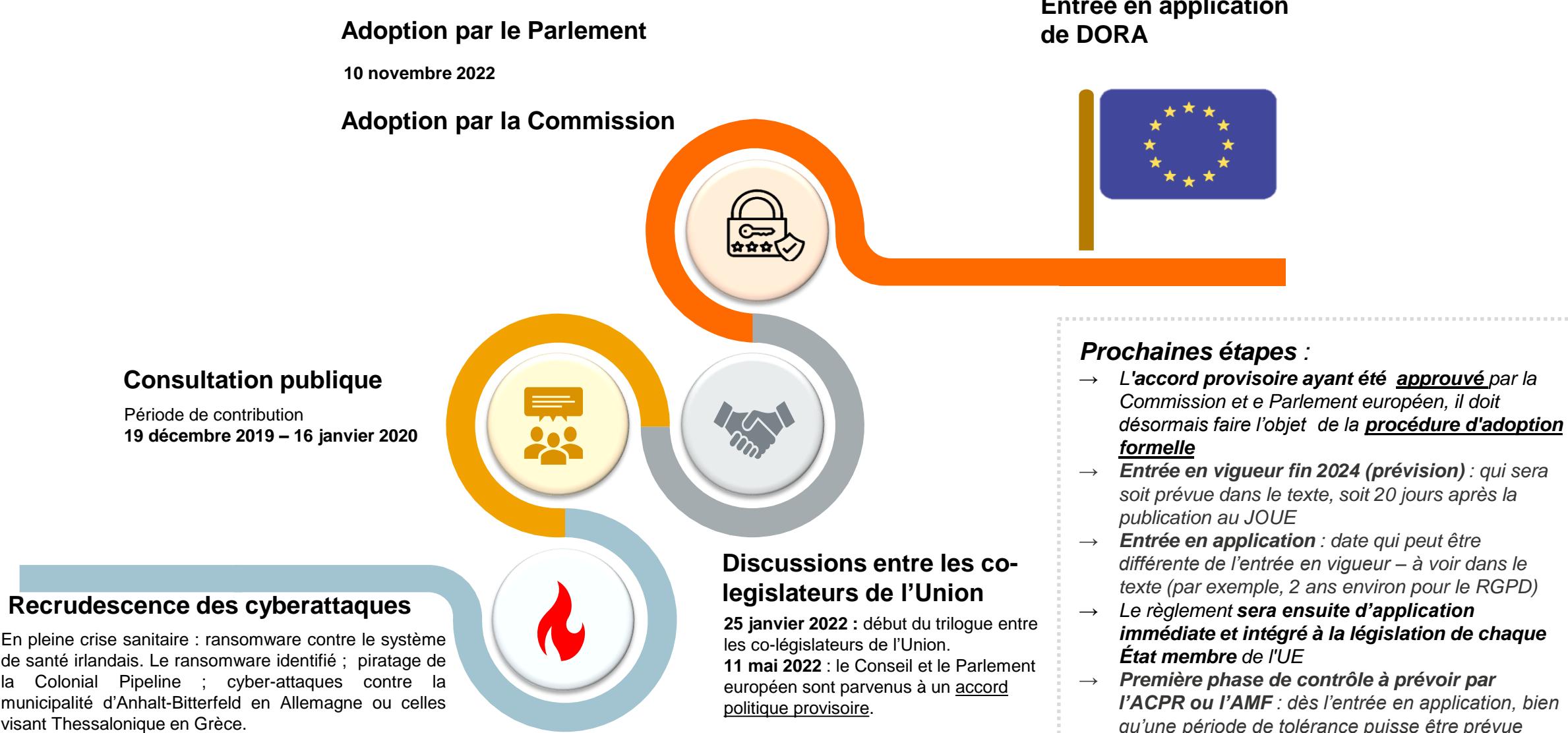
## 5.



### Partage d'informations et de renseignements (art. 40)

**Objectifs :**  
Mettre en place des accords de partage d'informations entre entreprises pour les cyber-menaces, y compris des exigences de confidentialité et la nécessité d'informer l'autorité de régulation.

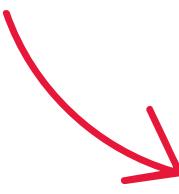
# Calendrier : où en sommes-nous ?



# Géographie : où s'applique le projet DORA ?



Il s'agit d'une proposition de règlement européen qui s'applique aux entités financières **réglementées au niveau de l'Union** (exposé des motifs, p.9)



Notre analyse : les **filiales européennes réglementées en Europe de grands groupes étrangers** (ex : Microsoft, Amazon...) pourraient se voir appliquer DORA.

# Panorama des lois & réglementations

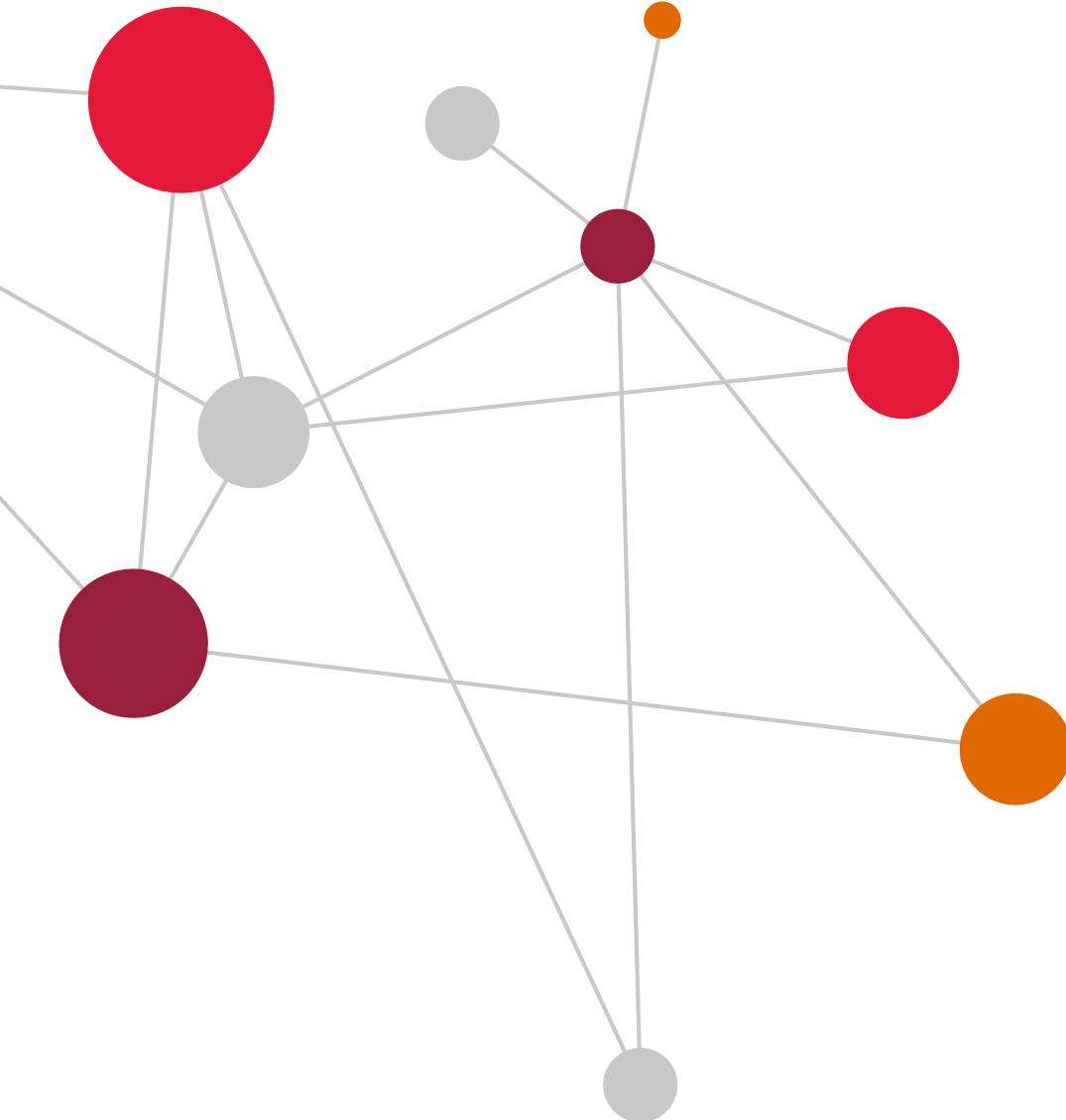
## Exercice:

*Une startup française se spécialise dans le domaine de santé en développant un outil Web de collecte et d'analyse de données médicales pour les hôpitaux. Cette solution sera hébergée dans le Cloud.*

1/ A quelles réglementations est soumise cette entreprise ?

2/ Avec quels référentiels cette entreprise est susceptible de devoir se mettre en conformité si elle bénéficie d'un fort développement, voire d'un développement international?





# NIST CSF

## Cybersecurity Framework



## 1

## Présentation du « National Institute of Standards and Technology »



**Laboratoire de recherche** public étasunien créé en 1901 ayant pour but **d'accompagner l'économie** par le développement des technologies, de la métrologie et des standards.



2900 personnes  
≈ 1Mds \$ US par an.



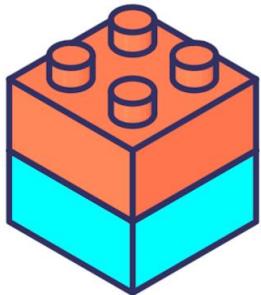
Placé sous l'égide du **comité des sciences, de l'espace et des technologies et de la chambre des représentants** des États-Unis. Une partie de l'organisation se réfère cependant directement au **département de la Défense**.



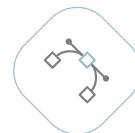
Parmi leurs **réalisations remarquables** on compte l'**étude à 18 millions d'euros étalée sur 3 ans** concernant l'**effondrement des tours jumelles** mais aussi l'élaboration de **NIST SP 800** qui est un référentiel de recommandations et technique concernant la sécurité informatique initialement créée pour les institutions traitants des informations classifiées

2

## Contexte de création du cadre de référence (1/2)



Le **USA PATRIOT Act** en 2001 définit comme priorité nationale la **protection de ses infrastructures critiques**.



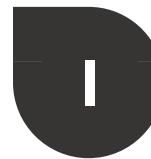
Les infrastructures critiques sont : « **des systèmes et des actifs, physiques ou virtuels, tellement vitaux pour les États-Unis que l'incapacité ou la destruction de tels systèmes et de tels actifs aurait un impact néfaste sur la sécurité, la sécurité économique nationale, la santé ou la sécurité publique nationale, ou toute combinaison de ces questions.** »



En 2004, le **Cybersecurity Enhancement Act** (CEA) officialise une collaboration entre les secteurs publics et privés autour de la cybersécurité en **organisant la R&D, la sensibilisation, l'éducation et l'avancement des normes**. Il réorganise certaines institutions qui se voit dotées de **nouvelles missions**.

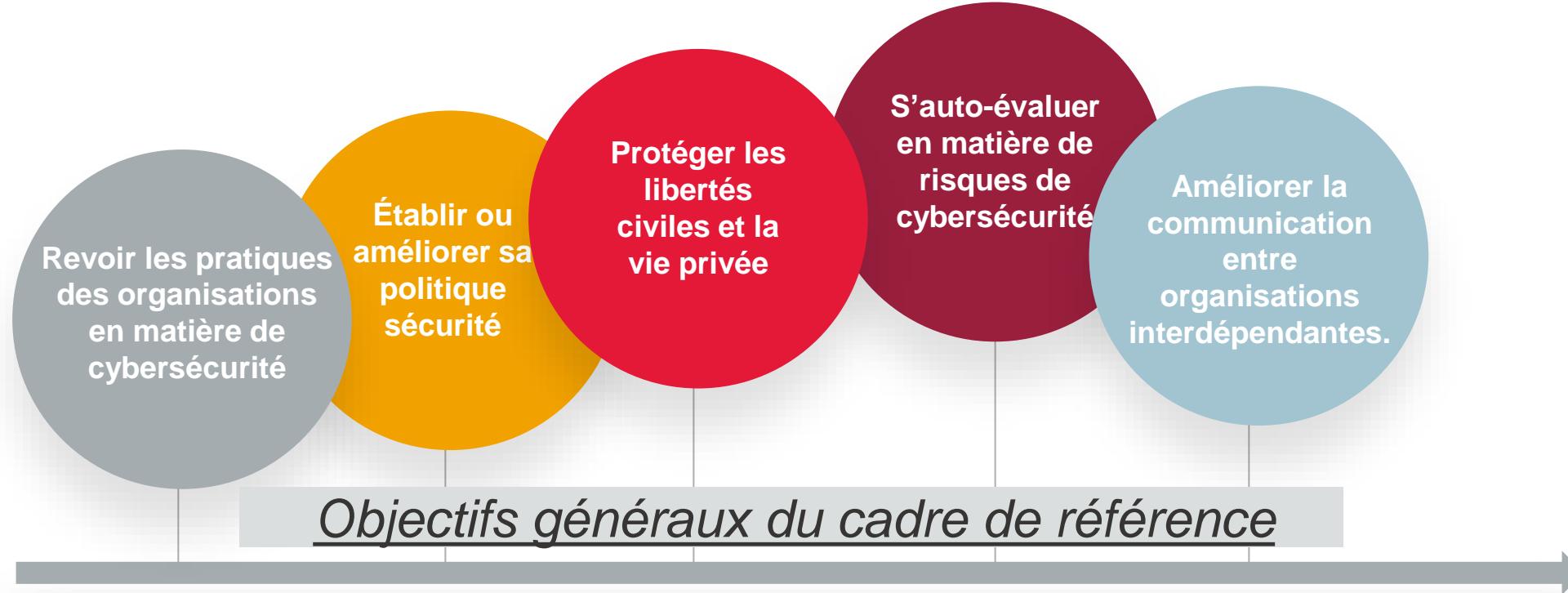


Parmi elles, **NIST** se voit chargée (sec 202 du CEA) de **développer et d'identifier un cadre de travail priorisant, flexible, répétable, basé sur la performance et les coûts facilitant la réduction des risques cyber** dans les infrastructures critiques.



# Le NIST et création du Cybersecurity Framework

## 2 Contexte de création du cadre de référence (2/2)



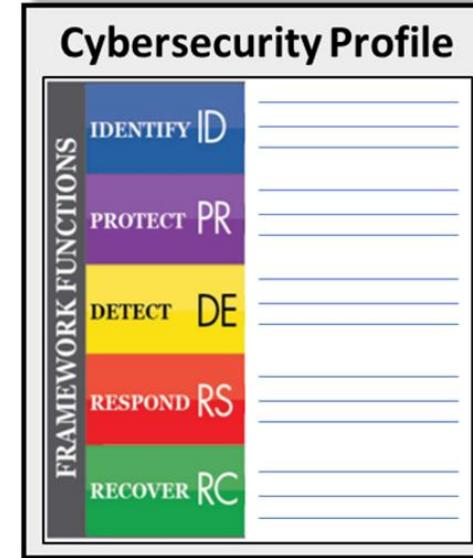
Ce Framework représente une approche de gestion des risques centrée sur la cybersécurité.



# Le NIST et création du Cybersecurity Framework

## 3 Outilage proposé par le NIST

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
Recover	Improvements	RS.IM
	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO



	Niveau 1 : Partiel	Niveau 2 : Informé	Niveau 3 : Itératif	Niveau 4 : Adaptatif
Processus de gestion des risques	Adaptation des pratiques de cybersécurité en fonction des activités passées et présentes-Amélioration continue intégrant technologies et pratiques-Adaptation à l'environnement réglementaires, des menaces et des technologies			
Programmes de gestion intégrée du risque	Politiques, processus et procédures tenant compte des risques- Relation entre le risque de cybersécurité et les objectifs organisationnels-Niveau de préoccupation de la cybersécurité-Budget-Culture organisationnelle			
Conscience de son interdépendance et des externalités	Compréhension de son rôle dans l'écosystème-Participation à une communauté centré sur le risque cyber-Partage d'informations-Niveau de formalisation du partage d'informations-Proactivité			

### Le “Core framework”

- 5 fonctions
- Activités issues de la gestion des risques

### Le “Cybersecurity profile”

- Framework adapté à l'organisation
- Pour organiser une roadmap

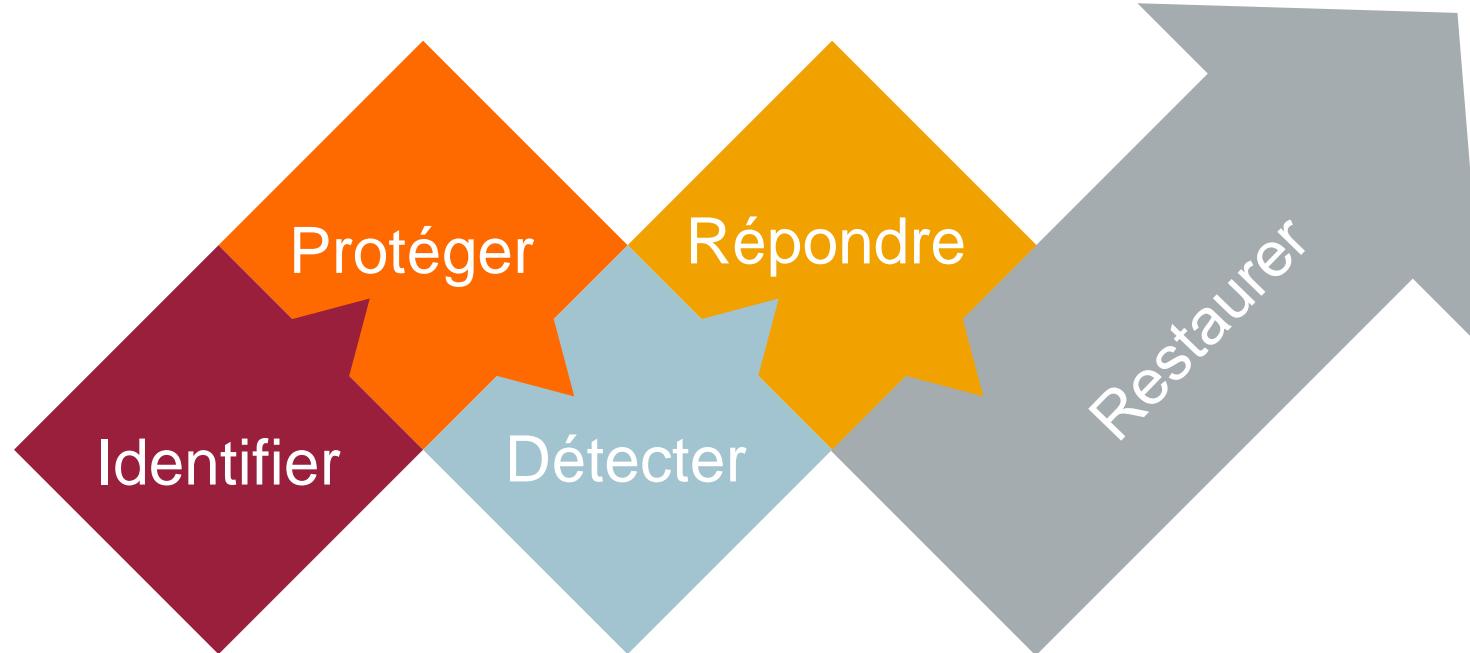
### Les “TIER”

- Maturité reflétant les choix stratégiques
- Aide à la décision tactique de gestion des risques

# Le NIST et création du Cybersecurity Framework

3

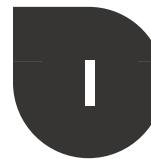
Outilage proposé par le NIST : Core Framework 1/2



Le « Core Framework » est une démarche de gestion découpée en 5 fonctions

Chaque fonction est découpée en catégories (22 en tout) répartie sur le cyber, le personnel et l'infrastructure.

Les catégories pouvant elles-mêmes être subdivisées en sous-catégories (108 en tout). Le niveau le plus fin de la subdivision étant systématiquement associé à d'autres référentiels (*Informative references*).



# Le NIST et création du Cybersecurity Framework

3

Outilage proposé par le NIST : Core Framework 2/2

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
Detect	Protective Technology	PR.PT
	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
Respond	Detection Processes	DE.DP
	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
Recover	Mitigation	RS.MI
	Improvements	RS.IM
	Recovery Planning	RC.RP
Recover	Improvements	RC.IM
	Communications	RC.CO

Sub-categories	Informative References
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP NIST SP 800-53 Rev. 4 AU Family800-53 Rev. 4 CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8

Le Framework Core permet d'organiser la gestion des risques cyber.

A contrario d'autres guidelines, les activités qui en découlent doivent être le fruit d'une gestion du risque cyber optimisée par l'établissement représenté.



# Le NIST et création du Cybersecurity Framework

3

## Outilage proposé par le NIST : Exemple d'exigence (catégorie)

Function	Category	Subcategory	Informative References
PROTECT (PR)	<b>Identity Management, Authentication and Access Control (PR.AC):</b> Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	<b>PR.AC-6:</b> Identities are proofed and bound to credentials and asserted in interactions	<b>CIS CSC</b> , 16 <b>COBIT 5</b> DSS05.04, DSS05.05, DSS05.07, DSS06.03 <b>ISA 62443-2-1:2009</b> 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 <b>ISA 62443-3-3:2013</b> SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 <b>ISO/IEC 27001:2013</b> A.7.1.1, A.9.2.1 <b>NIST SP 800-53 Rev. 4</b> AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		<b>PR.AC-7:</b> Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	<b>CIS CSC</b> 1, 12, 15, 16 <b>COBIT 5</b> DSS05.04, DSS05.10, DSS06.10 <b>ISA 62443-2-1:2009</b> 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 <b>ISA 62443-3-3:2013</b> SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 <b>ISO/IEC 27001:2013</b> A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 <b>NIST SP 800-53 Rev. 4</b> AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

5 Fonctions

23 Catégories

108 Sous-catégories

6 Références



# Le NIST et création du Cybersecurity Framework

## 3 Outilage proposé par le NIST : Exercice

### Exercice:

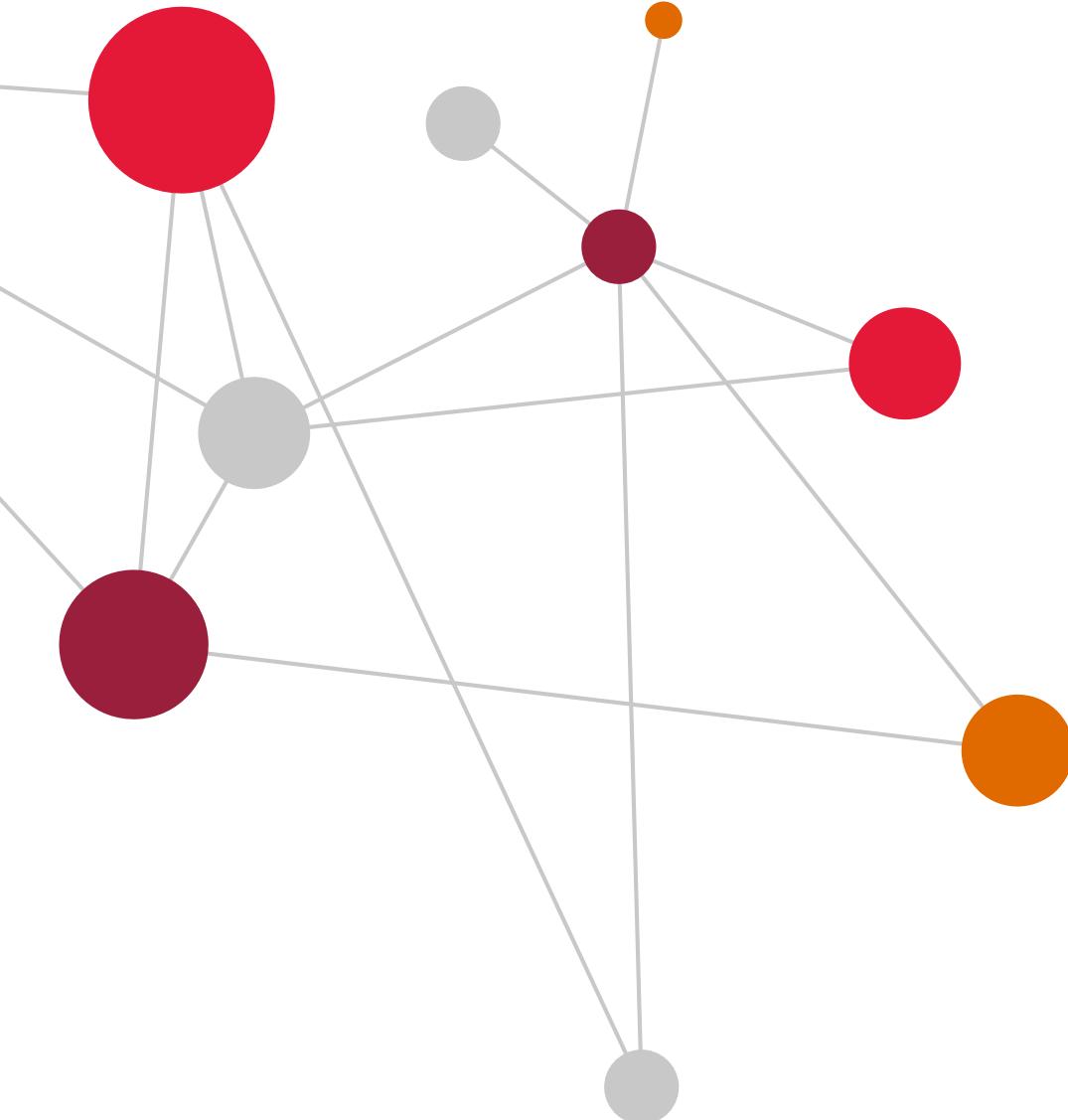
*La société XY s'appuie le framework NIST CSF pour identifier les mesures de sécurité à appliquer pour identifier les potentiels malwares se propageant sur son SI.*

1/ Quelle fonction(s), catégorie(s) et sous catégorie(s) du NIST CSF sont concernées ?

2/ Quelles bonnes pratiques peuvent être appliquées?

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Source Framework: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>



# ISO 27001



# Objectifs de la formation



**Comprendre l'utilité d'un Système de Management de la Sécurité de l'Information (SMSI) et sa filiation avec l'ISO9001**



**Connaître les points « clés » d'un SMSI**



Etre **sensibilisé aux problématiques** rencontrées dans le cadre de la **mise en œuvre d'un SMSI**

# Agenda



## Principes du SMSI

- **Introduction**
- Définition du Système de Management
- Introduction aux normes ISO27001 / ISO27002



## La Gestion de Risque

- Principes de la gestion des risques
- ISO27005 / ISO31000
- Application d'EBIOS à l'identification des risques de l'entreprise



## La mise en œuvre pratique

- Plan
- DO
- Check
- Act

# Agenda



## Principes du SMSI

- Introduction
- **Définition du Système de Management**
- Introduction aux normes ISO27001 / ISO27002



## La Gestion de Risque

- Principes de la gestion des risques
- ISO27005 / ISO31000
- Application d'EBIOS à l'identification des risques de l'entreprise



## La mise en œuvre pratique

- Plan
- DO
- Check
- Act

# Définition d'un SMSI

Notion de **système de management** introduite par l'ISO au travers de l'ISO9001 et l'ISO14001

## Système de management

- Ensemble **d'éléments corrélés ou interactifs** permettant d'établir une **politique et des objectifs** et d'atteindre ces objectifs
- Eléments = politiques, procédures, moyens humains et techniques

## Système de management de la sécurité

- **Système de management**, basé sur une **approche de gestion des risques**, visant à définir, mettre en œuvre et continuellement vérifier / maintenir / améliorer la sécurité de l'information au sein d'un organisme
- **Ensemble d'éléments corrélés ou interactifs permettant**, à partir d'une approche basée sur la gestion des risques, de définir, mettre en œuvre et continuellement vérifier / maintenir / améliorer la sécurité de l'information au sein de l'organisme
- Formalisation de la mise en œuvre d'une **démarche de management de la sécurité de l'information**

# Intérêt et utilisation d'une norme

L'intérêt d'une norme repose sur son mode d'élaboration



- croisement de **différentes compétences, cultures, expériences...** et... **motivations**
- **adoption par consensus**

Importance du consensus



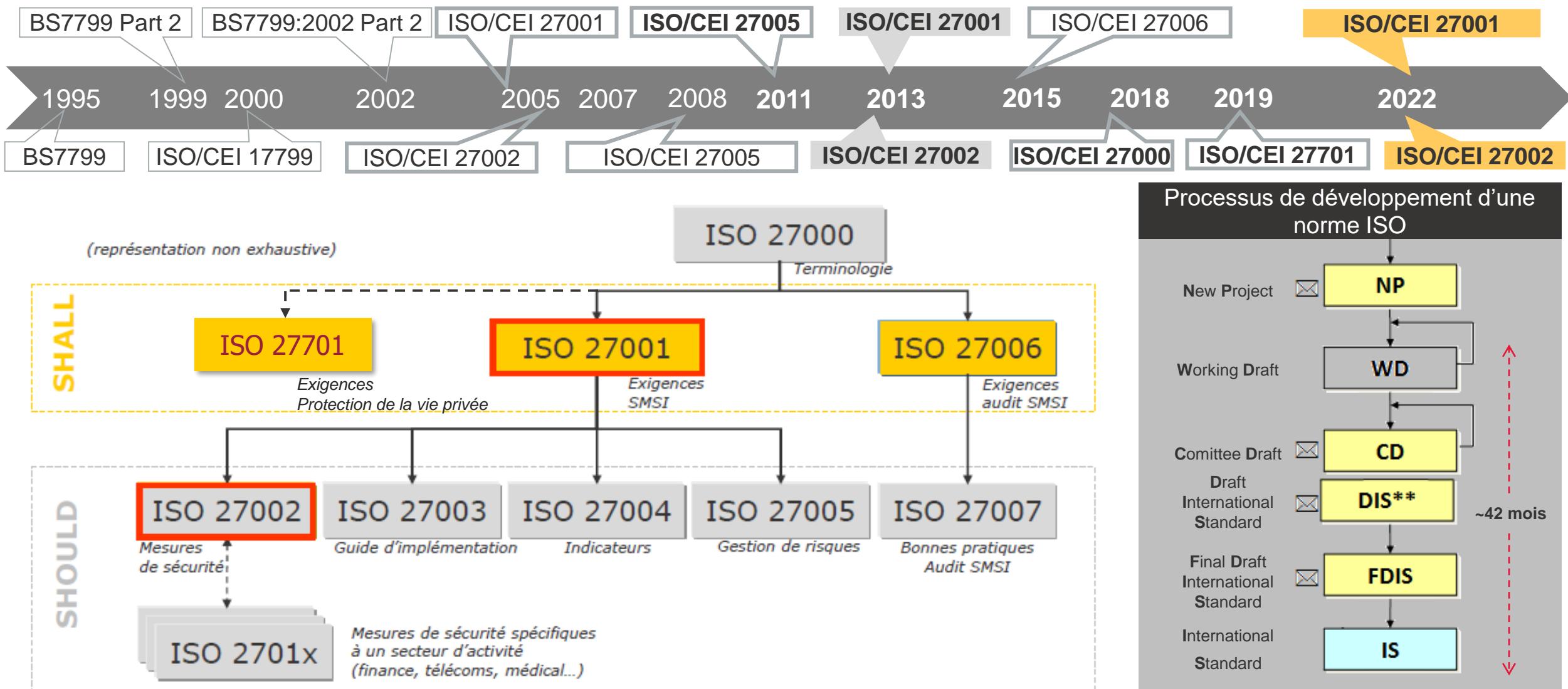
- "Accord général caractérisé par l'absence d'opposition ferme à l'encontre de l'essentiel du sujet [...]"  
→ **le consensus n'implique pas nécessairement l'unanimité**
- idéalement, il devrait réunir : experts, fournisseurs du service ou du produit, utilisateurs  
**en pratique : principalement experts et fournisseurs**

Une norme est un référentiel pour



- **développer** un produit ou un service, mettre en place un système ou une organisation
- faciliter la **comparaison et/ou l'interopérabilité** entre des produits, des services, des systèmes ou des organisations
- permettre la reconnaissance de l'**atteinte d'un certain niveau de qualité, de performance, de sécurité**, etc. (évaluation / certification)

# L'historique des normes ISO27XXX



**\*\*) By 100% approval ONLY**

Source : Welcome package of ISO/IEC JTC 1/SC 27 -- IT Security Techniques (2017)

# La série ISO27xxx (1/3)

**En résumé, ce sont 3 normes fondamentales :**

- 27001 : ISMS requirements, version actuelle 2022
- 27002 : Code of practice for ISM, version actuelle 2022
- 27005 : Information security risk management, version actuelle 2022

**Suivies de normes thématiques diverses:**

- 27000 : ISMS overview and vocabulary
- 27003 : ISM implementation guidance,
- 27004 : Monitoring, measurement, analysis and evaluation,
- 27006 : Requirements for bodies providing audit and certification of ISMS,
- 27010 : ISM for inter-sector and inter-organizational communications.
- 27013 : Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1,

# La série ISO27xxx (2/3)

Et d'autres documents (normes ou technical standard) publiés récemment pour compléter la série:

- 27009 : Sector-specific application of ISO/IEC 27001- Requirements,
- 27017 : Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002,
- 27019 (TS) : ISM guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry,
- 27018 : Code of practice for PII protection in public clouds acting as PII processors.
- **27701:2019 : Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management**

# La série ISO27xxx (3/3)

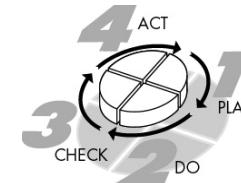
**La série ISO72xxx inclue également des normes plus techniques:**

- 27031 : Guidelines for ICT readiness for business continuity,
- 27032 : Guidelines for cybersecurity,
- 27033 : Network Security,
- 27034 : Guidelines for application security,
- 27035 : Information security incident management,
- 27036 : Security of outsourcing,
- 27037 : Guidelines for the identification, collection, acquisition, and preservation of digital evidence,
- 27039 : Selection, deployment, and operations of intrusion detection systems (IDPS)
- 27040 : Storage Security,
- 27050 : Electronic Discovery

# Principes du SMSI et normes associées

## Système de Management

- Le système de management repose sur la gestion d'**amélioration continue des processus** permettant d'**atteindre les objectifs fixés par l'organisme**
- Une **norme** de système de management fournit un **modèle à suivre** dans la mise en place et le fonctionnement d'un système de management
- Le cycle **Planifier – Faire – Vérifier – Agir (PDCA)** est le principe opératoire des normes de système de management de l'ISO :
  - **Planifier (Plan)** : Fixer des objectifs et des plans d'actions
  - **Faire (Do)** : Mettre en œuvre les plans définis
  - **Vérifier (Check)** : Mesurer les résultats issus des actions mises en œuvre
  - **Agir (Act)** : Corriger, améliorer les actions mises en œuvre



**ISO 26000**  
Système de Management de la  
**responsabilité sociale des**  
organisations



**ISO 9001**  
Système de Management de la  
**Qualité**



**ISO 22301**  
Système de Management de la  
**Continuité d'Activité**



**ISO 27001**  
Système de Management de la  
**Sécurité de l'Information**

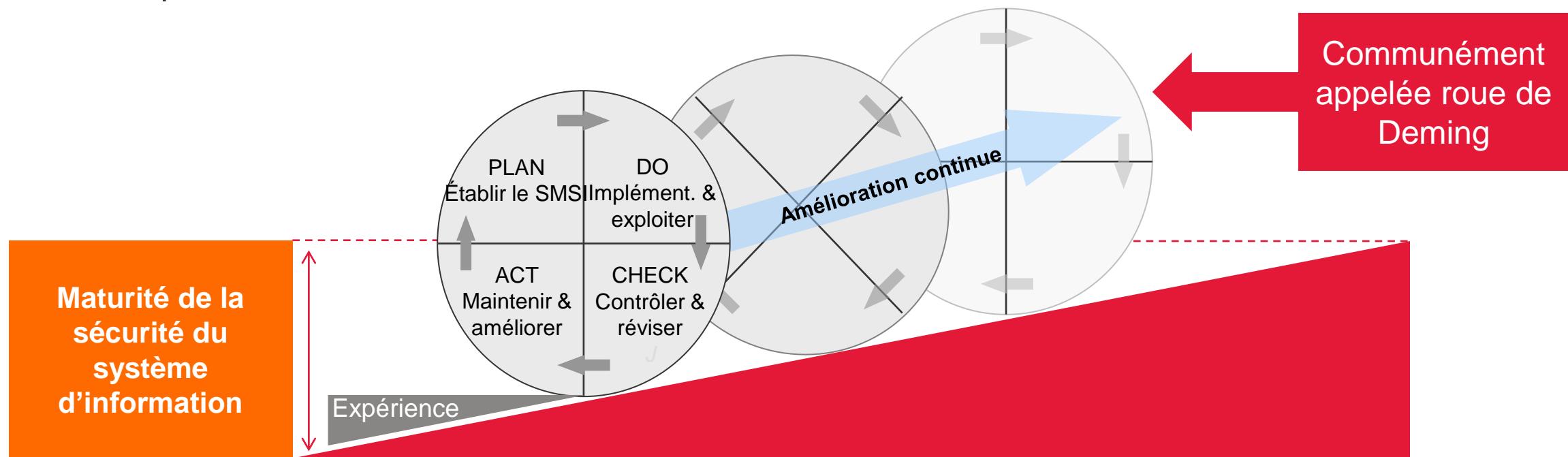


**ISO 20000**  
Système de Management des  
**Services Informatiques**

# Grands principes du SMSI

- Passage d'une logique de **protection du système d'information** à une logique de **protection de l'information**
- Le SMSI s'appuie sur une **démarche PDCA** (Plan - Do - Check – Act)

**Objectif : Améliorer la sécurité de l'information de façon progressive**, c'est-à-dire à chaque « tour de roue »



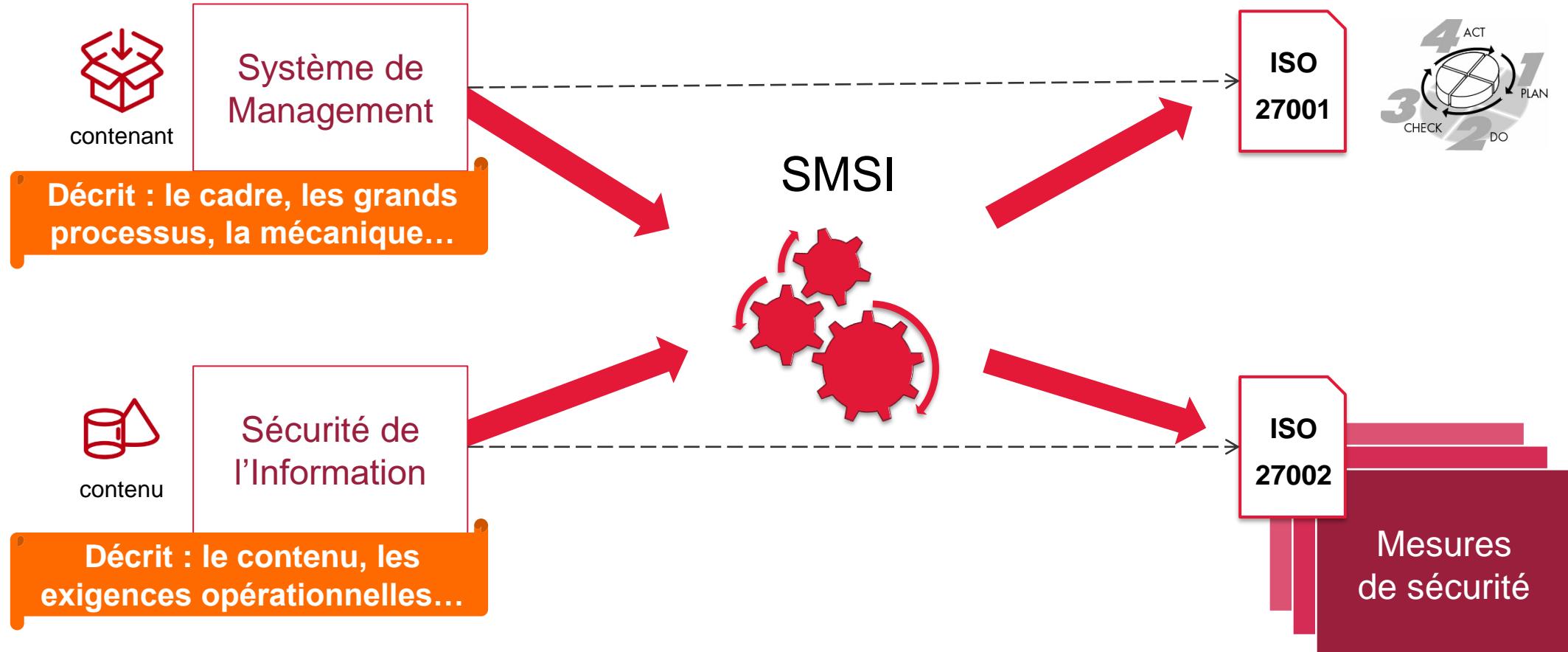
# Objectifs du SMSI

Le SMSI s'inscrit dans une **démarche globale d'entreprise** et participe ainsi à **l'atteinte des enjeux et objectifs stratégiques** de l'organisme



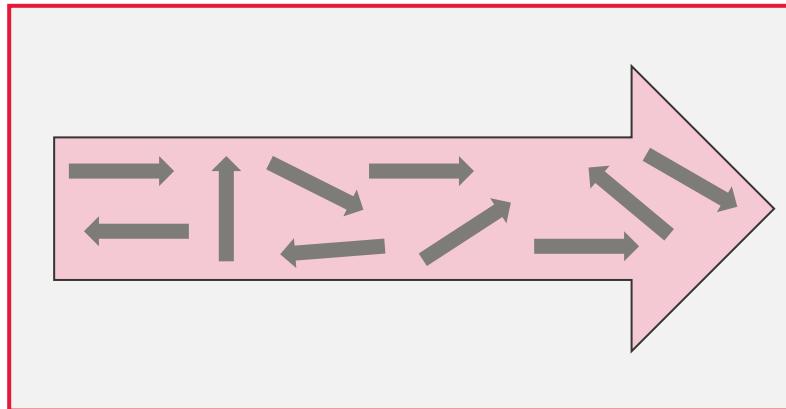
\* définition issue de la norme ISO 31000:2009

# Les normes clés : ISO 27001 et ISO 27002

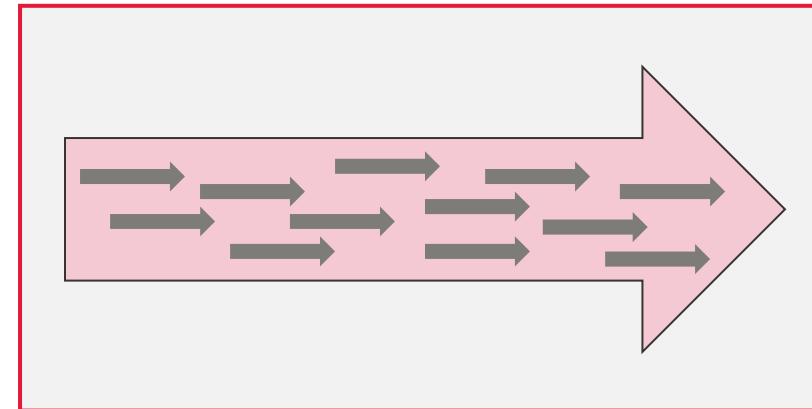


# Fédérer les approches du SMSI

Les projets de l'organisation **et les efforts humains et financiers** ne sont pas orientés dans la même direction. L'atteinte des objectifs individuels **ne garantit pas l'atteinte des objectifs collectifs**.



**Définir les objectifs stratégiques** comme moteur de la politique de gestion des risques et de la gouvernance en sécurité et **décliner ensuite les leviers d'atteinte de cette stratégie** permet de s'assurer que **l'ensemble des acteurs** de l'organisation contribue à la **construction de la même cible**.



# Agenda



## Principes du SMSI

- Introduction
- Définition du Système de Management
- **Introduction aux normes ISO27001 / ISO27002**



## La Gestion de Risque

- Principes de la gestion des risques
- ISO27005 / ISO31000
- Application d'EBIOS à l'identification des risques de l'entreprise



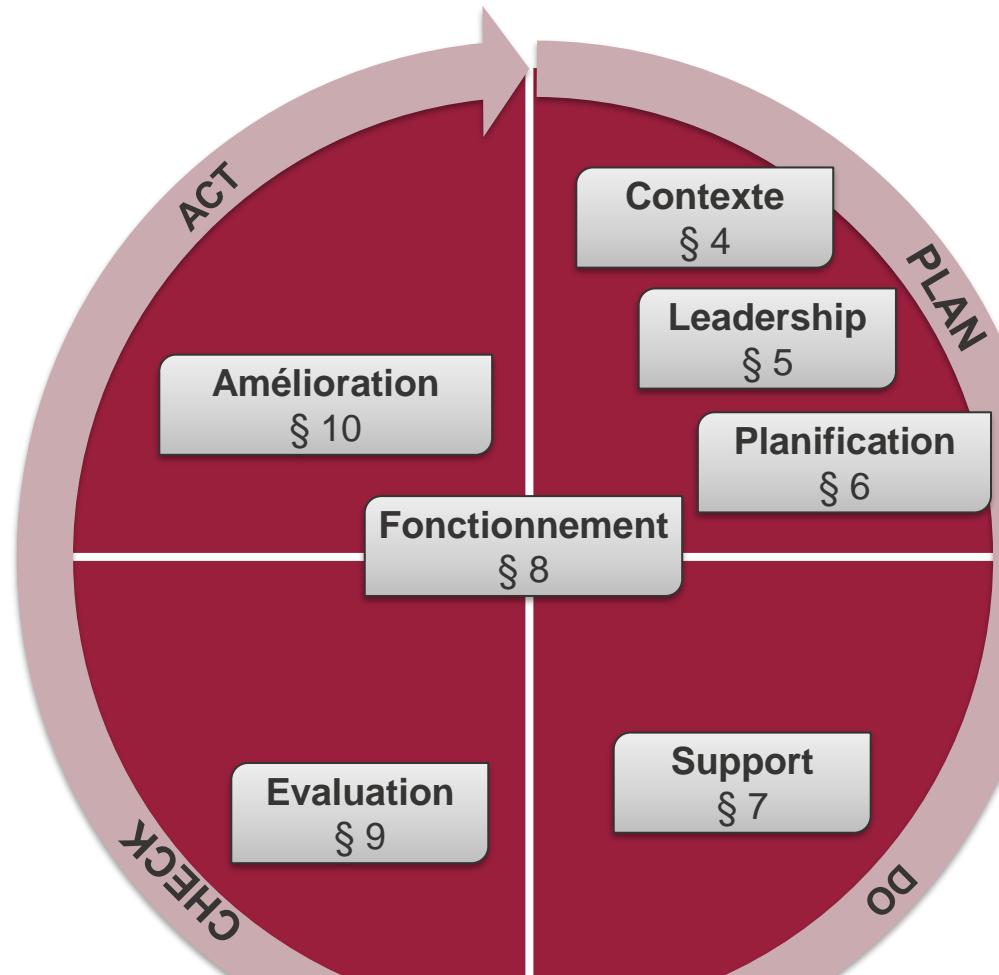
## La mise en œuvre pratique

- Plan
- DO
- Check
- Act

# Structure de la norme 27001:2022

## Sommaire

	Page
Avant-propos	iv
Introduction	v
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	1
4 Contexte de l'organisation	1
4.1 Compréhension de l'organisation et de son contexte	1
4.2 Compréhension des besoins et attentes des parties intéressées	2
4.3 Détermination du domaine d'application du système de management de la sécurité de l'information	2
4.4 Système de management de la sécurité de l'information	2
5 Leadership	2
5.1 Leadership et engagement	2
5.2 Politique	3
5.3 Rôles, responsabilités et autorités au sein de l'organisation	3
6 Planification	3
6.1 Actions à mettre en œuvre face aux risques et opportunités	3
6.1.1 Généralités	3
6.1.2 Appréciation des risques de sécurité de l'information	4
6.1.3 Traitement des risques de sécurité de l'information	5
6.2 Objectifs de sécurité de l'information et plans pour les atteindre	5
6.3 Planification des modifications	6
7 Supports	6
7.1 Ressources	6
7.2 Compétences	6
7.3 Sensibilisation	6
7.4 Communication	7
7.5 Informations documentées	7
7.5.1 Généralités	7
7.5.2 Création et mise à jour	7
7.5.3 Contrôle des informations documentées	7
8 Fonctionnement	8
8.1 Planification et contrôle opérationnels	8
8.2 Appréciation des risques de sécurité de l'information	8
8.3 Traitement des risques de sécurité de l'information	8
9 Évaluation de la performance	8
9.1 Surveillance, mesurages, analyse et évaluation	8
9.2 Audit interne	9
9.2.1 Généralités	9
9.2.2 Programme d'audit interne	9
9.3 Revue de direction	9
9.3.1 Généralités	9
9.3.2 Éléments d'entrée de la revue de direction	9
9.3.3 Résultats des revues de direction	10
10 Amélioration	10
10.1 Amélioration continue	10
10.2 Non-conformité et action corrective	10
Annexe A (normative) Référencement des mesures de sécurité de l'information	12
Bibliographie	21



# Structure de la norme 27001:2022

## Sommaire

	Page
Avant-propos	iv
Introduction	v
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	1
4 Contexte de l'organisation	1
4.1 Compréhension de l'organisation et de son contexte	1
4.2 Compréhension des besoins et attentes des parties intéressées	2
4.3 Détermination du domaine d'application du système de management de la sécurité de l'information	2
4.4 Système de management de la sécurité de l'information	2
5 Leadership	2
5.1 Leadership et engagement	2
5.2 Politique	3
5.3 Rôles, responsabilités et autorités au sein de l'organisation	3
6 Planification	3
6.1 Actions à mettre en œuvre face aux risques et opportunités	3
6.1.1 Généralités	3
6.1.2 Appréciation des risques de sécurité de l'information	4
6.1.3 Traitement des risques de sécurité de l'information	5
6.2 Objectifs de sécurité de l'information et plans pour les atteindre	5
6.3 Planification des modifications	6
7 Supports	6
7.1 Ressources	6
7.2 Compétences	6
7.3 Sensibilisation	6
7.4 Communication	7
7.5 Informations documentées	7
7.5.1 Généralités	7
7.5.2 Création et mise à jour	7
7.5.3 Contrôle des informations documentées	7
8 Fonctionnement	8
8.1 Planification et contrôle opérationnels	8
8.2 Appréciation des risques de sécurité de l'information	8
8.3 Traitement des risques de sécurité de l'information	8
9 Évaluation de la performance	8
9.1 Surveillance, mesures, analyse et évaluation	8
9.2 Audit interne	9
9.2.1 Généralités	9
9.2.2 Programme d'audit interne	9
9.3 Revue de direction	9
9.3.1 Généralités	9
9.3.2 Éléments d'entrée de la revue de direction	9
9.3.3 Résultats des revues de direction	10
10 Amélioration	10
10.1 Amélioration continue	10
10.2 Non-conformité et action corrective	10
Annexe A (normative) Référence des mesures de sécurité de l'information	12
Bibliographie	21

## Exigences

### 5.2 Politique

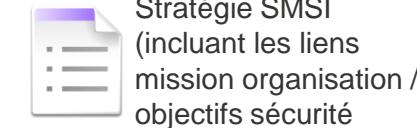
La direction doit établir une politique de sécurité de l'information qui:

- est appropriée à la **mission** de l'organisation;
- inclus des **objectifs de sécurité** de l'information ou fournit un cadre pour l'établissement de ces objectifs;
- inclus l'engagement de satisfaire aux **exigences applicables** en matière de sécurité de l'information; et
- inclus l'engagement d'oeuvrer pour **l'amélioration continue** du système de management de la sécurité de l'information.

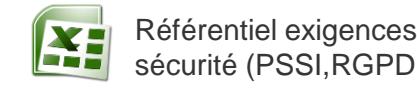
La politique de sécurité de l'information doit:

- être disponible sous forme d'**information documentée**;
- être **communiquée** au sein de l'organisation;
- être mise à la **disposition des parties intéressées**, le cas échéant.

## Preuves



Stratégie SMSI  
(incluant les liens  
mission organisation /  
objectifs sécurité)



Référentiel exigences  
sécurité (PSSI,RGPD..)



Processus  
d'amélioration continue  
sécurité de l'information



PSSI, Directives...



Mail avec A/R

# Structure de la norme 27001:2022

## Exercice:

- 1/ Quelles actions/activités peuvent être réalisées pour être conforme aux exigences du chapitre 7 Support ?
- 2/ Quelles enregistrements et preuves pourraient être demandées par un auditeur externe ?

Exigence	Activité à réaliser / Processus	Enregistrements / Preuves
7.2 Compétence		
7.3 Sensibilisation		
7.4 Communication		

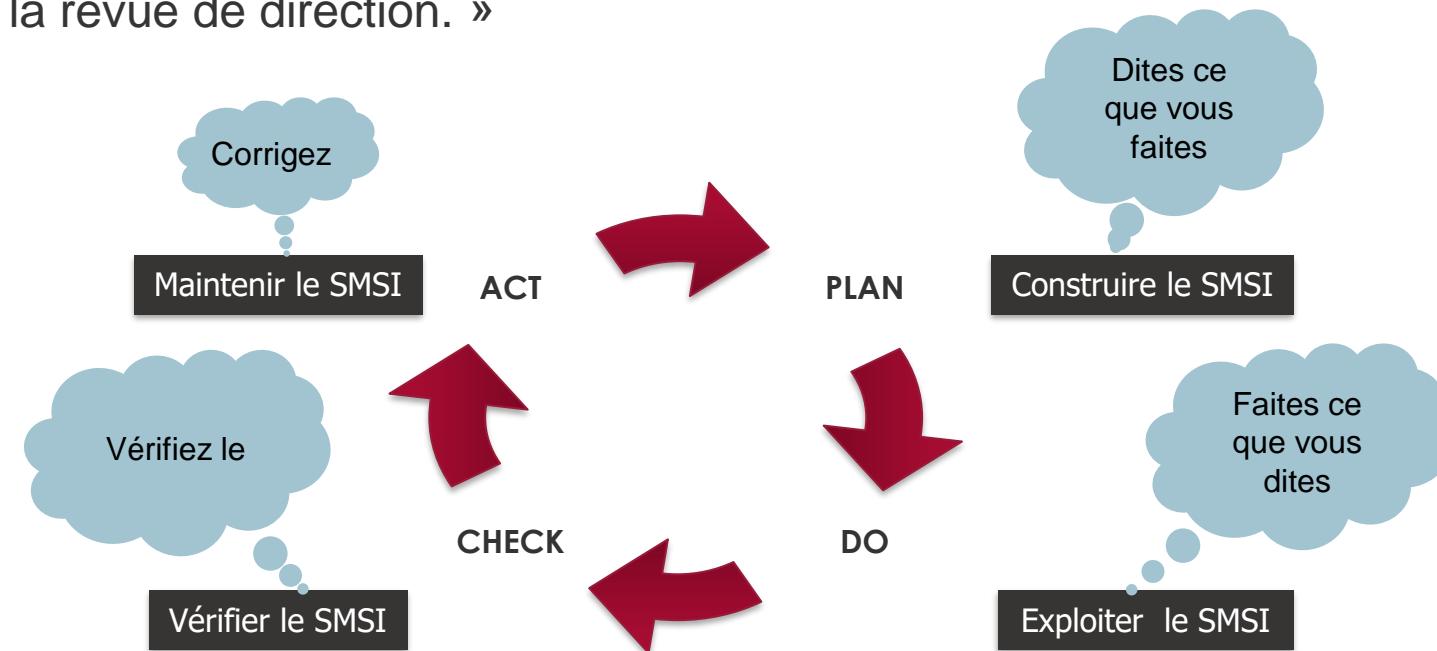
# Gérer le risque Cyber pour une organisation



- Schéma directeur
  - Diagnostic Cyber
  - Etude de cadrage
  - Analyse de risque
  - Analyse d'écart (conformité)
  - Mise en conformité
  - Pilotage des chantiers
  - Gestion de projet Cyber
  - Reporting Cyber
  - Audit organisationnel
  - Audit technique
  - Etude de maturité
  - Evaluation de fournisseur
  - Plan d'actions d'amélioration
  - Suivi & accompagnement
  - Formation / sensibilisation...

## Exigence de la norme

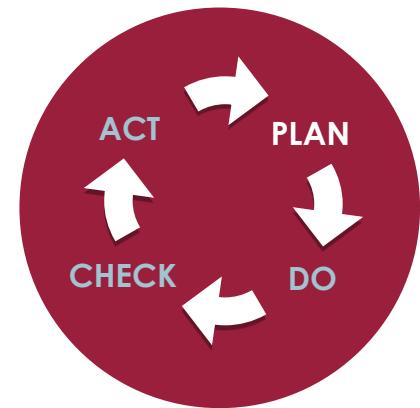
« L'organisme doit améliorer en permanence l'efficacité du SMSI en utilisant la politique en matière de sécurité de l'information, la réalisation des objectifs en termes de sécurité de l'information, les résultats d'audit, l'analyse des événements surveillés, les actions correctives et préventives et la revue de direction. »



**Déterminant pour la définition du périmètre** (impact direct sur les rôles et responsabilités) et  
**fixe les métriques communes** (méthodologie d'appréciation des risques)

## Elle consiste à

- Définir le périmètre du SMSI
- Elaborer la politique du SMSI
- Identifier et apprécier les risques
  - Peu de contraintes sur le choix de la méthode
  - Les risques doivent être validés par la Direction
- Elaborer la Déclaration d'Applicabilité (DdA)  
=> Sélectionner des mesures de sécurité applicables au périmètre

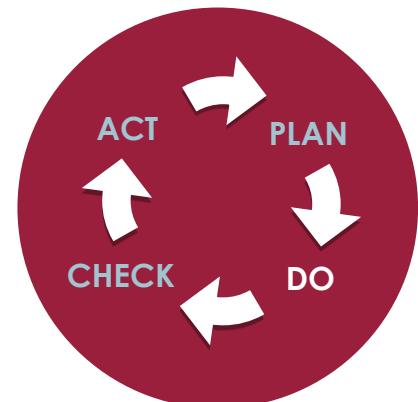


## Mise en application les principes définis dans l'étape PLAN

Sont notamment mis en œuvre : le Plan de Traitement des Risques, les Politiques de Sécurité, mais aussi les procédures définissant le fonctionnement du SMSI

### Elle consiste à

- Traiter les risques, conformément aux options choisies
  - Exploitation des mesures pour les risques couverts
  - Suivi pour le traitement des risques transférés
  - Suivi pour les risques résiduels (non couverts)
- Implémenter les moyens de la gouvernance
  - Ressources nécessaires
  - Procédures suivies
  - Formation et sensibilisation des acteurs

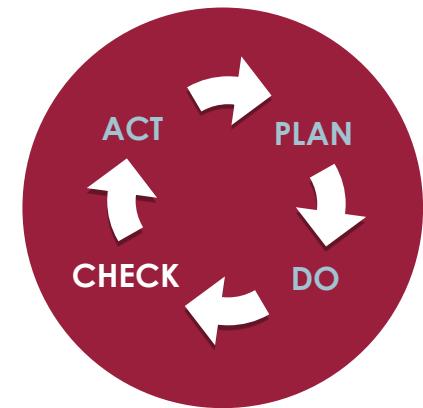


## **Consolidation des informations** avant l'amélioration du système.

La confidentialité des informations collectées est souvent un obstacle à leur analyse. Le SMSI doit s'entourer de personnes de confiance.

### Elle consiste à

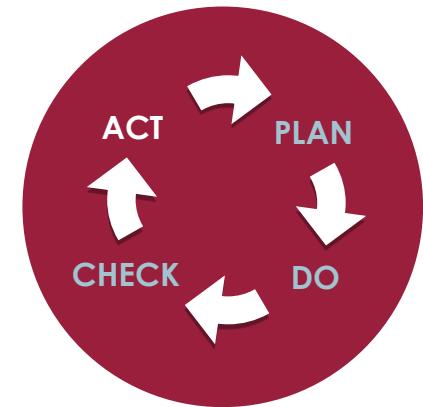
- Conduire les actions de suivi de
  - l'efficacité des mesures mises en place pour réduire les risques
  - la conformité du système
- Moyens
  - Audits internes du système
  - Production et analyse des indicateurs et tableaux de bord
  - Analyse des incidents survenus



Travail important de **définition des actions correctives et préventives**  
Il s'agit ici de **traiter les causes des problèmes rencontrés**, et non leurs conséquences

## Elle consiste à

- Planifier et suivre les actions correctives et préventives
- Eléments à intégrer
  - Non-conformité (potentielles et avérées)
  - Opportunités d'amélioration
- Moyens de suivi
  - Pilotage



Assurer la sécurité de son information nécessite des **principes de gestion rigoureux**, des plus simples aux plus complexes, au jour le jour, quel que soit son support.

**L'appropriation de ces pratiques par les opérationnels est indispensable**

## Elle repose sur

- Principes de gestion issus de la Qualité (ISO 9001)
- Distinction claire présentée par la norme
  - Documents : exigés par la norme ISO 27001  
(''informations documentées'') : politique SMSI, procédures de fonctionnement du SMSI)
  - Enregistrements : preuves de d'implémentation des mesures de sécurité et de preuves de fonctionnement
- Exigences de gestion moins fortes pour les enregistrements

## Les gestion des enregistrements

- Doivent être **établis et conservés** pour apporter la **preuve de la conformité aux exigences et du fonctionnement efficace du SMSI**
- Doivent être **protégés et maîtrisés**
- Doivent **rester lisibles, faciles à identifier et accessibles**

Le SMSI doit tenir compte des exigences légales ou réglementaires et des obligations contractuelles

## Points de contrôles

- Les **contrôles** permettant d'assurer l'identification, le stockage, la protection, l'accessibilité, la durée de conservation et l'élimination des enregistrements doivent être **documentés et mis en œuvre**
- Les **enregistrements** des performances du processus, ainsi que de toutes les occurrences des incidents de sécurité importants relatifs à le SMSI, **doivent être conservés**

# Points clés ISO 27001 : responsabilité de la Direction (leadership et engagement)

**La Direction doit porter la gouvernance de la sécurité** à travers la formation des collaborateurs, la communication auprès des autres équipes, etc.

Cet **engagement** est souvent **matérialisé par une lettre** (note de communication) qui définit les objectifs et qui est adressée par la Direction aux collaborateurs.

## La Direction doit démontrer son engagement dans la démarche

- Responsabilité
- Volonté de communication
- Sensibilisation et formation (engagement de compétences)
- Affectation de moyens (humains, financiers, organisationnels)

**En fonction du périmètre** du système (par exemple à l'échelle globale de l'entreprise), **la tâche d'audit** peut s'avérer lourde et nécessiter **une ou plusieurs personnes à plein temps**. **L'organisation** de l'entreprise et le **design de ses processus** compliquent également **cette tâche** (audit par direction, par processus...)

## Exigences

- Définition d'un plan d'audit
- Définition d'une méthode, de critères
- Sélection et formation des auditeurs

## Périmètre de l'audit

- Le Système de Management lui-même
- L'application des mesures de sécurité de la DdA\* sur le périmètre du SMSI

\* ) **DdA** : Déclaration d'Applicabilité

**S'assurer que le SMSI s'inscrit dans la stratégie globale de la SSI et qu'elle est cohérente avec la stratégie globale et dynamique de l'entreprise.**

## Objectif : réévaluation de la stratégie par la Direction

- Résultats d'audit
- Retours des parties prenantes
- Indicateurs
- Avancement des plans d'actions
- Identification des risques
- Changements de contexte

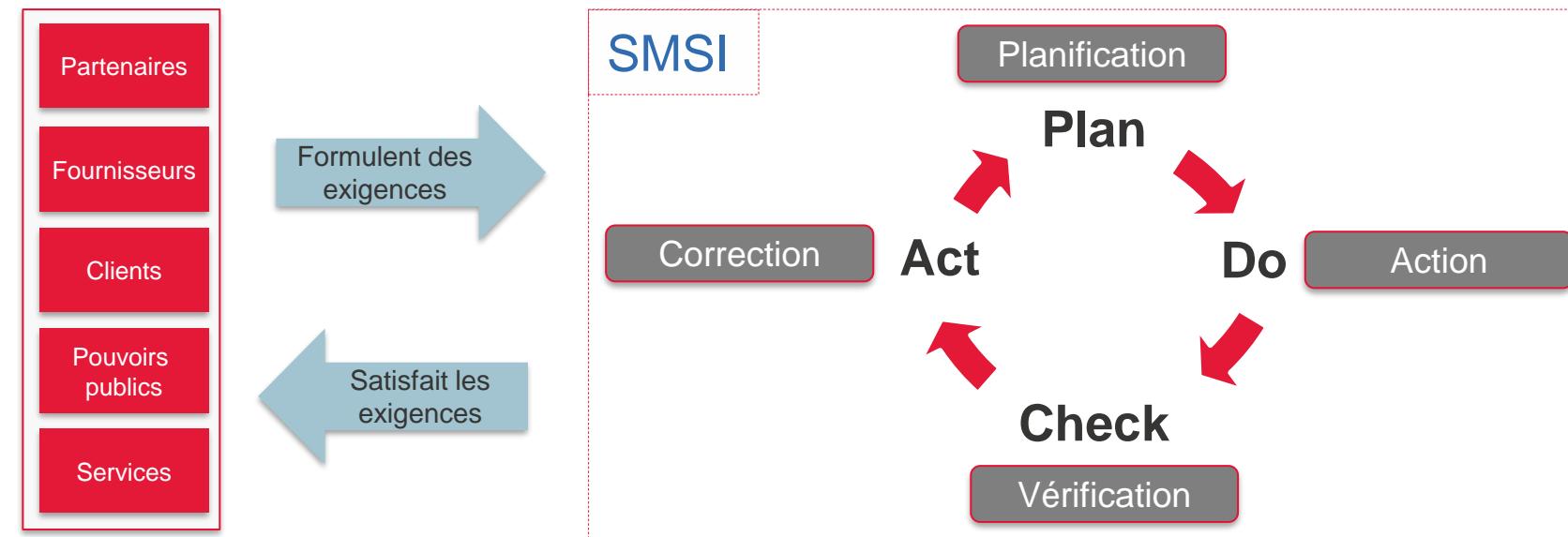


- Plan de Traitement des Risques
- Orientations pour le SMSI (opportunités de changements)
- Affectation des ressources

**Réexaminer périodiquement le SMSI (ISO 27001) pour assurer sa pertinence et son efficacité**

Ensemble de mesures organisationnelles et techniques permettant d'atteindre un objectif et de le maintenir dans la durée

Sécuriser l'information en termes de disponibilité, intégrité, confidentialité et traçabilité.



L'amélioration est une **étape critique** du système.

L'organisation associée doit permettre de **qualifier** l'ensemble des **éléments en entrée** afin de **définir** précisément les **actions à mettre en œuvre** et leur niveau de **priorité**.

Le **suivi** de ces actions est une tâche **non négligeable**

## Elément en entrée

- Tableaux de bord
- Rapports d'audit interne
- Remarques
- Rapports d'incidents
- Changement de contexte

## Elément de sortie

- Plan d'action priorisé et suivi

The image shows three vertically stacked forms, each with a header in French: "Formulaire à transmettre au responsable de l'ISMS", "Formulaire à remplir par le responsable de la remarque", and "Formulaire à remplir par le responsable de l'action". The first form has fields for "Prénom Nom", "Date", "Lieu", and "Niveau de confidentialité". The second form has sections for "Détails de la faille", "Cause(s) de l'écart", "Actions correctives", and "Priorité de l'action". The third form has sections for "Planification de l'action", "Responsable de l'action", "Responsable du contrôle", and "Description de l'action".

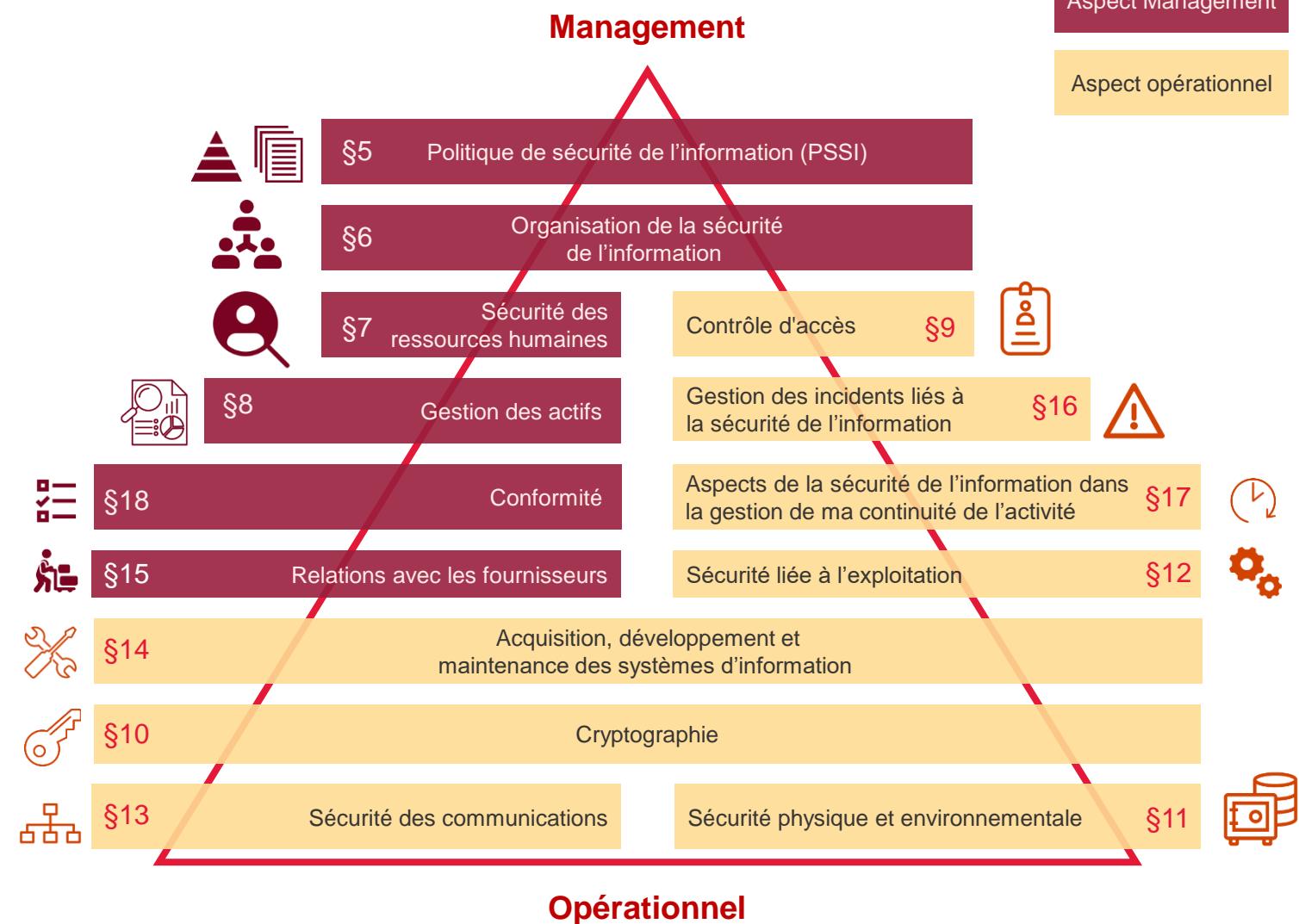
## Limites

*La mise en œuvre de certaines actions nécessite des ressources importantes.*

*Lorsque l'action est prioritaire et que ces ressources ne sont pas disponibles, une Revue de Direction devra probablement être provoquée*

# Structure de la norme 27002:2013

5	Politiques de sécurité de l'information	2
5.1	Orientations de la direction en matière de sécurité de l'information	2
6	Organisation de la sécurité de l'information	4
6.1	Organisation interne	4
6.2	Appareils mobiles et télétravail	7
7	La sécurité des ressources humaines	9
7.1	Avant l'embauche	9
7.2	Pendant la durée du contrat	11
7.3	Rupture, terme ou modification du contrat de travail	14
8	Gestion des actifs	15
8.1	Responsabilités relatives aux actifs	15
8.2	Classification de l'information	16
8.3	Méthodologie de manipulation des supports	19
9	Contrôle d'accès	21
9.1	Exigences métier en matière de contrôle d'accès	21
9.2	Gestion de l'accès utilisateur	23
9.3	Responsabilités des utilisateurs	27
9.4	Contrôle de l'accès au système et aux applications	28
10	Cryptographie	31
10.1	Mesures cryptographiques	31
11	Sécurité physique et environnementale	34
11.1	Zones sécurisées	34
11.2	Matériels	37
12	Sécurité liée à l'exploitation	42
12.1	Procédures et responsabilités liées à l'exploitation	42
12.2	Protection contre les logiciels malveillants	46
12.3	Sauvegarde	47
12.4	Journalisation et surveillance	48
12.5	Maîtrise des logiciels en exploitation	50
12.6	Gestion des vulnérabilités techniques	51
12.7	Considérations sur l'audit du système d'information	53
13	Sécurité des communications	54
13.1	Management de la sécurité des réseaux	54
13.2	Transfert de l'information	56
14	Acquisition, développement et maintenance des systèmes d'information	60
14.1	Exigences de sécurité applicables aux systèmes d'information	60
14.2	Sécurité des processus de développement et d'assistance technique	63
14.3	Données de test	68
15	Relations avec les fournisseurs	69
15.1	Sécurité de l'information dans les relations avec les fournisseurs	69
15.2	Gestion de la prestation du service	72
16	Gestion des incidents liés à la sécurité de l'information	74
16.1	Gestion des incidents liés à la sécurité de l'information et améliorations	74
17	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	78
17.1	Continuité de la sécurité de l'information	78
17.2	Redondances	80
18	Conformité	81
18.1	Conformité aux obligations légales et réglementaires	81
18.2	Revue de la sécurité de l'information	84



# Structure de la norme 27002:2013

5	Politiques de sécurité de l'information	2
5.1	Orientations de la direction en matière de sécurité de l'information	2
6	Organisation de la sécurité de l'information	4
6.1	Organisation interne	4
6.2	Appareils mobiles et télétravail	7
7	La sécurité des ressources humaines	9
7.1	Avant l'embauche	9
7.2	Pendant la durée du contrat	11
7.3	Rupture, terme ou modification du contrat de travail	14
8	Gestion des actifs	15
8.1	Responsabilités relatives aux actifs	15
8.2	Classification de l'information	16
8.3	Méthodologie de manipulation des supports	19
9	Contrôle d'accès	21
9.1	Exigences métier en matière de contrôle d'accès	21
9.2	Gestion de l'accès utilisateur	23
9.3	Responsabilités des utilisateurs	27
9.4	Contrôle de l'accès au système et aux applications	28
10	Cryptographie	31
10.1	Mesures cryptographiques	31
11	Sécurité physique et environnementale	34
11.1	Zones sécurisées	34
11.2	Matériels	37
12	Sécurité liée à l'exploitation	42
12.1	Procédures et responsabilités liées à l'exploitation	42
12.2	Protection contre les logiciels malveillants	46
12.3	Sauvegarde	47
12.4	Journalisation et surveillance	48
12.5	Maîtrise des logiciels en exploitation	50
12.6	Gestion des vulnérabilités techniques	51
12.7	Considérations sur l'audit du système d'information	53
13	Sécurité des communications	54
13.1	Management de la sécurité des réseaux	54
13.2	Transfert de l'information	56
14	Acquisition, développement et maintenance des systèmes d'information	60
14.1	Exigences de sécurité applicables aux systèmes d'information	60
14.2	Sécurité des processus de développement et d'assistance technique	63
14.3	Données de test	68
15	Relations avec les fournisseurs	69
15.1	Sécurité de l'information dans les relations avec les fournisseurs	69
15.2	Gestion de la prestation du service	72
16	Gestion des incidents liés à la sécurité de l'information	74
16.1	Gestion des incidents liés à la sécurité de l'information et améliorations	74
17	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	78
17.1	Continuité de la sécurité de l'information	78
17.2	Redondances	80
18	Conformité	81
18.1	Conformité aux obligations légales et réglementaires	81
18.2	Revue de la sécurité de l'information	84

## 9.4.1 Restriction d'accès à l'information

### Mesure

Il convient de **restreindre l'accès** à l'information et aux fonctions d'application système conformément à la politique de contrôle d'accès.

→ **Version 2022:** 8.3 - L'accès aux informations et autres actifs associés doit être restreint conformément à la politique spécifique à la thématique du contrôle d'accès qui a été établie.

### Préconisations de mise en oeuvre

Il convient que les restrictions d'accès soient fonction des exigences de chaque application métier et conformes à la politique de contrôle d'accès définie.

Pour soutenir les exigences relatives aux restrictions d'accès, il convient d'envisager de:

- créer des menus permettant de contrôler l'accès aux **fonctions** d'application système;
- contrôler les **données** auxquelles peut accéder un utilisateur donné;
- contrôler les **droits d'accès** des utilisateurs, par exemple: lecture, écriture, suppression et exécution;
- contrôler les droits d'accès aux autres applications;
- limiter les informations contenues dans les **éléments de sortie**:
- fournir des **contrôles d'accès physiques ou logiques** permettant d'isoler les applications, les données des applications ou les systèmes sensibles.

# Structure de la norme 27002:2013

## Exercice:

- 1/ Quelles mesures/préconisation peuvent être mises en œuvre pour être conforme à l'exigence exigence 11.1.2 du chapitre Sécurité physique et environnementale ?
- 2/ Quelles enregistrements et preuves pourraient être demandées par un auditeur externe ?

Exigence	Préconisations à mettre en oeuvre	Preuves associées
11.1.2 Contrôles physiques des accès		

L'**ISO 27002:2013** est organisée en chapitres (14) / sous-chapitres (35) thématiques proposant des **objectifs et des mesures de sécurité** (114) contribuant à leur atteinte

**Objectif** : Prise en compte des **risques de sécurité des informations relatives aux critères DIC** (Disponibilité, Intégrité et Confidentialité)

## Disponibilité\*

*"propriété d'être accessible et utilisable à la demande par une entité autorisée"*

## Intégrité\*

*"propriété d'exactitude et de complétude"*

## Confidentialité\*

*"propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisé"*



\*Définitions provenant de l'ISO 27000:2018

# ISO 27002:2022 - Evolution de la norme

ISO/IEC 27002:2017

ISO/IEC 27002:2022

114 mesures de sécurité

93 mesures de sécurité

11 nouvelles mesures de sécurité



## ➤ Organizational controls

5.7 Threat intelligence

5.23 Information security for use of cloud services

5.30 ICT readiness for business continuity

## ➤ Physical controls

7.4 Physical security monitoring

## ➤ People controls

Ø Pas de nouvelles mesures

## ➤ Technological controls

8.9 Configuration management

8.10 Information deletion

8.11 Data masking

8.12 Data leakage prevention

8.16 Monitoring activities

8.23 Web filtering

8.28 Secure coding

## Evolution du SMSI La Poste

Une transition à effectuer dans les 2 ans suivant la publication.

Un audit de transition de l'ISO 27001 lors de l'**audit de surveillance**.

Les documents nécessaires :

- ✓ Une analyse d'impact ;
- ✓ MAJ déclaration d'applicabilité ;
- ✓ MAJ plan de traitement des risques ;
- ✓ La mise en œuvre et l'efficacité des **mesures nouvelles ou modifiées**.

Organisation de la norme, les attributs et nouvelles notions

## Mesures de sécurité

Les mesures de sécurité données dans les articles de 5 à 8 sont catégorisées sous forme de thèmes:

- Article 5 – Mesures organisationnelles
- Article 6 – Mesures liées aux personnes
- Article 7 – Mesure d'ordre physique
- Article 8 – Mesures technologiques

## Nouvelles notions – #Les attributs

**01** # Types de mesures de sécurité

**02** # Propriétés de sécurité de l'information

**03** # Concepts de cybersécurité

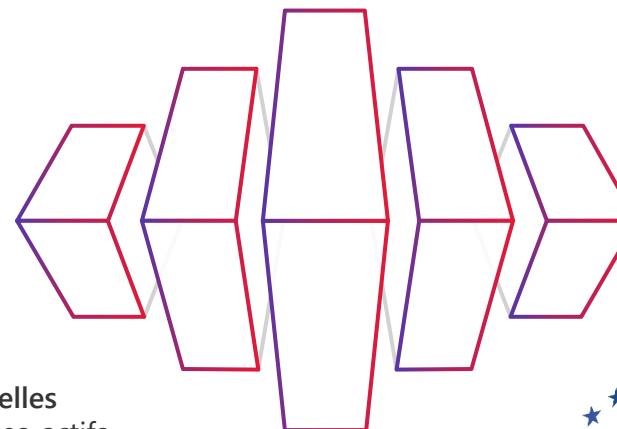
**04** # Capacités Opérationnelles

**05** # Domaines de sécurité

Types de mesures de sécurité  
# Prévention # Détection  
# Correction

Capacités Opérationnelles  
#Gouvernance #Gestion\_des\_actifs  
#Protection\_des\_informations  
#Sécurité\_des\_ressource\_humaines #Sécurité\_Physique  
#Sécurité\_système\_et\_réseau #Sécurité\_des\_applications  
#Configuration\_sécurisée #Gestion\_des\_identiités\_et\_des\_accès  
#Gestion\_des\_menaces\_et\_des\_vulnérabilités #Continuité  
#Sécurité\_des\_relations\_fournisseurs #Législation\_et\_conformité  
#Gestion\_des évènement\_de\_sécurité\_de\_l'information  
#Assurance\_de\_sécurité\_de\_l'information

Propriété de sécurité de l'information  
# Confidentialité #  
Intégrité #Disponibilité



Concepts de cybersécurité  
# Identification  
#Protection #Détection  
#Traitement #Traitement  
#Récupération



Domaines de sécurité  
#Gouvernance\_et\_ecosystème  
#Protection #Défense #Résilience

# Une catégorisation des mesures & un mapping avec d'autres référentiels

## 5 « Operational Capabilities »

Governance	Asset management	Information protection	Human resource security	Physical security	System and network security	Application security	Secure configuration
8 mesures identifiées	16 mesures identifiées	15 mesures identifiées	6 mesures identifiées	16 mesures identifiées	17 mesures identifiées	11 mesures identifiées	6 mesures identifiées
Identity and access management	Threat and vulnerability management	Continuity	Supplier relationships security	Legal and compliance	Information security event management	Information security assurance	
11 mesures identifiées	3 mesures identifiées	6 mesures identifiées	7 mesures identifiées	6 mesures identifiées	10 mesures identifiées	3 mesures identifiées	

**Notes additionnelles :**

- ✓ Mapping des exigences ISO 27002 : 2017 avec les nouvelles exigences ISO 27002 : 2022 ;
- ✓ Les organisations peuvent choisir d'ignorer les tags mis à disposition dans la norme.

## 5 « Cybersecurity concepts »

NIST



Identify	Protect	Detect	Respond	Recover
22 mesures identifiées	71 mesures identifiées	14 mesures identifiées	11 mesures identifiées	8 mesures identifiées

## 4 « Security domains »



Governance and Ecosystem	Protection	Defence	Resilience
27 mesures identifiées	69 mesures identifiées	22 mesures identifiées	8 mesures identifiées

- ISO 27001

- Le **corps** de la norme :

Un recueil d'exigences de système de management dans le domaine de la sécurité de l'information : PDCA, gestion de risques

- **Annexe A** (normative) :

Une série de mesures de sécurité (basées sur le référentiel ISO 27002), contribuant à des objectifs prédéfinis, par rapport à laquelle l'organisme devra se positionner

- ISO 27002

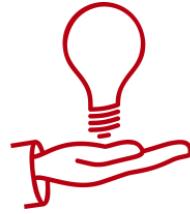
- Un **guide d'implémentation** des mesures de sécurité

## Rappels & Questions

### Principes du SMSI

- ❖ Introduction
- ❖ Définition du Système de Management
- ❖ Introduction aux normes ISO27001 / ISO27002

# Agenda



## Principes du SMSI

- Introduction
- Définition du Système de Management
- Introduction aux normes ISO27001 / ISO27002



## La Gestion de Risque

- Principes de la gestion des risques
- ISO27005 / ISO31000
- Application d'EBIOS à l'identification des risques de l'entreprise



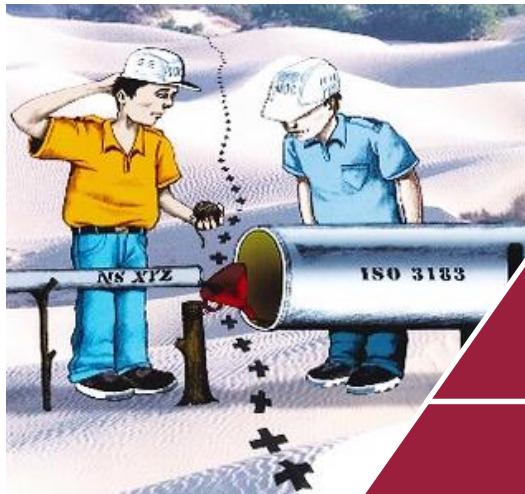
## La mise en œuvre pratique

- Plan
- Do
- Check
- Act

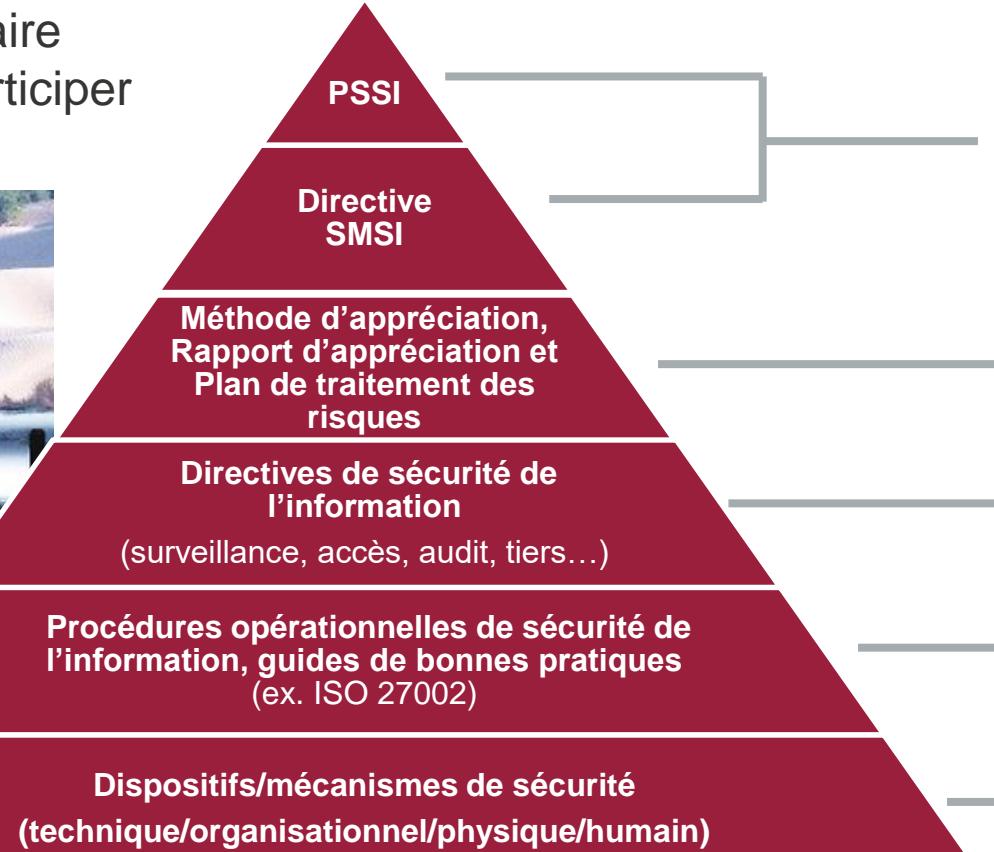
# Lien entre ISO 27001 et RGS



« La norme est volontaire  
Vous pouvez ou non y participer  
et vous y référer »



## ISO 27001



→ Viser l'amélioration continue

## RGS

PSSIE (ou déclinaison)  
Stratégie d'homologation

E BIOS (conforme à l'ISO 27001, 27005 et 31000)

Audit, Contrôle (homologation)

Procédures d'exploitation de sécurité (PES),  
Guide d'hygiène

Utilisation de matériels & prestations qualifiés, audit PASSI...



L'HOMOLOGATION DE SÉCURITÉ  
en neuf étapes simples



E BIOS  
RISK MANAGER

# Définition de la notion d'actif

“

[...] L'information est considérée comme un actif qui est doté d'une valeur et qui doit bénéficier d'une protection appropriée contre la perte de disponibilité, de confidentialité et d'intégrité, par exemple [...]



27000:2018 (4.1)

“

[...] Un actif désigne tout élément ayant de la valeur pour l'organisme et nécessitant, par conséquent, une protection [...]



27005:2011 (8.2.1.2)

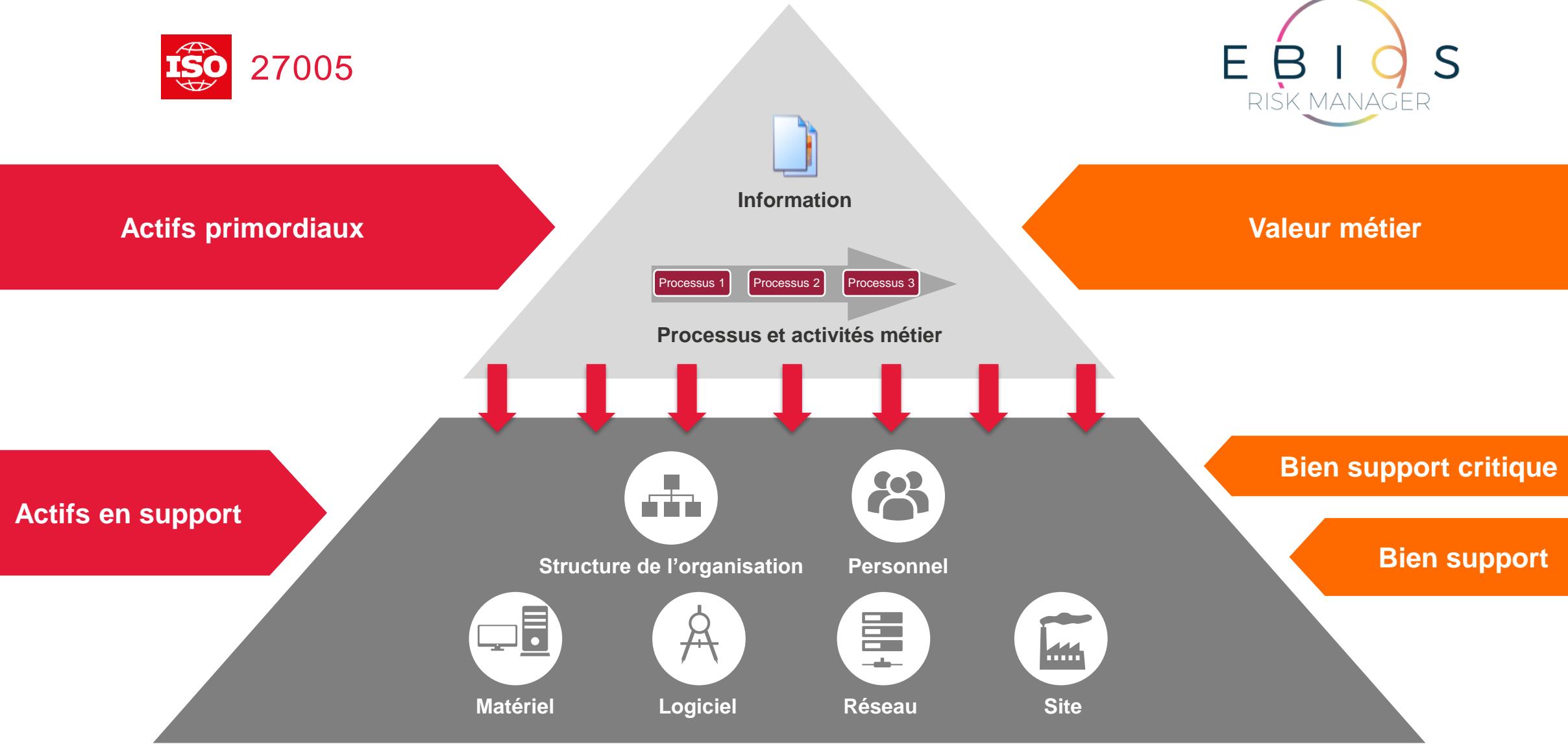


**La norme ISO 27001:2013 n'impose pas d'identifier les risques à partir des actifs, cependant l'inventaire des actifs est toujours requis (A.8)**

# Quelques variantes de la notion d'actif



27005

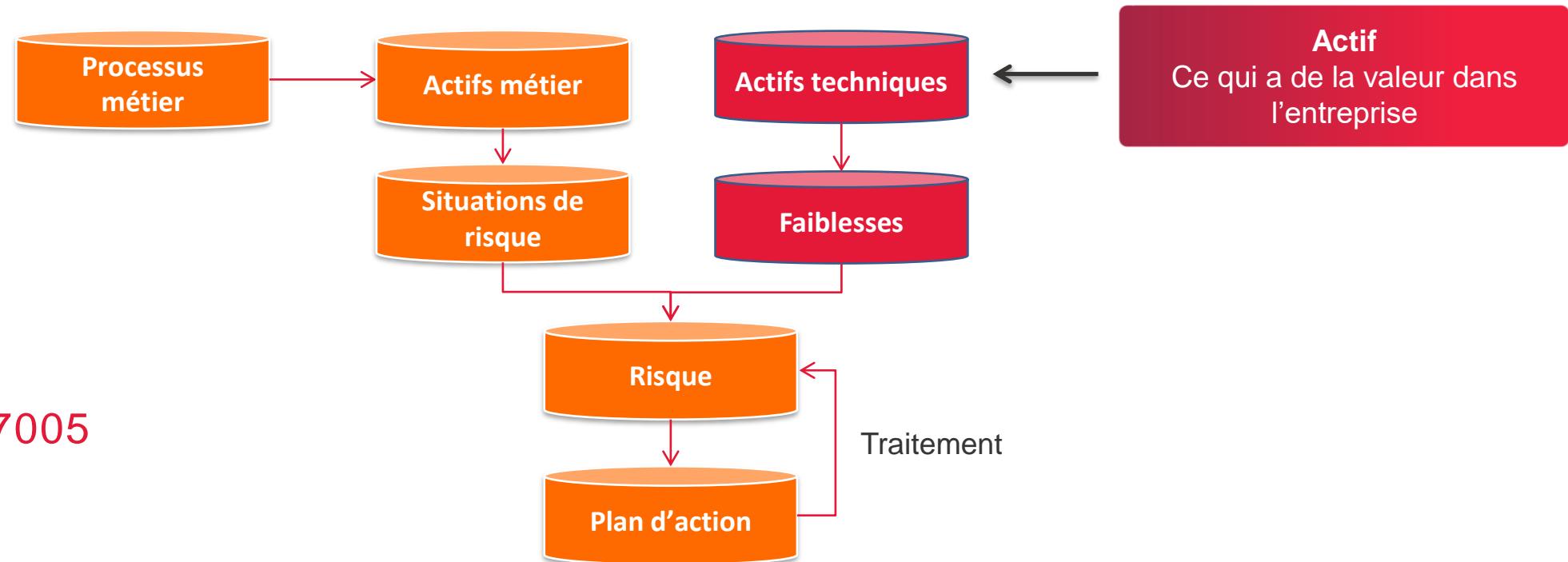


# Gestion des risques par les actifs

L'approche par les risques s'appuie sur les actifs métiers et IT

- Cette approche consiste à identifier les faiblesses des actifs
- Un risque est un croisement entre une situation de risque crainte par le métier et une faiblesse d'un actif

Ces risques sont généralement traités via la mise en œuvre de plans d'actions visant à combler les faiblesses



27005

## Actif

- Tout élément **présentant de la valeur** pour l'organisme
- **Information sensible** qui, si elle est révélée à des personnes mal intentionnées, peut entraîner la **perte d'un avantage ou une dégradation du niveau de sécurité**



Exemples : Fichiers des clients, information sur l'architecture du SI

## Menace

- Cause potentielle d'un **incident indésirable**, qui peut aboutir au dysfonctionnement d'un système ou d'une organisation
- Catégories : physiques, évènements naturels, perte de service, radiations, compromissions, techniques, actions non autorisées, usurpations



Exemple : Espionnage d'une communication électronique

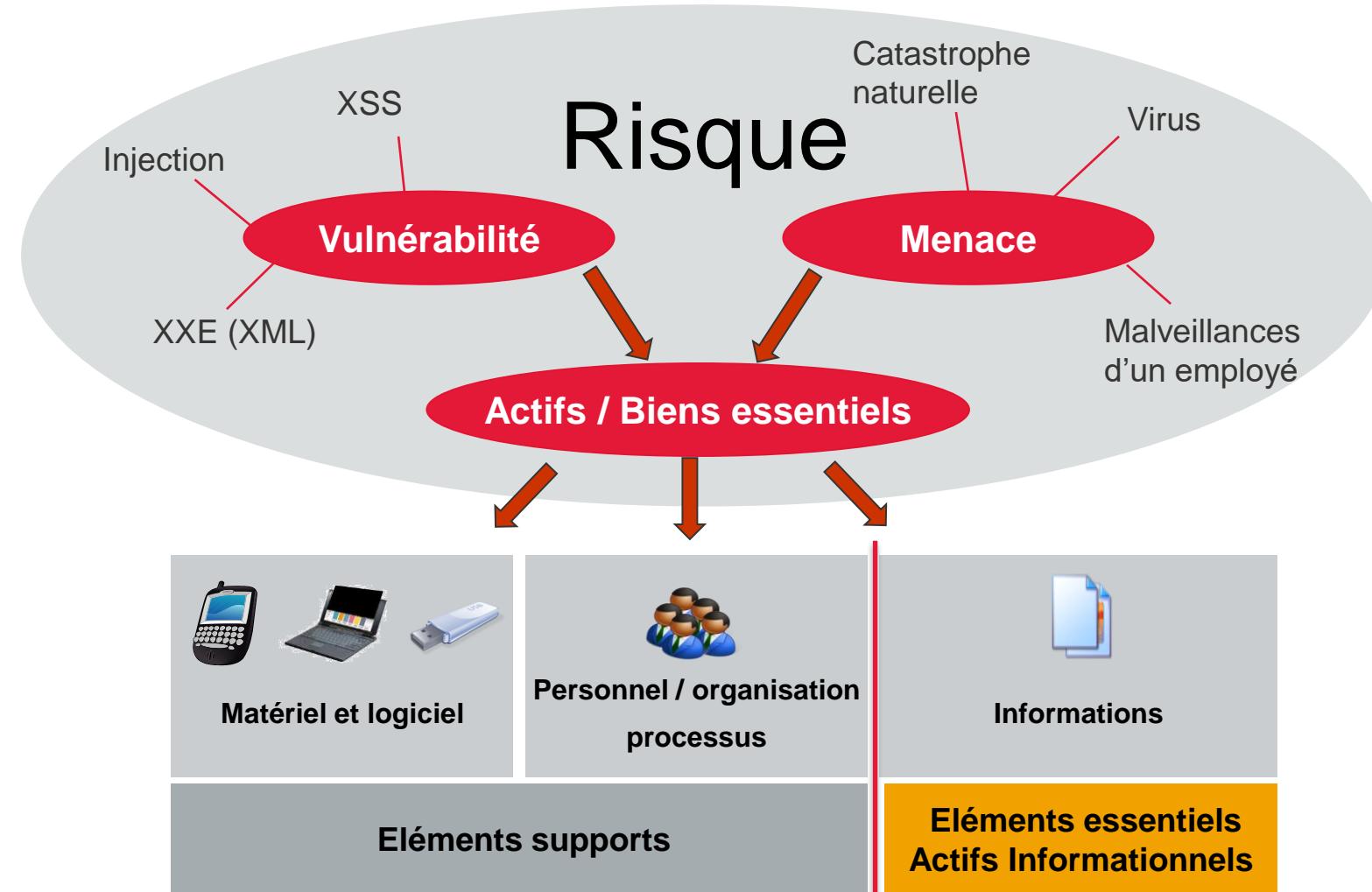
## Vulnérabilité

- **Faiblesse d'un actif ou d'un groupe d'actifs** qui peut être exploitée par une menace

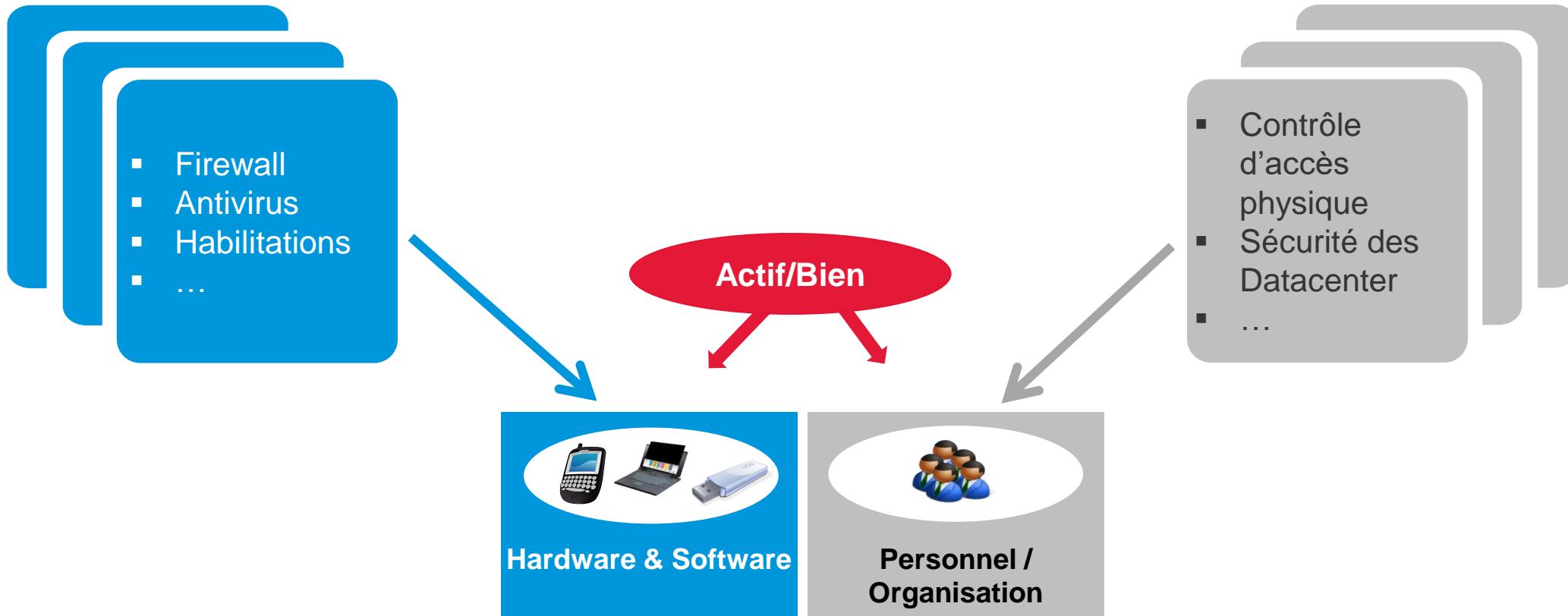
Exemple : Non suppression des accès au SI après le départ d'un employé



# Définition (simplifiée) du risque

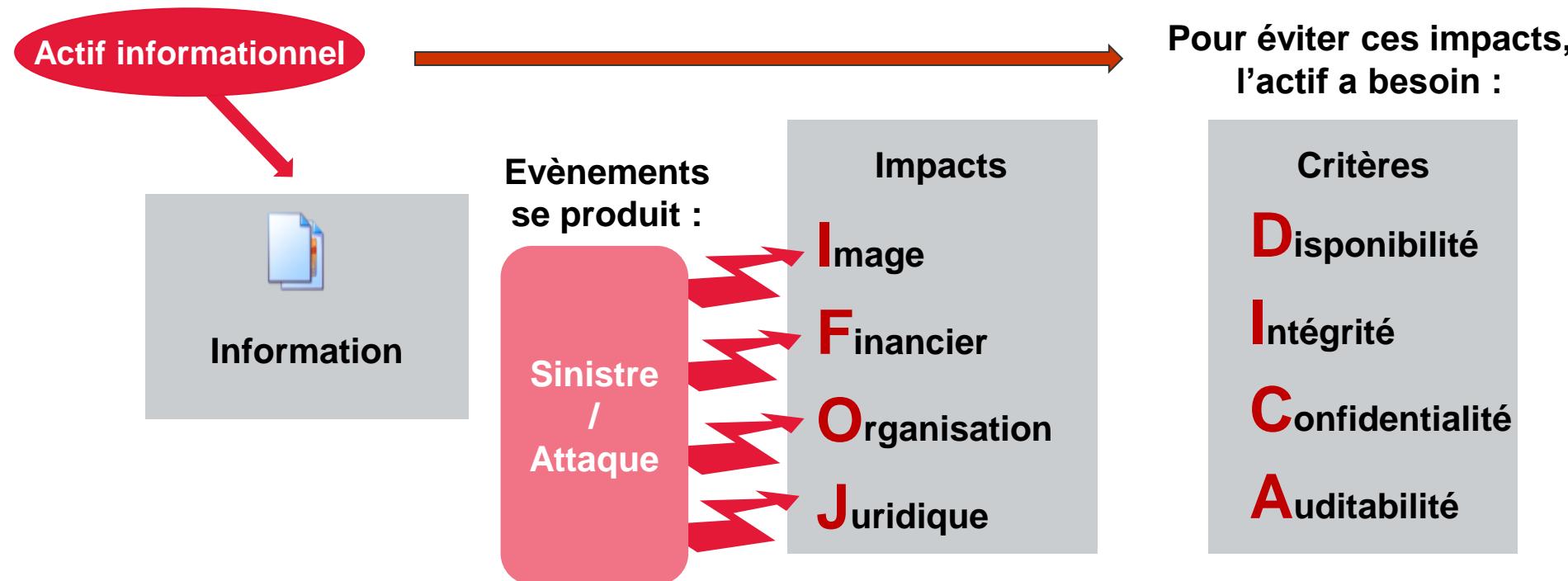


Les dispositifs de protection sont orientés éléments supports



# Besoin de sécurité sur les actifs

La notion de **besoin de sécurité** est attachée aux **actifs informationnels**. Le besoin peut s'exprimer **selon une classification** suivant des critères **définis dans la méthode d'appréciation des risques**

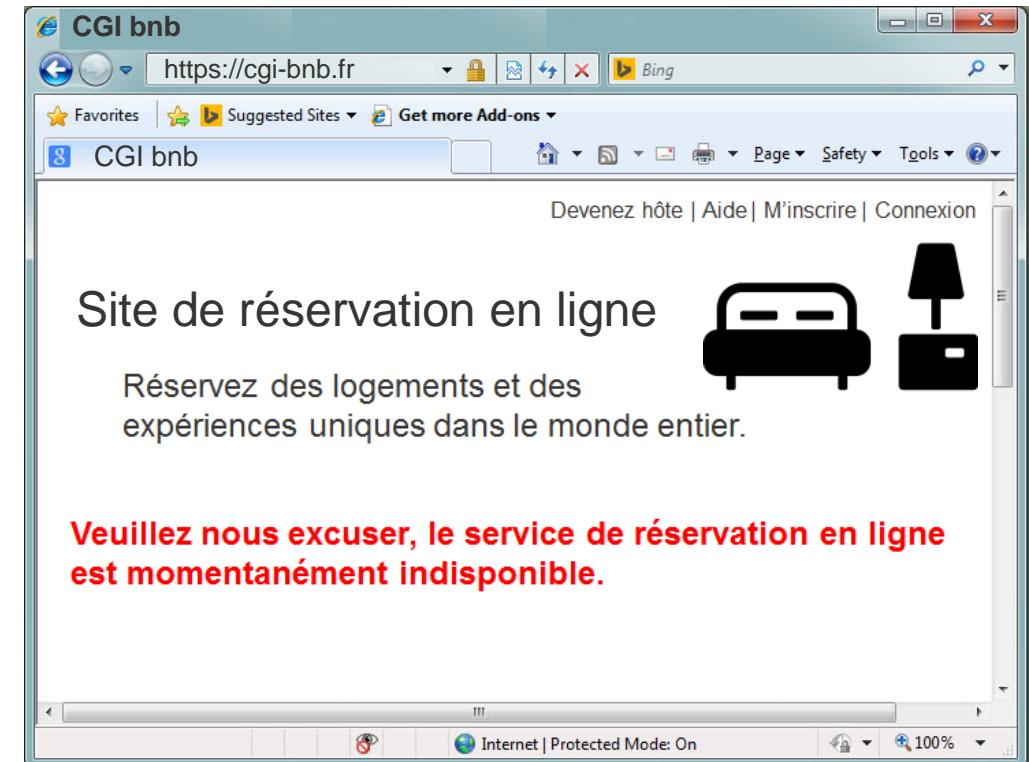


**Le site de réservation de chambre en ligne « CGI-bnb » vient de subir une attaque informatique :**

- Quel est l'actif ?
- Quelle type de vulnérabilité est exploitée ?
- A quel type de menace fait-on face ?
- Quel scénario de menace s'est produit ?
- Que redoute l'entreprise ?
- Quel est l'impact probable ?

**Quelles mesures permettrait de réduire la fréquence d'occurrence de l'évènement ?**

**Quelles mesures permettraient de réduire les impacts ?**



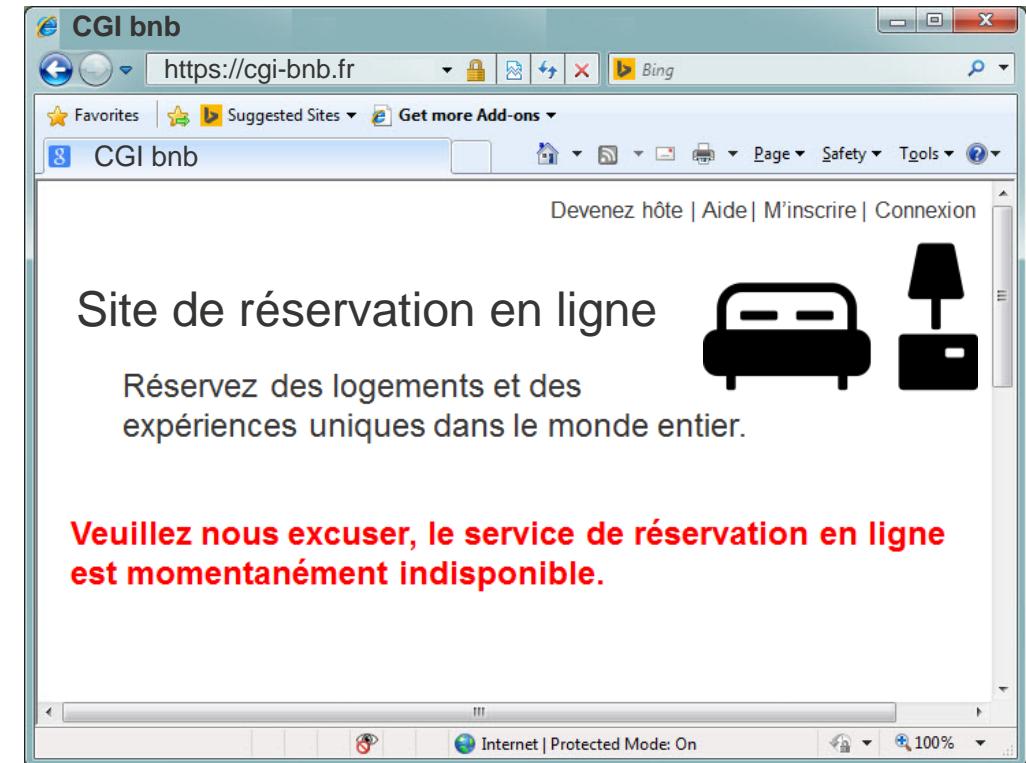
# Cas pratique

**Le site de réservation de chambre en ligne « CGI-bnb » vient de subir une attaque informatique :**

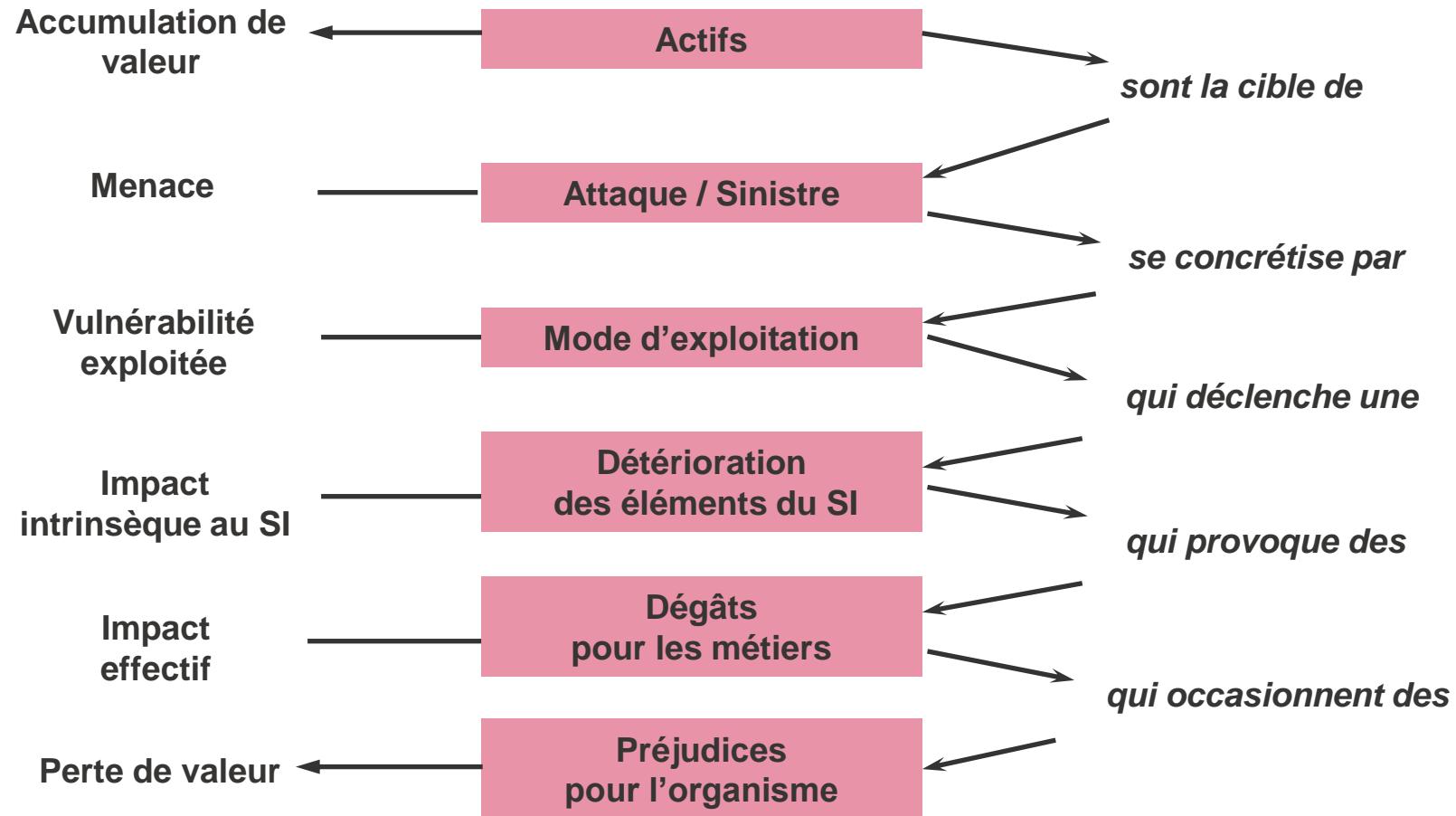
- L'actif : Plateforme de réservation en ligne
- La vulnérabilité : Absence de contrôle des données saisies permettant une Injection SQL
- Menace : Détournement de l'interface de connexion au site de réservation
- Scénario de menace : L'attaquant réalise une injection SQL sur le site Web de réservation
- Evènement redouté: Arrêt du site Web
- Impact : Perte financière de x heures / jours

**Quelles mesures permettrait de réduire la fréquence d'occurrence de l'évènement ?**

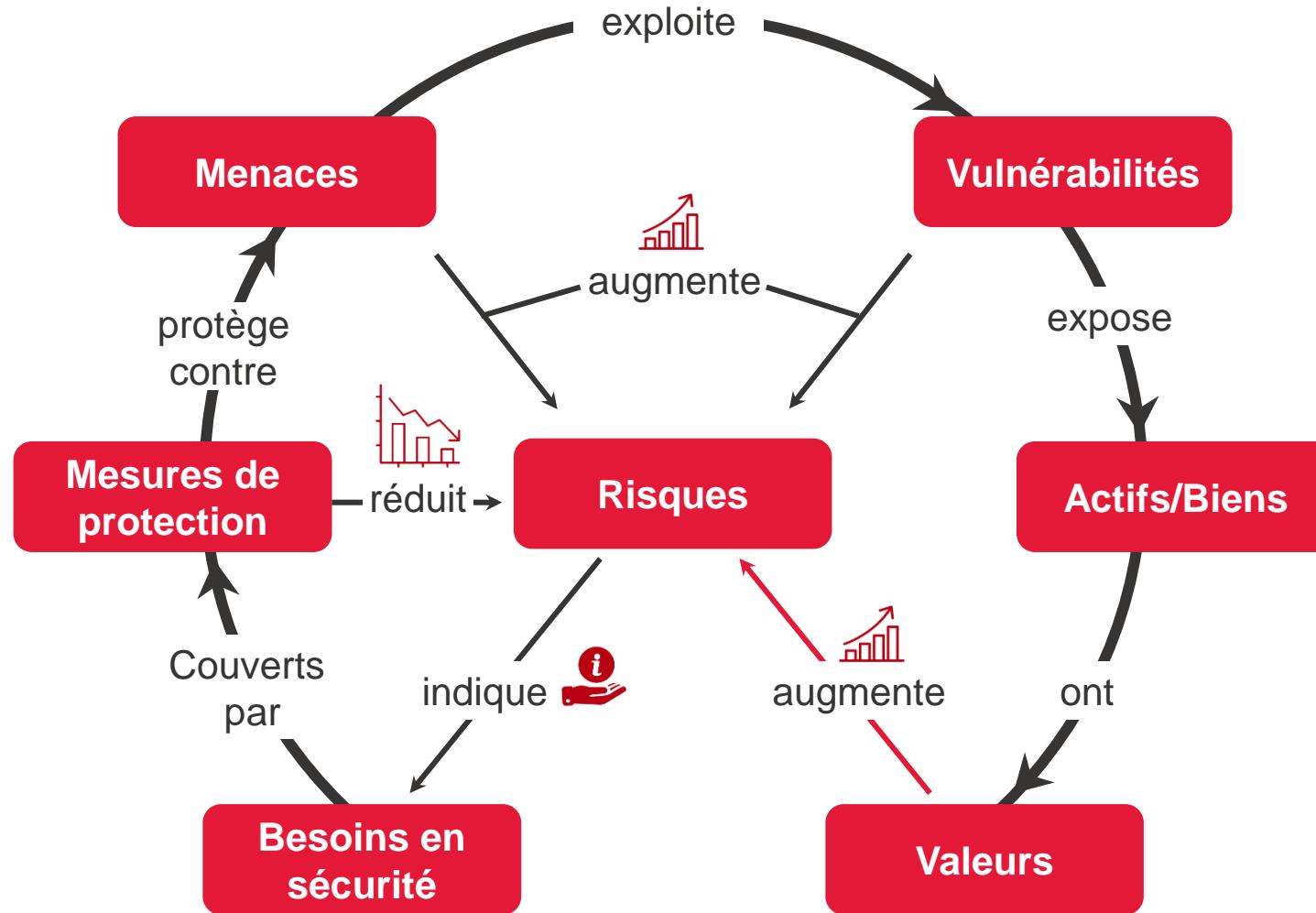
**Quelles mesures permettraient de réduire les impacts ?**



# Identification des scénarios de risque



# Relations dans le traitement du risque



# Exemples sur les critères d'évaluation

Niveau	Impact d'image	Impact financier	Impact juridique	Impact sur l'activité
<i>Peu significatif</i>	<b>1</b> Faible perte de crédibilité perçue par les parties prenantes et/ou l'opinion publique.	1,5 M€ de CA 150 000 € de PF	Condamnation(s) civile(s) isolée(s).	Impact peu significatif sur l'activité.
<i>Gênant</i>	<b>2</b> Réclamations potentielles et lancement de débats publics.	15 M€ de CA 1,5 M€ de PF	Nombreuses condamnations civiles.	Incident significatif occasionnant une gêne dans le fonctionnement de l'entreprise.
<i>Grave</i>	<b>3</b> Perte de confiance des clients pouvant entraîner des contentieux.	150 M€ de CA 15 M€ de PF	Non respect législatif, réglementaire ou contractuel entraînant l'arrêt d'une activité.	Perturbation ayant des effets à court et moyen terme.
<i>Critique</i>	<b>4</b> Atteinte grave à la réputation de l'entreprise et perte massive de clients.	1 000 M€ de CA 100 M€ de PF	Condamnation pénale engageant la personne morale.	Forte perturbation de l'activité ayant des conséquences à long terme.

Tableau de synthèse des impacts					
Niveau	Impact d'image	Impact financier	Impact juridique	Impact sur l'activité	
Peu significatif	1	Faible perte de crédibilité perçue par les parties prenantes et/ou l'opinion publique.	1,5 M€ de CA 150 000 € de PF	Condamnation(s) civile(s) isolée(s).	Impact peu significatif sur l'activité.
Gênant	2	Réclamations potentielles et lancement de débats publics.	15 M€ de CA 1,5 M€ de PF	Nombreuses condamnations civiles.	Incident significatif occasionnant une gêne dans le fonctionnement de l'entreprise.
Grave	3	Porte de confiance des clients pouvant entraîner des contentieux.	150 M€ de CA 15 M€ de PF	Non respect législatif, réglementaire ou contractuel entraînant l'arrêt d'une jeu ou d'une activité.	Perturbation ayant des effets à court et moyen terme.
Critique	4	Atteinte grave à la réputation de l'entreprise et perte massive de clients.	1 000 M€ de CA 100 M€ de PF	Condamnation pénale engageant la personne morale.	Forte perturbation de l'activité ayant des conséquences à long terme.

Tableau de synthèse des probabilités				
Niveau	Probabilité d'apparition du risque	Dificulté à renier l'attaque	Matrice de gravité des risques	
Probabilité	1	Faible – événement dont l'apparition sur les trois périodes annuelles est jugé peu probable	Dificulté à renier l'attaque	
	2	Moyen – événement dont l'apparition sur les trois périodes annuelles est jugé probable	Moyenne – reproduction nécessitant des moyens importants et/ou un fort niveau de compétences	
	3	Fort – événement dont l'apparition sur les trois périodes annuelles est jugé très probable	Moyenne – reproduction nécessitant peu de moyens importants, ou nécessitant peu de compétences, ou une compétence interne	
	4	Très fort – facile à reproduire sans compétence particulière, si moyen, si compété	Fort – facile à reproduire sans compétence particulière, si moyen, si compété	

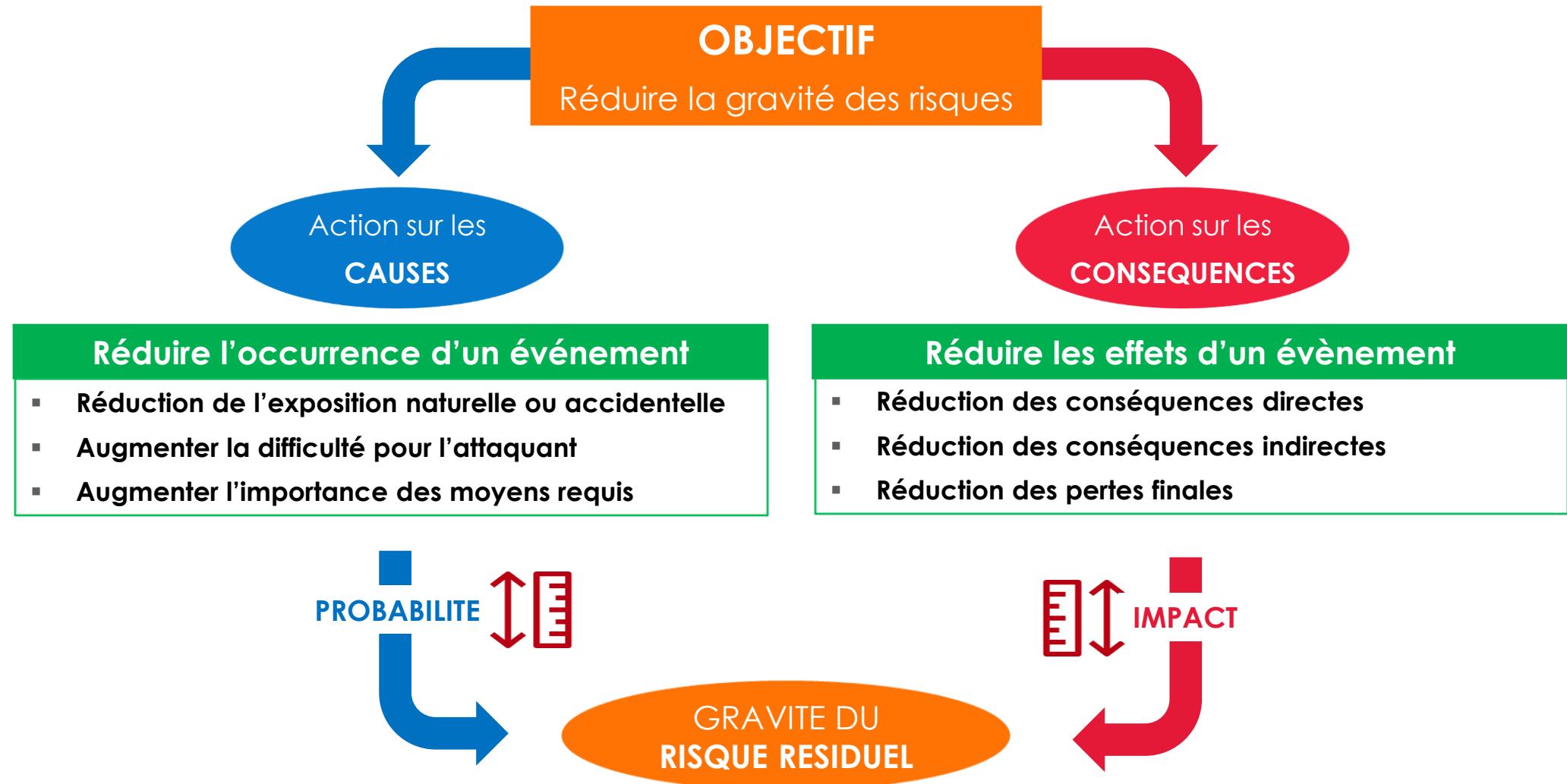
Echelle des besoins de sécurité				
Niveau	Disponibilité	Intégrité	Confidentialité	Transférabilité
1	Indisponibilité au sein des systèmes compris entre 2 secondes et 1 mois.	La partie d'intégrité n'a pas d'incident si elle peut être <u>réinitialisée</u> à posteriori.	L'accès ne doit pas être divulgué au-delà de la FAU (i.e. divulgation au public).	Toute action doit être tracée, mais sans impératilité.
2	Indisponibilité au sein des systèmes compris entre 2 jours et 2 semaines ou indisponibilité de 4h répétée plusieurs fois dans l'année.	La partie d'intégrité n'a pas d'incident si elle peut être <u>réinitialisée</u> à posteriori.	L'accès ne doit pas être divulgué au-delà de catégories particulières de personnes autorisées au sein de la FAU.	Toute action doit être tracée avec impératilité fonctionnelle des actions principales.
3	Indisponibilité au sein des systèmes compris entre 24 heures et 2 jours ou indisponibilité de 4h répétée plusieurs fois dans l'année.	L'accès peut ne pas être intégré dans un statut transitoire si les usagers peuvent être déconnectés et corrigés à temps.	L'accès ne doit pas être divulgué au-delà de personnes explicitement habilitées (fonctionnellement).	Tous les accès doivent être tracés avec impératilité individuelle des actions principales uniquement.
4	Indisponibilité au sein des systèmes inférieure à 24 heures ou indisponibilité de 2h répétée plusieurs fois dans l'année.	L'accès doit être intégré pendant toute sa période d'utilisation et ultérieurement.	L'accès ne doit pas être divulgué au-delà de personnes explicitement habilitées (non fonctionnellement).	Toute action doit être tracée avec impératilité individuelle.

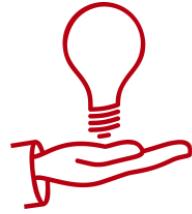
Appréciation du niveau de confiance				
Niveau de confiance	Méthode d'évaluation des contrôles et/ou des mesures utilisées			
1 – Déclaratif	La méthode a consisté à s'appuyer sur une déclaration des parties prenantes quant à l'application des contrôles et/ou la mise en place des mesures de sécurité et à leur efficacité.			
2 – Documenté	La méthode a consisté à vérifier sur la base de documentation la présence de contrôle et/ou de mesure de sécurité et de leur efficacité.			
3 – Testé	La méthode a consisté à tester les contrôles et/ou les mesures de sécurité pour vérifier leur application et leur efficacité.			

Appréciation du niveau de maîtrise				
Niveau de maîtrise	Critères caractérisant le niveau			
1 – Non maîtrisé	Des mesures de sécurité manquantes, soit inefficaces ou déficientes ce qui montre que le risque n'est pas parfaitement couvert. Contrôles non appliqués.			
2 – Mal maîtrisé	Mesures de sécurité largement insuffisantes pour traiter le risque. Contrôles non appliqués.			
3 – Reasonnablement maîtrisé	Toutes les mesures raisonnables ont été mises en œuvre, mais celle-ci ne permettent pas de couvrir complètement le risque pour autant. Contrôles appliqués partiellement.			
4 – Maîtrisé	Il n'existe pas de mesures de sécurité manquantes ou inefficaces, le risque est complètement couvert. Contrôles appliqués et formalisés.			



# Agenda



## Principes du SMSI

- Introduction
- Définition du Système de Management
- Introduction aux normes ISO27001 / ISO27002



## La Gestion de Risque

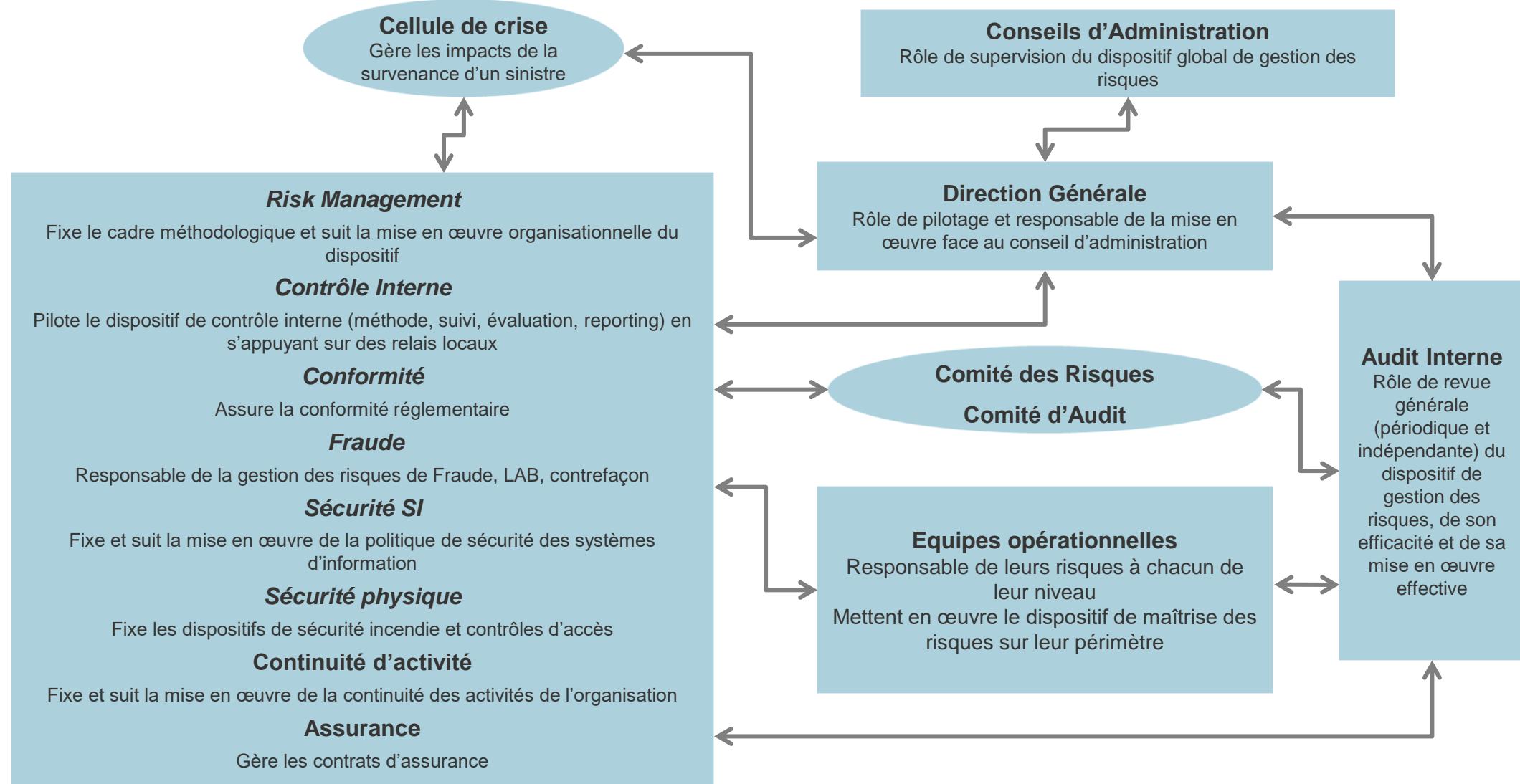
- Principes de la gestion des risques
- ISO27005 / ISO31000
- Application d'EBIOS à l'identification des risques de l'entreprise



## La mise en œuvre pratique

- Plan
- Do
- Check
- Act

# Organisation type de la Gestion des Risques dans une organisation



# Organisation type de la Gestion des Risques dans une organisation – 3 lignes de défense



Les lignes directrices d'une appréciation des risques sont décrites par les normes ISO 27001 et ISO 31000

**ISO 27001:2013**



< 1 page

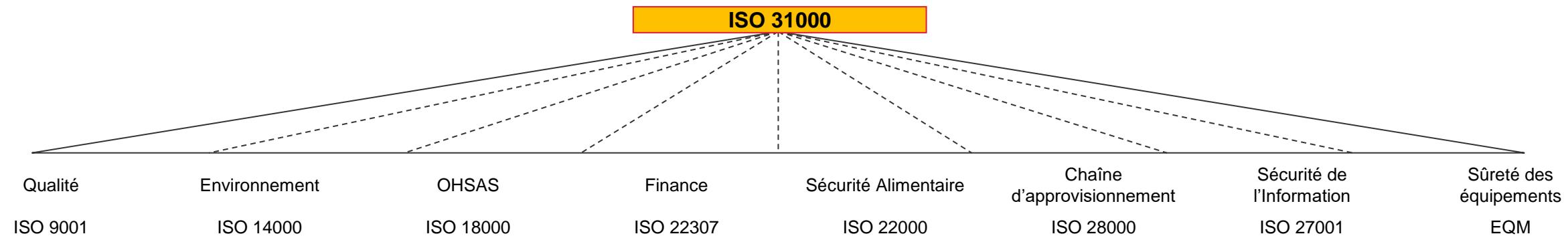
**ISO 31000**



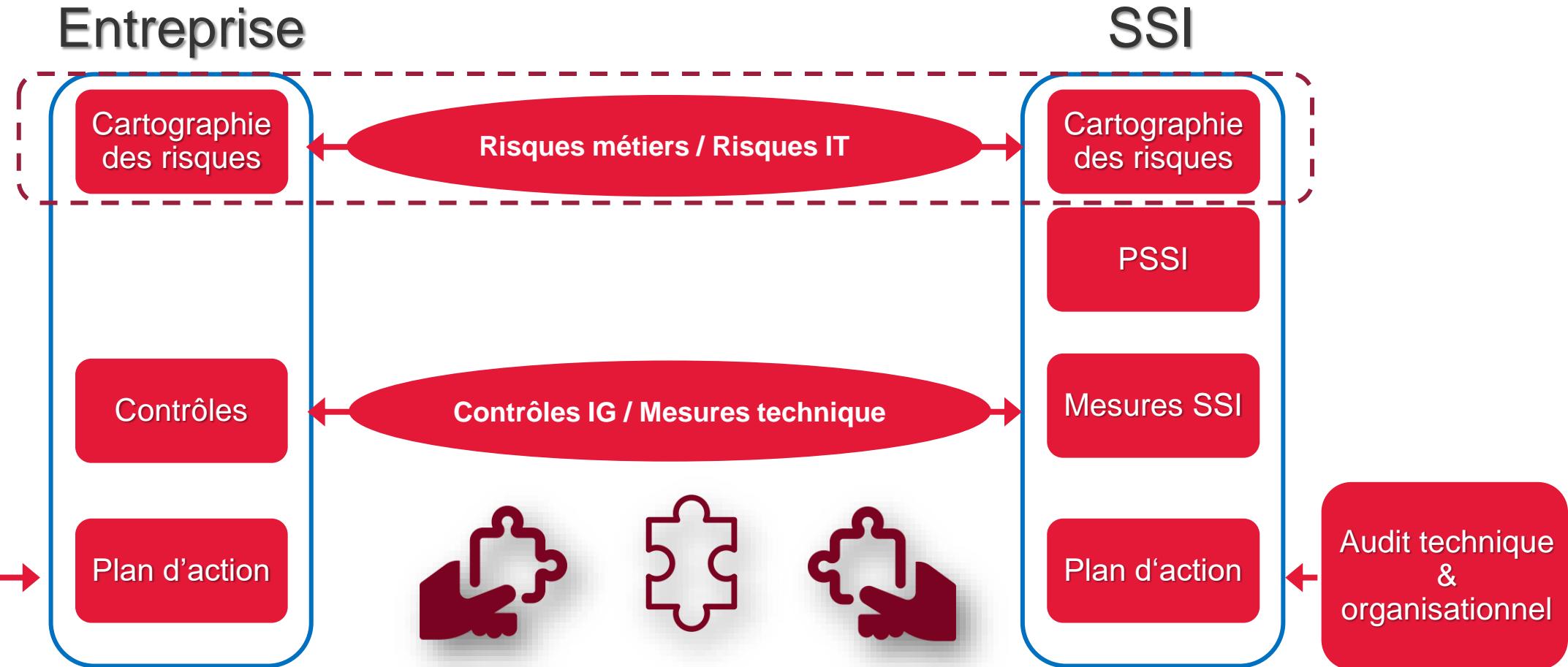
~18 pages

Cette norme internationale fournit des principes génériques et des lignes directrices pour la mise en œuvre efficace du management du risque.

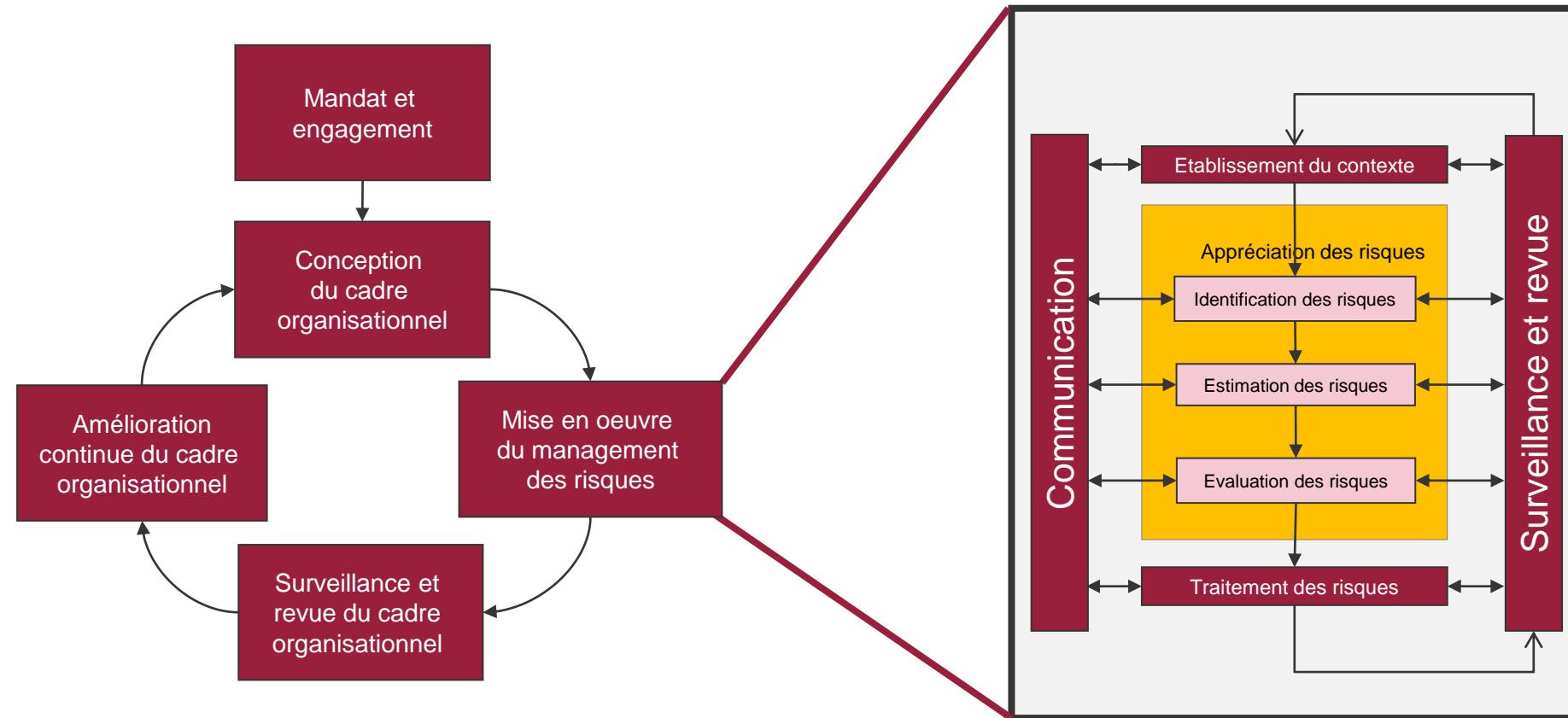
- Elle est applicable à **toute organisme ou partie**, indépendamment de son secteur et de sa taille
- Elle est **adaptable aux besoins spécifiques**, contexte, structure de l'organisme concerné
- Elle vise à **harmoniser les processus de management du risque** dans les normes existantes et futures
- Elle **n'a pas pour mission** d'être utilisée pour des besoins de **certification et/ou enregistrements**



# La SSI est partie intégrante d'un plan de maîtrise plus global



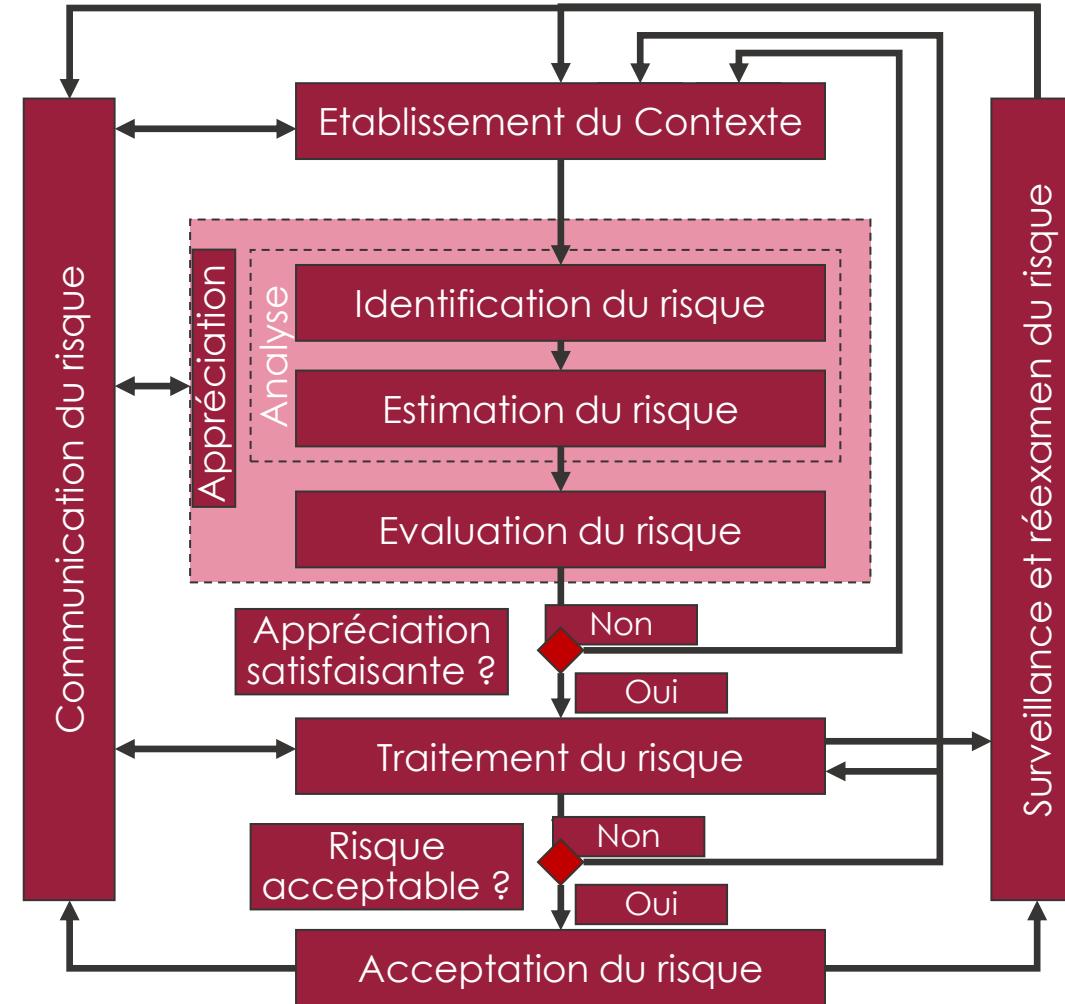
## Principes de management des risques



# Processus de gestion du risque



ISO 27005



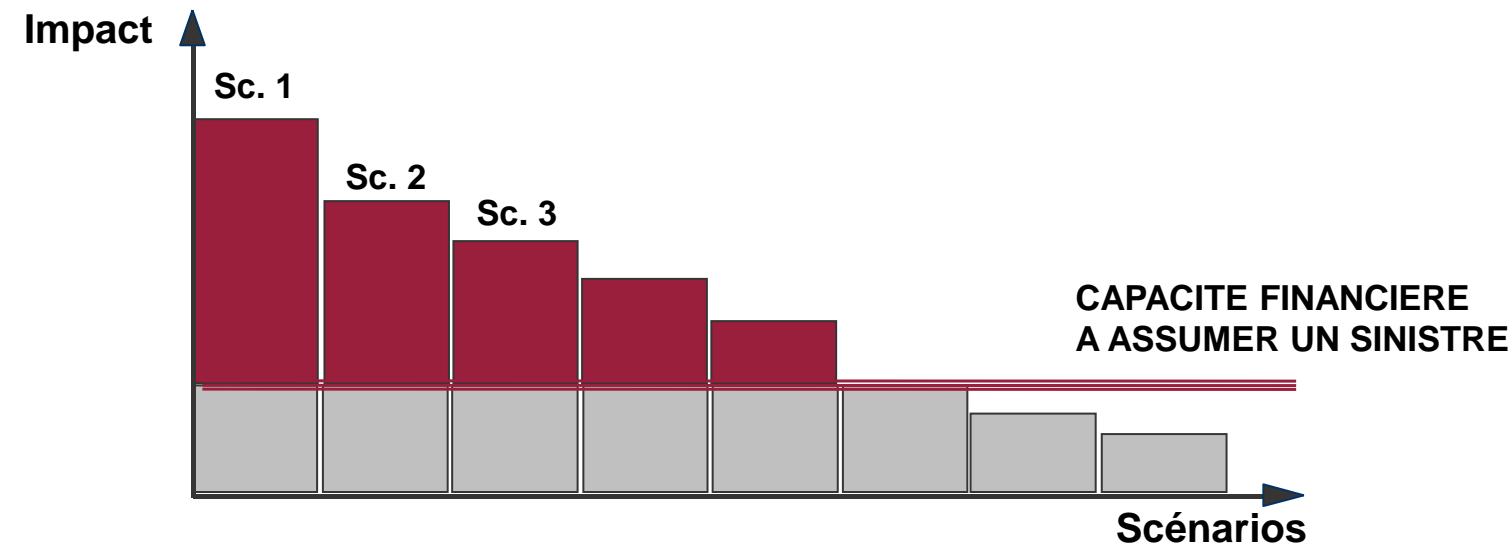
**La gestion des risques** est le processus par lequel les risques sont évalués en utilisant une **approche systématique** qui les identifie et les organise par **priorité** et qui met ensuite en place les **stratégies** permettant de les réduire

## L'approche comprend à la fois

- **L'identification et l'appréciation** des risques
- **La prévention** des problèmes potentiels
- **Le déploiement de moyens de détection et de réaction** aux agressions adaptés aux enjeux
- La mise en œuvre d'actions de correction visant à **limiter la possibilité de réapparition d'un problème** ou à en **limiter les conséquences potentielles**

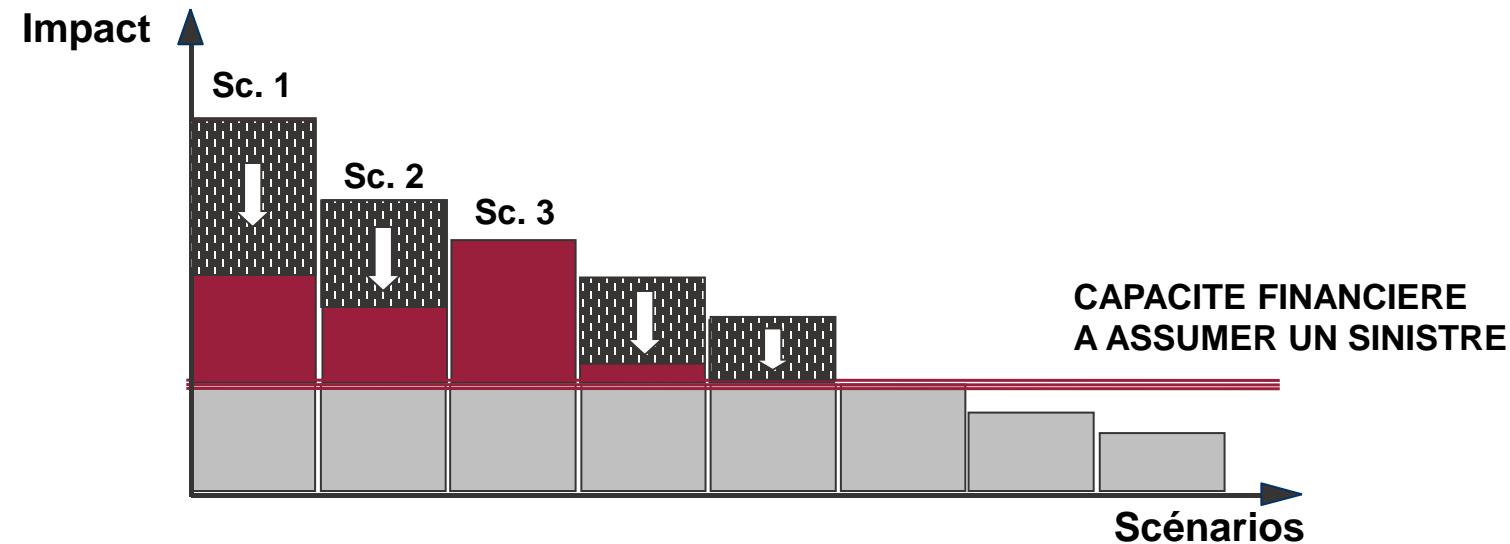
Comment trouver un **équilibre** entre les **risques encourus** par l'entreprise et les **sommes à investir pour se protéger** ?

## Identifier les risques :



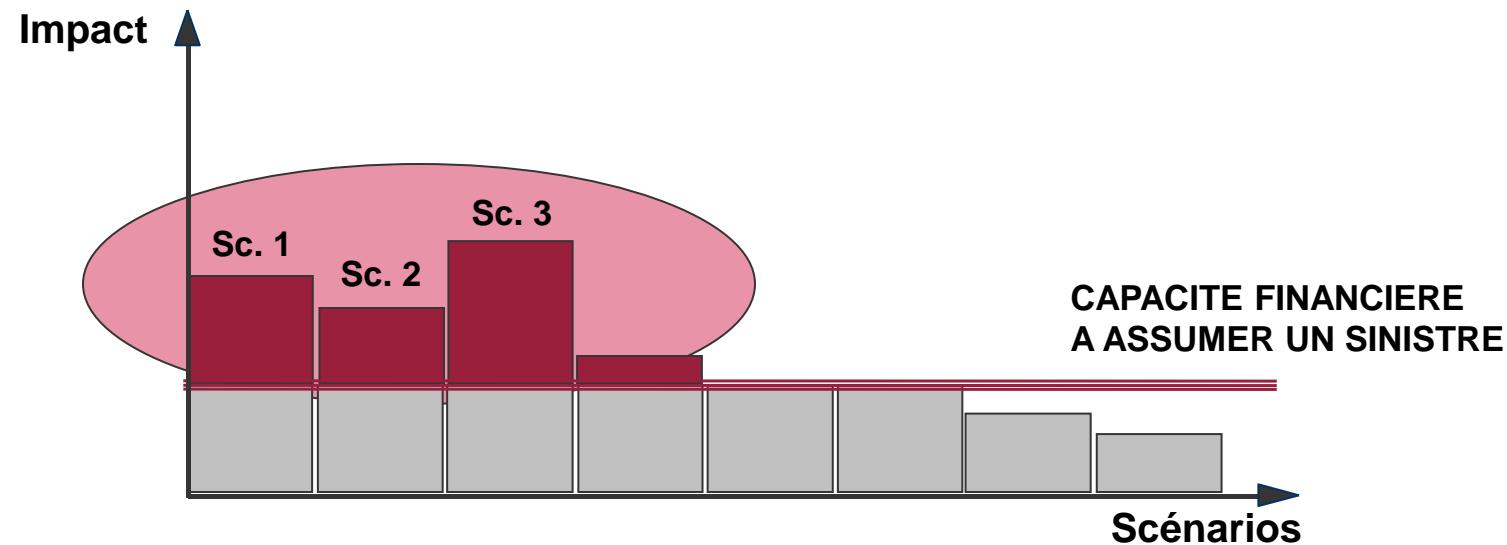
Comment trouver un **équilibre** entre les **risques encourus** par l'entreprise et les **sommes à investir pour se protéger** ?

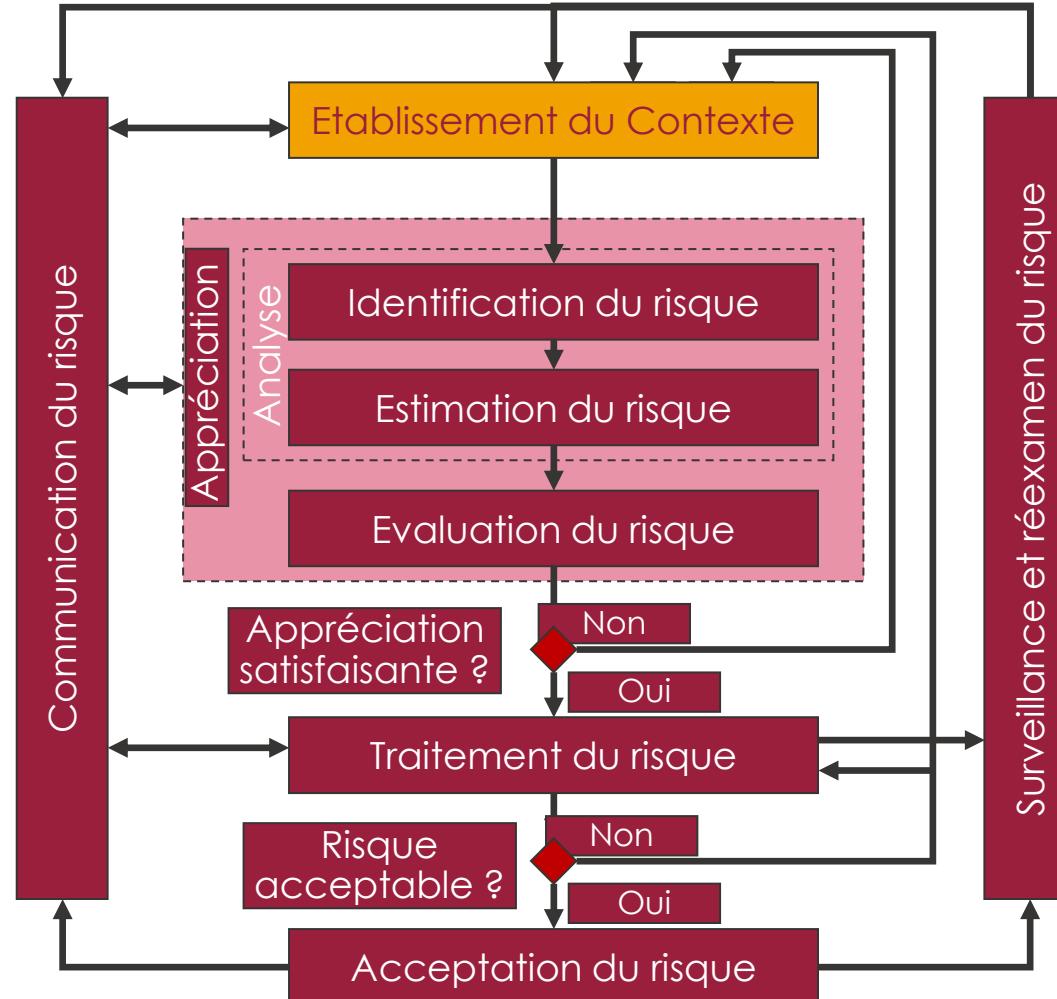
## Réduire les risques :



Comment trouver un **équilibre** entre les **risques encourus** par l'entreprise et les **sommes à investir pour se protéger** ?

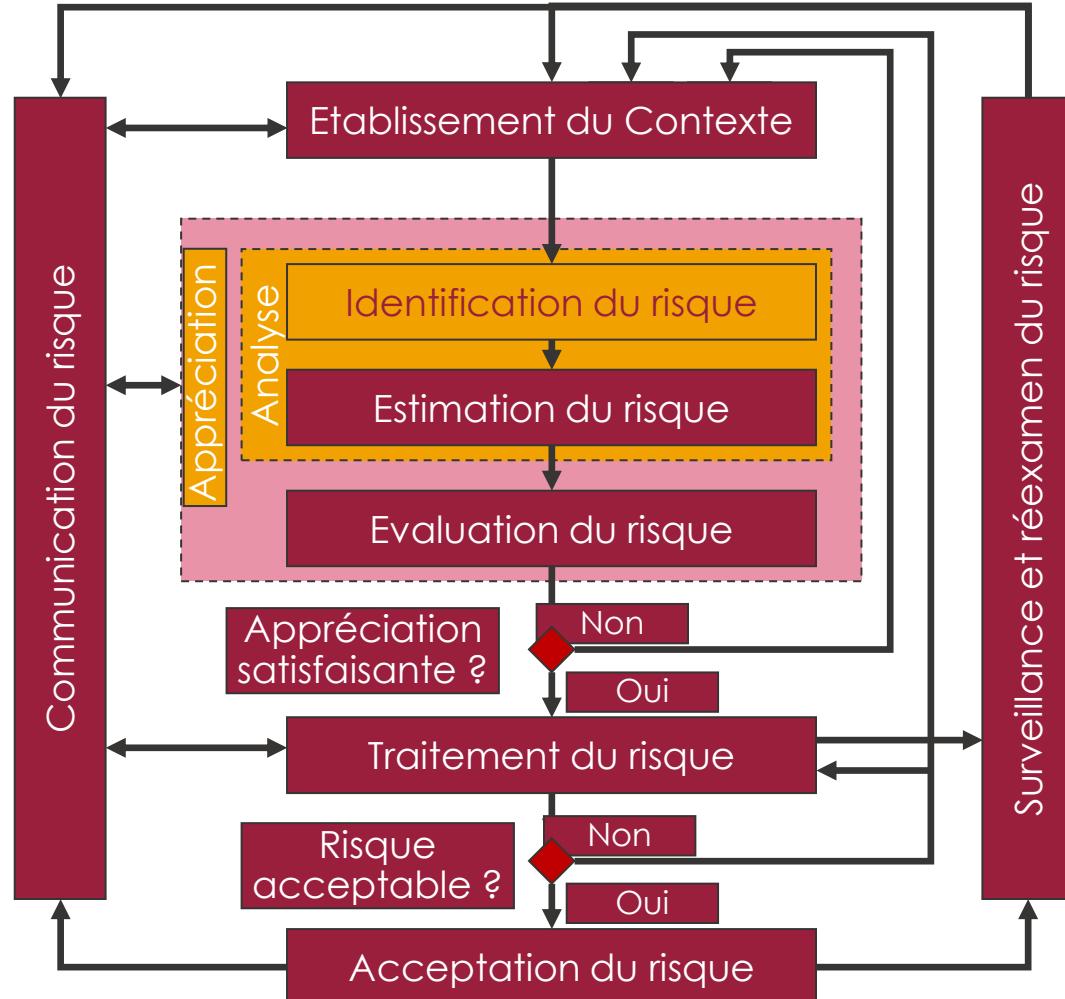
**Fiabiliser le système :**



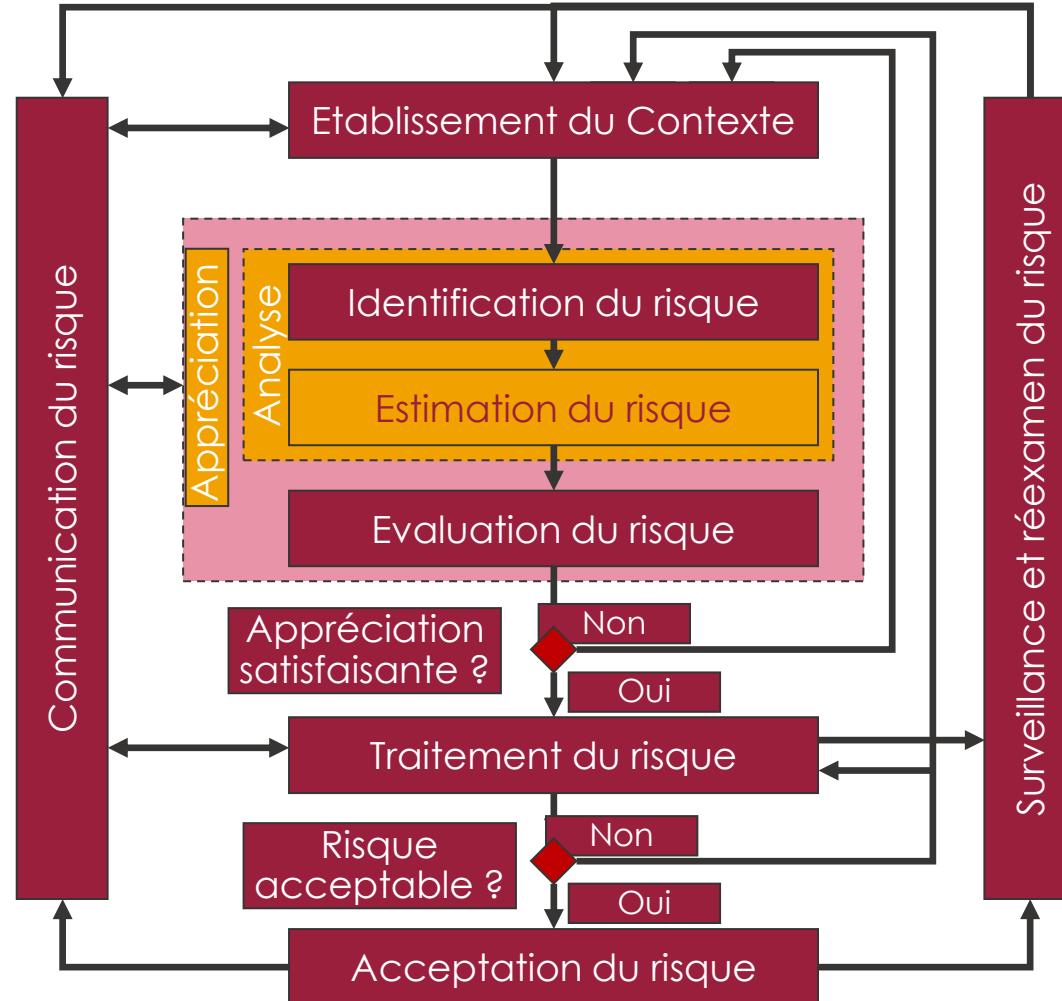


- Définir le périmètre.
- Définir les critères de base
  - Evaluation du risque : Disponibilité, Intégrité, Confidentialité, etc.
  - Impact : Image, Financier, Organisationnel, Juridique
  - Acceptation du risque
- Définir les ressources de l'appréciation des risques
  - Organisationnelle
  - Financières

# Points clés ISO 27005 : « Identification du risque »



- Identifier les actifs
- Identifier les menaces
- Identifier les mesures de sécurité existantes
- Identifier les vulnérabilités
- Identifier les conséquences



- Estimer des impacts
- Estimer de la probabilité d'occurrence des scénarios
- Estimer le niveau de risque

Ces estimations peuvent être :

- Qualitatives
- Quantitatives

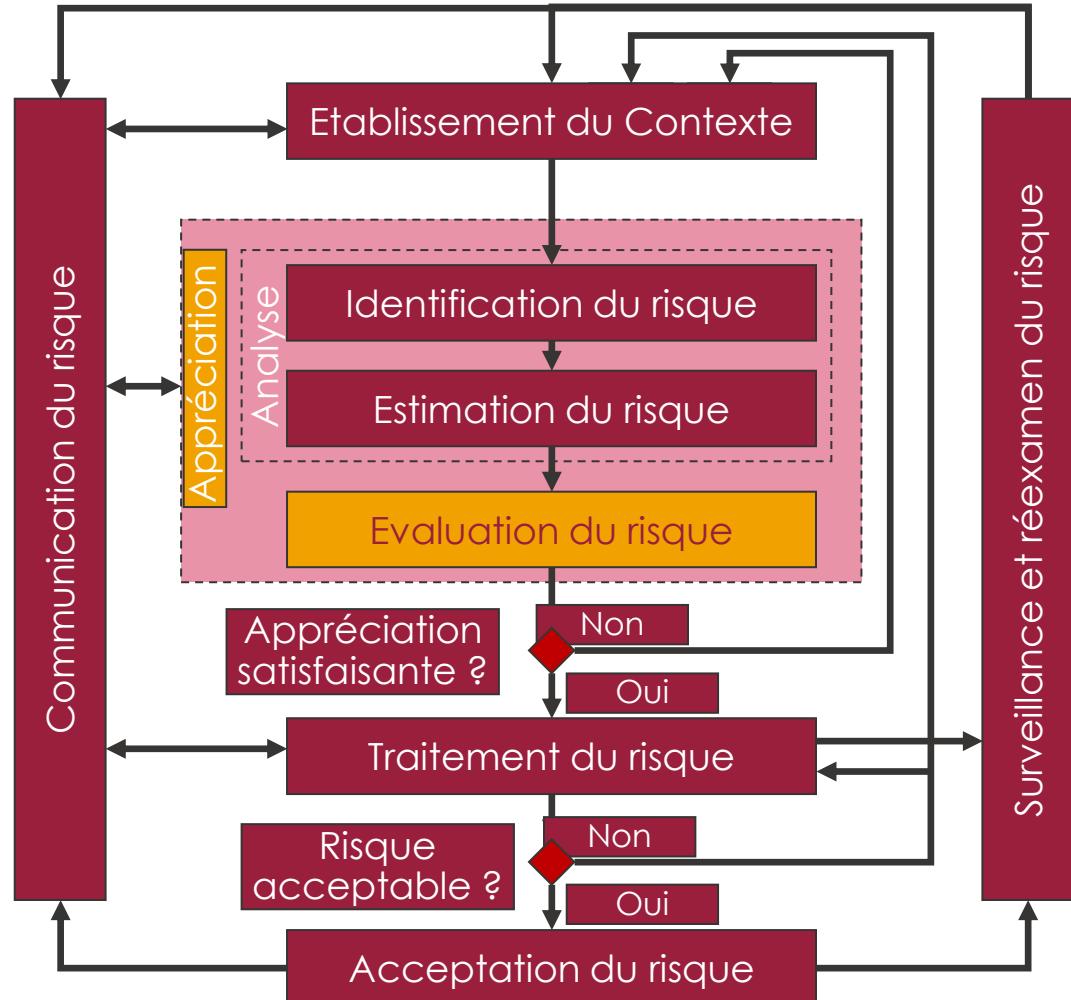
Le terme "**propriétaire**" identifie une personne ou une entité ayant accepté la **responsabilité du contrôle de la production, de la mise au point, de la maintenance, de l'utilisation et de la protection des biens**. Ce terme ne signifie pas que la personne jouit à proprement parler de droits de propriété sur le bien.

# Estimation du risque

Tableau de synthèse des impacts					
Niveau		Impact d'image	Impact financier	Impact juridique	Impact sur l'activité
<i>Peu significatif</i>	1	Faible perte de crédibilité perçue par les patients et/ou l'opinion publique.	1,5 M€ de CA 150 000 € de PF	Condamnation(s) civile(s) isolée(s).	Impact peu significatif sur l'activité.
<i>Gênant</i>	2	Réclamations potentielles et lancement de débats publics.	15 M€ de CA 1,5 M€ de PF	Nombreuses condamnations civiles.	Incident significatif occasionnant une gêne dans le fonctionnement de l'entreprise.
<i>Grave</i>	3	Perte de confiance des patients pouvant entraîner des contentieux.	150 M€ de CA 15 M€ de PF	Non respect législatif, réglementaire ou contractuel entraînant l'arrêt d'un jeu ou d'une activité.	Perturbation ayant des effets à court et moyen terme.
<i>Critique</i>	4	Atteinte grave à la réputation de l'hôpital, mort de patients.	1 000 M€ de CA 100 M€ de PF	Condamnation pénale engageant la personne morale.	Forte perturbation de l'activité ayant des conséquences à long terme.

Échelle des besoins de sécurité				
Niveau	Disponibilité	Intégrité	Confidentialité	Traçabilité
1	Indisponibilité maximum comprise entre 2 semaines et 1 mois.	La perte d'intégrité n'a pas d'incidence si elle peut être <u>détectée a posteriori</u> .	L'actif ne doit pas être divulgué en dehors de l'organisme (i.e. divulgation au public).	Toute action doit être tracée, mais sans imputabilité.
2	Indisponibilité maximum comprise entre 2 jours et 2 semaines ou indisponibilité de 8h répétée plusieurs fois dans l'année.	La perte d'intégrité n'a pas d'incidence si elle peut être <u>corrigée a posteriori</u> .	L'actif ne doit pas être divulgué en dehors de catégories particulières de personnels autorisés au sein de l'organisme.	Toute action doit être tracée avec imputabilité fonctionnelle des actions principales.
3	Indisponibilité maximum comprise entre 24 heures et 2 jours ou indisponibilité de 4h répétée plusieurs fois dans l'année	L'élément peut ne pas être intégré dans un état transitoire si les erreurs peuvent être détectées et corrigées à temps.	L'actif ne doit pas être divulgué en dehors de personnels explicitement habilités (fonctionnellement).	Les actions doivent être tracées avec imputabilité individuelle des actions principales uniquement.
4	Indisponibilité maximum inférieure à 24 heures ou indisponibilité de 2h répétée plusieurs fois dans l'année.	L'élément doit être intégré pendant toute sa période d'utilisation et ultérieurement.	L'actif ne doit pas être divulgué en dehors de personnels explicitement habilités (nominativement).	Toute action doit être tracée avec imputabilité individuelle.

# Points clés ISO 27005 : « Evaluation du risque »



- Comparer les niveaux de risques avec les critères d'évaluation et d'acceptation des risques
- Définir les priorités de traitement des risques

# Evaluation du risque

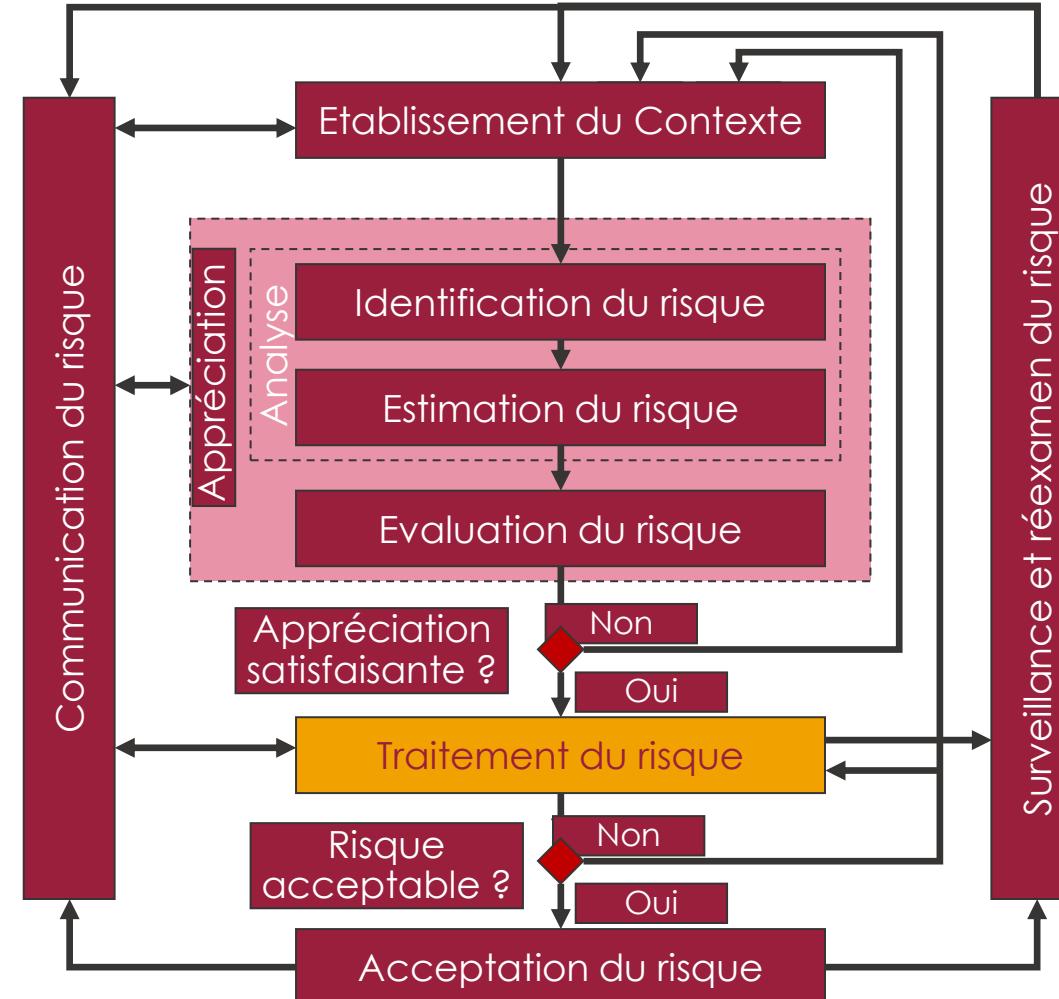
Tableau de synthèse des probabilités		
Niveau	Probabilité d'apparition du risque	Difficulté à mener l'attaque
1	Faible – évènement dont l'apparition sur les trois prochaines années est jugé peu probable	Difficile – reproduction nécessitant des moyens importants et/ou un fort niveau de compétences
2	Moyen – évènement dont l'apparition sur les trois prochaines années est jugé probable	Moyenne – reproduction ne nécessitant pas de moyens importants, ou nécessitant peu de compétences, ou une complicité interne
3	Fort – évènement dont l'apparition sur les trois prochaines années est jugé très probable	Forte – facile à reproduire sans compétence particulière, ni moyen, ni complicité

Gravité	Impact			
	1	2	3	4
Probabilité	1	1	3	5
	2	2	4	6
	3	3	5	7

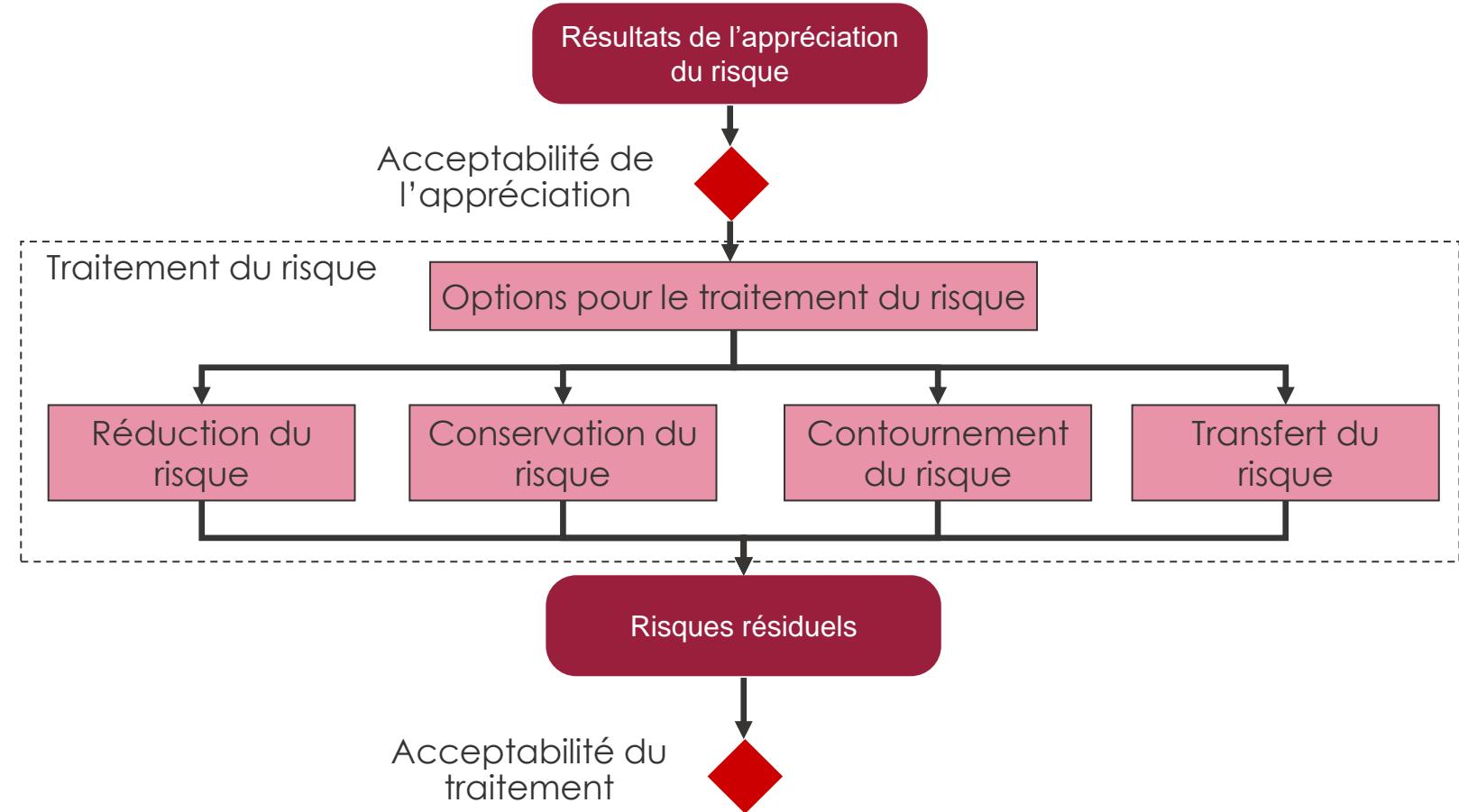
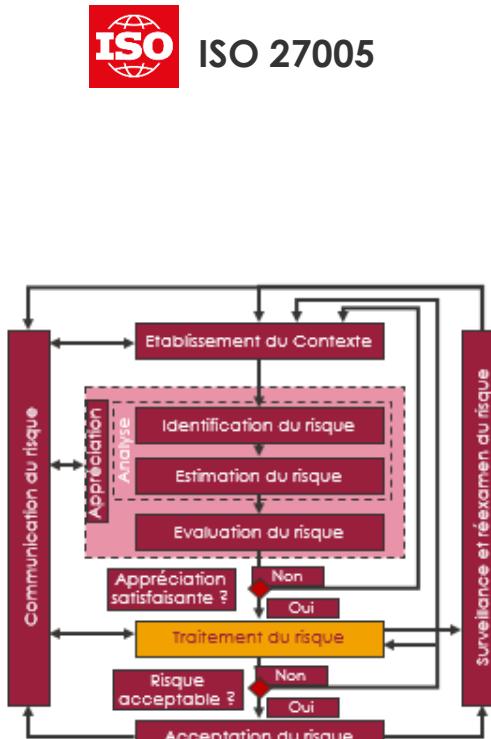
# Points clés ISO 27005 : « Traitement du risque » [1/6]



ISO 27005

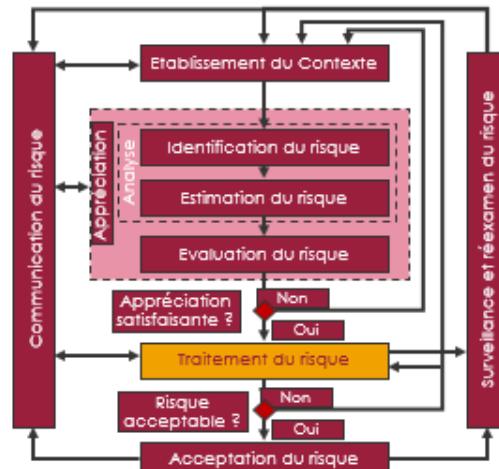


# Points clés ISO 27005 : « Traitement du risque » [2/6]

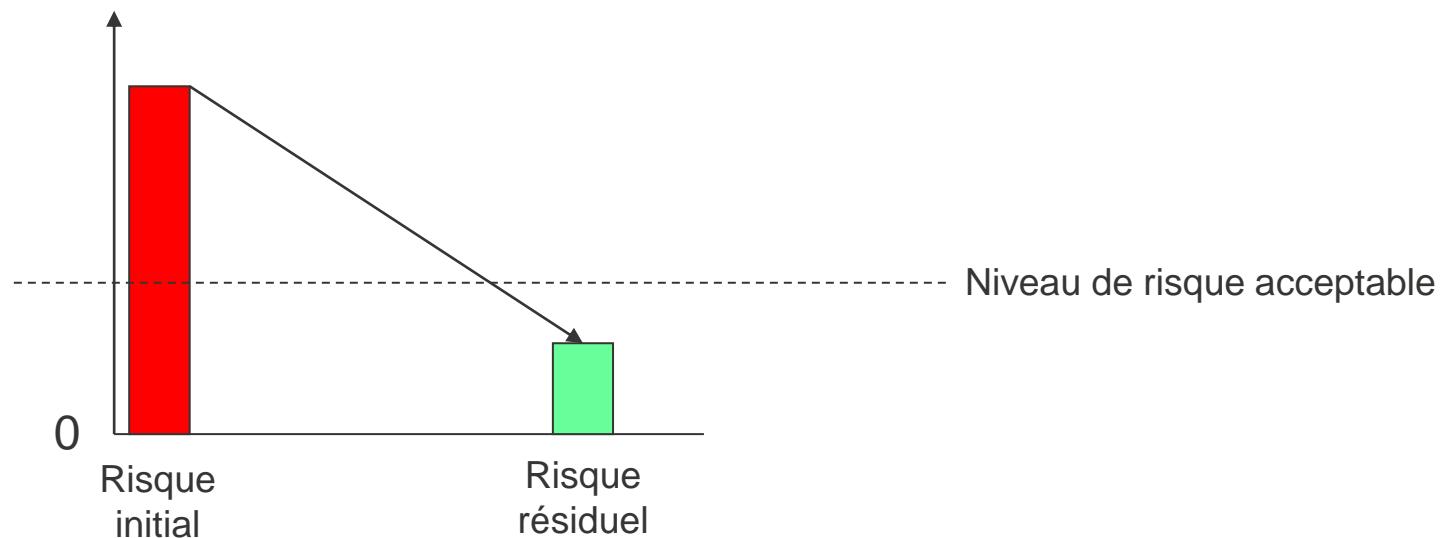


## Réduction du risque

- La réduction du risque passe par l'application de mesures de sécurité afin de réduire le risque à un niveau acceptable. Ces mesures peuvent être préventives (agir sur les menaces et les vulnérabilités) ou curatives (agir sur les conséquences)

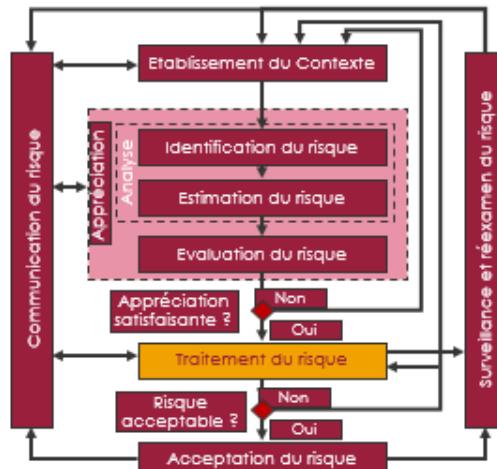


Niveau de risque

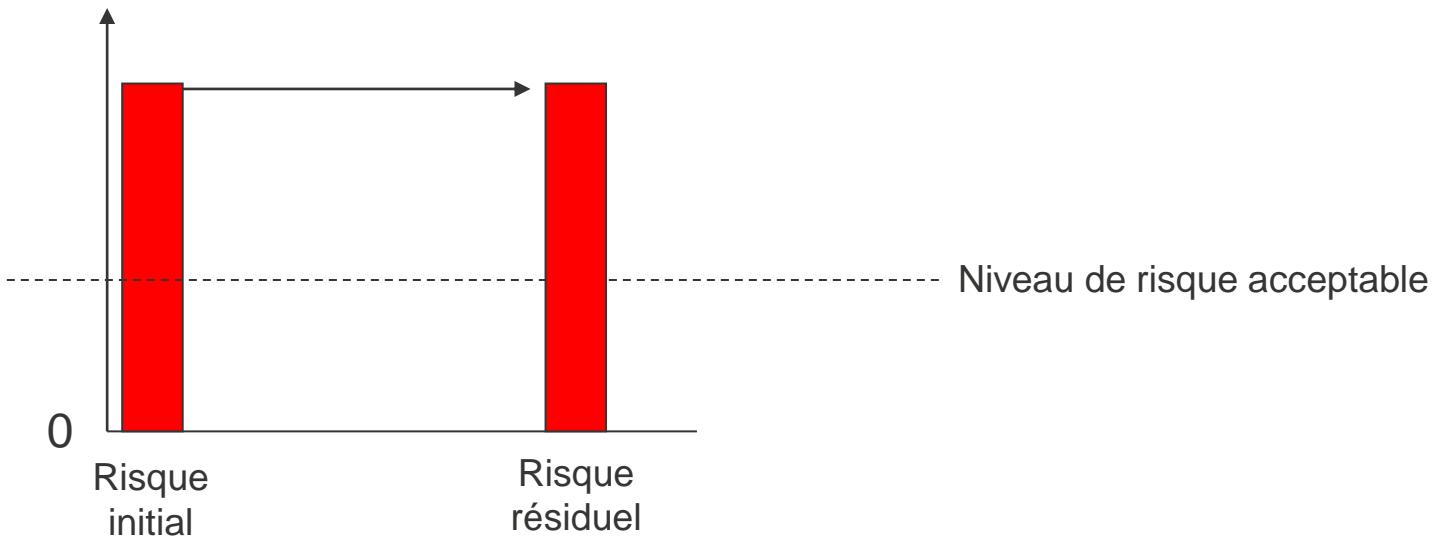


## Conservation du risque

- Même si le niveau risque est au-delà des critères d'acceptation du risque définis préalablement, il est possible de conserver un risque afin de répondre à des objectifs stratégiques

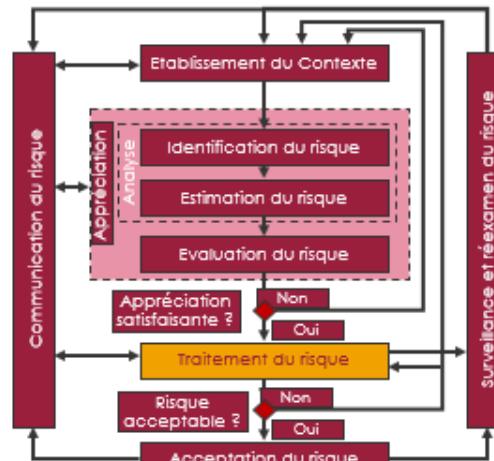


Niveau de risque

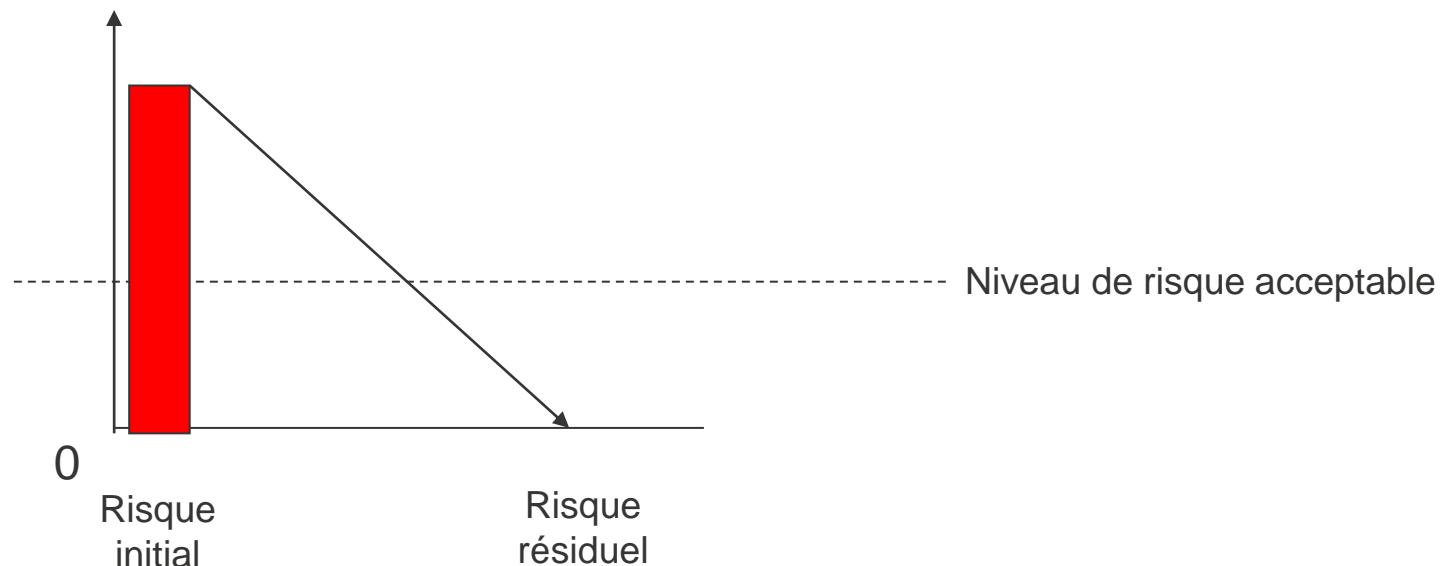


## Contournement du risque

- Quand le risque est trop important, la décision d'éviter le risque dans son ensemble peut être prise
  - Par exemple, afin d'éviter des catastrophes naturelles, en déplaçant les locaux

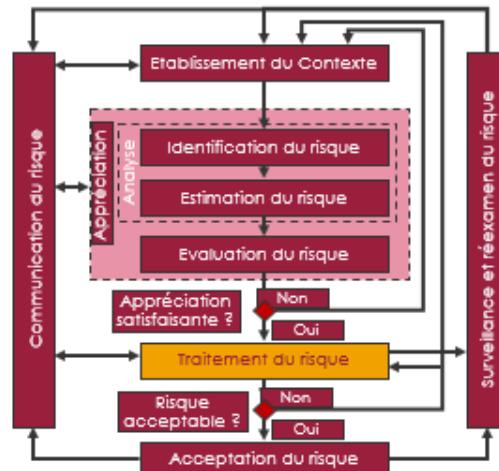


Niveau de risque

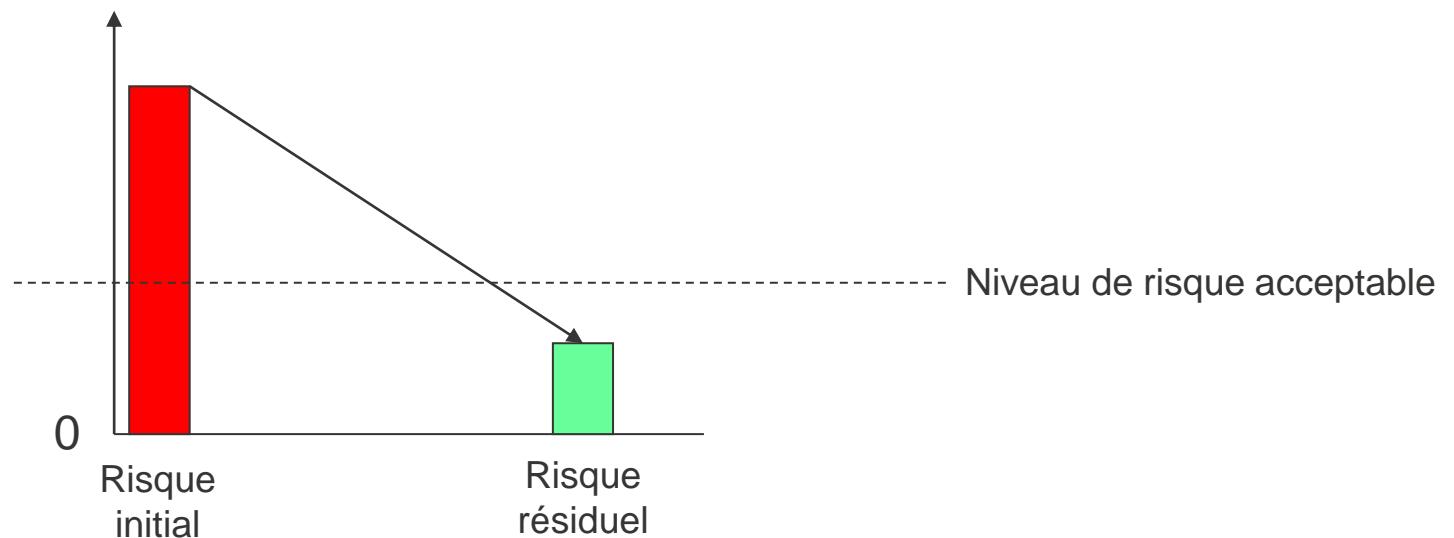


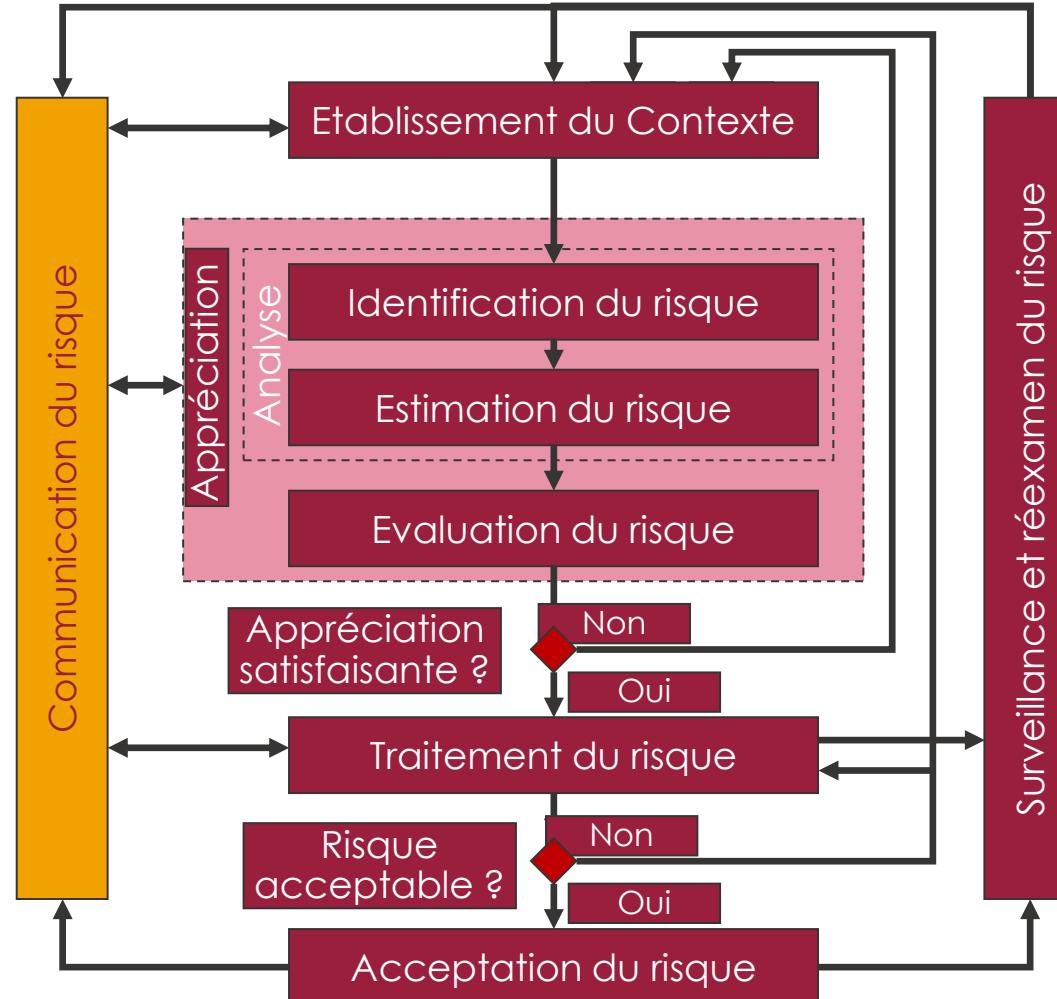
## Transfert du risque

- Le transfert du risque implique la décision de partager le risque avec des parties externes. Le transfert du risque peut créer de nouveaux risques, ou en modifier



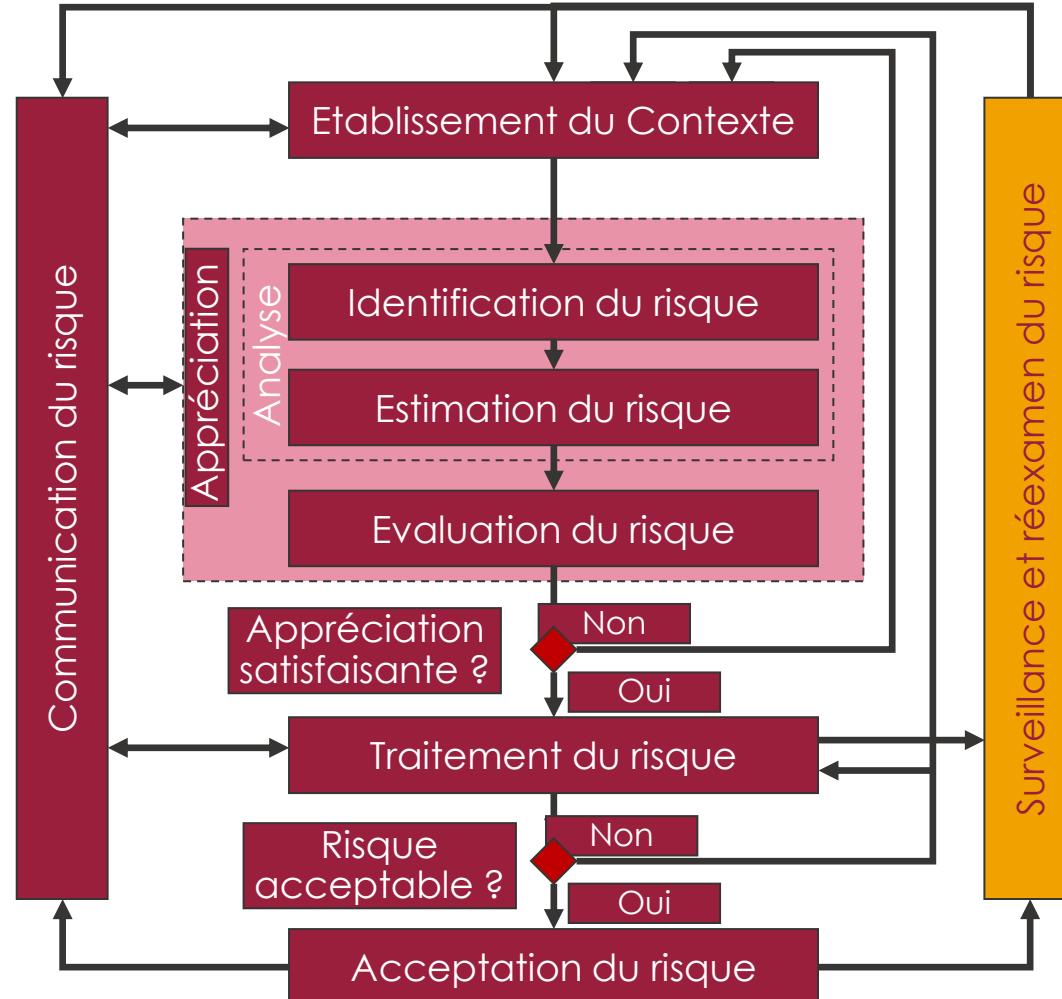
Niveau de risque





- Collecter l'information
- Réduire l'occurrence des scénarii de risque par une meilleure compréhension entre les décideurs et les parties-prenantes
- Coordonner l'ensemble des parties concernées et préparer les réponses afin de réduire les conséquences d'incidents
- Fournir aux décideurs et aux parties prenantes la mesure de leur responsabilité dans la gestion du risque.
- Améliorer la sensibilisation

# Points clés ISO 27005 : « Surveillance et réexamen du risque »



- Surveiller et réexaminer les risques et leurs facteurs à savoir
  - valeur des actifs
  - impacts
  - menaces
  - vulnérabilités
  - vraisemblance
- Identifier au plus tôt toutes les modifications dans le contexte de l'organisation
- Maintenir une cartographie complète des risques

## 1 - Evaluation Avant traitement

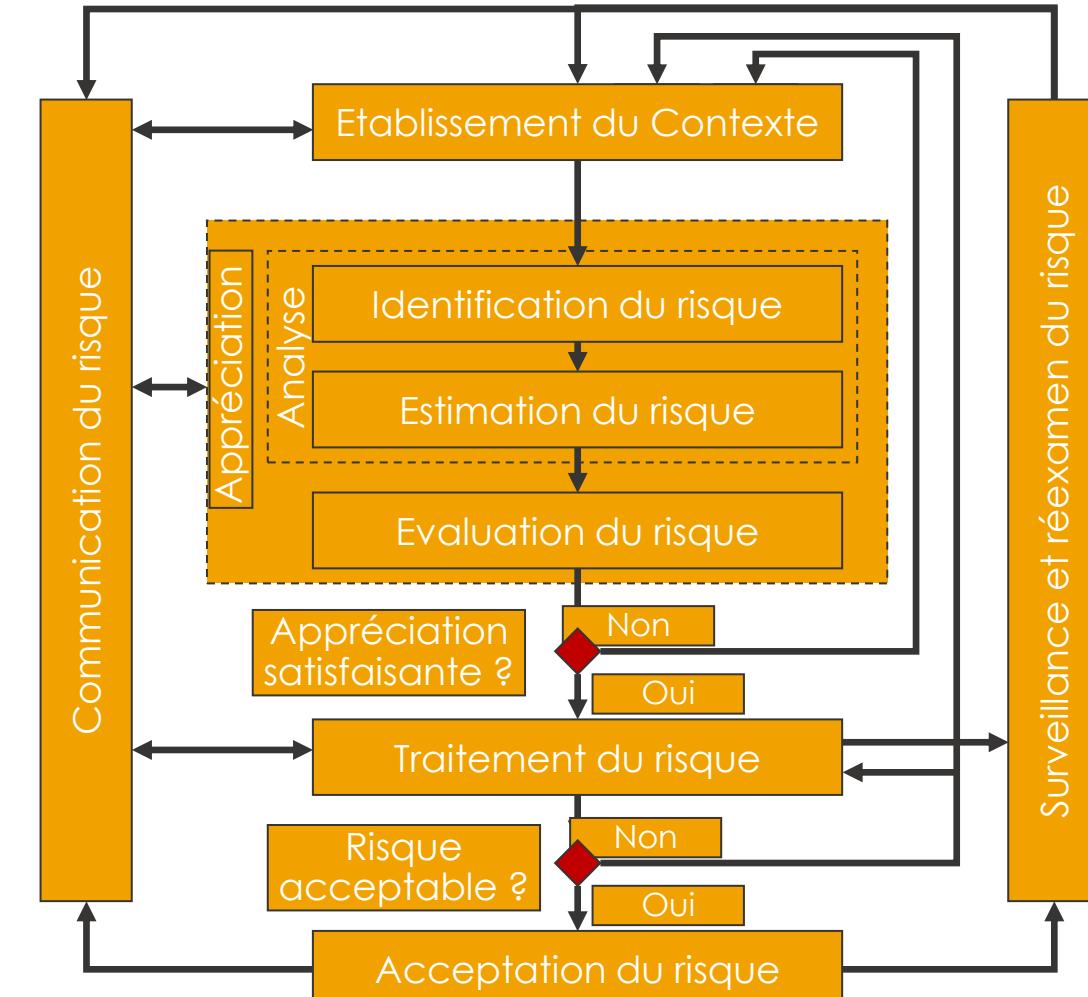
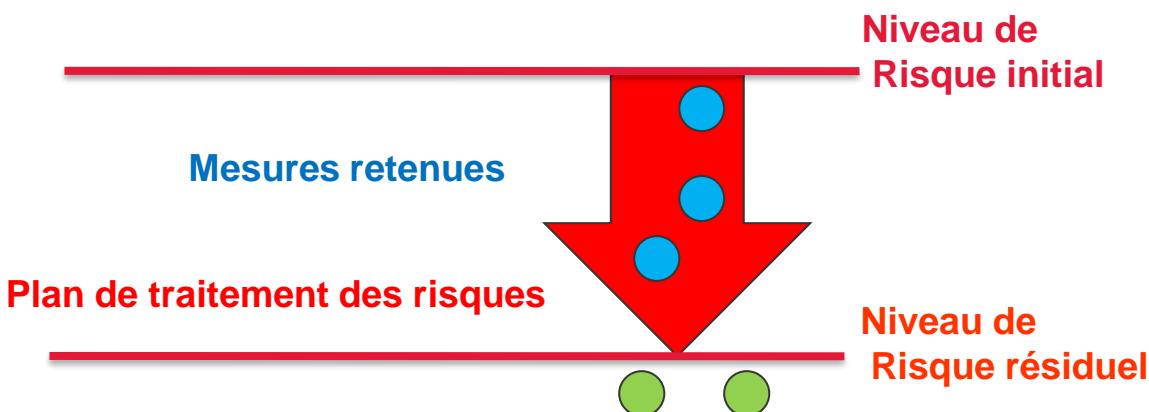
- Rapport d'appréciation des Risques

## 2 - Décision du traitement

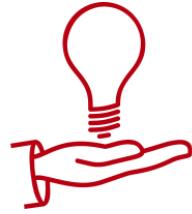
- Revue de Direction

## 3 - Acceptation après traitement

- Plan de Traitement des Risques



# Agenda



## Principes du SMSI

- Introduction
- Définition du Système de Management
- Introduction aux normes ISO27001 / ISO27002



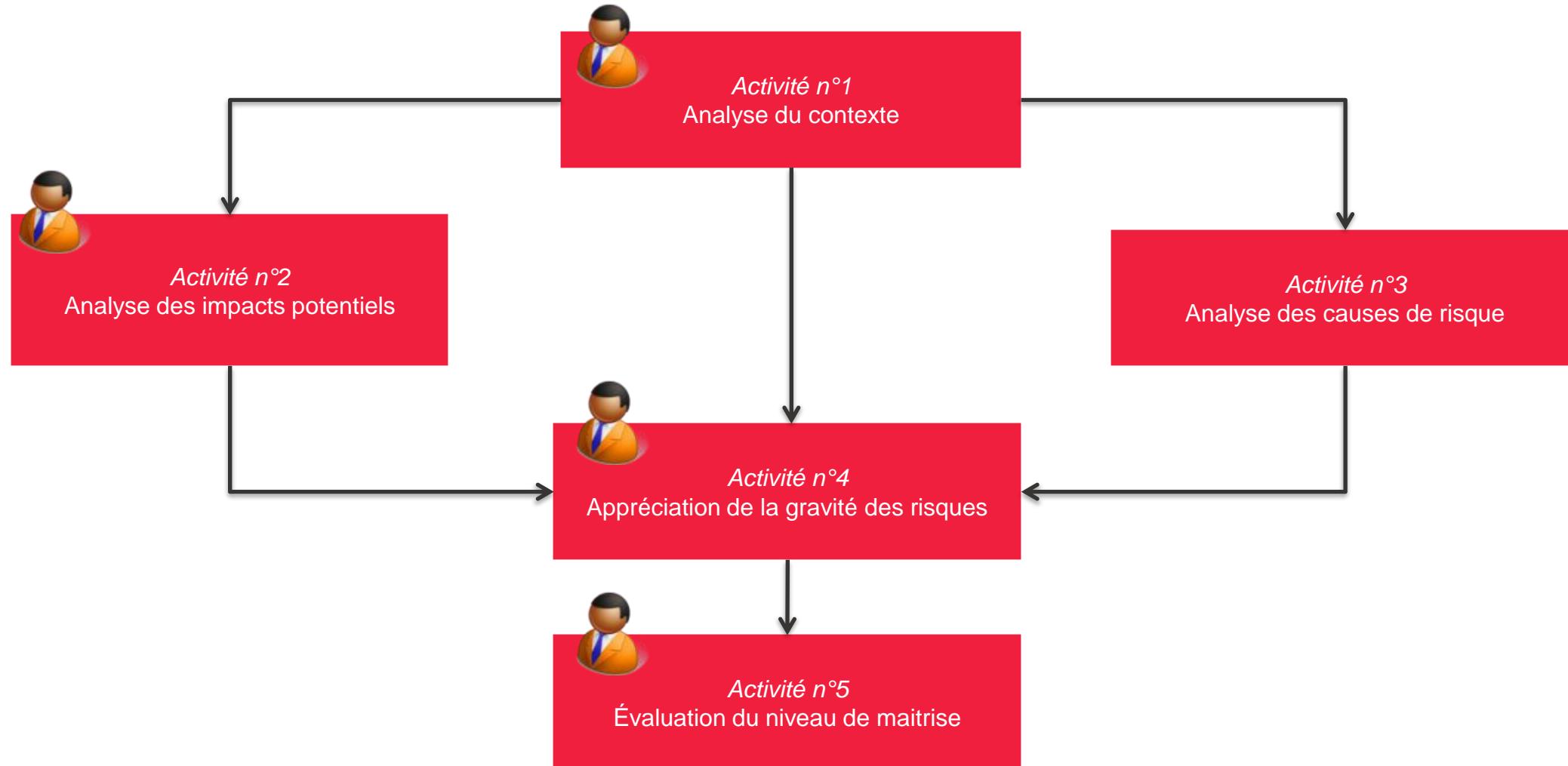
## La Gestion de Risque

- Principes de la gestion des risques
- ISO27005 / ISO31000
- Application d'EBIOS à l'identification des risques de l'entreprise

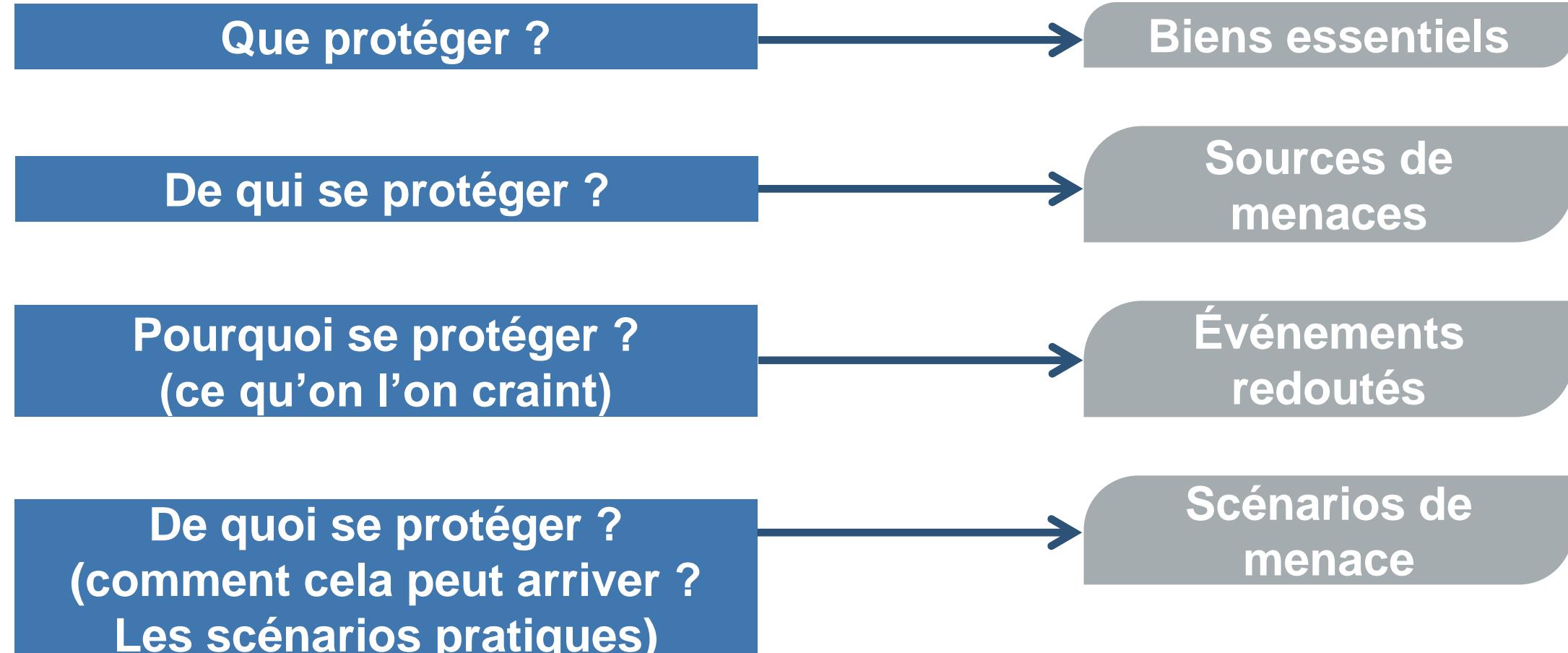


## La mise en œuvre pratique

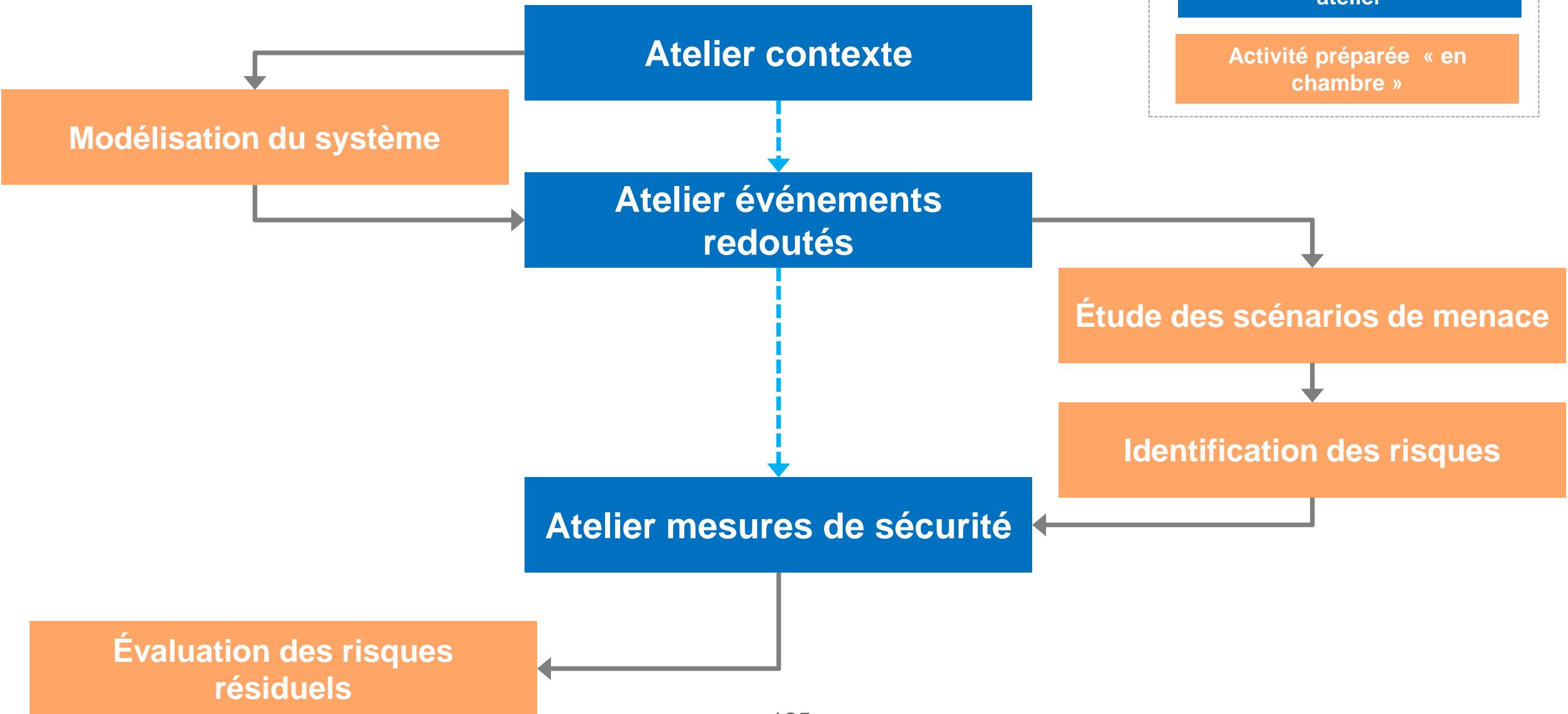
- Plan
- Do
- Check
- Act

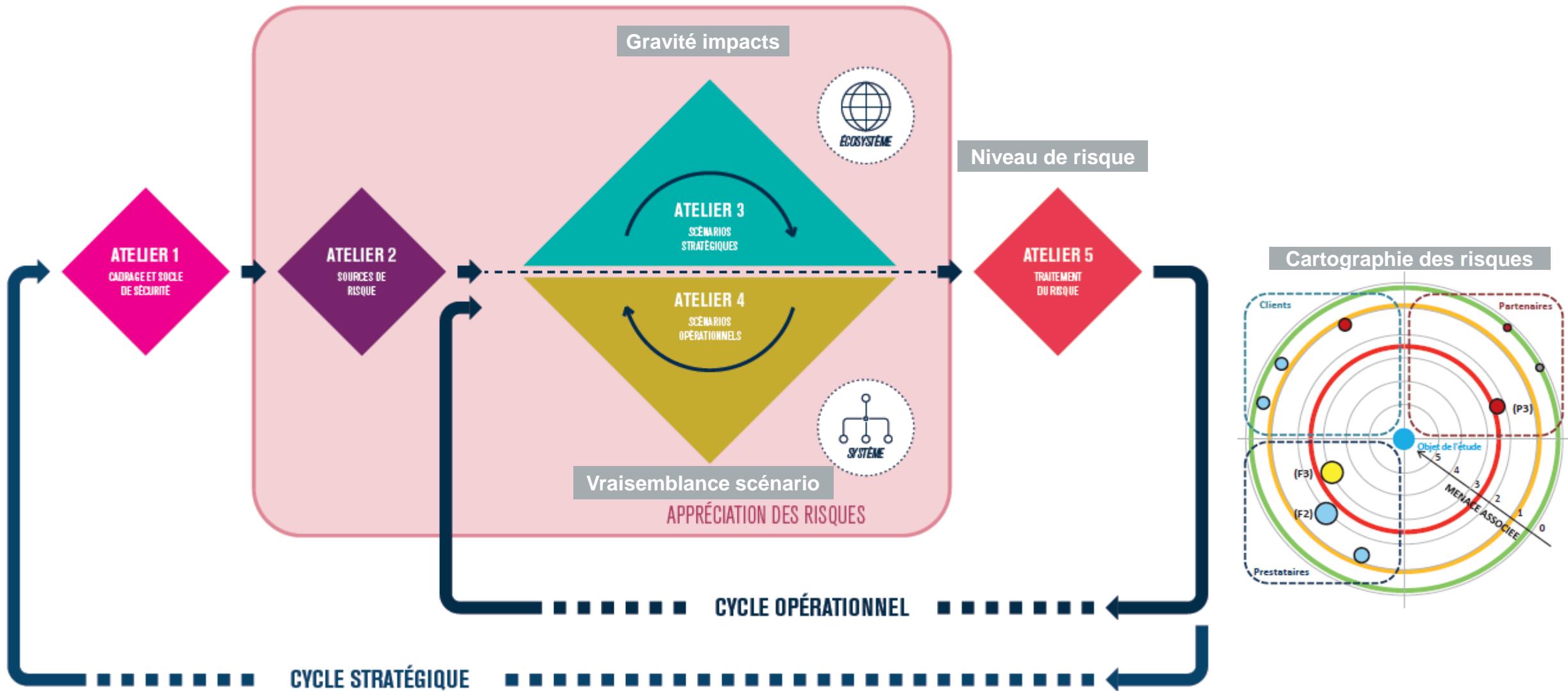


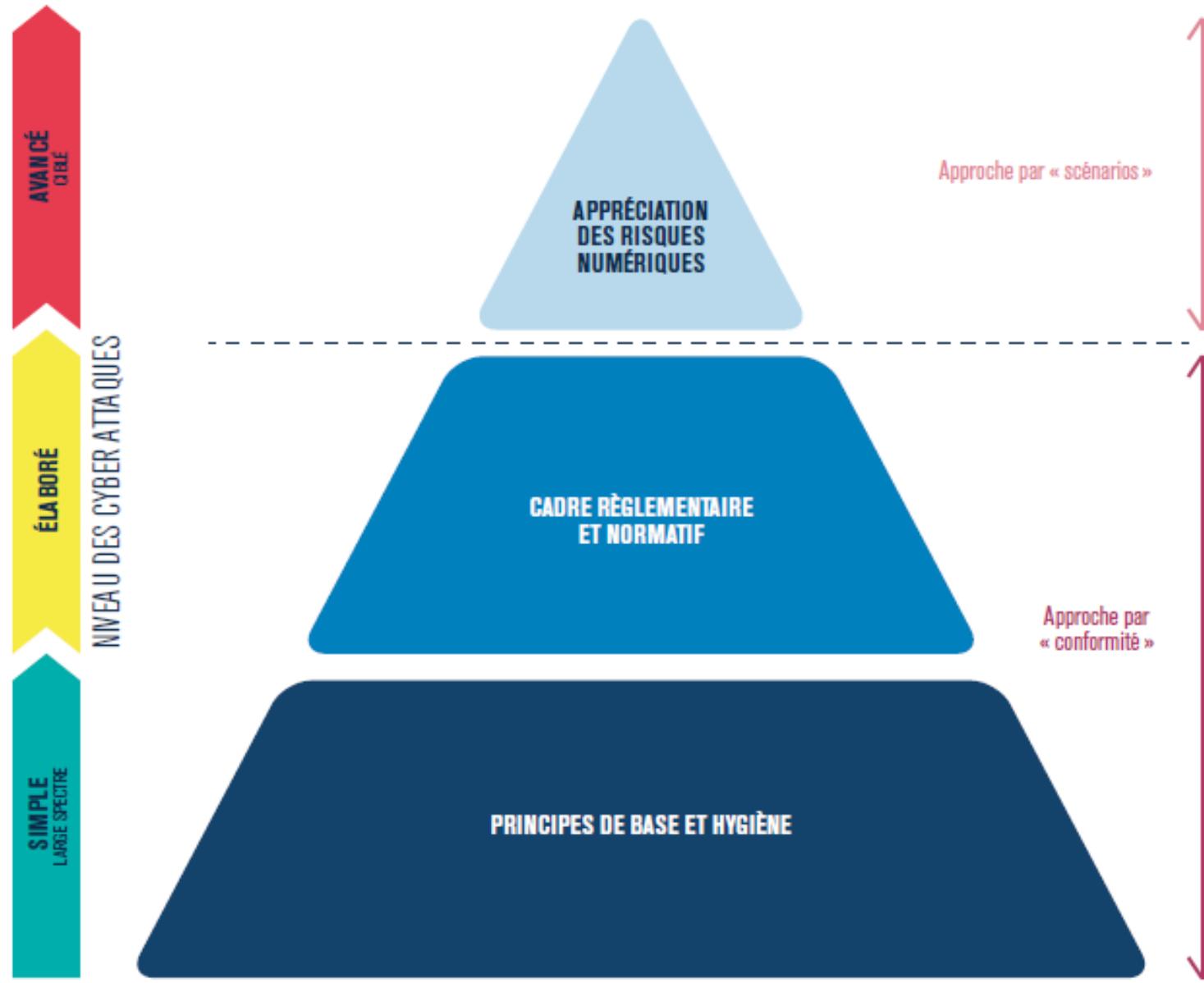
# L'analyse de risques en langage courant



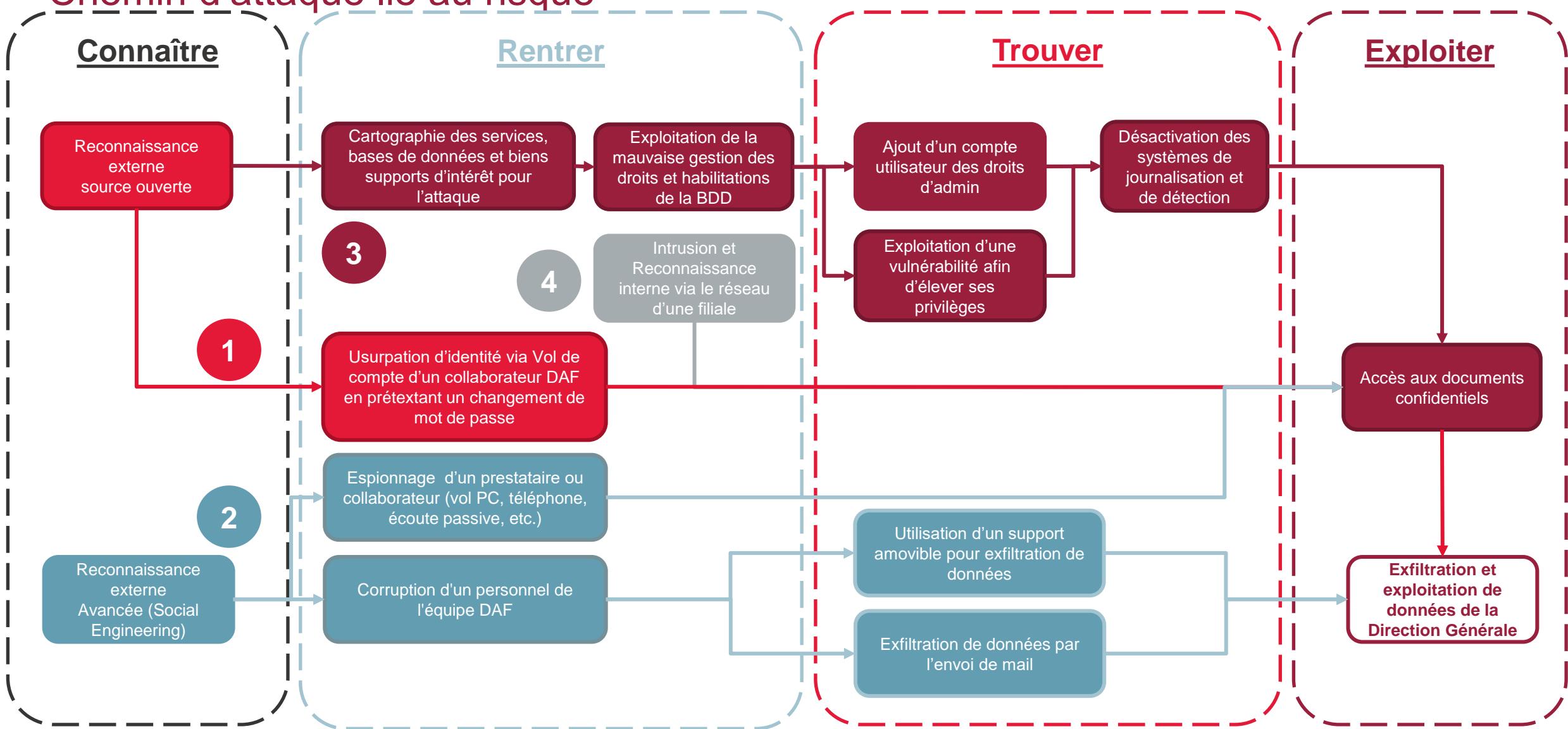
# Les étapes de la méthode

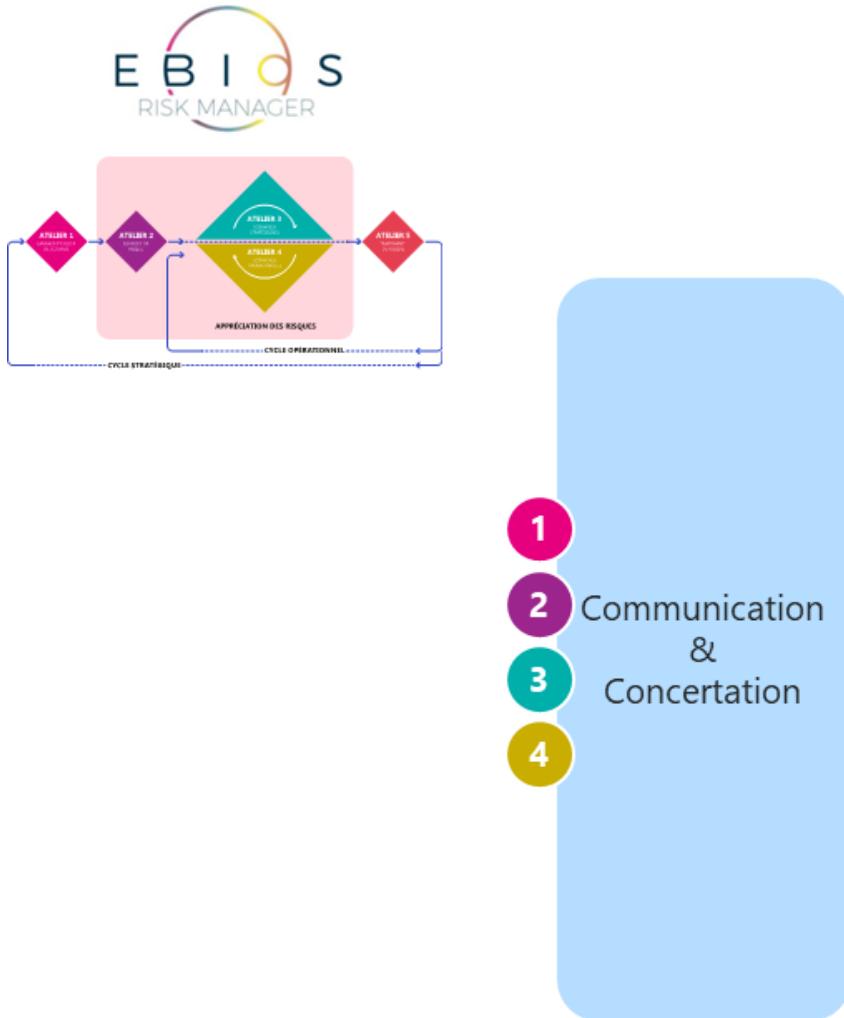






# Cartographie des risques de sécurité de l'information- Chemin d'attaque lié au risque







EBIOS RM	ISO 27005
Partie prenante	Partie intéressée
Cadrage et socle de sécurité	Etablissement du contexte
Scénario stratégique	Approche par évènements
Scénario opérationnel	Approche par les biens support
Évènement redouté	Conséquence
Évènement intermédiaire	Conséquence intermédiaire
Valeur métier	Bien primaire
Bien support	Bien support
Source de risque	Source de risque
Niveau de Menace	Niveau de danger
PACS	Plan de traitement du risque
Impact	Critères de conséquences
Besoin de sécurité	Objectif de sécurité
Gravité	Gravité
N/A	Déclencheur

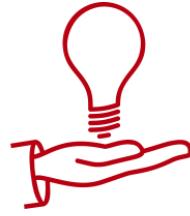


## Rappels & Questions

La gestion de risque

- ❖ Principes de la gestion des risques
- ❖ ISO27005 / ISO31000
- ❖ Application d'EBIOS à l'identification des risques de l'entreprise

# Agenda



## Principes du SMSI

- Introduction
- Définition du Système de Management
- Introduction aux normes ISO27001 / ISO27002



## La Gestion de Risque

- Principes de la gestion des risques
- ISO27005 / ISO31000
- Application d'EBIOS à l'identification des risques de l'entreprise

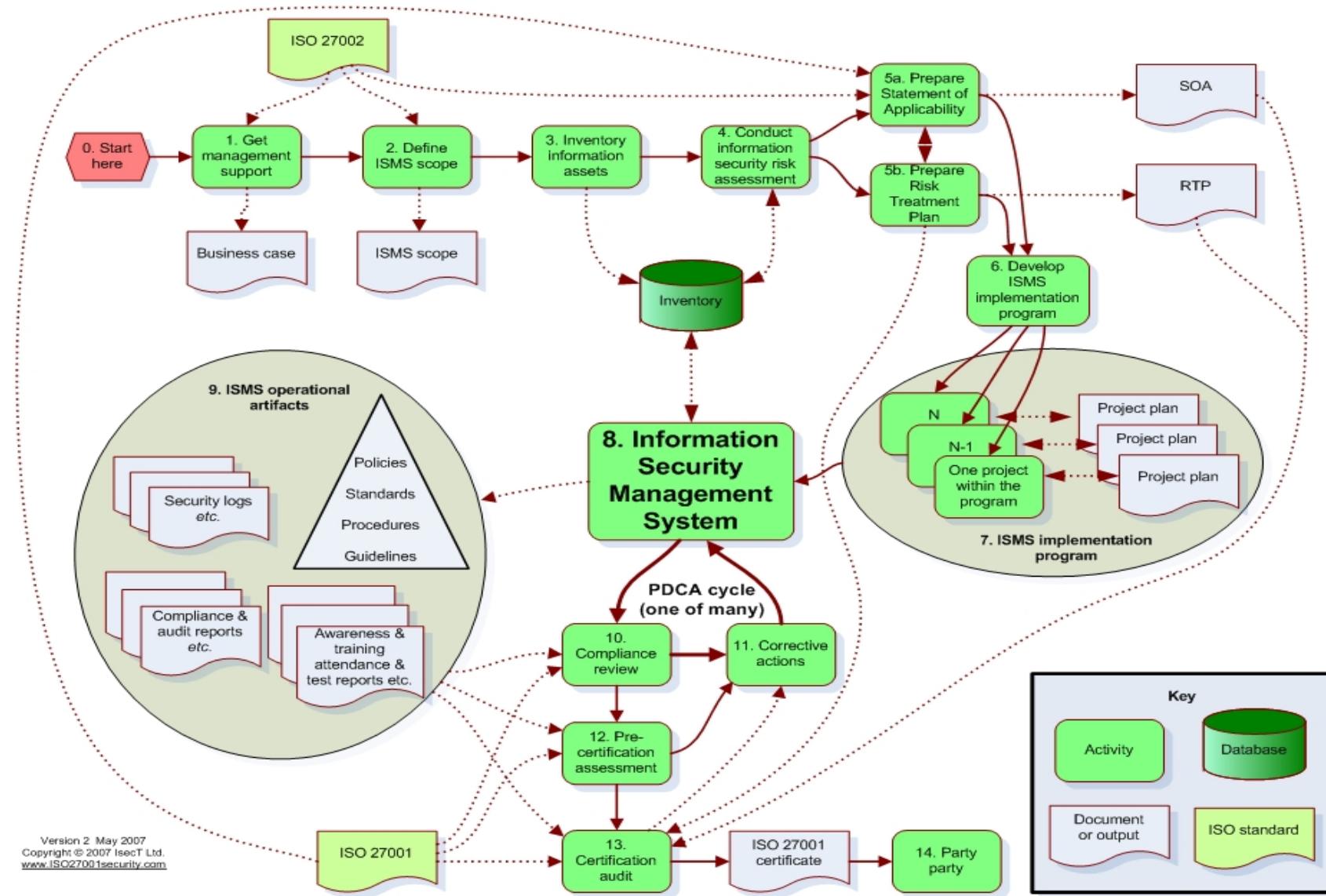


## La mise en œuvre pratique

- Plan
- Do
- Check
- Act

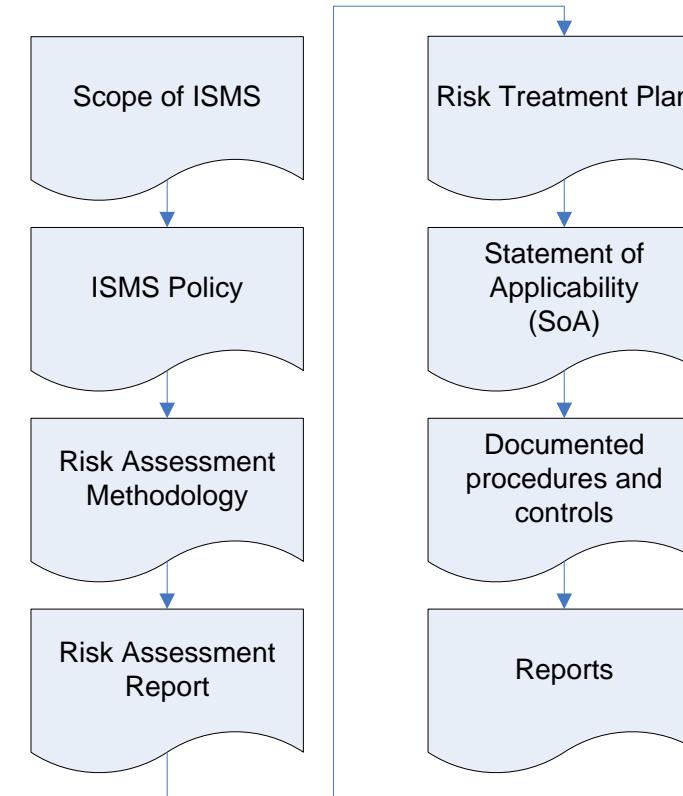


# Etapes du projet SMSI (selon ISO27003)



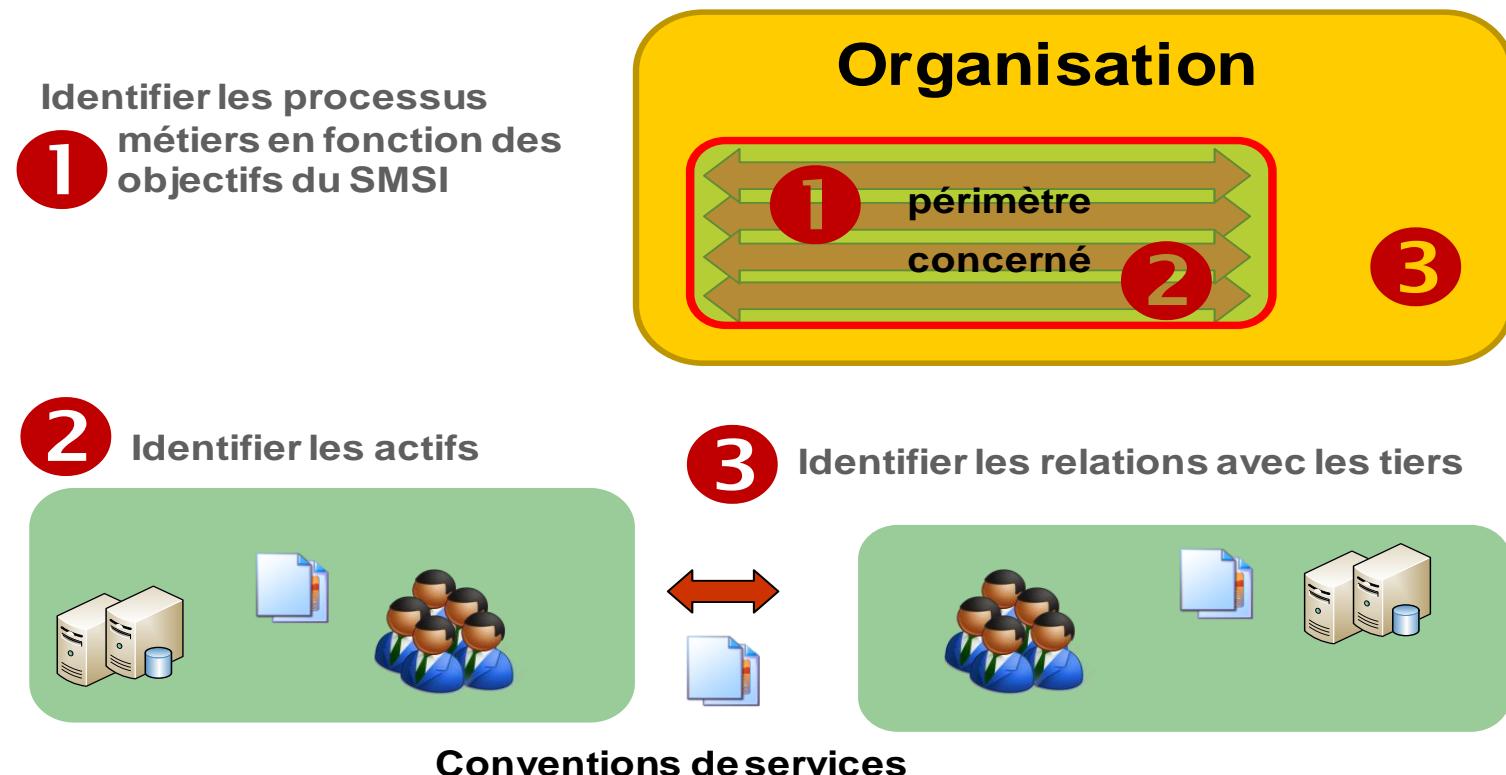
## Démarche projet

1. Définir le périmètre du SMSI
2. Analyser l'existant en matière de sécurité
3. Définir la politique du SMSI
4. Modéliser les processus du SMSI
5. Élaborer une méthode et conduire l'appréciation de risques
6. Construire le Plan de Traitement des Risques
7. Élaborer la SOA
8. Mettre en cohérence l'existant et les éléments requis par la certification
9. Procéder à des audits à blanc
10. Réaliser l'audit de certification



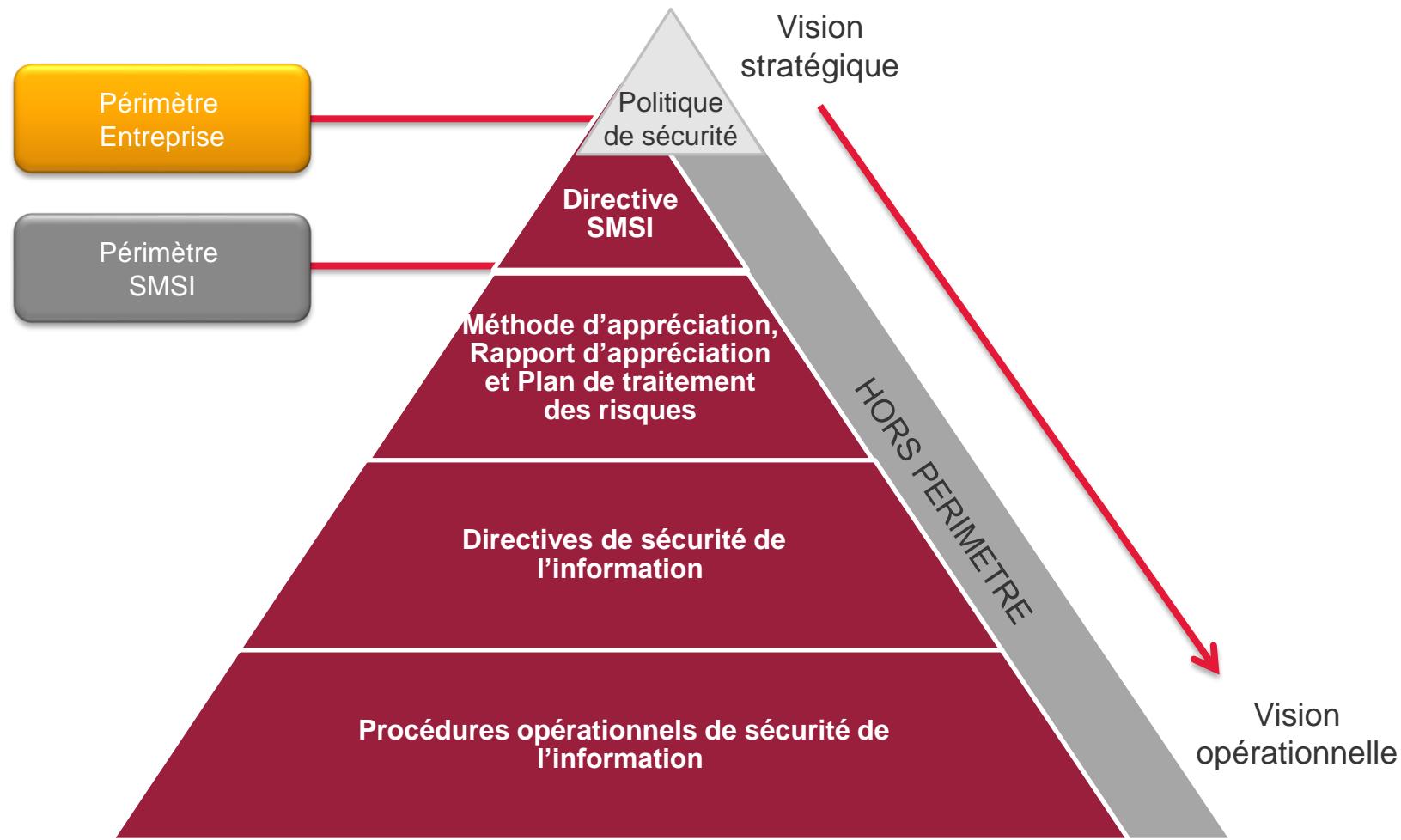
# Quel périmètre pour le SMSI ?

- a) Il convient d'identifier les processus métiers (DSI, Business) couverts par le SMSI,
- b) à l'intérieur de ce périmètre, il s'agit ensuite d'identifier les actifs informationnels et les éléments supports de ces actifs
- c) et enfin de considérer l'ensemble des autres processus et entités comme des tiers au sens de la norme.



- La documentation doit inclure les **enregistrements** des décisions de gestion et assurer que les **actions** entreprises sont identifiables grâce aux **décisions** et aux politiques de la direction, et que les **résultats** consignés sont reproductibles.
- Il est important de pouvoir démontrer la relation entre les **mesures sélectionnées** et les **résultats** du processus d'appréciation du risque et de traitement du risque, et par conséquent, la politique et les **objectifs** du SMSI.
- La documentation du SMSI doit inclure :
  - les déclarations documentées de la politique et des objectifs du SMSI ;
  - le domaine d'application du SMSI ;
  - les procédures et les mesures d'assistance du SMSI ;
  - une description de la méthodologie d'appréciation du risque ;
  - le **rappor t d'appréciation du risque** ;
  - le **plan de traitement du risque**;
  - les procédures documentées dont a besoin l'organisme pour s'assurer de la planification, du fonctionnement et du contrôle effectifs de ses processus de sécurité de l'information et pour spécifier comment évaluer l'efficacité des mesures appliquées;
  - les enregistrements exigés par l'ISO27001 ;
  - la SoA (déclaration d'applicabilité).

# Organiser la structure documentaire



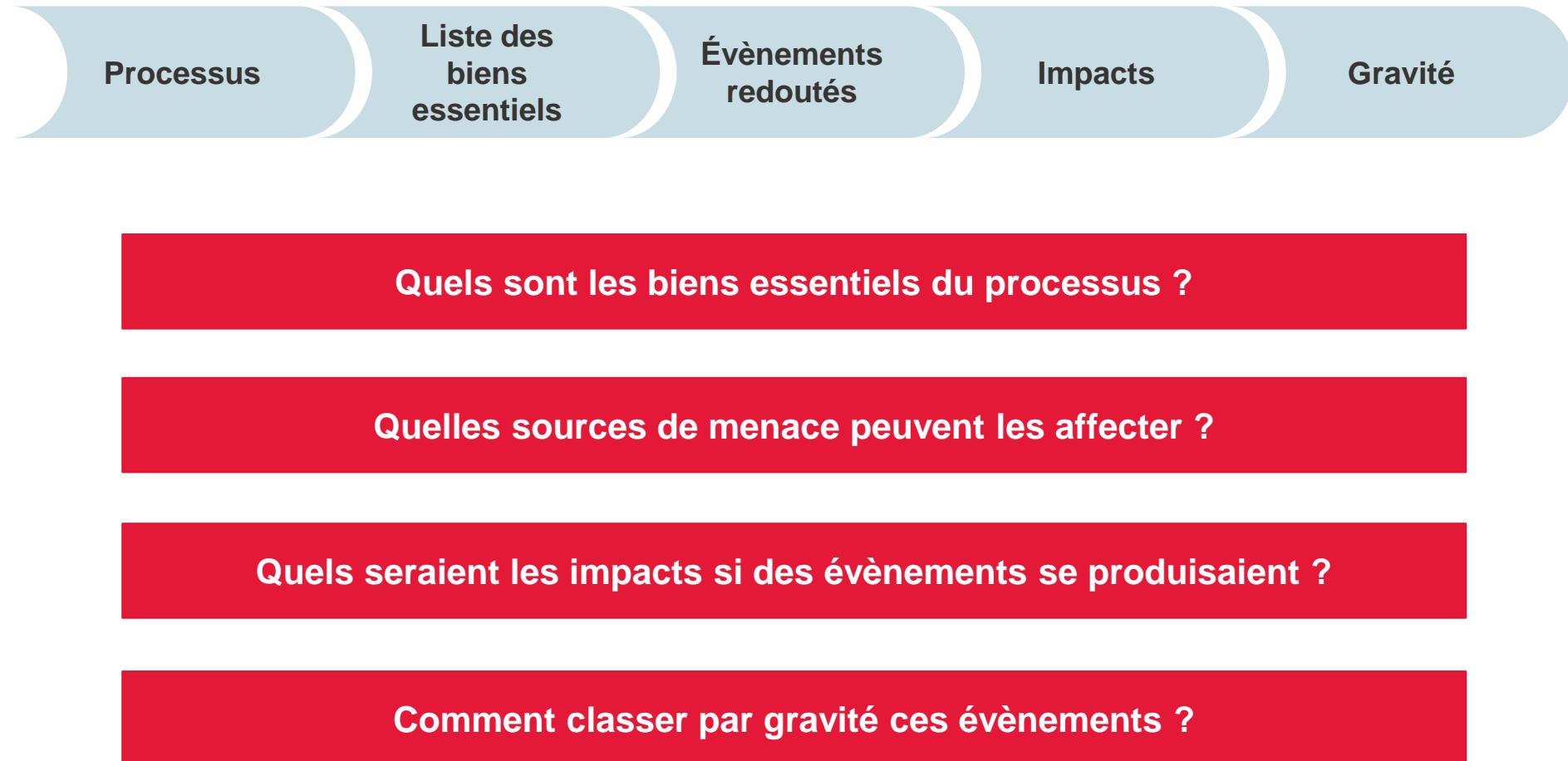
Identifier et évaluer la gravité des évènements redoutés sur les activités de l'organisme

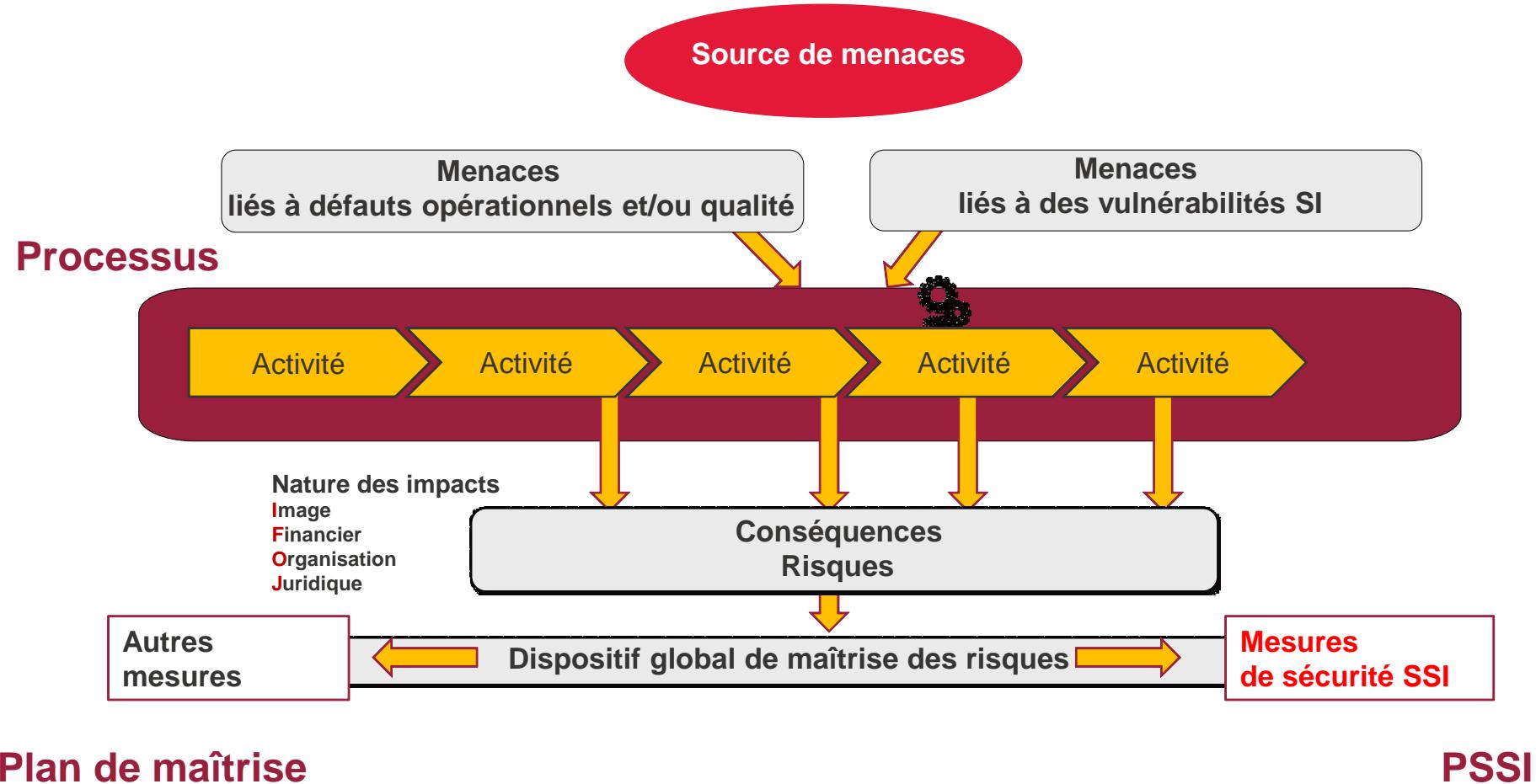
**Responsables de processus / métiers**

Identifier et évaluer la vraisemblance des menaces qui pèsent sur le système d'information

**Responsables informatiques et SSI**

Recueillir un retour d'expérience et les attentes en matière de PSSI  
**Direction de l'organisme**





Gravité	Description
<b>4. Stratégique</b>	Pourrait mettre en cause la pérennité des missions de l'institution : <b>incapacité</b> des organismes à <b>délivrer</b> une (ou plusieurs) des missions de service public, <b>divulgation</b> massive de données assurés, <b>pertes</b> financières importantes ( détournement de sommes, par exemple), <b>poursuite</b> judiciaires de l'institution voire de ses dirigeants, etc.
<b>3. Critique</b>	Provoquerait une modification importante dans les structures et la capacité de l'institution à effectuer ses missions : <b>incapacité</b> d'un organisme de taille importante (ou de plusieurs organismes simultanément de petite ou moyenne taille) à réaliser ses (leurs) activités de production, <b>diffusion dans les médias</b> de la situation entraînant une <b>dégradation de l'image</b> de marque, plaintes au Tribunal Administratif, <b>pertes</b> financières importantes, révocation de dirigeants, etc.
<b>2. Sensible</b>	Pourrait <b>amoindrir notablement les capacités</b> de l'institution à effectuer ses missions : incapacité d'un organisme à réaliser ses activités, <b>possibles recours</b> administratifs sur des dossiers non traités, pertes financières, etc.
<b>1. Faible</b>	Provoquerait une <b>gêne</b> dans le fonctionnement de l'institution : réorganisation de certains services d'un organisme, <b>faibles pertes</b> financières, etc.

Processus

Liste des biens support

Scénarios de menaces

Vraisemblance

**Quels sont les biens support qui participent au processus ?**

**Quelles sources de menace peuvent les affecter ?**

**Quels seraient le scénario de menace ?**

**Comment classer, par vraisemblance, ces scénarios ?**

# Planification des entretiens techniques - Exemple

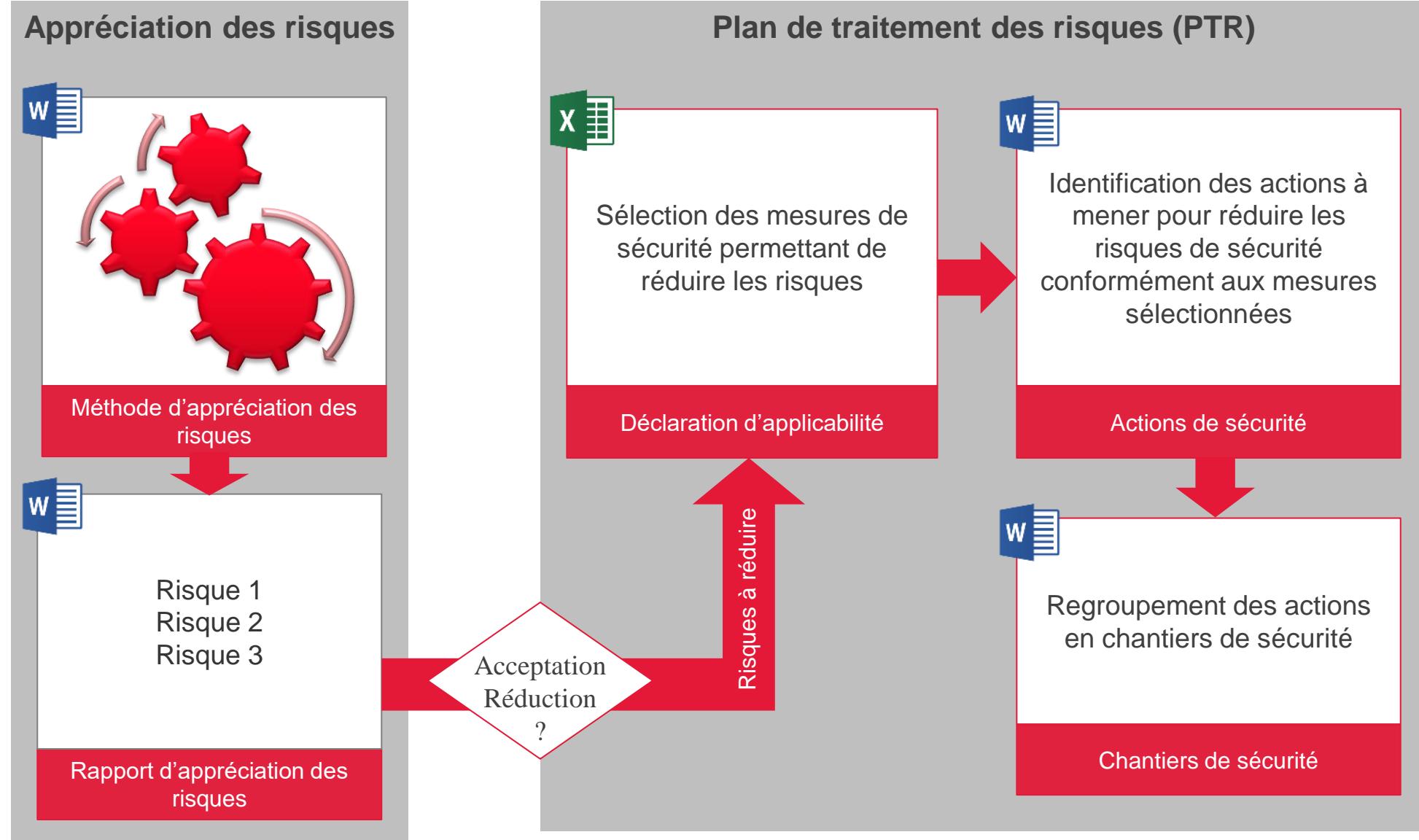
Thématique ISO 27002	Interlocuteur(s) - Responsable ou représentant -	N° entretien
<b>5 Politiques de sécurité de l'information</b>	Département SSI de la DSi (ou RSSI)	1
<b>6 Organisation de la sécurité de l'information</b>	Département SSI de la DSi (ou RSSI)	1
<b>7 La sécurité des ressources humaines</b>	Ressources humaines	2
<b>8 Gestion des actifs</b>	RSSI, Risk Manager, Qualité	3
<b>9 Contrôle d'accès</b>	RSSI, Sécurité opérationnelle	4
<b>10 Cryptographie</b>	RSSI, Sécurité opérationnelle	4
<b>11 Sécurité physique et environnementale</b>  + Visite locaux techniques	Sureté, HSE, Moyens généraux, PC Sécurité	5 (Siège) & 6 (Filiale)
<b>12 Sécurité liée à l'exploitation</b>	Production/Exploitation (DSI)	7
<b>13 Sécurité des communications</b>	Production/d'exploitation/réseau (DSI)	7
<b>14 Acquisition, développement et maintenance des systèmes d'information</b>	Etudes, Développement MOA Projets métier	8 9
<b>15 Relations avec les fournisseurs</b>	Achats	10
<b>16 Gestion des incidents liés à la sécurité de l'information</b>	RSSI, Sécurité opérationnelle	4
<b>17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité</b>	RSSI, Risk manager, RPCA	11
<b>18 Conformité</b>	Audit interne, Direction des risques Juridique	12 13

Niveau	Acte non délibéré	Acte délibéré
<b>4. Maximale</b>	<b>Très fréquent</b> Évènement qui va se (re)produire plusieurs fois dans l'année.	<b>Très facile</b> La menace est réalisable par des moyens standards ou des connaissances de base, sans même un recours à une complicité interne.
<b>3. Forte</b>	<b>Fréquent</b> Évènement qui a une forte opportunité de se (re)produire dans l'année.	<b>Facile</b> La menace est réalisable avec des connaissances sur le fonctionnement du système et/ou des moyens / connaissances à disposition d'un profil de type « technicien et pouvant se baser sur l'exploitation de failles techniques simples.
<b>2. Significative</b>	<b>Probable</b> Évènement ayant une forte plausibilité de se (re)produire dans une période de 3 ans.	<b>Difficile</b> La menace est réalisable à condition que la source puisse disposer de droits/d'accès supplémentaires à ceux dont ils disposent (élévation de priviléges ou complicité avec un agent) et/ou maîtrisent de connaissances et techniques poussées d'attaque.
<b>1. Minime</b>	<b>Peu probable</b> Évènement qui a peu de chance de se (re)produire.  Situations exceptionnelles	<b>Très difficile</b> La menace est réalisable à condition que la source puisse disposer de la complicité de plusieurs acteurs (tant internes qu'externes) ainsi que de connaissances (techniques et sur le système) poussées et/ou de moyens coûteux.

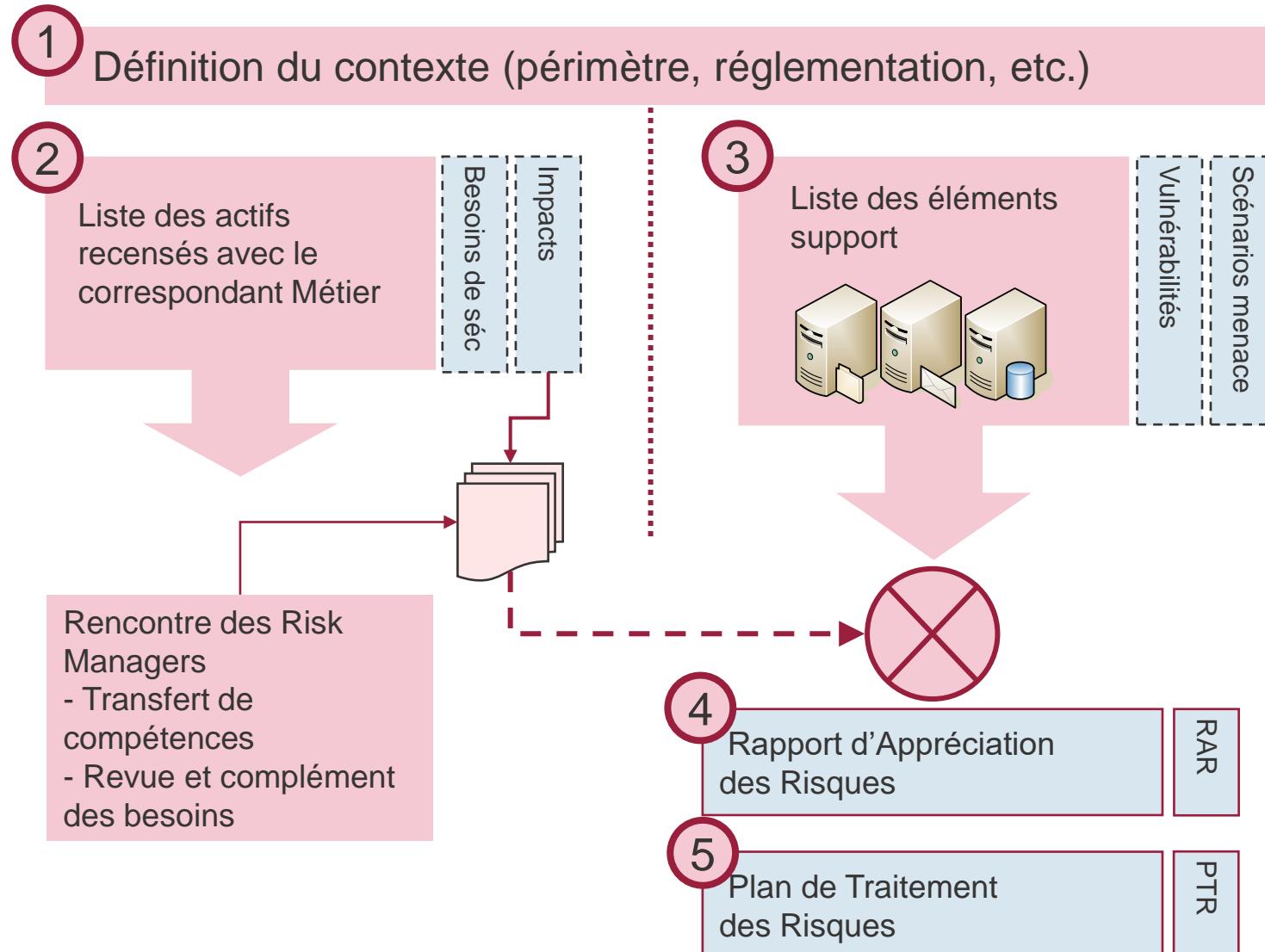
# Appréciation et Plan de traitement des risques

CGI

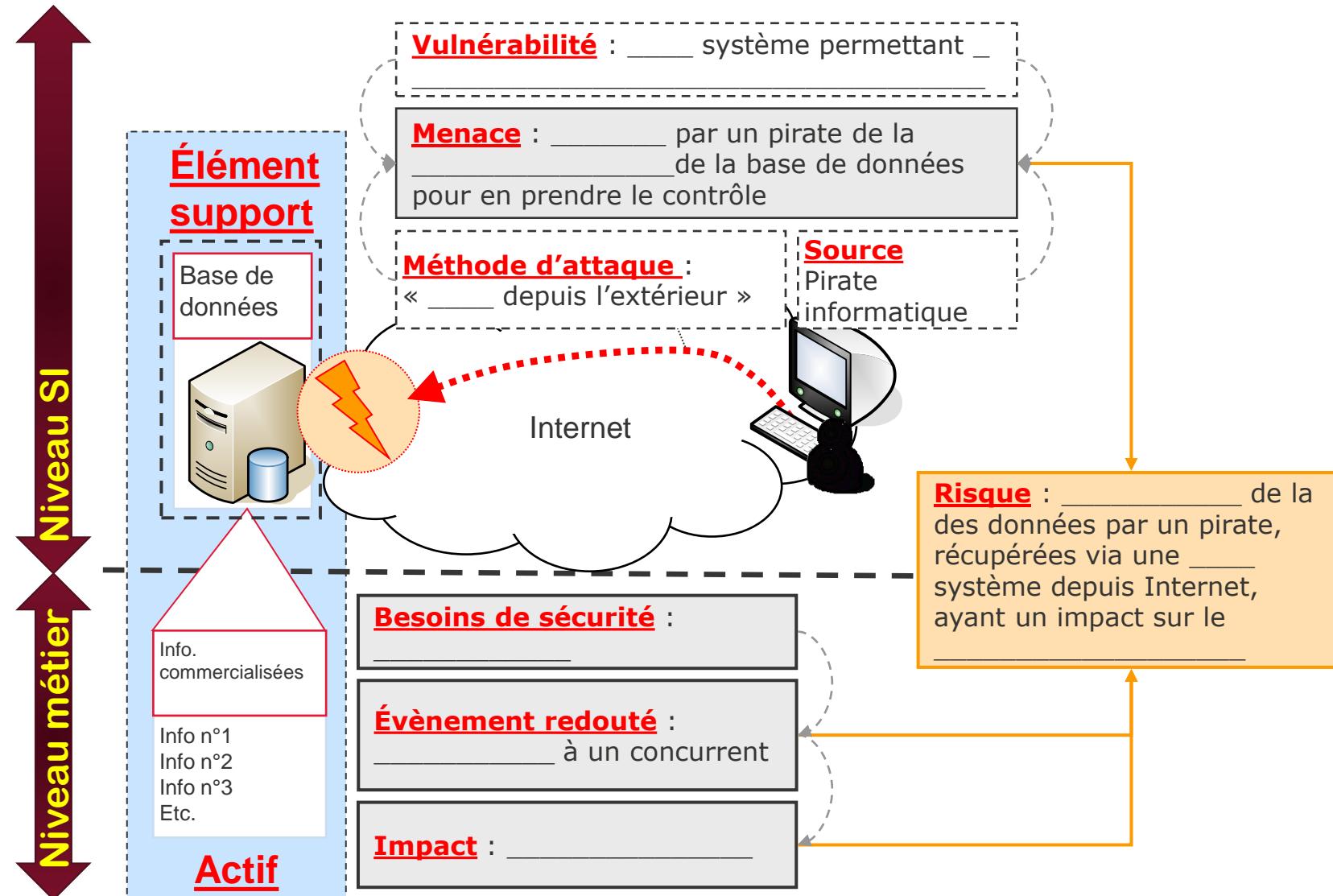
Business Consulting

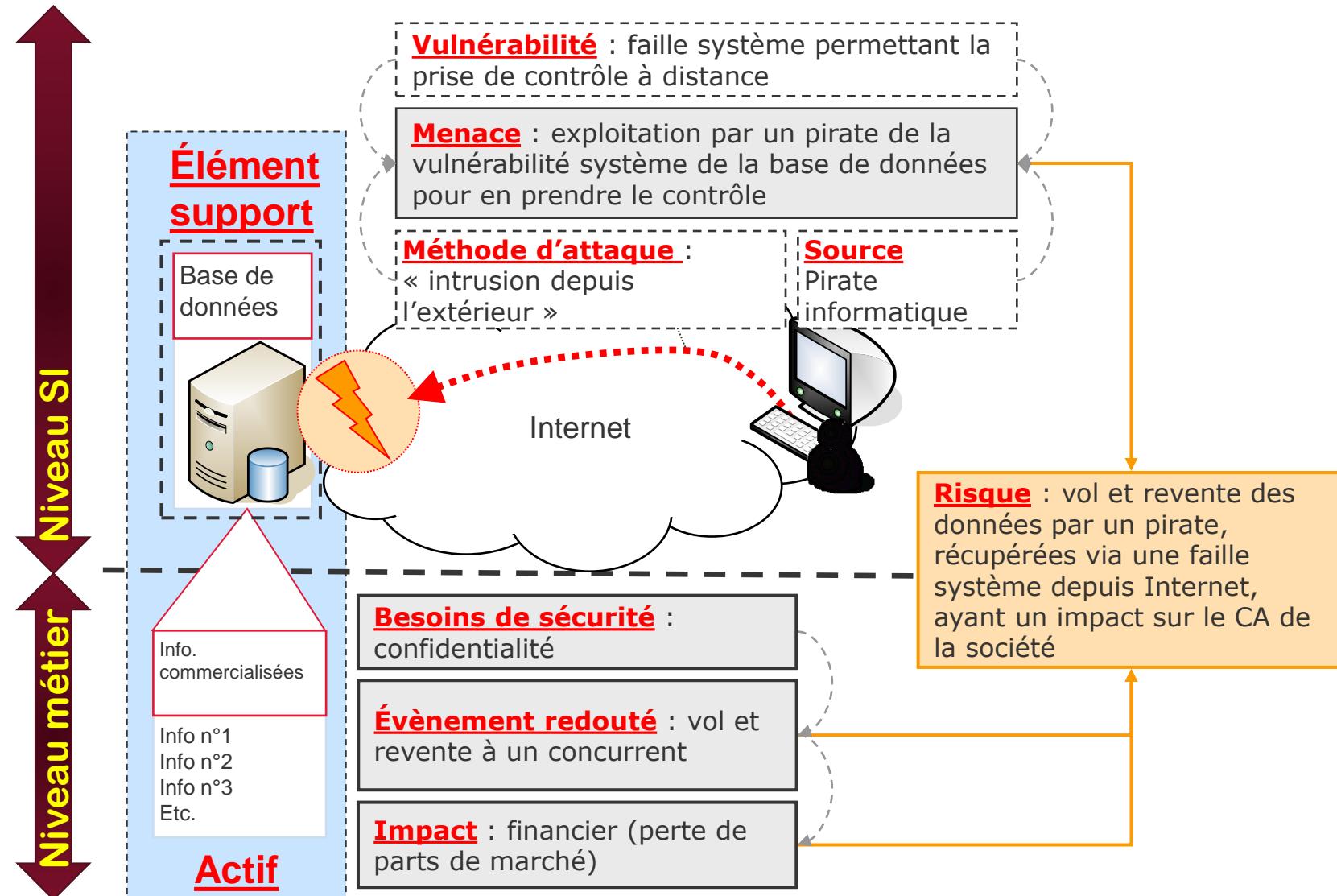


# Appréciation des risques - Exemple 1 : Périmètre

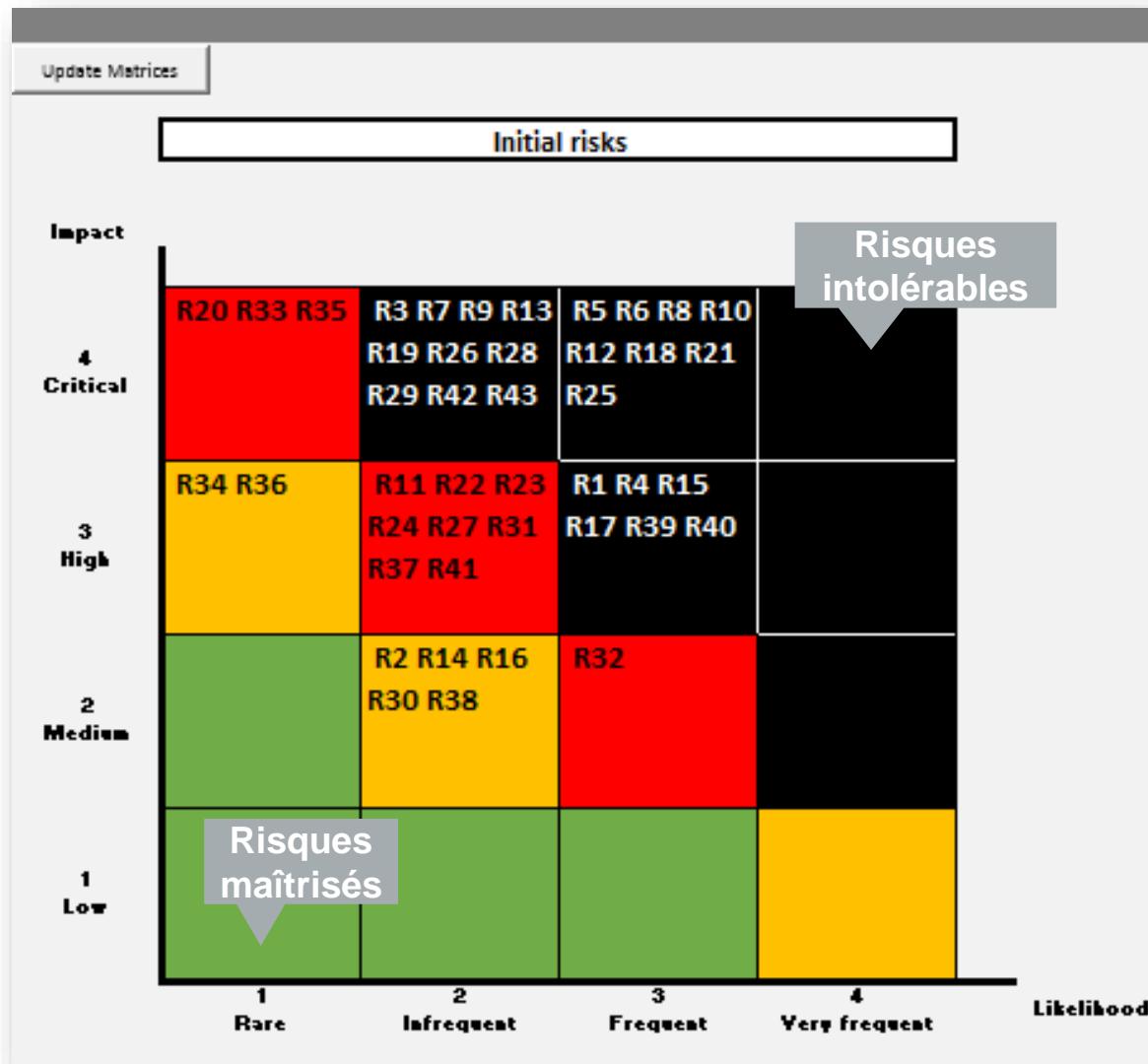


- **Dissociation entre actif & élément support :**
  - L'actif « porte » le besoin de sécurité du métier
  - L'élément support (matériel, les logiciels, les réseaux, etc.) comporte des vulnérabilités identifiées par la DSI



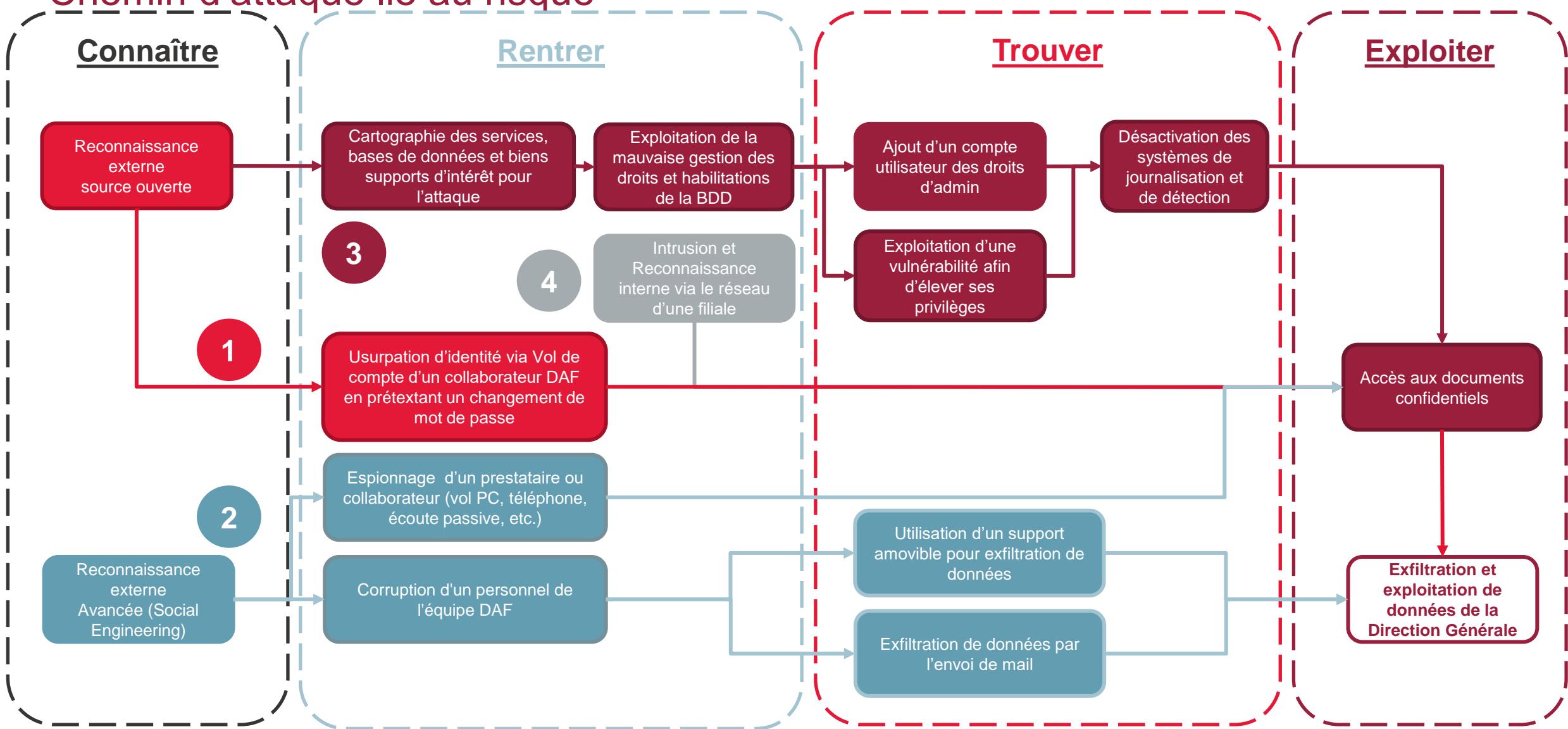


# Cartographie des risques de sécurité de l'information- Identification des risques majeurs

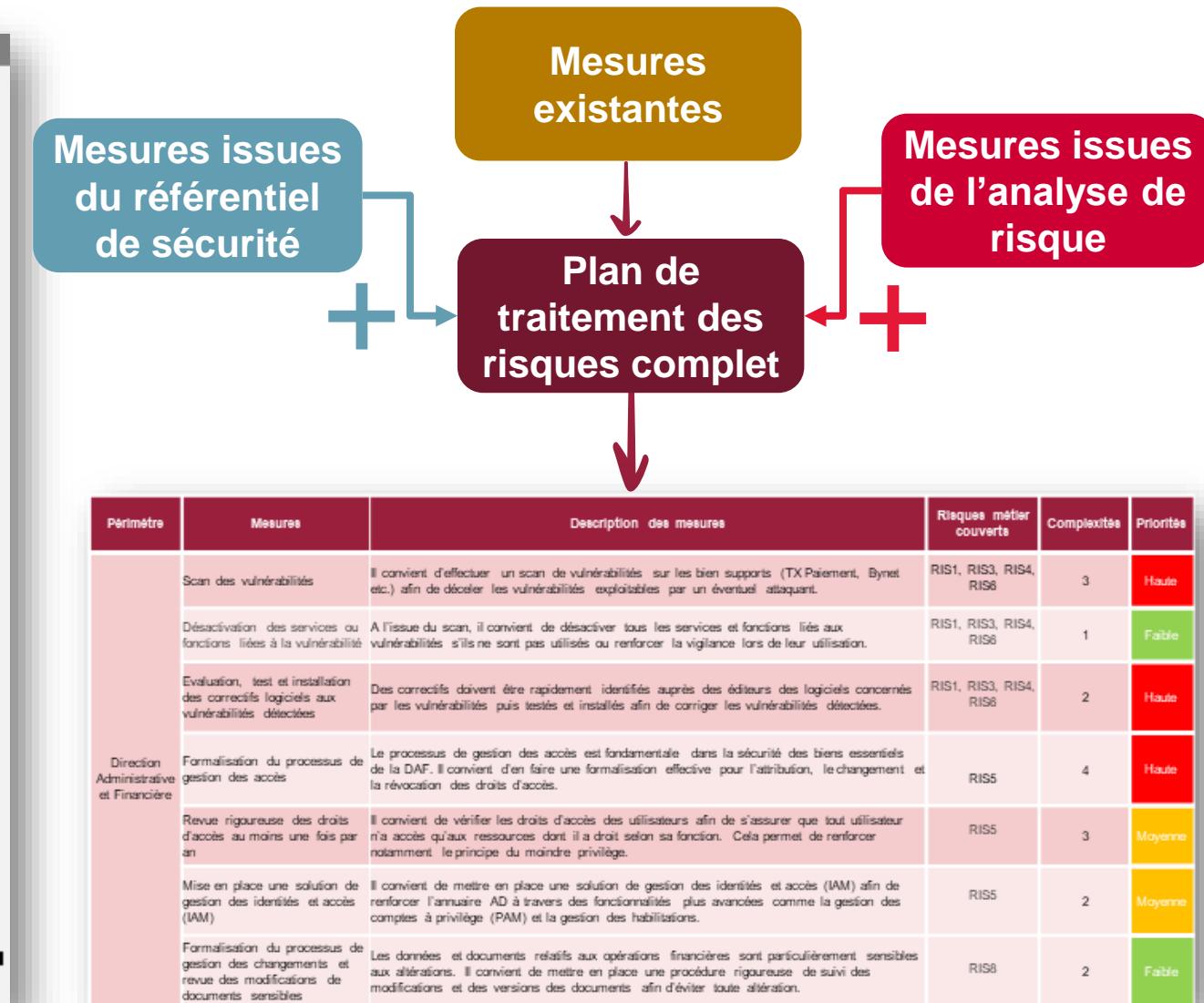
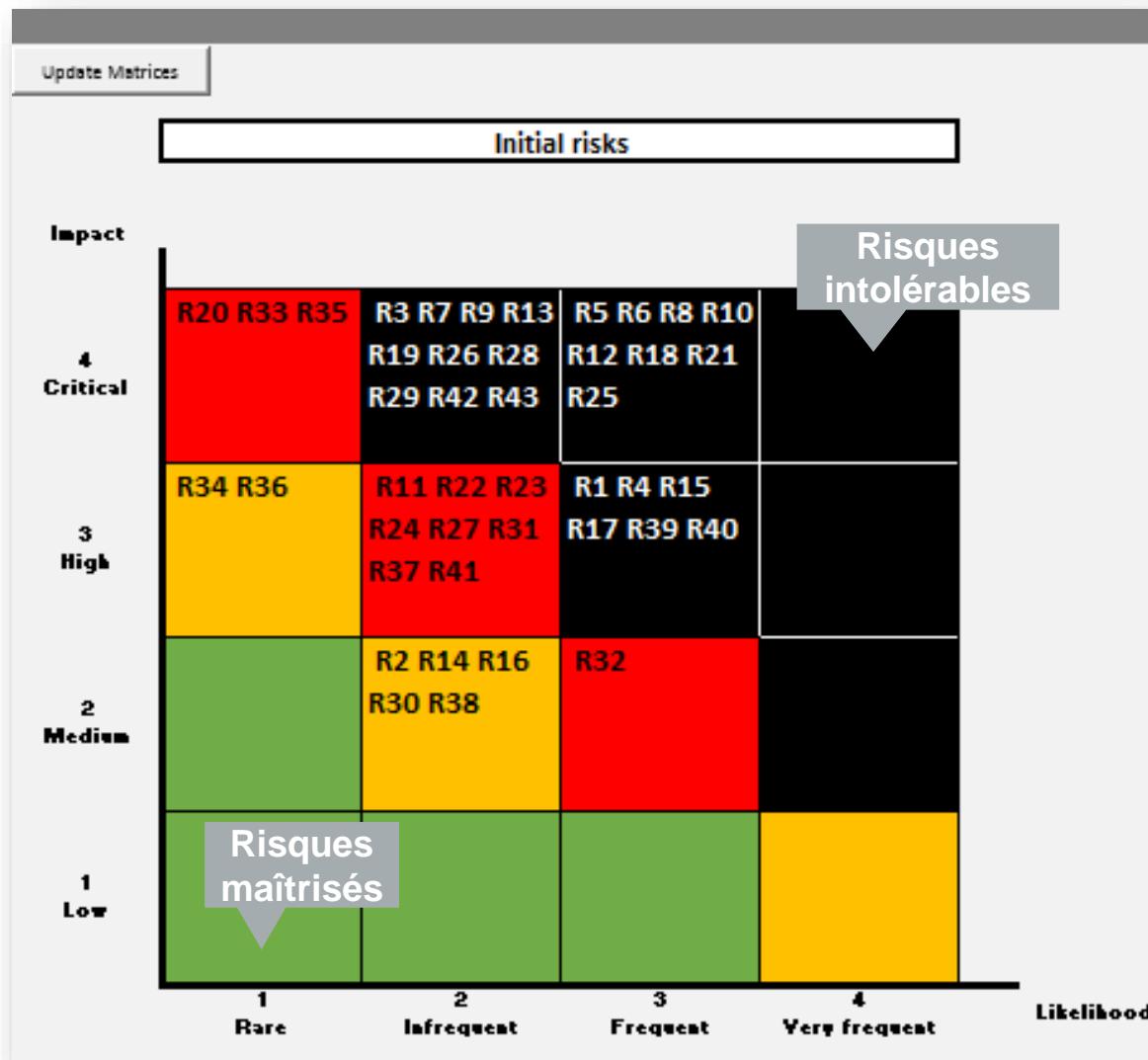


ID	Description de l'événement redouté associé au risque				
R1	Exfiltration et exploitation de données R&D				
R5	<b>Exfiltration et exploitation de données de la Direction Générale</b>				
R13	Indisponibilité du site de vente en ligne				
Gravité	Scénarios de menace	Sources de risque			
4 <b>Vraisemblance</b>	<ul style="list-style-type: none"> <li>Prestataire ou collaborateur mécontent récupérant les données de la base de données XXX à cause d'une gestion des droits et habilitations inexiste</li> </ul>	<ul style="list-style-type: none"> <li>Utilisateur interne</li> </ul>			
4	<b>Mesures Existantes</b>				
	<ul style="list-style-type: none"> <li>Sensibilisation annuelle des dirigeants à la sécurité</li> </ul>				

# Cartographie des risques de sécurité de l'information- Chemin d'attaque lié au risque



# Cartographie des risques de sécurité de l'information



# Déclaration d'Applicabilité

**Liste de 114 mesures de sécurité (tirées de l'annexe A de l'ISO27001:2013) sur lesquelles l'organisme doit se positionner et se justifier :**

- Oui, j'applique cette mesure
- Non, je n'applique pas cette mesure (non-applicable, risques acceptés, pas de risques, etc.)
- Cette déclaration est requise pour la certification sur le périmètre du SMSI

#REF	NORME ISO 27001:2013				Libellé de la mesure ISO 27001	SELECTION				
	Rubrique ISO 27001	Sous Rubrique ISO 27001	Titre de la mesure ISO 27001			Sélection	Date de MEO	Vérification	Chantier de MEO	Commentaires
A.9.2.3	Contrôle d'accès	Gestion de l'accès utilisateur	Politique de contrôle d'accès	Une politique de contrôle d'accès doit être établie, documentée et revue sur la base des exigences métier et de sécurité de l'information.		T2	NOK			La politique est incomplète et ne décrit pas la séparation des tâches d'administration et de bureautique. Il est demandé de mettre à jour la documentation.
A.11.1.2	Sécurité physique et environnementale	Zones sécurisées	Contrôle d'accès physique	Les zones sécurisées doivent être protégées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis.		T1	OK			

# Cartographie des risques de sécurité de l'information – Mesures de sécurité retenues (réduction du risque)

## Mesures organisationnelles

### Redondance

- Sauvegarde régulière



### Processus

- Revue des droits d'accès



### Documents et chartes

- PSSI, Charte IT, Charte admin



## Chiffrement des Disques



Permet	Mesure	Description de la mesure	Risque métier couvert	Compatibilité	Priorité
Bien des vulnérabilités	Il convient d'effectuer un scan de vulnérabilités sur les bien supportés (TX-Payments, Symet, etc.) afin de déceler les vulnérabilités exploitable par un attaquant.	RIS1, RIS2, RIS4, RIS5	3	Rouge	Haute
Désactivation des services ou fonctions liées à la vulnérabilité	A l'issue du scan, il convient de désactiver tous les services et fonctions liés aux vulnérabilités si elles ne sont pas utilisées ou rediriger la vigilance lors de leur utilisation.	RIS1, RIS2, RIS4, RIS5	1	Jaune	Normale
Evaluation, test et installation des correctifs pour les vulnérabilités détectées	Des correctifs doivent être rapidement identifiés après les détections des logiciels concernés par les vulnérabilités, puis testés et installés afin de corriger les vulnérabilités détectées.	RIS1, RIS2, RIS4, RIS5	2	Rouge	Haute
Directive Administrateur de France	Formulation du processus de gestion des accès	Le processus de gestion des accès est fondamental dans la sécurité des biens essentiels du DAF. Il convient d'en faire une formalisation effectuée pour l'utilisation, le déclassement, et la réécriture des droits d'accès.	RIS2	4	Rouge
	Revue rigoureuse des droits d'accès au moins une fois par an	Il convient de vérifier les droits d'accès des utilisateurs afin de s'assurer que tout utilisateur a accès à ce qu'il a besoin et n'a pas accès à ce qu'il n'a pas besoin. Cela permet de renforcer notamment, le principe du moindre privilège.	RIS2	3	Jaune
	Mise en place une solution de gestion des identités et accès (AMM)	Il convient de mettre en place une solution de gestion des identités et accès (AMM) afin de faciliter la gestion des identités et accès, et de simplifier les opérations d'audit, comme la gestion des comptes à privilège (PM) et la gestion des habilités.	RIS2	2	Jaune
	Formulation du processus de gestion des changements et mise en place d'un système de suivi des documents sensibles	Les données et documents relatifs aux opérations financières sont particulièrement sensibles aux alterations. Il convient de mettre en place une procédure rigoureuse de suivi des modifications et des versions des documents afin d'éviter toute altération.	RIS2	2	Vert



## Firewalls



## Solutions de scan des patches

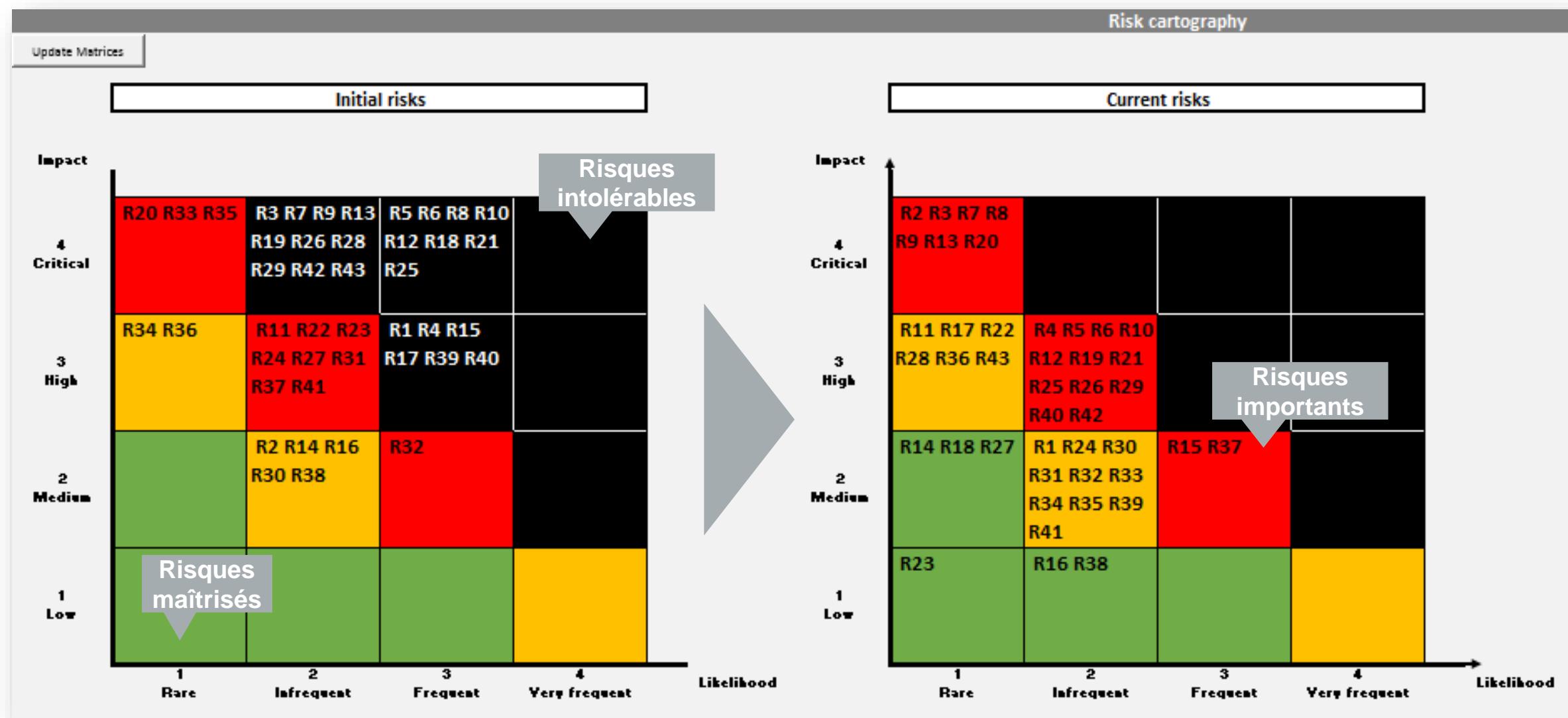


## Solutions de monitoring



## Solutions antimalwares

# Cartographie des risques de sécurité de l'information



# Cas pratique

## Contexte:

- Cas n°1: Votre réseau de distribution de jouets du sud-ouest de la France est indisponible 6 heures suite à une coupure télécom (c'était malheureusement le 24 décembre).
- Cas n°2 :Un collaborateur remet au RSSI un document trouvé sur une imprimante réseau. Il s'agit de la cartographie des risques de l'entreprise.
- Cas n°3 :Un de vos collaborateurs travaillant au département R&D s'avère, en fait, travailler pour vos concurrents (vous comprenez pourquoi vos demandes de brevet sont refusées depuis quelques temps pour des questions d'antériorité).
- Cas n°4: 6 mois après le licenciement d'un de vos développeurs, votre base de données clients disparaît mystérieusement (vos backups sont également corrompus).

## Tâches à réaliser:

- Définitions des échelles de mesure
- Identification des actifs
- Identification des risques (menaces, vulnérabilités)
- Appréciation des risques
- Identification des mesures de sécurité à mettre en œuvre
- Elaboration d'un projet de Plan de Traitement des Risques (planning, coût, niveau de risque résiduel)
- Choix des options de traitement des risques

# Cas pratique

## Définition des échelles de mesure

Probabilité	
1	
2	
3	

Impact	
Type	_____
1	
2	
3	

Impact	
Type	_____
1	
2	
3	

GRAVITE		Impact		
		1	2	3
Proba	1			
	2			
	3			

## Phase d'identification des actifs et des risques

- Identification des actifs
  - -
  - -
  - -
  - -
  
- Identification des risques (menaces, vulnérabilités)
  - -
  - -
  - -
  - -
  - -

# Cas pratique

## Phase d'appréciation des risques

Risque	Probabilité	Impact (type1)	Impact (type2)	Impact Global	Gravité

# Cas pratique

## Choix des options de traitement (premier choix)

Risque	Gravité	Option de traitement

**Réduction du risque**

**Conservation du risque**

**Contournement du risque**

**Transfert du risque**

## Limites de l'exercice

# Cas pratique

## Phase d'identification des mesures de sécurité à mettre en œuvre

### Chapitres de l'ISO 27002 (ou annexe A de l'ISO 27001) à mettre en œuvre?

- -
- -
- -
- -
- Elaboration d'une proposition de Plan de Traitement des Risques
  - Quels sont les chantiers à mener ?
  - Quel planning et quel coût ?
  - Quel est le risque résiduel après la réalisation des chantiers?

5	Politiques de sécurité de l'information	2
5.1	Orientations de la direction en matière de sécurité de l'information	2
6	Organisation de la sécurité de l'information	4
6.1	Organisation interne	4
6.2	Appareils mobiles et télétravail	7
7	La sécurité des ressources humaines	9
7.1	Avant l'embauche	9
7.2	Pendant la durée du contrat	11
7.3	Rupture, terme ou modification du contrat de travail	14
8	Gestion des actifs	15
8.1	Responsabilités relatives aux actifs	15
8.2	Classification de l'information	16
8.3	Méthodologie de la gestion des supports	19
9	Contrôle d'accès	21
9.1	Exigences métier en matière de contrôle d'accès	21
9.2	Gestion de l'accès utilisateur	23
9.3	Responsabilités des utilisateurs	27
9.4	Contrôle de l'accès au système et aux applications	28
10	Cryptographie	31
10.1	Mesures cryptographiques	31
11	Sécurité physique et environnementale	34
11.1	Zones sécurisées	34
11.2	Matériels	37
12	Sécurité liée à l'exploitation	42
12.1	Procédures et responsabilités liées à l'exploitation	42
12.2	Protection contre les logiciels malveillants	46
12.3	Sauvegarde	47
12.4	Journalisation et surveillance	48
12.5	Maîtrise des logiciels en exploitation	50
12.6	Gestion des vulnérabilités techniques	51
12.7	Considérations sur l'audit du système d'information	53
13	Sécurité des communications	54
13.1	Management de la sécurité des réseaux	54
13.2	Transfert de l'information	56
14	Acquisition, développement et maintenance des systèmes d'information	60
14.1	Exigences de sécurité applicables aux systèmes d'information	60
14.2	Sécurité des processus de développement et d'assistance technique	63
14.3	Données de test	68
15	Relations avec les fournisseurs	69
15.1	Sécurité de l'information dans les relations avec les fournisseurs	69
15.2	Gestion de la prestation du service	72
16	Gestion des incidents liés à la sécurité de l'information	74
16.1	Gestion des incidents liés à la sécurité de l'information et améliorations	74
17	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	78
17.1	Continuité de la sécurité de l'information	78
17.2	Redondances	80
18	Conformité	81
18.1	Conformité aux obligations légales et réglementaires	81
18.2	Revue de la sécurité de l'information	84

# Agenda



## Principes du SMSI

- Introduction
- Définition du Système de Management
- Introduction aux normes ISO27001 / ISO27002



## La Gestion de Risque

- Principes de la gestion des risques
- ISO27005 / ISO31000
- Application d'EBIOS à l'identification des risques de l'entreprise



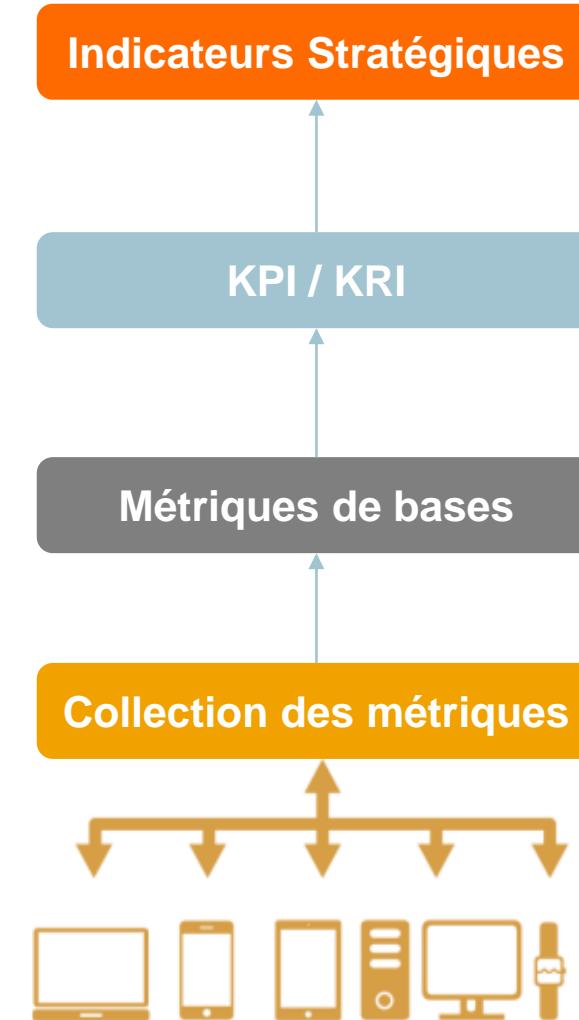
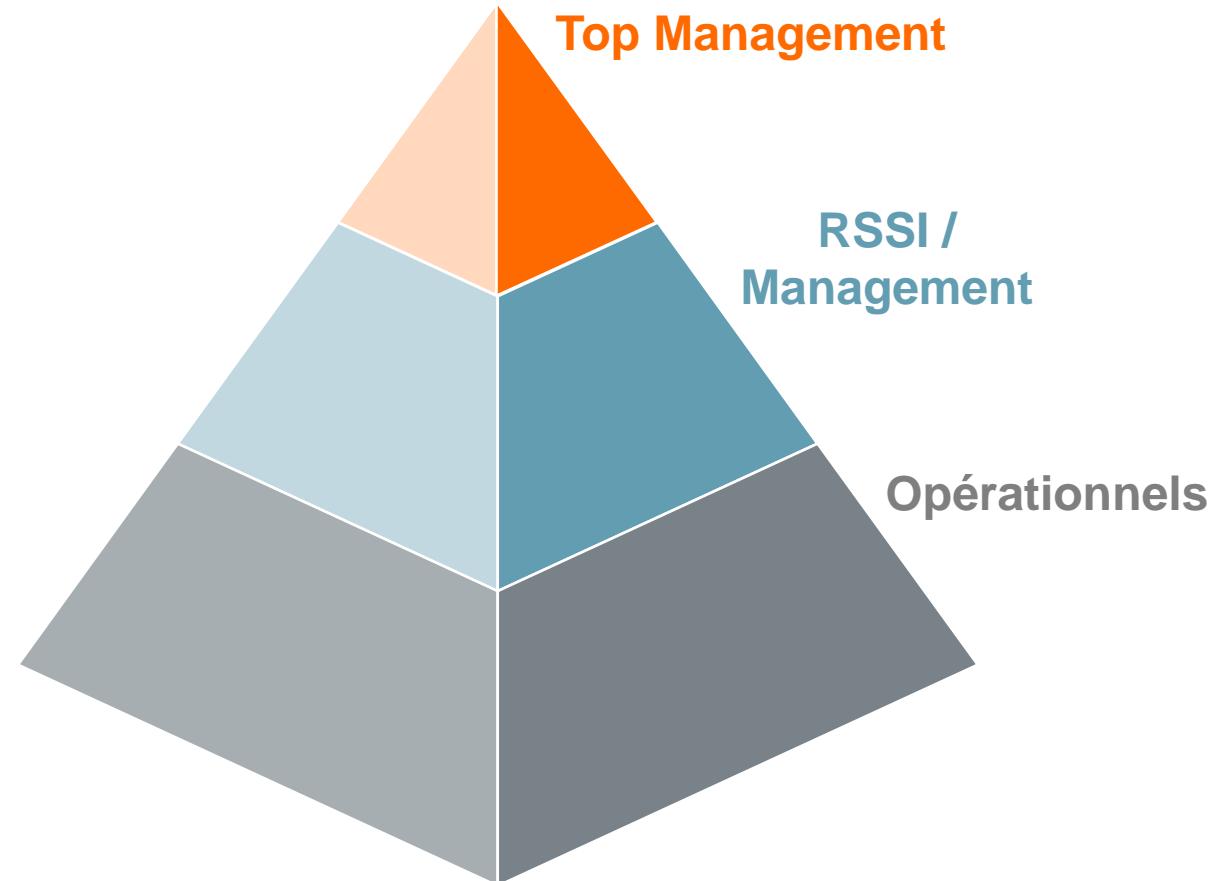
## La mise en œuvre pratique

- Plan
- Do
- Check
- Act



# Implémentation du SMSI

*Construire un tableau de bord*



# 1 Suivre le Plan de aitement

# 2

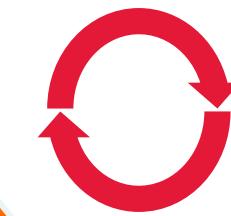
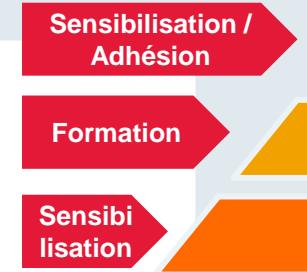
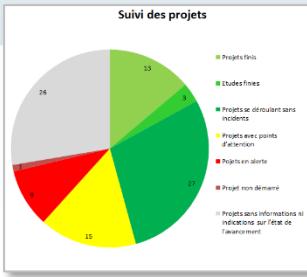
## Choisir les indicateurs de suivi

# 3 Former/ Sensibiliser

# 4

# Maintenir le SMSI

Méthode	Resumé	Description des mesures	Risque pour l'objectif	Complexité	Préférence
Sur des variables	Envoi d'offres ou un sondage à la fin de l'année.	PIB, BESI, RSE, RAE	3	Facile	
Demande des services ou les retours	Envoi d'un questionnaire à la fin de l'année. Il convient de faire des demandes de services, mais pas nécessairement volontaires, si le but est de recueillir ou renforcer la ligne de notre offre.	PDS, PDSI, RSE	1	Facile	
Evaluations, et les mesures de suivi et d'évaluation des variables déclencheuses	Des données doivent être collectées, utilisées dans les débats de l'élaboration, comparées avec les objectifs et, si nécessaire, modifiés en fonction des résultats des évaluations.	PIB, BESI, RSE, RAE	2	Facile	
Demande des services ou les retours en France	Formulation du programme de services et de l'offre de services en fonction des besoins et des intérêts des clients et partenaires.	PDS, PDSI	4	Facile	
	Formulation du programme de services et de l'offre de services en fonction des besoins et des intérêts des clients et partenaires.	PDS, PDSI	4	Facile	
	Réunions régulières des élus locaux et des élus nationaux pour discuter des sujets qui nous intéressent.	PDS, PDSI	3	Facile	
	Le conseil de fabrique doit être informé des résultats de nos enquêtes.	PDS, PDSI	3	Facile	
	Met en place une solution de suivi et d'évaluation des variables déclencheuses et de l'efficacité des stratégies.	PDS, PDSI	2	Facile	
	Formulation du programme de services et de l'offre de services en fonction des besoins et des intérêts des clients et partenaires.	PDS, PDSI	2	Facile	



# Suivre le plan de traitement – Exemple

## Tableau de bord global de la phase 1 - suivi

Météo Projet :



10/11/2019

### Résumé Etape 1 : Analyse de l'existant

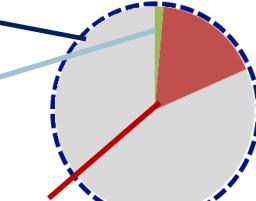
Avancement	<div style="width: 100%;">100%</div>
Respect Planning	<div style="width: 10%;"></div>
Tendance	Périmètre d'entretiens OK, fichier d'index OK
Commentaires	

### Mise à jour initiale de la base de données

**15** Applications analysées

**+1** Projet en cours

**3** Projets arrêtés



### Résumé Etapes 2 & 3 –Réalisation des entretiens DSi et métiers

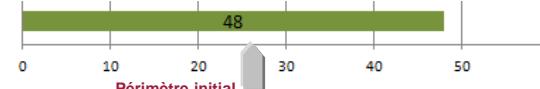
Avancement	<div style="width: 100%;">100%</div>
Respect Planning	<div style="width: 20%;"></div>
Tendance	Entretiens terminés. Analyse effectuée et CR rédigés.
Commentaires	En attente CR

### Résumé Etapes 4 – Rédaction du fichier d'analyse complète

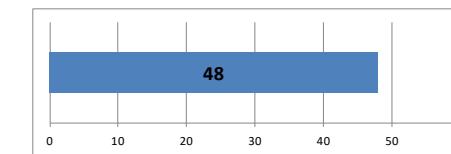
Avancement	<div style="width: 95%;">95%</div>
Respect Planning	<div style="width: 10%;"></div>
Tendance	Analyse finale initialisée : tous les entretiens ont été pris en compte.
Commentaires	Anticipation Lot 2 : Récupération de la documentation d'applications.

### Campagne d'entretiens métiers / DSi

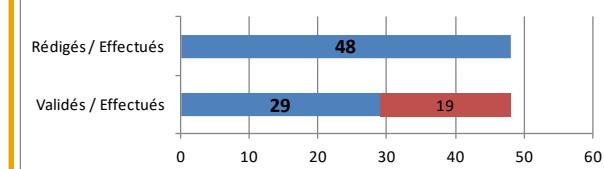
#### Entretiens planifiés / restants à planifier



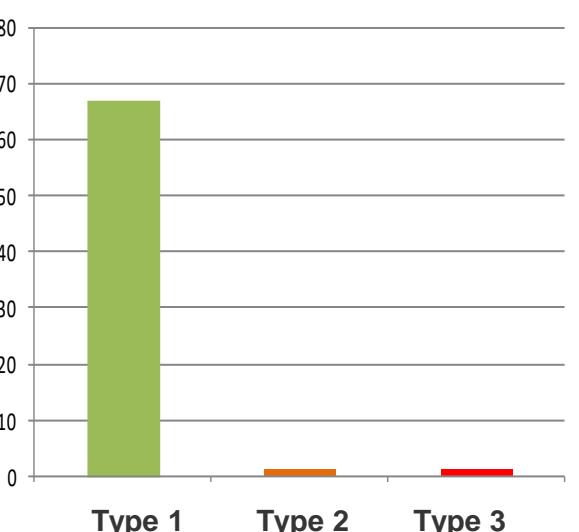
#### Entretiens effectués / total d'entretiens



#### Suivi des comptes rendus



### Synthèse de notre analyse après étude



## Les indicateurs stratégiques

Donnent une vue globale de la situation du SMSI et du niveau de traitement des risques de sécurité. Ils permettent également d'obtenir une vue sur le niveau de déploiement des mesures de sécurité.

## Les indicateurs de pilotage

Permettent de suivre la mise en œuvre du SMSI et des mesures de sécurité de manière macroscopique. Ils permettent également d'obtenir une vue globale sur le traitement des risques sur le niveau associé de mise en œuvre de la politique de sécurité par thématique

## Les indicateurs opérationnels

Rendent compte de l'efficacité des mesures décrites au sein de la PSSI et du Plan de Traitement des Risques (exemple : disponibilité du réseau).

# Indicateurs stratégiques

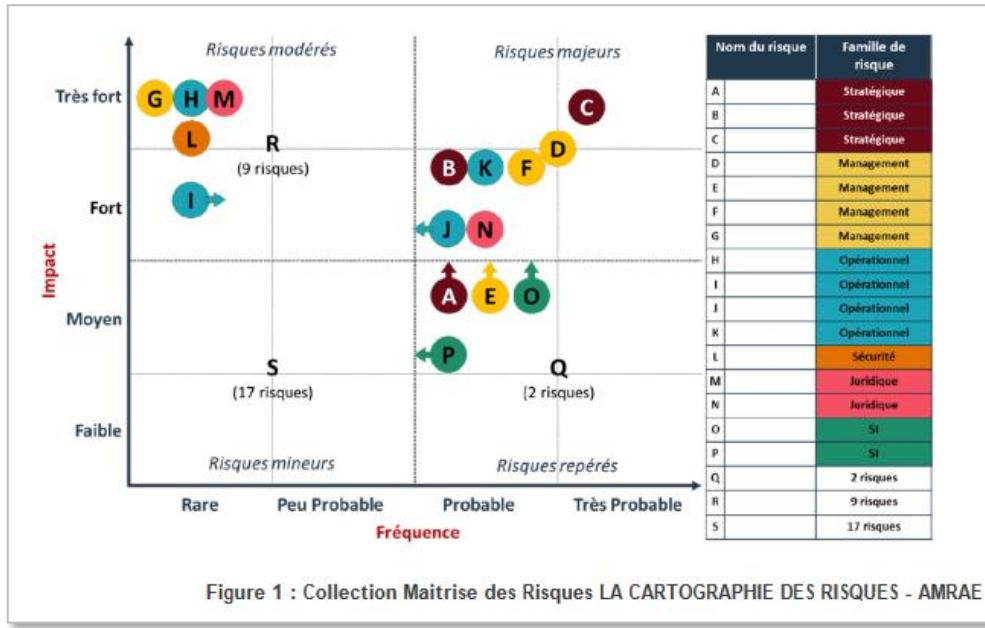


Figure 1 : Collection Maitrise des Risques LA CARTOGRAPHIE DES RISQUES - AMRAE

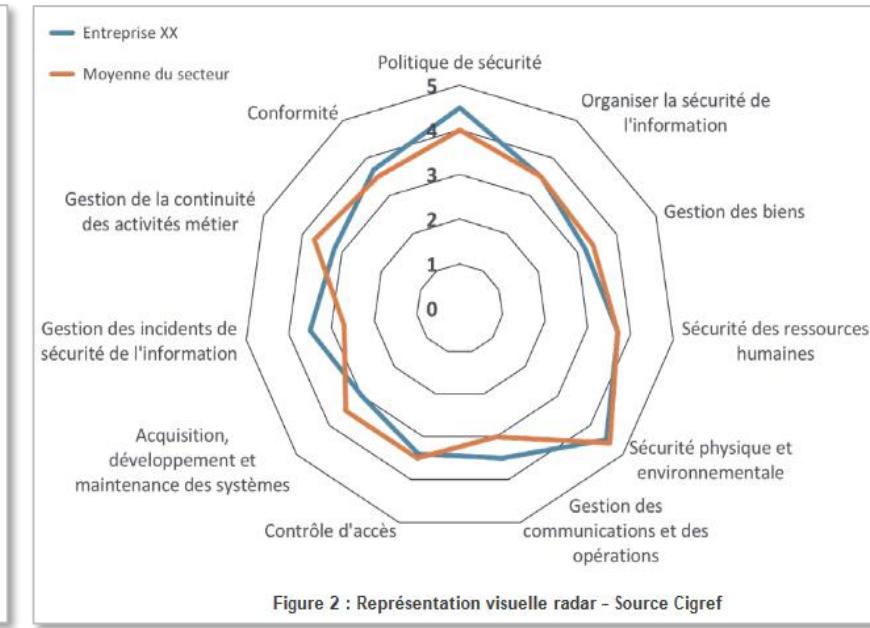
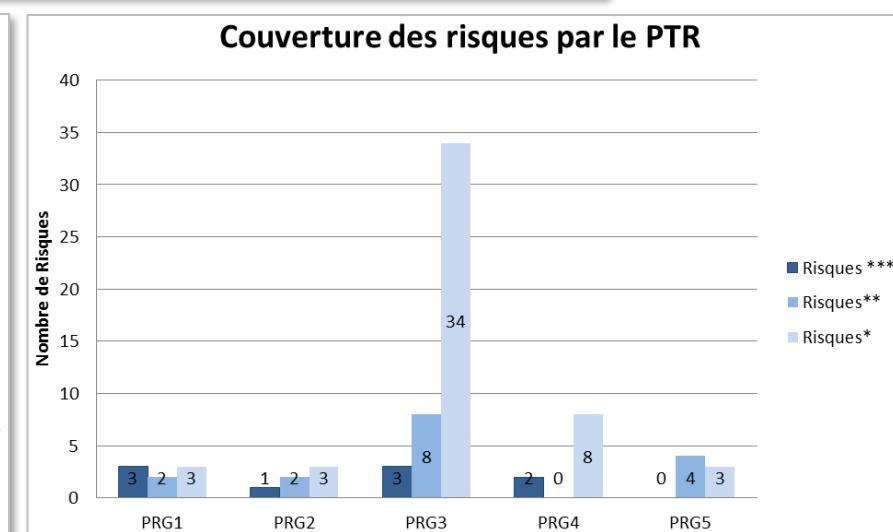
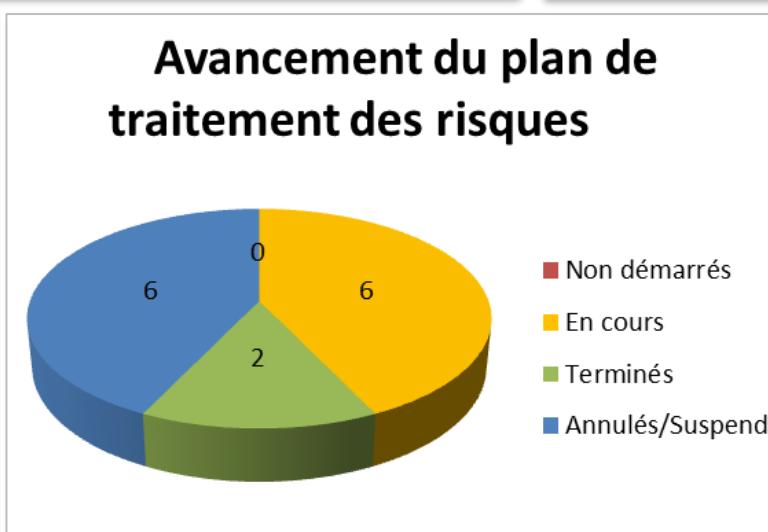
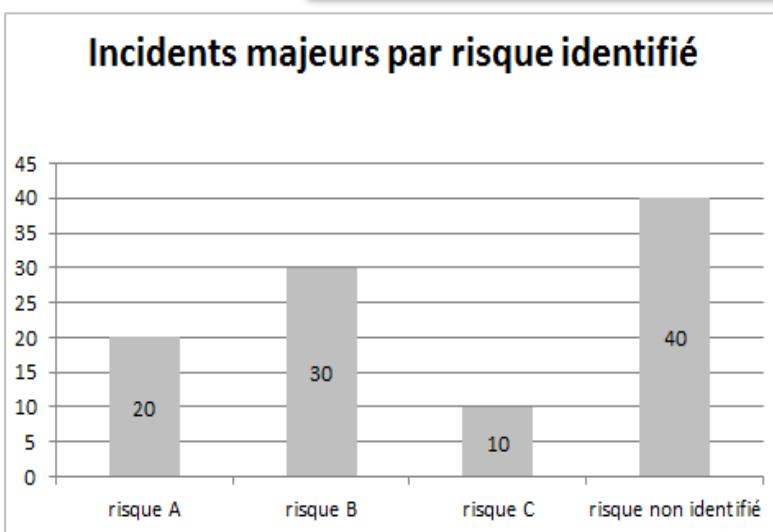
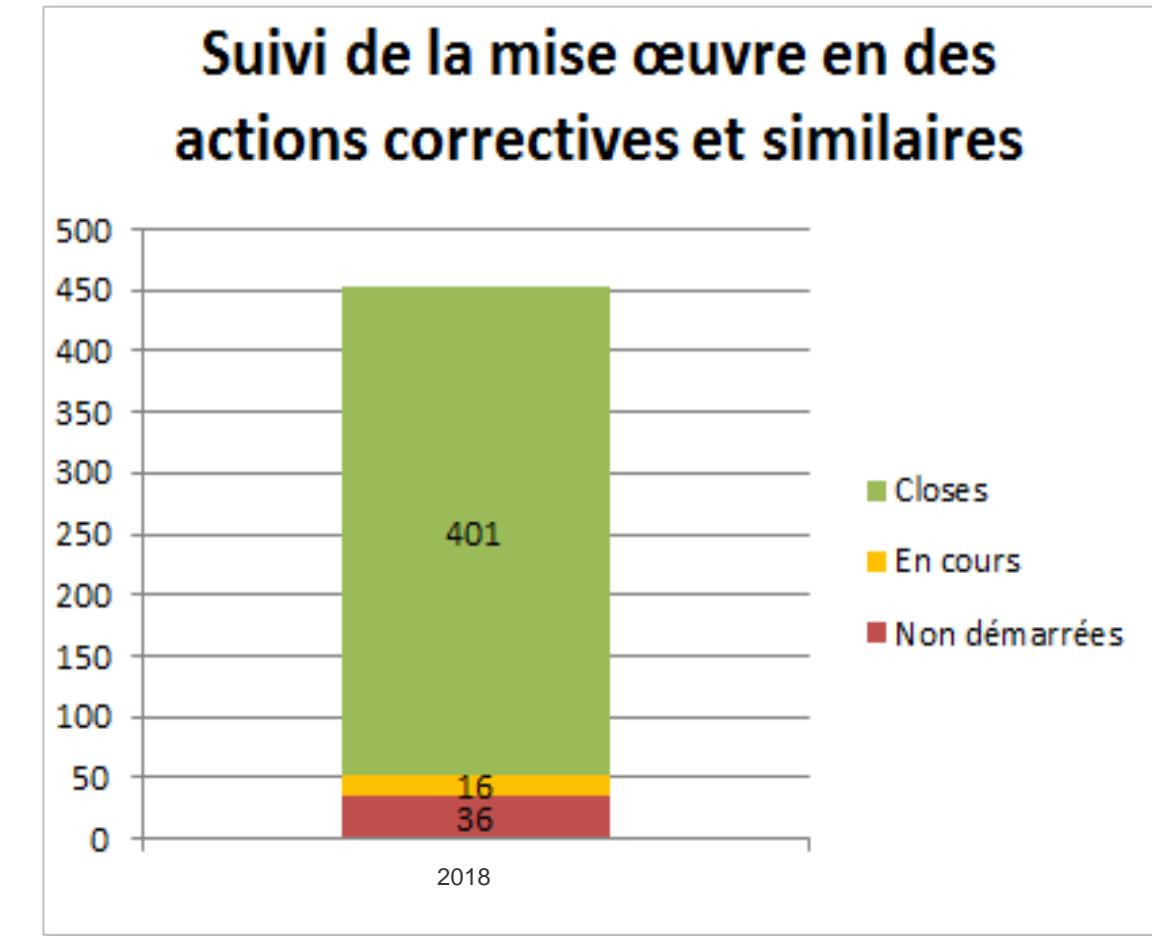
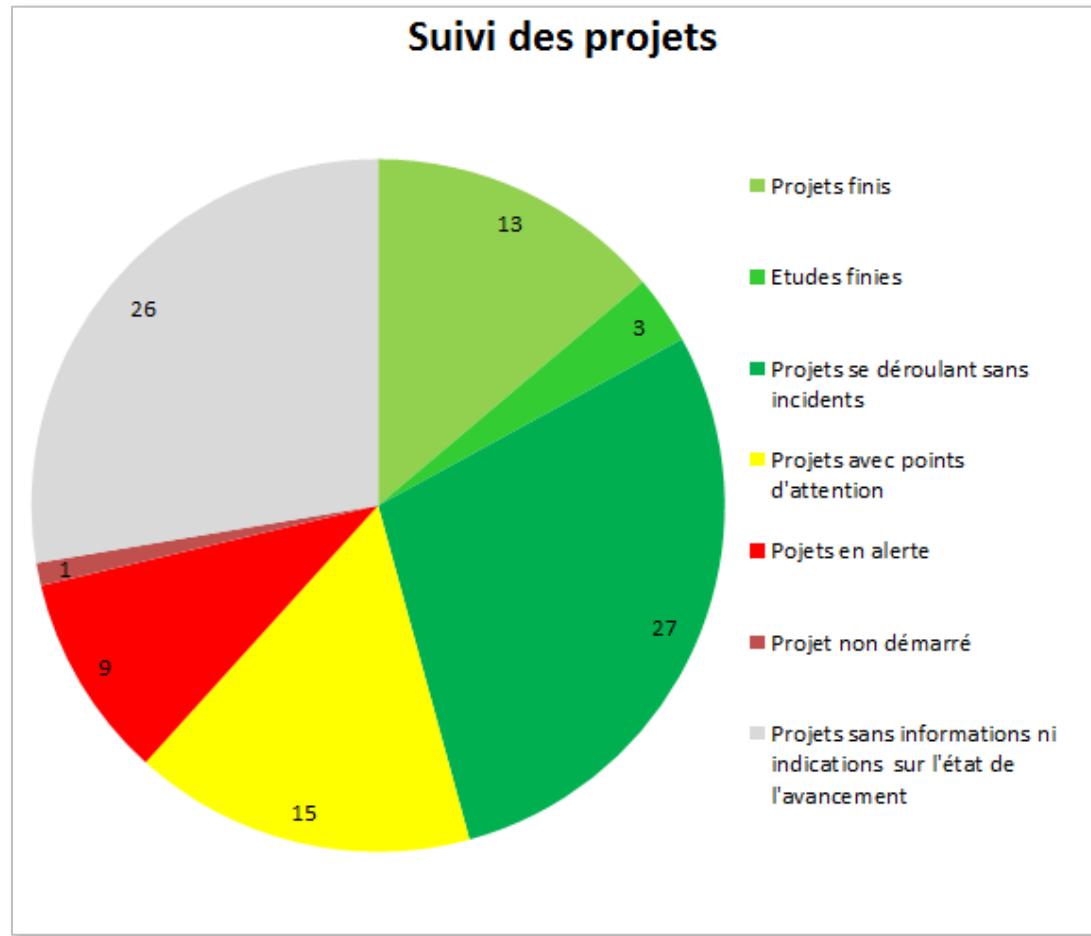


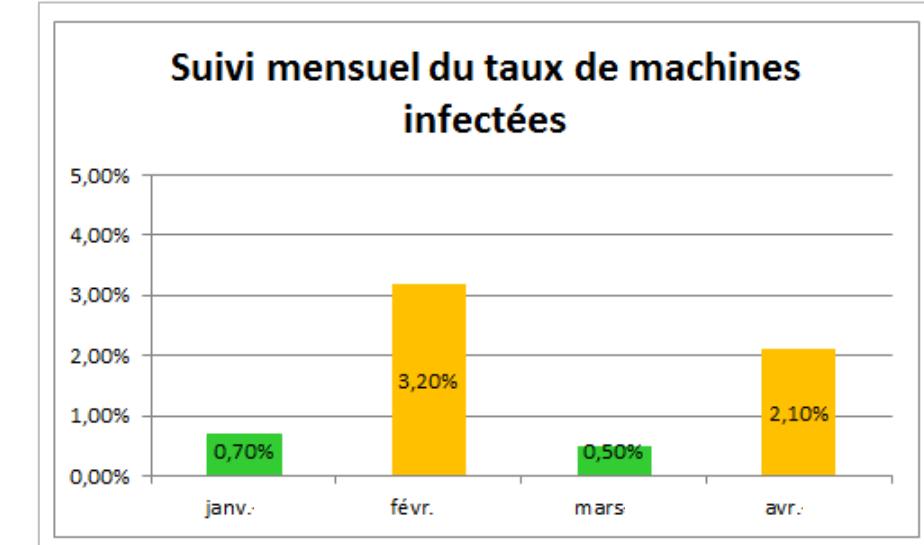
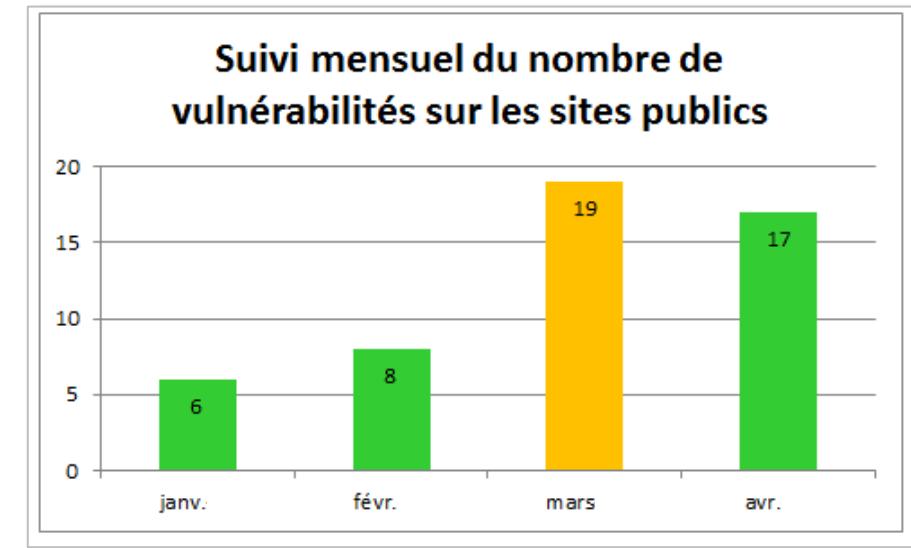
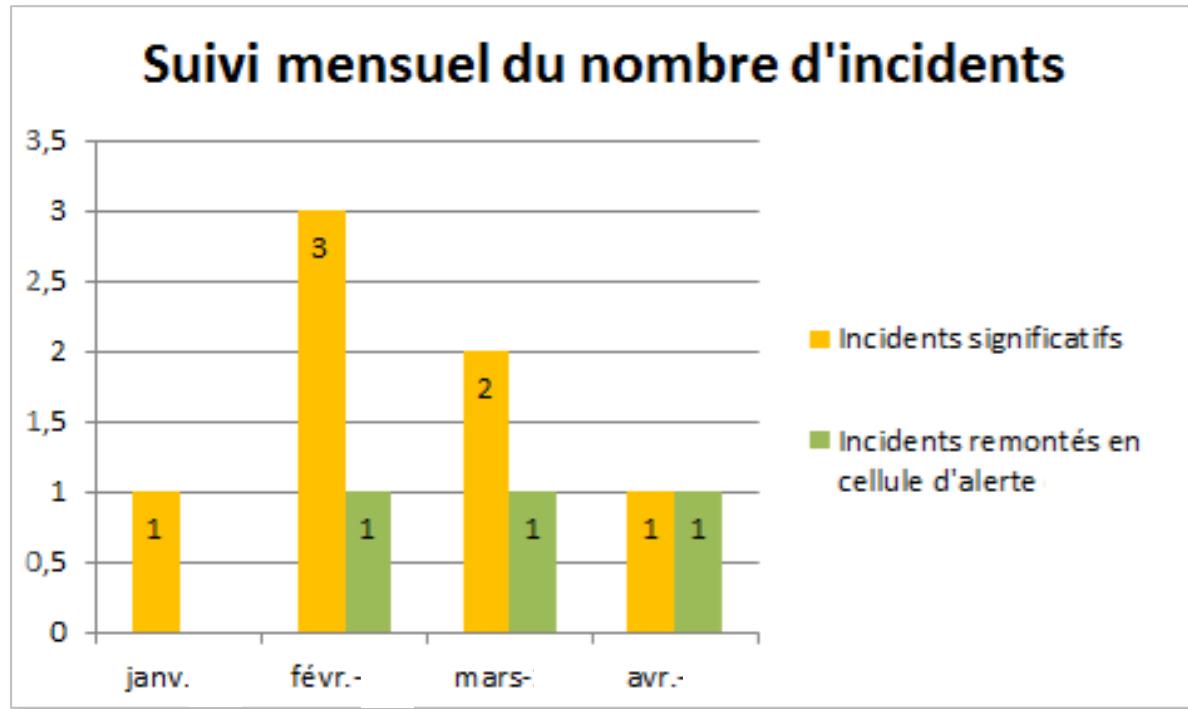
Figure 2 : Représentation visuelle radar - Source Cigref



# Indicateurs de pilotage

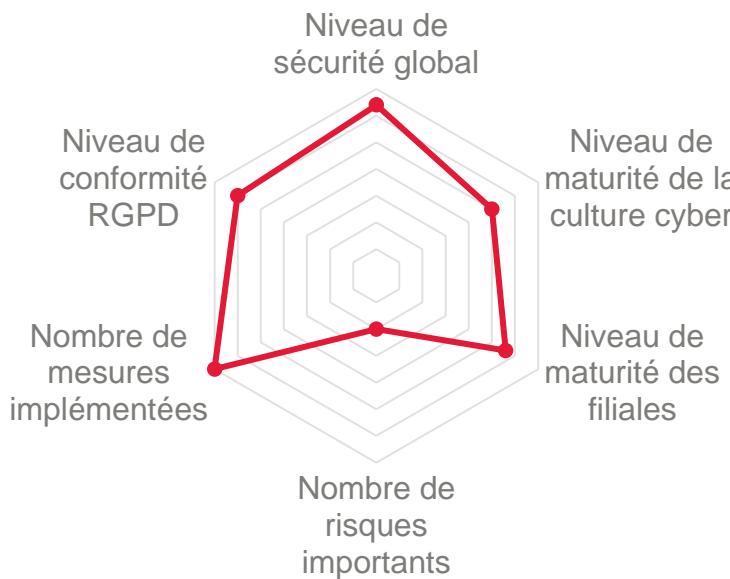


# Indicateurs opérationnels

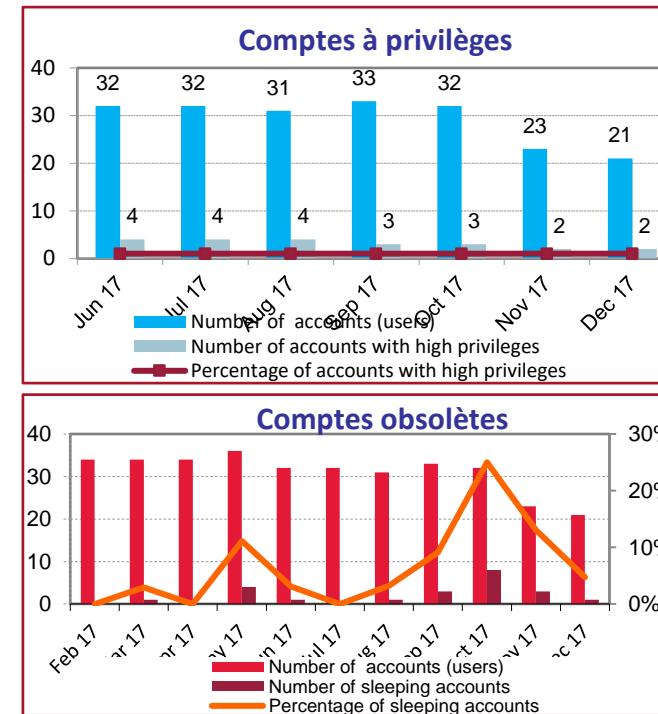


# Cadre de mise en œuvre des indicateurs de sécurité - Exemple

## Vue Top Management



## Vue Comité Cyber



## Vue Opérationnelle

- Evolution d'une infection virale sur un serveur
- % de postes nomades chiffrés
- Evolution du nb de Smartphones perdus
- Nombre d'incidents de sécurité de niveau critique
- Nombre de comptes génériques
- Proportion de comptes administrateurs désactivés
- % de tests PRA réalisés, % de tests PRA réussis
- % avancement des projets Sécurité
- Nombre de tests d'intrusion réalisés
- Nombre d'accès hors heures ouvrées au Datacenter
- % de spams traités, % de faux positifs sur l'antispam
- Nombre d'utilisateurs ayant suivi une sensibilisation à la sécurité
- Nombre d'AIPD réalisées, nombre de risques importants ou critiques non couverts

# Cadre de mise en œuvre des indicateurs de sécurité – Exemple d'indicateur de performance

Nom de l'indicateur	Délai moyen de traitement des actions SMSI														
Objectifs concernés	Renforcer la confiance accordée par les clients et partenaires														
Déclinaison de l'objectif	Réduire le délai de traitement des actions de sécurisation														
Type d'indicateur	Indicateur de suivi / <u>performance</u>														
Cible / Seuil	150 jours														
Méthode de calcul	Moyenne (date d'ouverture de l'action – date de clôture de l'action) par an														
Fréquence de production	Bimensuelle														
Producteur	Equipe SSI														
Fréquence de revue	Bimensuelle														
Tableau de bord concerné	Stratégique / <u>Pilotage</u> / Opérationnel														
Lieu de stockage	Support de comité de pilotage SSI														
Evaluateur	Equipe SMSI														
Exemple d'illustration	<div style="text-align: center;"><p><b>Délai moyen de traitement des actions SMSI</b></p><table border="1"><thead><tr><th>Année</th><th>Délai moyen (jours)</th></tr></thead><tbody><tr><td>2008</td><td>~50</td></tr><tr><td>2009</td><td>~250</td></tr><tr><td>2010</td><td>~350</td></tr><tr><td>2011</td><td>~500</td></tr><tr><td>2013</td><td>~1200</td></tr><tr><td>2014</td><td>~100</td></tr></tbody></table></div>	Année	Délai moyen (jours)	2008	~50	2009	~250	2010	~350	2011	~500	2013	~1200	2014	~100
Année	Délai moyen (jours)														
2008	~50														
2009	~250														
2010	~350														
2011	~500														
2013	~1200														
2014	~100														

# Cadre de mise en œuvre des indicateurs de sécurité – Exemple d'indicateur de suivi/performance

Nom de l'indicateur	
Objectifs concernés	
Déclinaison de l'objectif	
Type d'indicateur	
Cible / Seuil	
Méthode de calcul	
Fréquence de production	
Producteur	
Fréquence de revue	
Tableau de bord concerné	
Lieu de stockage	
Evaluateur	
Exemple d'illustration	

# Exigences concernant la formation et la sensibilisation

L'organisme doit **s'assurer que tout le personnel**, dont les responsabilités qui lui ont été affectées sont définies dans le SMSI, **a les compétences nécessaires pour exécuter les tâches requises**, en :

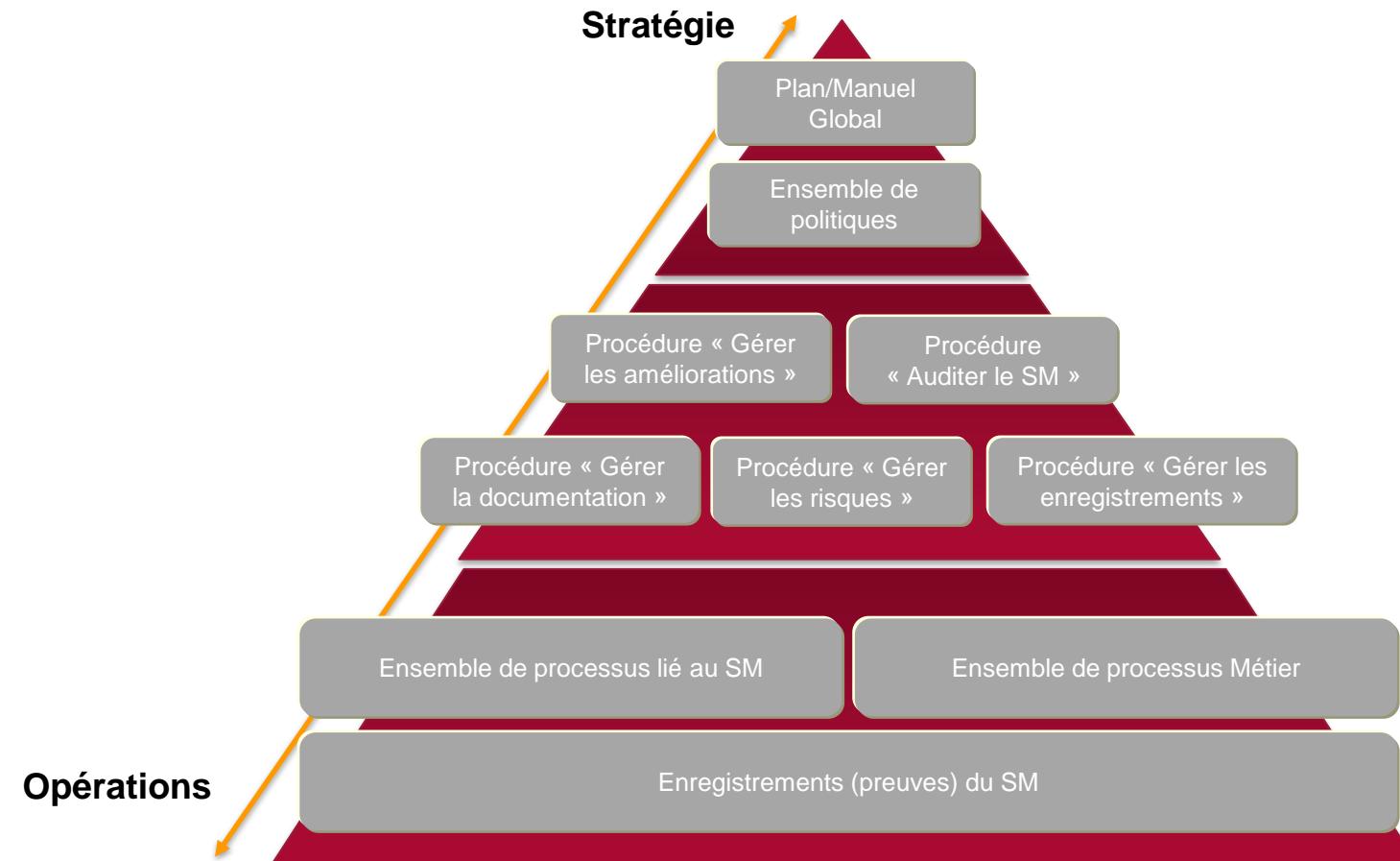
- déterminant les compétences nécessaires pour le personnel effectuant un travail ayant une incidence sur le SMSI
- pourvoyant à la formation ou en entreprenant d'autres actions (par exemple emploi d'un personnel compétent) pour satisfaire ces besoins
- évaluant l'efficacité des actions entreprises
- conservant les enregistrements concernant la formation initiale et professionnelle, le savoir-faire, l'expérience et les qualifications

L'organisme doit également s'assurer que tout le personnel approprié a conscience de la pertinence et de l'importance de ses activités liées à la sécurité de l'information et de la façon dont ces dernières contribuent à l'atteinte des objectifs du SMSI.

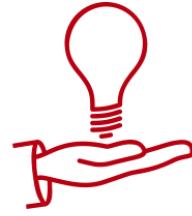
# Formation et sensibilisation en sécurité



Un ensemble documentaire hiérarchisé sous forme pyramidale → à maintenir à jour



# Agenda



## Principes du SMSI

- Introduction
- Définition du Système de Management
- Introduction aux normes ISO27001 / ISO27002



## La Gestion de Risque

- Principes de la gestion des risques
- ISO27005 / ISO31000
- Application d'EBIOS à l'identification des risques de l'entreprise



## La mise en œuvre pratique

- Plan
- Do
- Check
- Act



# Les différents types d'audit

Interne

Externe

Conformité

Règlements

RGPD, NIS, ePrivacy

Conformité clients

ISAE 3402, Annexe de Sécurité, PAS

Homologations

Homologations LPM

Organisationnels

Systèmes de Management

ISO 27001, 22301, COBIT

Bonnes Pratiques

COBIT, ITIL, ISO 27002

Techniques

Tests d'intrusion

Boites, Red Team, Bug Bounty

Audits de code

Audit de configuration

Audit d'architecture

# Différences entre audit et analyse de risques



## ANALYSE DE RISQUES

Une analyse de risques vise à identifier les conséquences de l'exploitation d'une vulnérabilité éventuelle et hypothétique.

L'analyse de risques se réalise plutôt en début de projet dans le but d'inclure les mesures de sécurité au cours de la réalisation du projet.

L'analyse permet de prioriser les actions à mener sur le projet. Certains risques étant plus graves et probables, les efforts se porteront d'abord sur eux.

## AUDIT

L'audit se réalise plutôt en fin de projet, sur une infrastructure existante, dans le but d'identifier ses vulnérabilités.

L'audit préconise des mesures de sécurité afin de corriger les vulnérabilités qui ont été détectées.

- **L'organisme doit mener des audits internes du SMSI à intervalles planifiés pour déterminer si les objectifs des mesures, les mesures, les processus et les procédures de son SMSI :**
  - sont **conformes aux exigences de l'ISO27001 et à la législation ou aux règlements pertinents** ;
  - sont **conformes aux exigences de sécurité de l'information identifiées** ;
  - sont **mis en œuvre et tenus à jour de manière efficace** et
  - sont **exécutés tel que prévu**
- Un programme d'audit doit être planifié en tenant compte de l'état et de l'importance des processus et des domaines à auditer, ainsi que des résultats des audits précédents.
- Les critères, le champ, la fréquence et les méthodes d'audit doivent être définis.
- Le choix des auditeurs et la réalisation des audits doivent assurer l'objectivité et l'impartialité du processus d'audit.
- Les auditeurs ne doivent pas auditer leur propre travail.
- Les responsabilités et les exigences pour planifier, mener les audits, rendre compte des résultats et conserver des enregistrements doivent être définies dans une procédure documentée.
- L'encadrement responsable du domaine audité doit assurer que des actions sont entreprises sans délai indu pour éliminer les non-conformités détectées et leurs causes.
- Les activités de suivi doivent inclure la vérification des actions entreprises et le compte-rendu des résultats de cette vérification

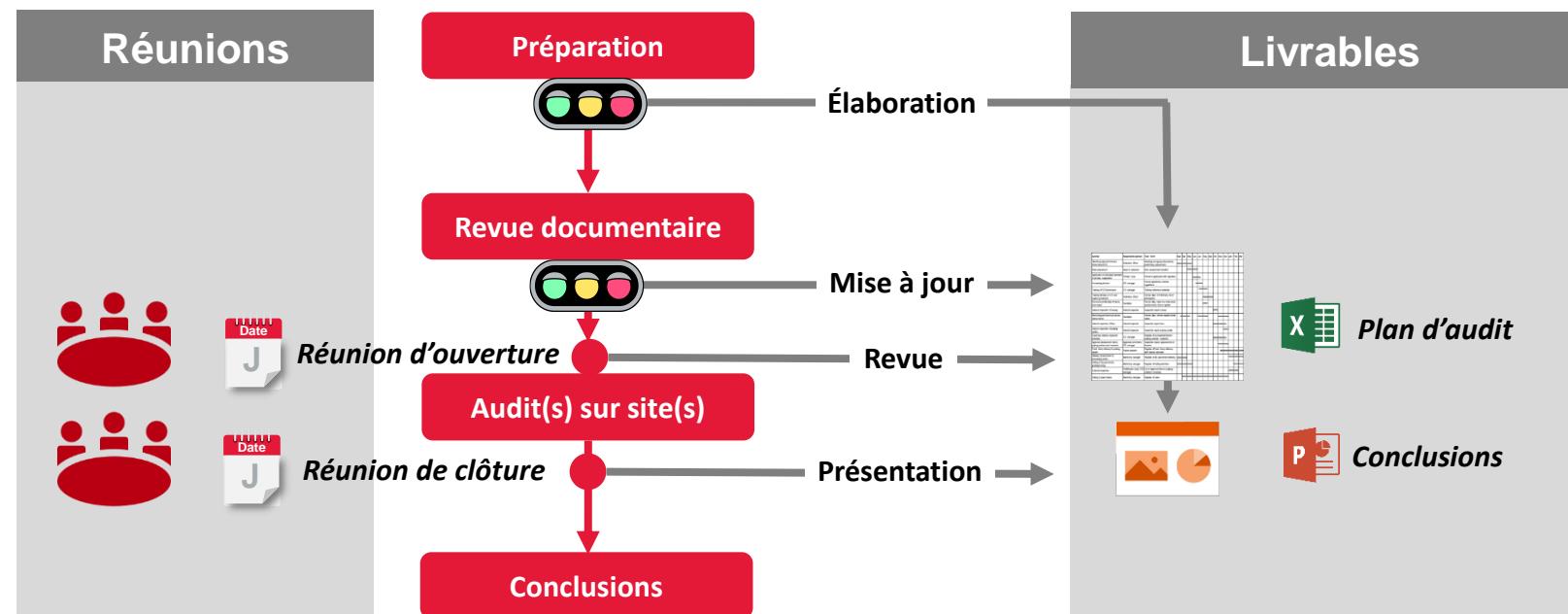
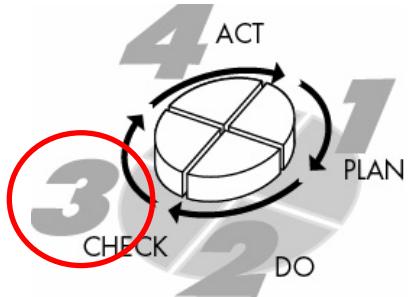
# Procéder à des audits à blanc

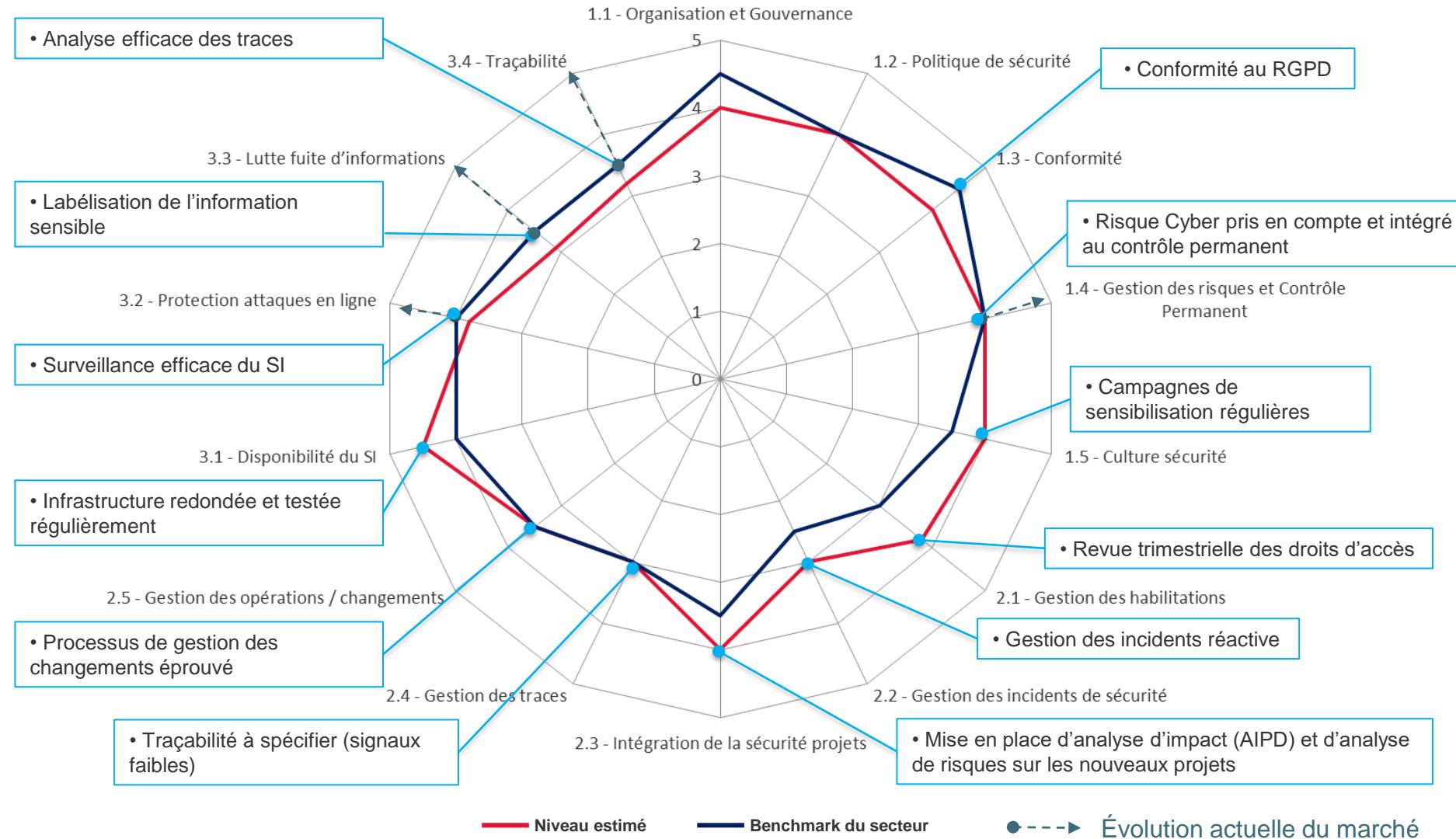
Il est important de pouvoir démontrer la relation entre

- les objectifs définis dans la politique du SMSI.
- les résultats du processus d'appréciation du risque et de traitement du risque,
- les mesures sélectionnées

La documentation doit inclure les enregistrements des décisions de gestion et s'assurer que

- les actions entreprises sont identifiables
- les résultats consignés sont reproductibles.





# Audits techniques de vérification de l'application des mesures de sécurité

Action à réaliser	Audit technique	Audit de code	Tests d'intrusion
Mettre à l'épreuve la résistance des environnements testés	+	++	+++
Identifier avec un niveau d'assurance et d'efficience élevé les failles techniques entraînant des risques d'atteinte à la sécurité des environnements audités	++	+++	+
Identifier les risques métiers les plus importants liés aux failles techniques identifiées	+++	+++	+++
Obtenir des recommandations efficaces et précises pour réduire les risques	++	+++	+
Mesurer les progrès et le respect des règles	+++	++	++
Remplir les obligations de conformité et de contrôle périodique	+++	+	++
Tester l'application des procédures de réaction aux incidents et la réactivité des équipes IT	+	+	+++
Sensibiliser les acteurs (IT, management, utilisateurs)	+	+	+++
Atteindre ces objectifs avec un impact minimal sur les SI et les équipes IT et autres interlocuteurs	++	+++	++
Atteindre ces objectifs en maîtrisant la communication interne sur les résultats	++	++	+++

# Concepts généraux de l'audit du Système de Management

## Un audit a pour objectif

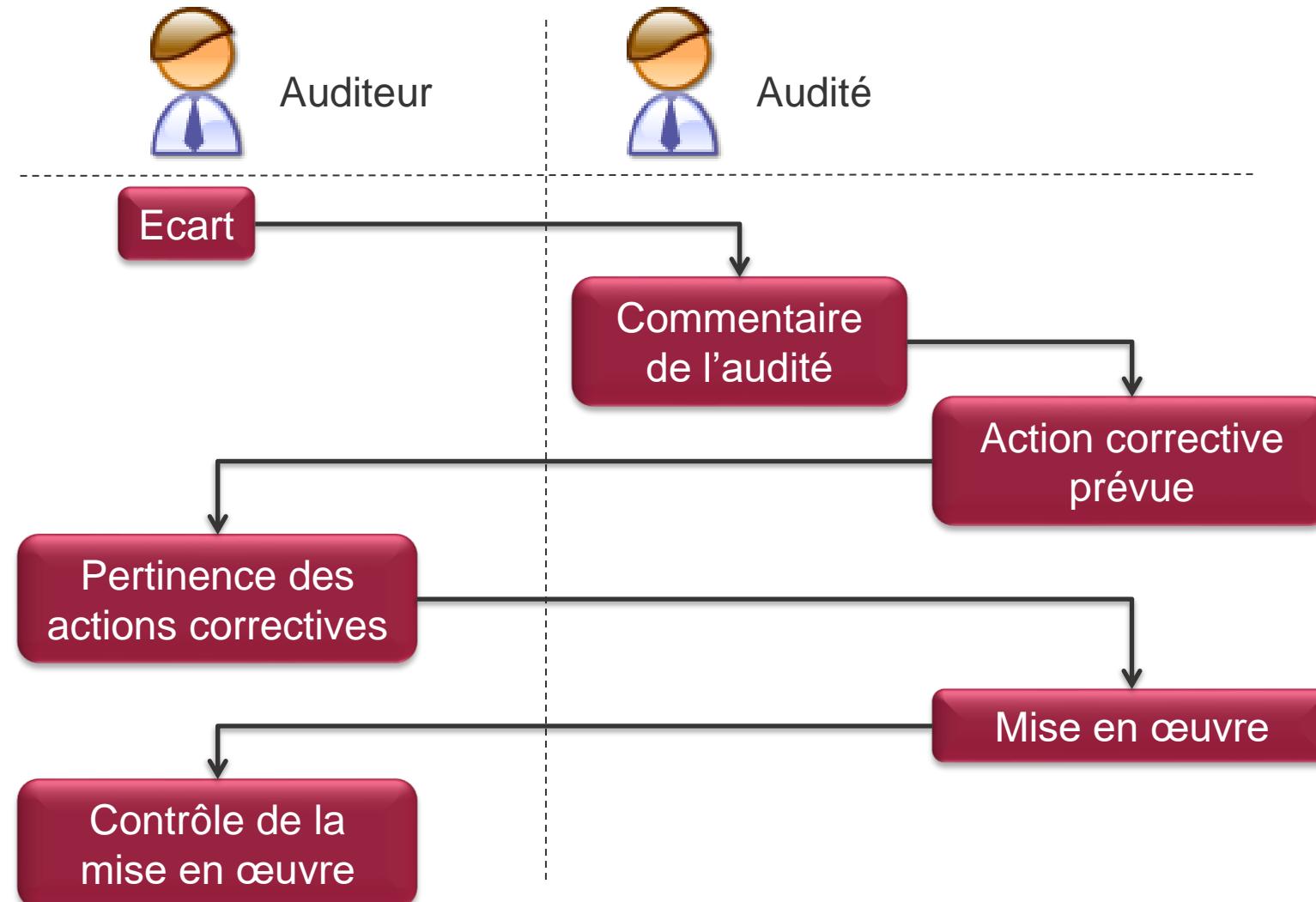
- De faire une photo d'une situation à un instant t
- De démontrer d'un niveau de conformité à un référentiel

## Méthodologie d'audit selon l'ISO 19011

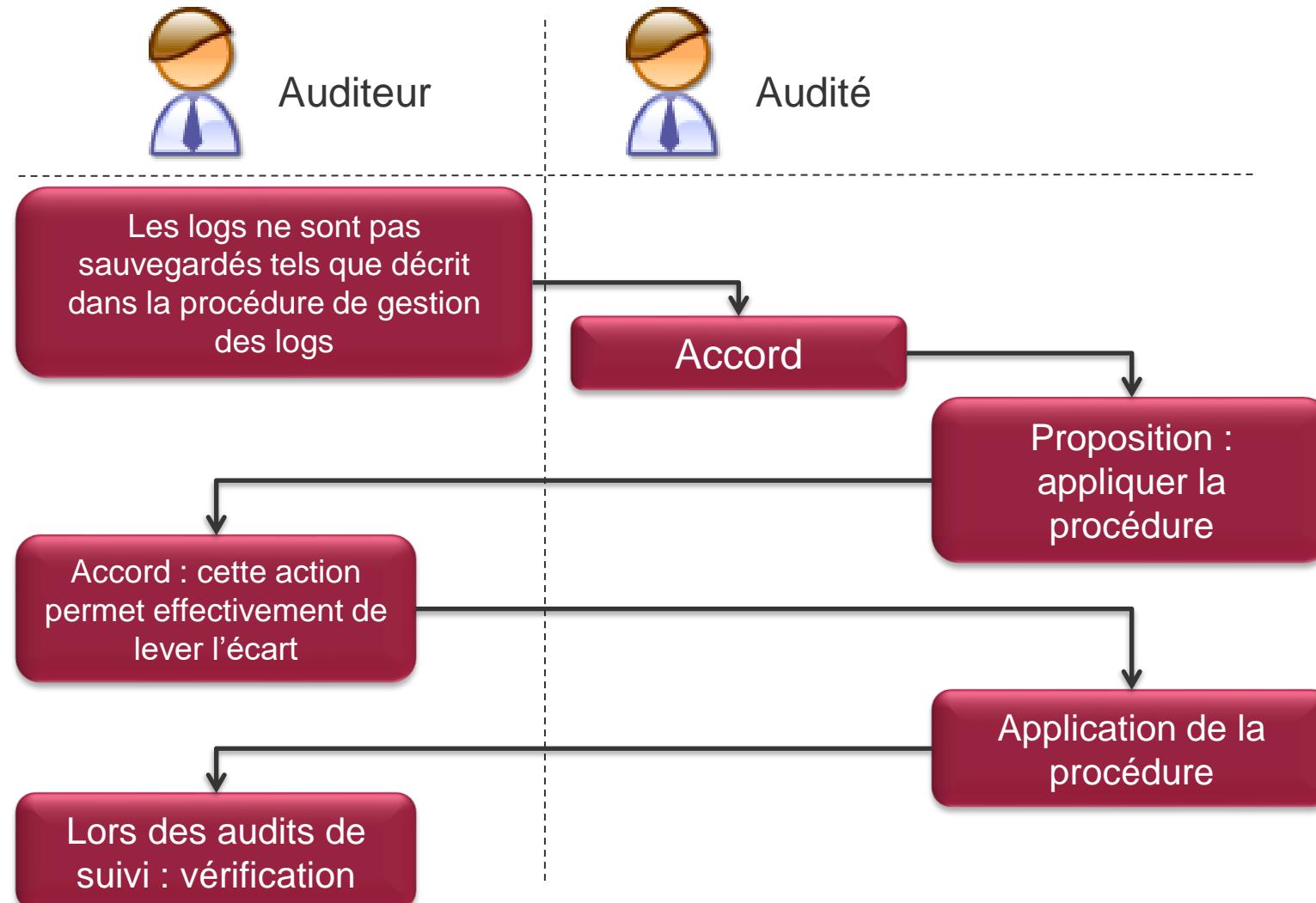
- Préparation
- Exécution
- Rapport
- Restitution



# Démarche d'identification d'un écart [1/2]



# Démarche d'identification d'un écart [2/2]



# Exemple de classification des écarts

## LAC1 : Attribution des identifiants utilisateurs

Chaque utilisateur ayant accès au système d'information doit être reconnu par un identifiant utilisateur personnalisé. L'utilisation du même identifiant utilisateur par plus d'une personne est strictement interdite. [...]

Niveau de non-conformité	Définition
<b>Majeure</b>	<p>L'exigence n'est pas respectée. Ce non-respect met en danger de manière significative la sécurité du ou des systèmes / métiers.</p> <p><u>Exemple :</u> L'utilisation d'identifiants génériques est généralisée.</p>
<b>Mineure</b>	<p>L'exigence n'est pas respectée. Ce non-respect met en danger la sécurité de l'activité d'un utilisateur ou d'un groupe d'utilisateurs.</p> <p><u>Exemple :</u> Il existe des identifiants génériques.</p>
<b>Remarque</b>	<p>L'exigence est respectée. Il existe cependant des possibilités d'amélioration (efficacité, coûts, délais, etc.)</p> <p><u>Exemple :</u> La suppression des identifiants génériques est effectuée manuellement. Elle pourrait être facilité par l'utilisation d'un outil.</p>
Type de non-conformité	Définition
<b>Application</b>	<b>Une procédure existe mais n'est pas appliquée.</b>
<b>Procédure</b>	<b>La procédure n'existe pas.</b>

## La revue documentaire

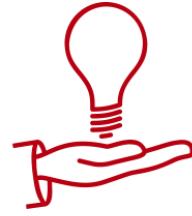
- détermine la conformité de la documentation
- peut être un point d'arrêt de l'audit : si la documentation n'est « massivement » pas conforme, le responsable de l'équipe d'audit peut suspendre l'audit.

## Le plan d'audit

- rappelle des accords entre auditeur et audité (objectif, périmètre, langue de travail, etc.)
- précise le planning détaillé de l'audit (qui, quand, quoi, où ?)

**« L'audité a toujours le bénéfice du doute »**

# Agenda



## Principes du SMSI

- Introduction
- Définition du Système de Management
- Introduction aux normes ISO27001 / ISO27002



## La Gestion de Risque

- Principes de la gestion des risques
- ISO27005 / ISO31000
- Application d'EBIOS à l'identification des risques de l'entreprise



## La mise en œuvre pratique

- Plan
- Do
- Check
- **Act**





L'organisme doit améliorer en permanence l'**efficacité du SMSI** ➤ **PDCA**



## Actions correctives

- L'organisme doit mener des **actions pour éliminer les causes de non-conformités avec les exigences du SMSI**, afin d'éviter qu'elles ne se reproduisent.
- La **procédure documentée pour l'action corrective doit définir les exigences relatives à**
  - l'identification des non-conformités
  - la détermination des causes des non-conformités
  - l'évaluation du besoin d'entreprendre des actions pour que les non-conformités ne se reproduisent pas
  - la détermination et la mise en œuvre de l'action corrective requise
  - la consignation des résultats de l'action entreprise et le réexamen de l'action corrective entreprise

## Actions préventives

- L'organisme doit **déterminer l'action permettant d'éliminer la cause des non-conformités potentielles** avec les exigences du SMSI, afin d'éviter qu'elles ne surviennent
- Les **actions préventives** doivent être adaptées aux **effets des problèmes potentiels**
- La **procédure documentée** pour l'action préventive **doit définir les exigences relatives à**
  - L'identification des non-conformités potentielles et de leurs causes
  - L'évaluation du besoin d'entreprendre des actions pour éviter l'apparition de non-conformités
  - La détermination et la mise en œuvre de l'action préventive requise
  - La consignation des résultats de l'action entreprise et
  - Le réexamen de l'action préventive entreprise
- L'organisme doit **identifier les risques modifiés et les exigences relatives aux actions préventives**, en concentrant son attention sur les risques soumis à une modification importante
- La **priorité des actions préventives** doit être déterminée sur la base des résultats de l'**appréciation du risque**

# Gestion des actions correctives et préventives

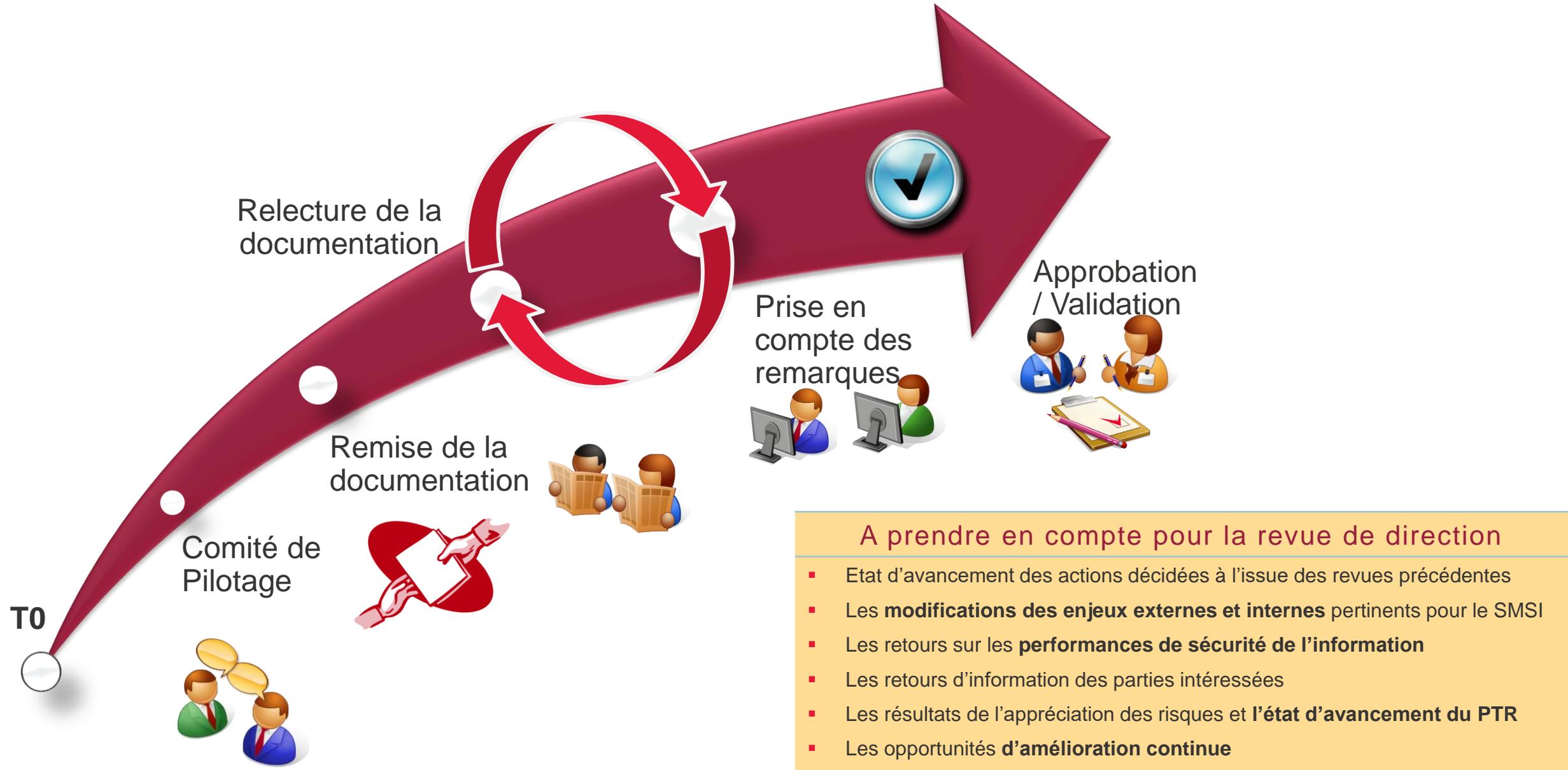
N°	Type de remarque	Critère	Description de la remarque	Description de l'action	Responsable	Date
1	Ecart	4.2.3.b 4.2.3.c	Indicateurs du SMSI non mesurés, absence d'indicateur d'efficacité du SMSI.	Mesure des indicateurs du SMSI. Création d'indicateurs d'efficacité.		
2	Ecart	4.2.1.h	Les niveaux de risques à obtenir à l'issue des chantiers mis en oeuvre dans le plan de traitement des risques ne sont pas définis. Validation de la Direction Générale à formaliser.	Formalisation des niveaux de risque résiduels et validation de la Direction Générale.		
4	Ecart	8	Procédures d'actions correctives et préventives non mises en œuvre.	Mise en œuvre de la procédure d'actions correctives et préventives à compter du 08/07/2008.		
7	Ecart	4.3.3	La gestion des enregistrements n'est traitée qu'en partie. Les éléments d'identification, de conservation et d'élimination doivent être mieux définies par les directions concernées.	Modification de la procédure de gestion des enregistrements.		
8	Ecart	4.3.2	L'identification des documents d'origine extérieure n'est pas traitée dans la procédure de gestion documentaire du SMSI.	Modification de la procédure des gestion documentaire.		
9	Ecart	A.15.1.1	Le suivi des évolutions des textes réglementaires est insuffisamment formalisé (Nature des évolutions, Dates des évolutions, Date de mise à jour du récapitulatif).	Amélioration du suivi des évolutions réglementaires.		
10	Ecart	A.10.5	La politique de sauvegarde n'est pas formalisée.	Rédaction de la politique de sauvegarde.		

## Objectifs

- La direction doit, à intervalles planifiés (au moins une fois par an), procéder au réexamen du SMSI de l'organisme pour assurer qu'il demeure pertinent, adéquat et efficace.
- Ce réexamen doit comprendre l'évaluation des opportunités d'amélioration et du besoin de modifier le SMSI, y compris la politique et les objectifs des mesures de l'information.
- Les résultats des réexamens doivent être clairement documentés et les enregistrements doivent être conservés

## Eléments d'entrée du réexamen

- Les éléments d'entrée d'une revue de direction doivent comprendre des informations sur :
  - Les résultats des audits et des réexamens du SMSI ;
  - Les retours d'information des parties intéressées ;
  - Les techniques, produits ou procédures que pourrait utiliser l'organisme pour améliorer les performances et l'efficacité du SMSI ;
  - L'état des actions préventives et correctives ;
  - Les vulnérabilités ou les menaces qui n'ont pas été traitées de manière adéquate dans l'appréciation du risque précédente ;
  - Les résultats des mesures de l'efficacité ;
  - Les actions de suivi issues des revues de direction précédentes ;
  - Tous changements pouvant affecter le SMSI et
  - Les recommandations d'amélioration.



## Eléments de sortie du réexamen

- Les éléments de sortie de la revue de direction doivent comprendre les décisions et actions relatives aux informations suivantes :
  - L'amélioration de l'efficacité du SMSI ;
  - La mise à jour du plan d'appréciation du risque et de traitement du risque ;
  - La modification des procédures et mesures qui affectent la sécurité de l'information, si nécessaire, pour répondre aux événements intérieurs ou extérieurs qui peuvent exercer une influence sur le SMSI, y compris les modifications :
    - Des exigences métier ;
    - Des exigences de sécurité ;
    - Des processus métier affectant les exigences métier existantes ;
    - Des exigences légales ou réglementaires ;
    - Des obligations contractuelles et
    - Des niveaux de risque et/ou des critères d'acceptation des risques.
  - Les besoins en ressources ;
  - L'amélioration de la méthode d'évaluation de l'efficacité des mesures.

## L'organisme doit déterminer et fournir les ressources nécessaires pour

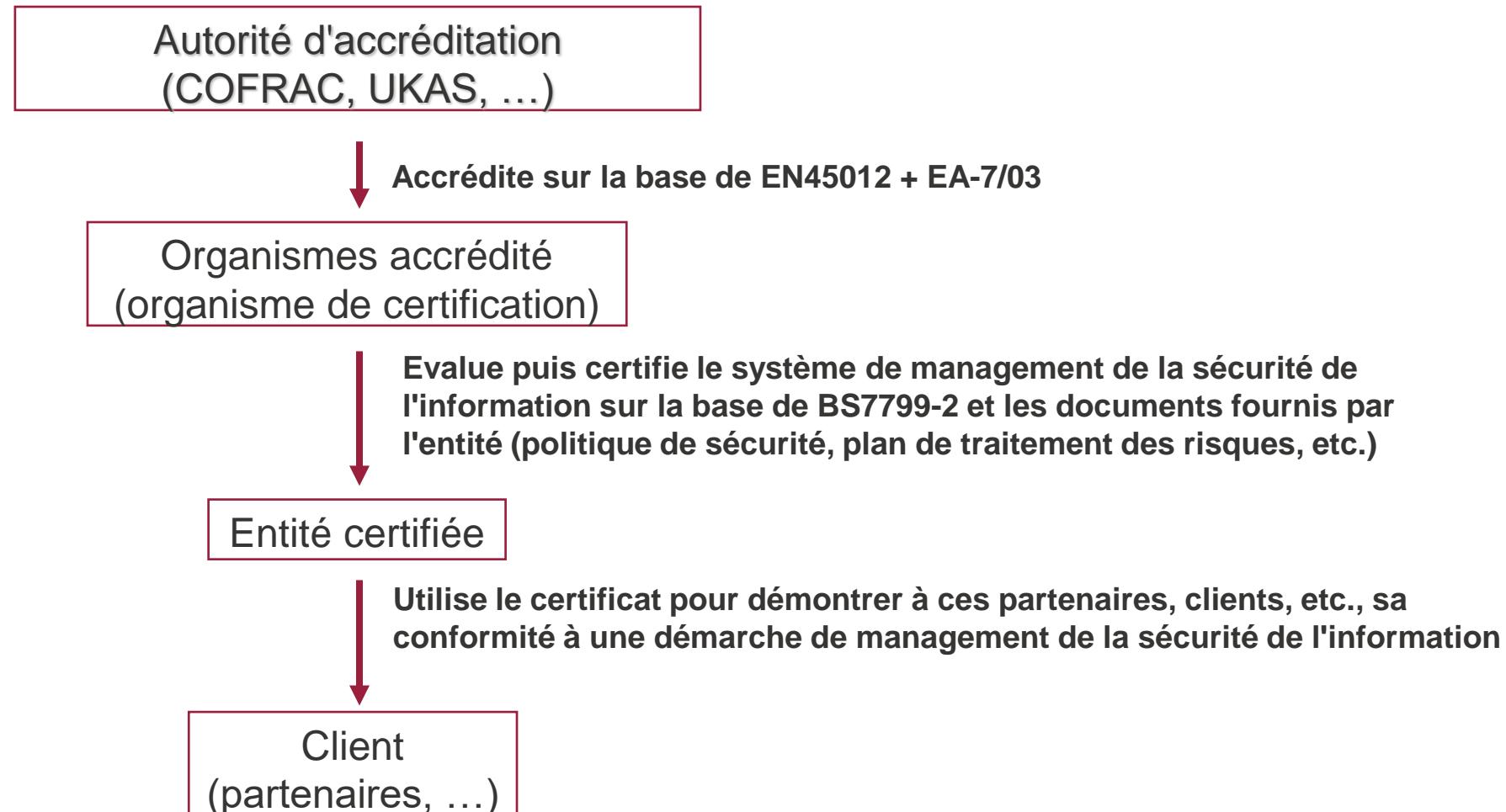
- Etablir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer un SMSI ;
- Assurer que les procédures de sécurité de l'information soutiennent les exigences métier ;
- Identifier et traiter les exigences légales et réglementaires, ainsi que les obligations de sécurité contractuelles ;
- Maintenir une sécurité adéquate par une application correcte de toutes les mesures mises en œuvre ;
- Effectuer des réexamens si nécessaire, et réagir de manière appropriée aux résultats de ces réexamens et
- Améliorer, le cas échéant, l'efficacité du SMSI.

# Focus sur la certification

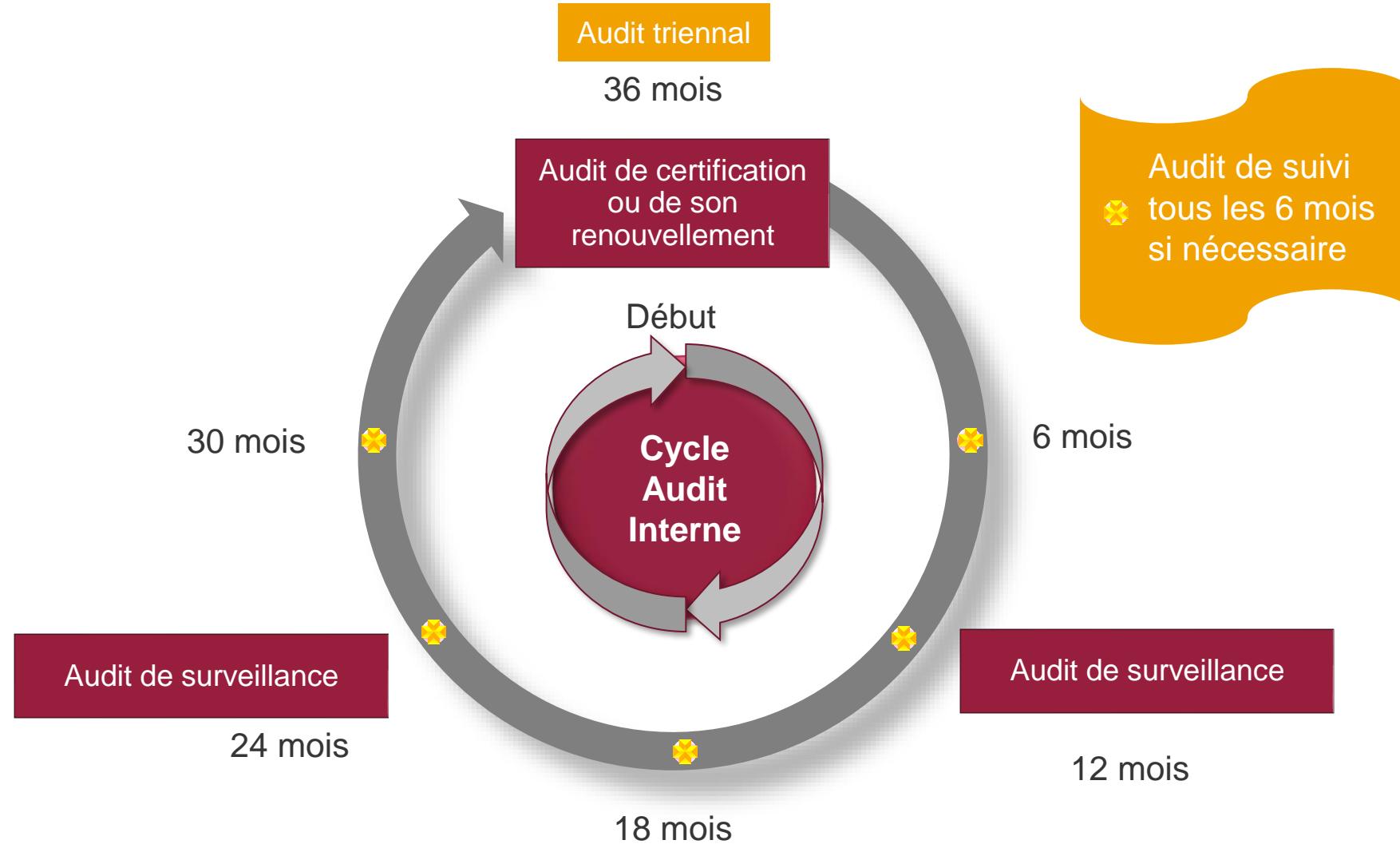
Afin d'obtenir la certification ISO27001, il est requis par les organismes certificateurs de vérifier que l'ensemble des phases Plan, Do, Check, Act soit réalisé au moins 1 fois. Bureau Veritas exige un délai minimal de 3 mois pour effectuer l'ensemble du cycle d'amélioration continue entre 2 revues de direction. Cela signifie concrètement :

1. Réaliser une première revue de direction afin de valider l'ensemble du SMSI par le comité de direction
2. Réaliser un audit à blanc par l'organisme certificateur choisi.
3. Corriger les non-conformités et produire des actions d'amélioration du SMSI
4. Réaliser une seconde revue de direction validant les principes d'amélioration continue par le comité de direction
5. Réaliser l'audit de certification proprement dit.

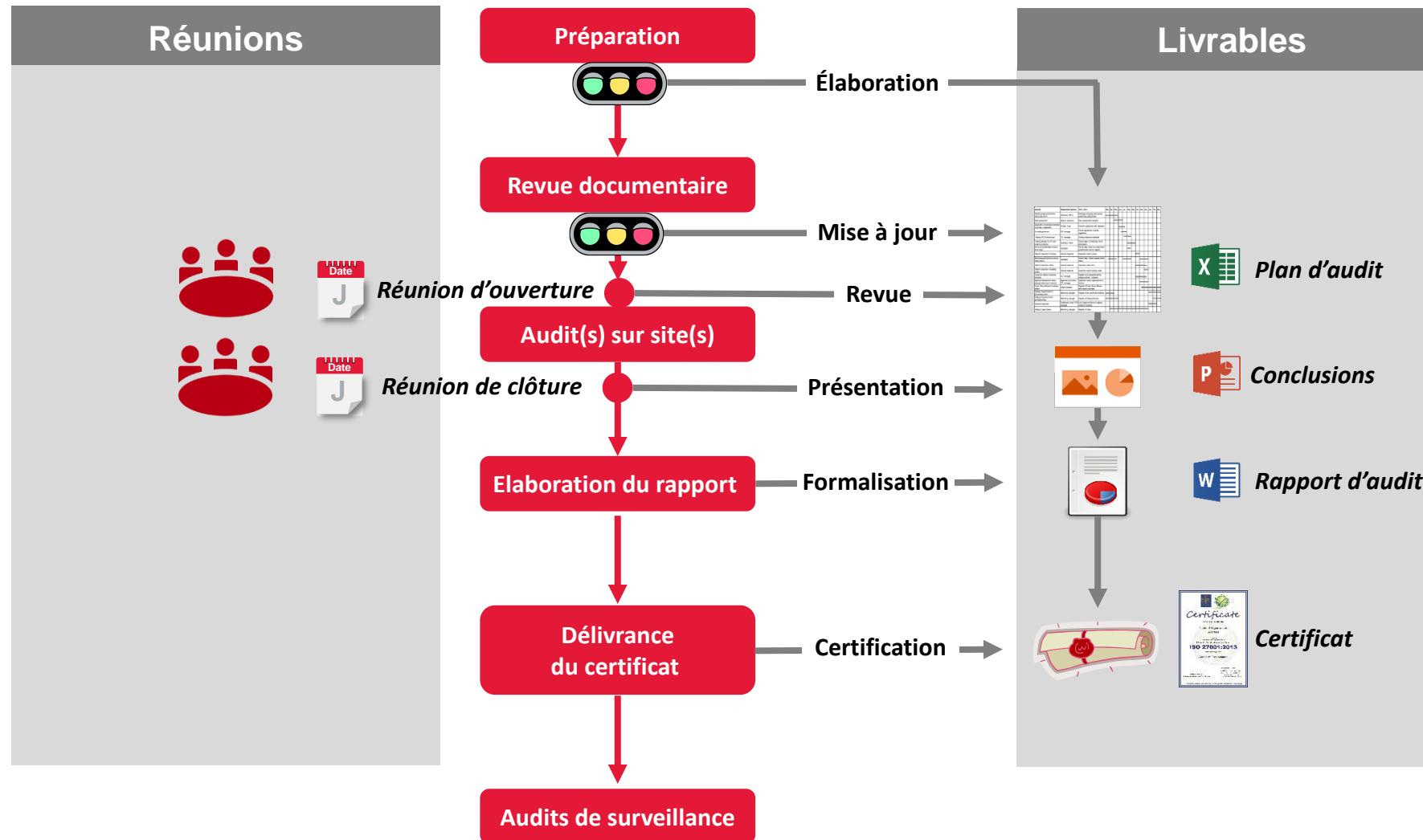




# Le cycle d'audit de certification



# Réaliser l'audit de certification



# Focus sur les certifications individuelles

# Certifications individuelles

- **Lead Implementer**
  - L'examen final certifie que vous possédez les connaissances et les compétences nécessaires pour définir et mettre en place un système de management de la sécurité de l'information conforme **ISO/IEC 27001**
- **Lead Auditor**
  - L'examen final certifie que vous possédez les connaissances et les compétences nécessaires pour réaliser des audits de SMSI suivant la norme **ISO/IEC 27001**
- **Risk Manager**
  - L'examen final certifie que vous possédez les connaissances et les compétences nécessaires pour maîtriser l'appréciation et l'analyse des risques pour la sécurité de l'information suivant la norme **ISO/CEI 27005**

Les **certifications individuelles sont valables 3 ans**, leur validité est subordonnée à la continuité de la compétence en implémentation de SMSI.



# Questions?

CGI Business Consulting

**Anthony AUGEREAU**

Vice-Président Consulting Services  
[CISSP, ISO 27001 Lead Implementor, ITIL]

E-mail : [anthony.augereau@cgi.com](mailto:anthony.augereau@cgi.com)