

# Technologies de l'information



**Cours:**

**Sécurité des systèmes  
informatiques**

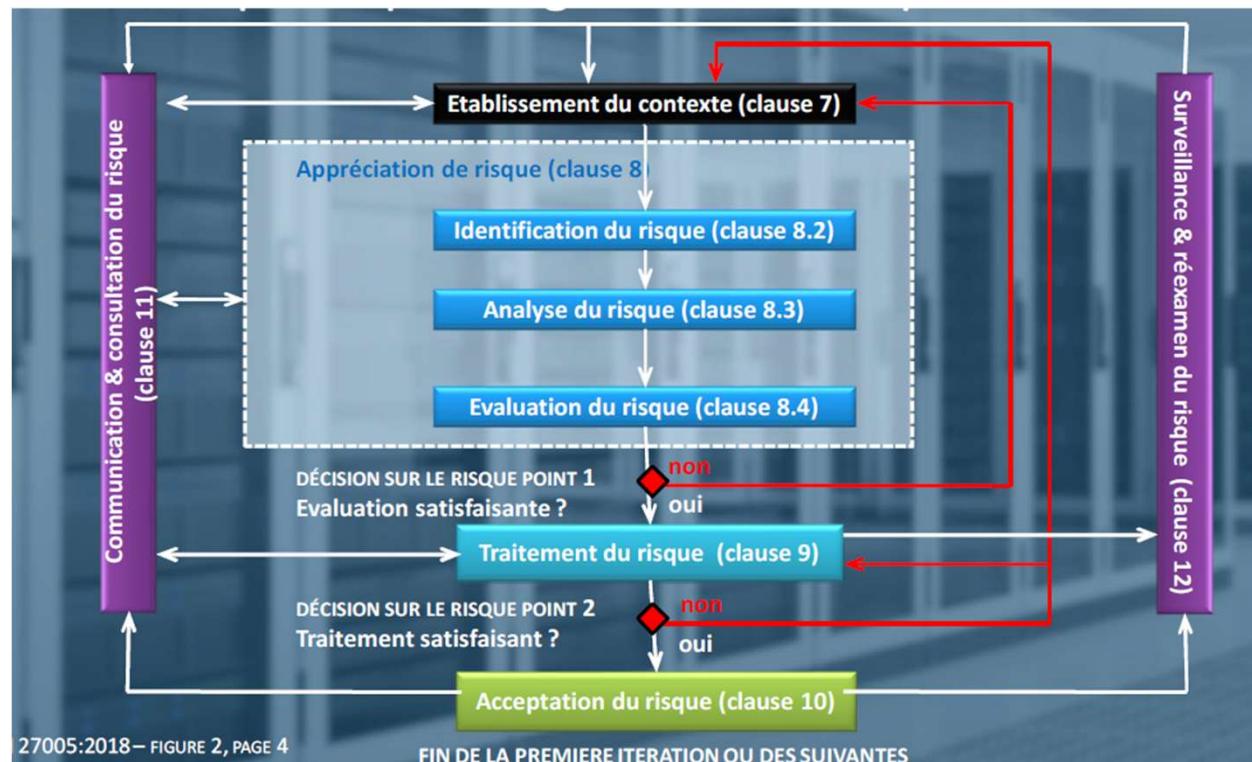
Séance # 4

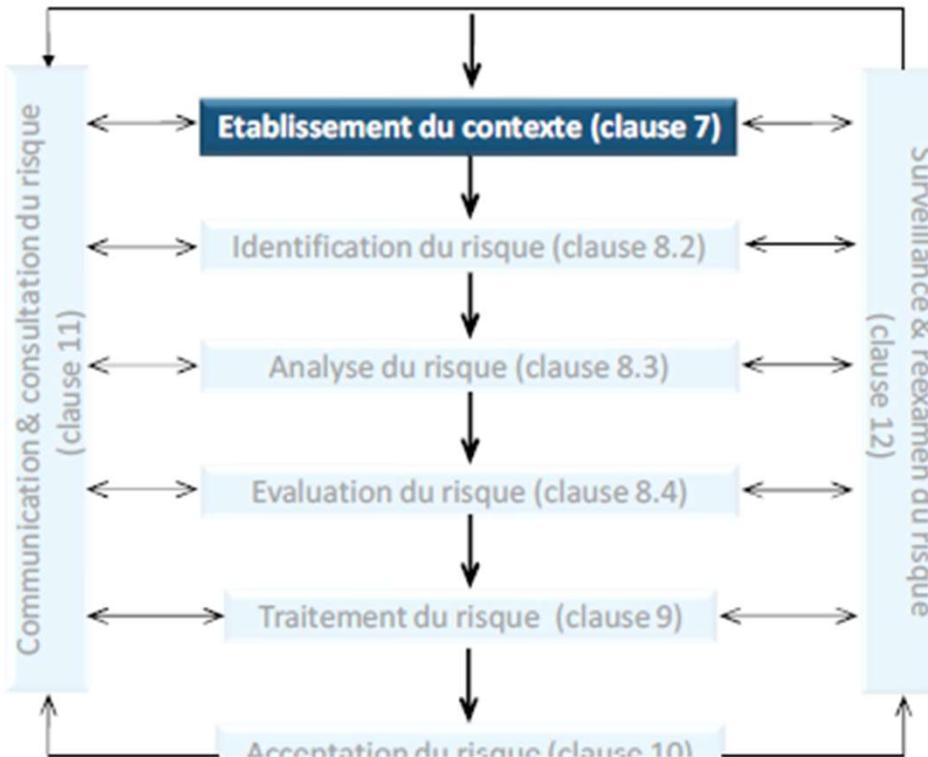
Préparé par: Blaise Arbouet

**DESS**



# Processus de gestion de risque avec ISO 27005





### Eléments d'entrée

Toutes les informations relatives à l'organisme permettant l'établissement du contexte de la gestion des risques en sécurité de l'information.

### Activités

Il convient d'établir le contexte externe et interne de la gestion des risques en sécurité de l'information, ce qui implique de déterminer les critères de base nécessaires à la gestion des risques en sécurité de l'information, de définir le domaine d'application et ses limites et d'établir une organisation adaptée au fonctionnement de la gestion des risques en sécurité de l'information.

### Eléments de sortie

La spécification des critères de base, le domaine d'application et ses limites, et l'organisation dédiée au fonctionnement du processus de gestion des risques en sécurité de l'information.

# **Etape 1**

## **Evaluation du contexte de l'organisation**

# Étude de l'organisme

L'étude de l'organisme rappelle les éléments caractéristiques qui définissent l'identité d'un organisme. Cette étude concerne l'objectif, l'activité, les missions, les valeurs et les stratégies de cet organisme. Il convient d'identifier ces éléments ainsi que les éléments contribuant à leur développement.



# Comprendre l'organisation

Gouvernance

Structure  
organisationnelle

Politiques et  
objectifs

Ressources et  
savoirs

Flux  
d'informations

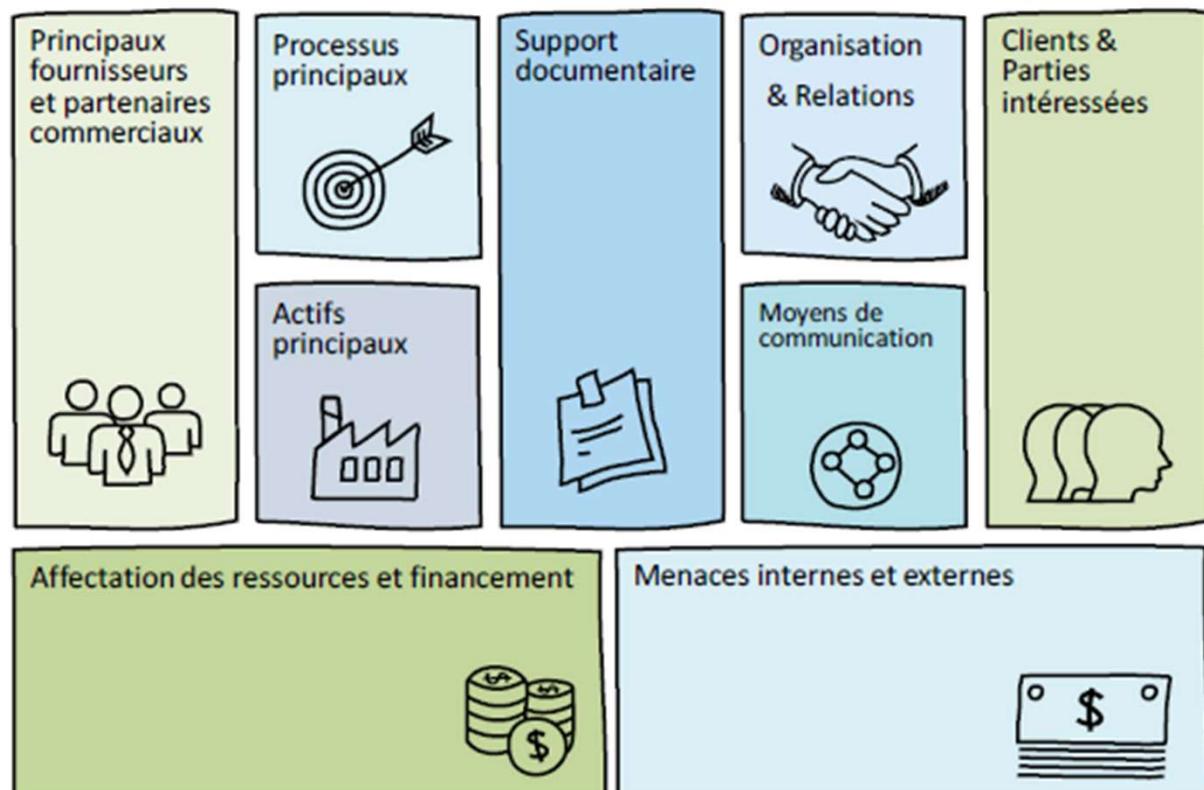
Relation avec les  
parties prenantes

Culture de  
l'organisation

Relations  
contractuelles

# Compréhension de l'organisme et son contexte

Lors de la conception du cadre organisationnel de management du risque, il convient que l'organisme analyse et comprenne son contexte externe et interne



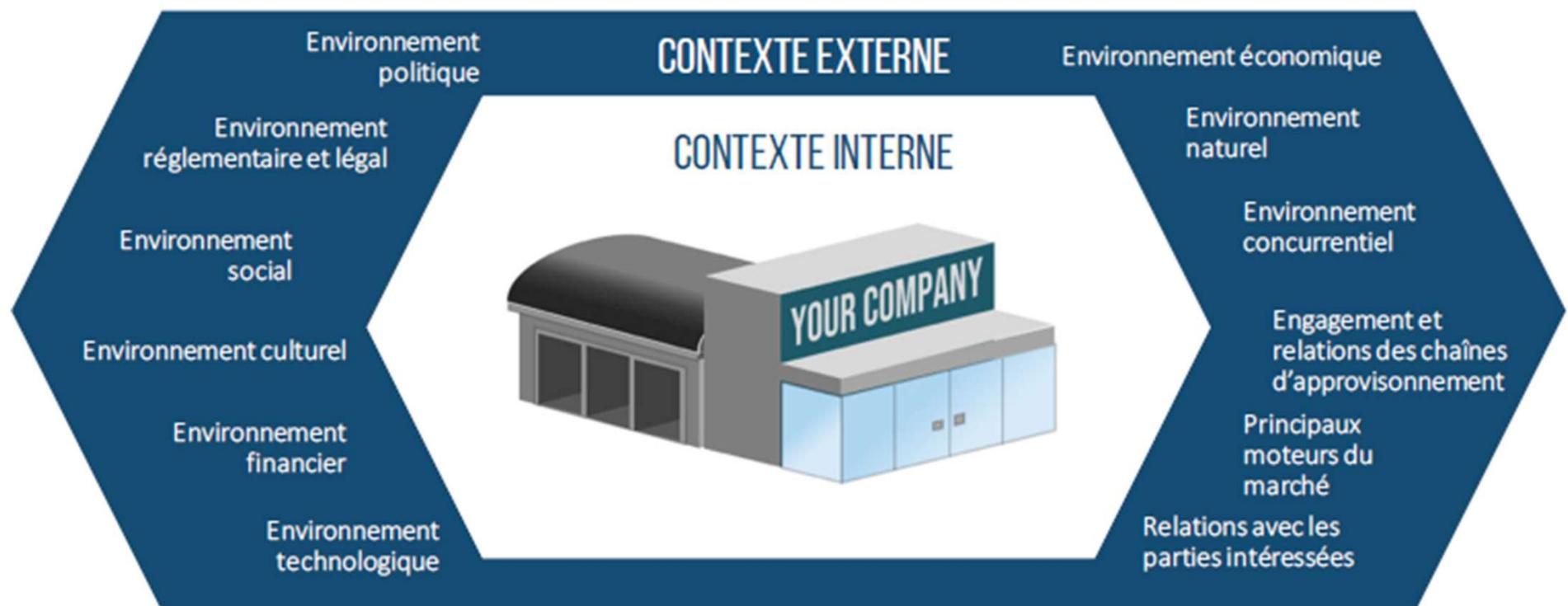
## Enjeux internes et externes



# Contexte externe de l'organisation

- Le contexte externe est l'environnement externe dans lequel les organisations cherchent à atteindre leurs objectifs.
- La compréhension du contexte externe est importante pour s'assurer que les objectifs et les préoccupations des **parties prenantes externes** sont considérées quand les critères de risques et les objectifs de sécurité de l'informations sont développés.
- Il est basé sur le contexte de l'organisation élargie, mais avec des détails spécifiques **d'exigences règlementaires et légales**, des **perceptions des parties prenantes** et autres aspects des risques spécifiques à la sécurité de l'information

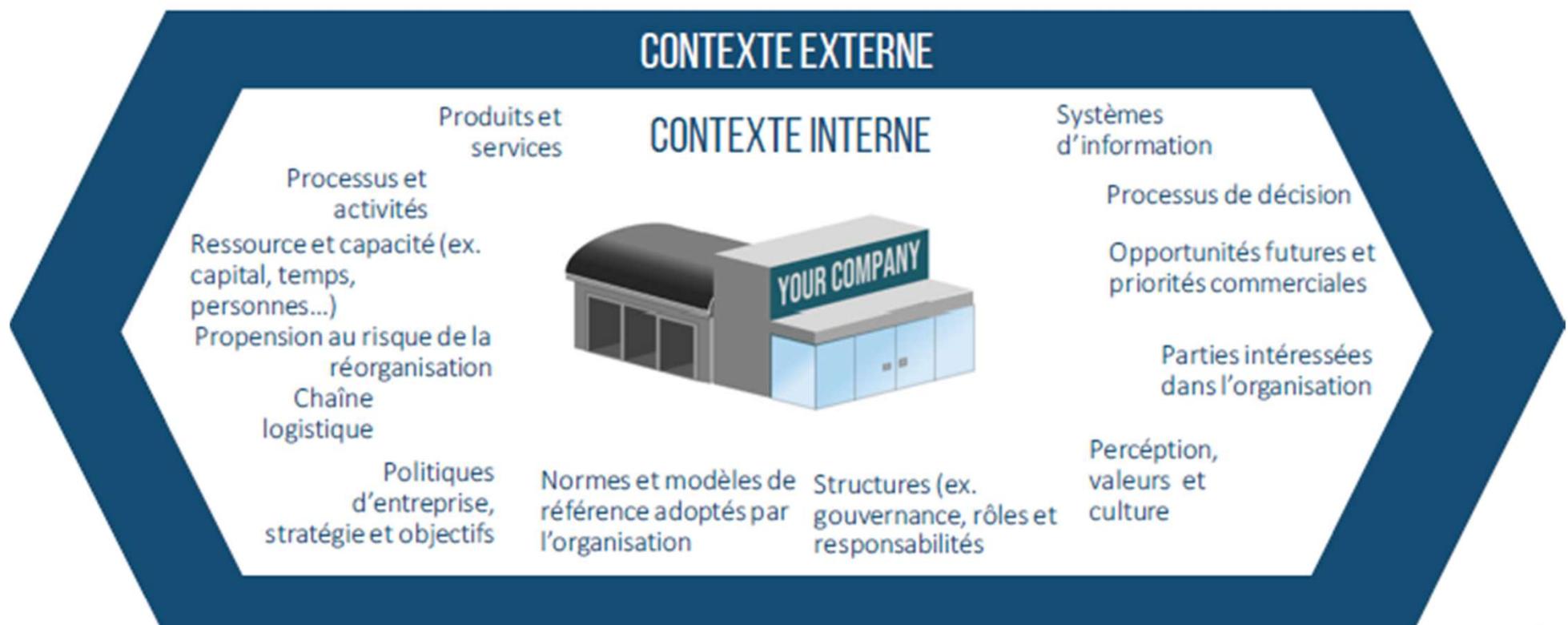
# Ce qui devrait être analysé dans le contexte externe



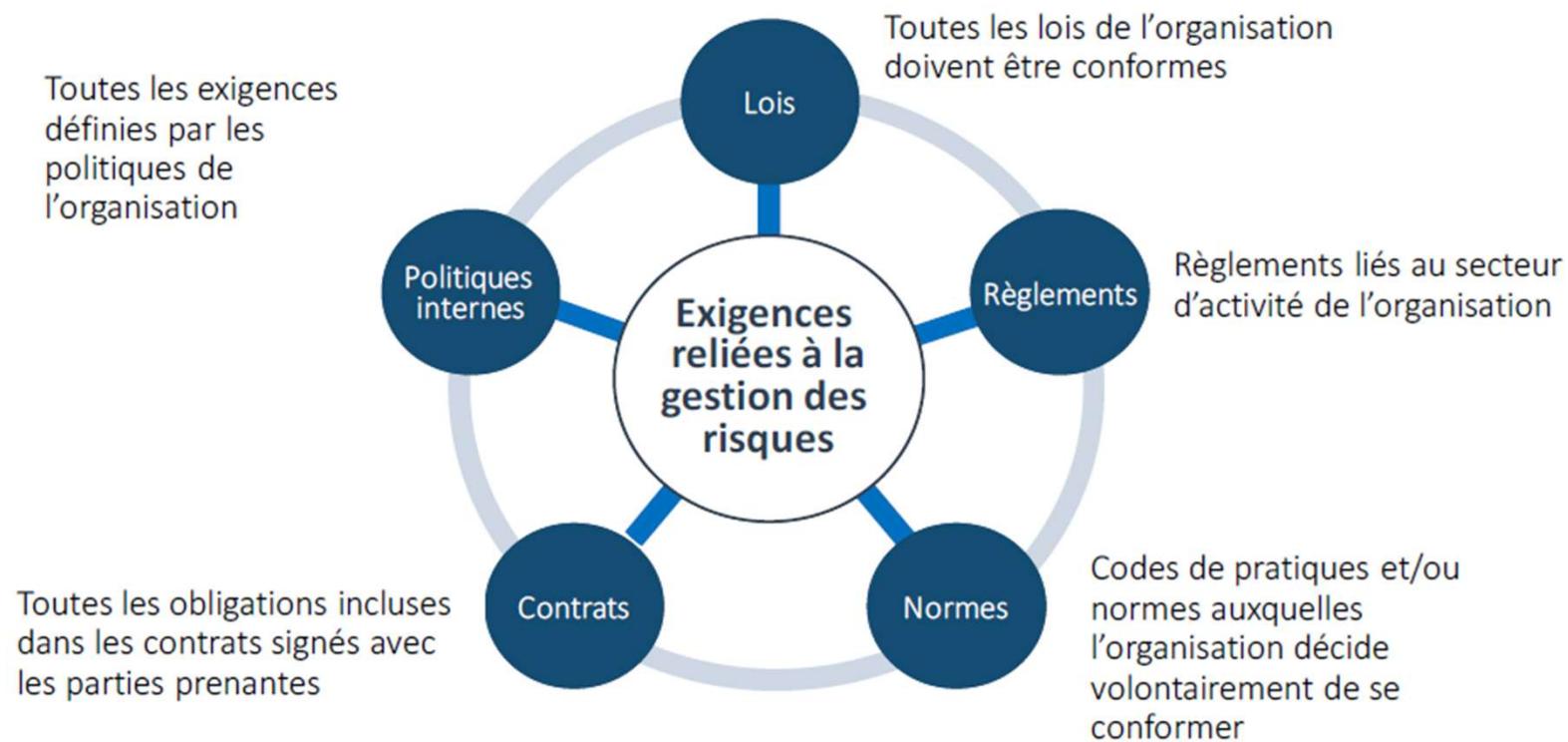
# Contexte interne de l'organisation

- Le contexte interne est l'environnement interne dans lequel l'organisation cherche à atteindre ses objectifs.
- La gestion du risque devrait être aligné avec la **culture**, les **processus**, la **structure** et la **stratégie de l'organisation**. Le contexte interne c'est tout ce qui dans l'organisation peut influencer la manière dont l'organisation gèrera le risque.
- Il devrait être déterminé parce que la gestion de la sécurité de l'information prend place dans le contexte des objectifs de l'organisation.

## Ce qui devrait être analysé dans le contexte interne



# Détermination des exigences reliées à la gestion des risques

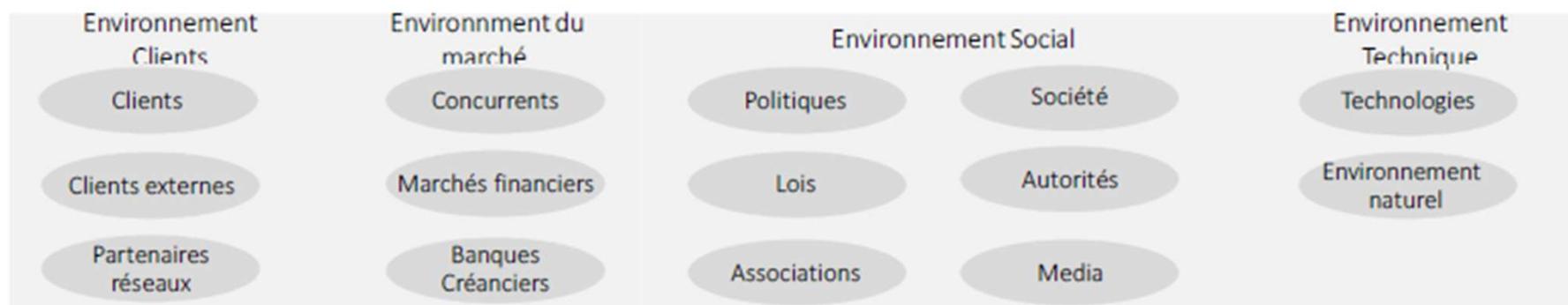


# Identification et analyse des parties prenantes

## ENVIRONNEMENT INTERNE



## ENVIRONNEMENT EXTERNE (OU ENVIRONNEMENT PUBLIC)



# Détermination des objectifs en gestion des risques

Les objectifs de la gestion du risque en sécurité de l'information peuvent être, par exemple :

- Répondre aux exigences d'un SMSI
- Ce qui sera fait pour gérer les risques
- Se conformer à la loi
- Préparer d'un plan de continuité d'activité
- Faire preuve de **due diligence ou due care**
- Analyser un produit, service ou mécanisme

# Élaboration de la gouvernance des risques



La gouvernance des risques permet d'assurer que les pratiques de gestion des risques sont intégrées au tissu organisationnel de l'entreprise et qu'elles permettent d'envisager en retour une sécurité optimisée vis-à-vis de ces risques. Elle en couvre 4 objectifs principaux:

- Etablir et maintenir une vision commune
- Intégrer la gestion de risque au sein de l'entreprise
- Assurer que les mesures de sécurité sont implémentées et fonctionnent
- Prendre des décisions basées sur les risques

# Attribution des rôles, pouvoirs et responsabilités



La direction doit désigner qui a la responsabilité et l'autorité pour:

1. assurer une coordination adéquate de la gestion du risqué
2. Rendre compte à la direction des performances du programme de gestion des risqué



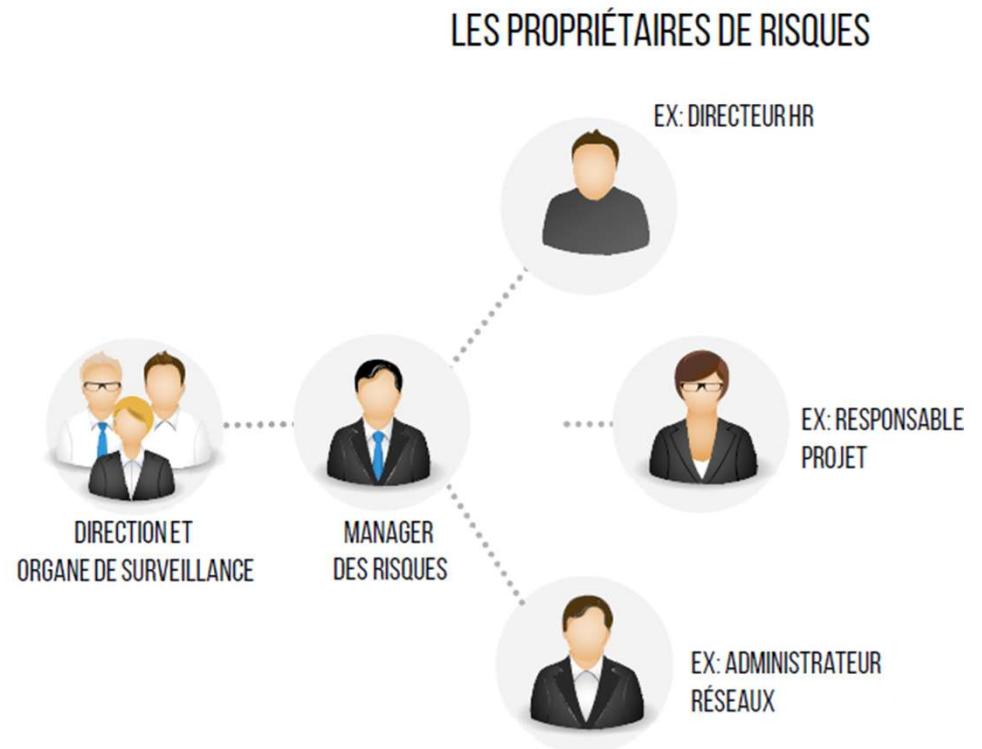
La Direction doit s'assurer que les responsabilités et autorités des rôles concernés sont attribués et communiqués au sein de l'organisation

# Nomination d'un manager et de propriétaires des risques

## Nomination d'un manager et de propriétaires des risques

Rôles, pouvoirs et responsabilités

- Pour assurer une coordination adéquate de la gestion du risque, un responsable devrait être nommé.
- Le responsable de la gestion du risque devrait avoir un profil transversal en s'intéressant à tous les aspects des activités de l'organisme.
- Son rôle l'amène à être en interrelation avec les propriétaires des risques (juridique, financier, RH, technologies de l'information, audit interne, sûreté et sécurité, environnement, etc.) ainsi qu'avec la direction



# Définir les responsabilités des principaux intervenants

ISO 31000, Clause 5.4.3 & ISO 27005, Clause 7.4

## DIRECTION

Approuve les risques et est l'ultime responsable du programme.

## DIRECTION FINANCIÈRE

Évalue le ration coûts-bénéfices des risques et budgétisent les plans d'action pour réduire les risques.

## RESSOURCES HUMAINES

Identifient les besoins en formation du personnel et contribuent à la sensibilisation aux risques.

## RSSI ET ÉQUIPE DE SÉCURITÉ DE L'INFORMATION

Identifient et mettent en œuvre les mesures de sécurité qui répondent le mieux aux risques tels qu'appréciés.

## DIRECTION DES SYSTÈMES D'INFORMATION (DSI)

Mettent en place les solutions technologiques et les mesures techniques de réponse aux risques.

## SERVICE JURIDIQUE

Identifie les exigences légales, réglementaires et contractuelles en termes de conformité et de régularité.

## AUDIT INTERNE

Donne l'assurance interne sur la maîtrise risques et recommande de façon continue les mesures qui permettent de les garder sous contrôle.

## RELATIONS PUBLIQUES

Approuve les risques et est l'ultime responsable du programme.

# Affectation des ressources



Il convient que la direction et les organes de surveillance, le cas échéant, assurent l'affectation des ressources nécessaires au management du risque



Les ressources et leur allocation devraient être revues périodiquement pour s'assurer de leur adéquation



Il convient que l'organisme prenne en compte les capacités et les contraintes des ressources existantes.



## Les Types de ressources:

- Finances
- Personnes
- Equipements
- Communication avec les parties intéressées
- TIC
- Information documentée



## Publication d'une politique de gestion des risques

La politique doit inclure:

- Les objectifs
- Le cadre de gestion de risque
- Le RACI
- L'engagement de la haute gestion
- La surveillance
- L'amélioration continue
- Etc..

# Autres choses à considérer

Périmètre de la gestion de risque

Alignement du périmètre de risques avec les besoins des parties intéressées

Culture du risque interne

Appétence au risque

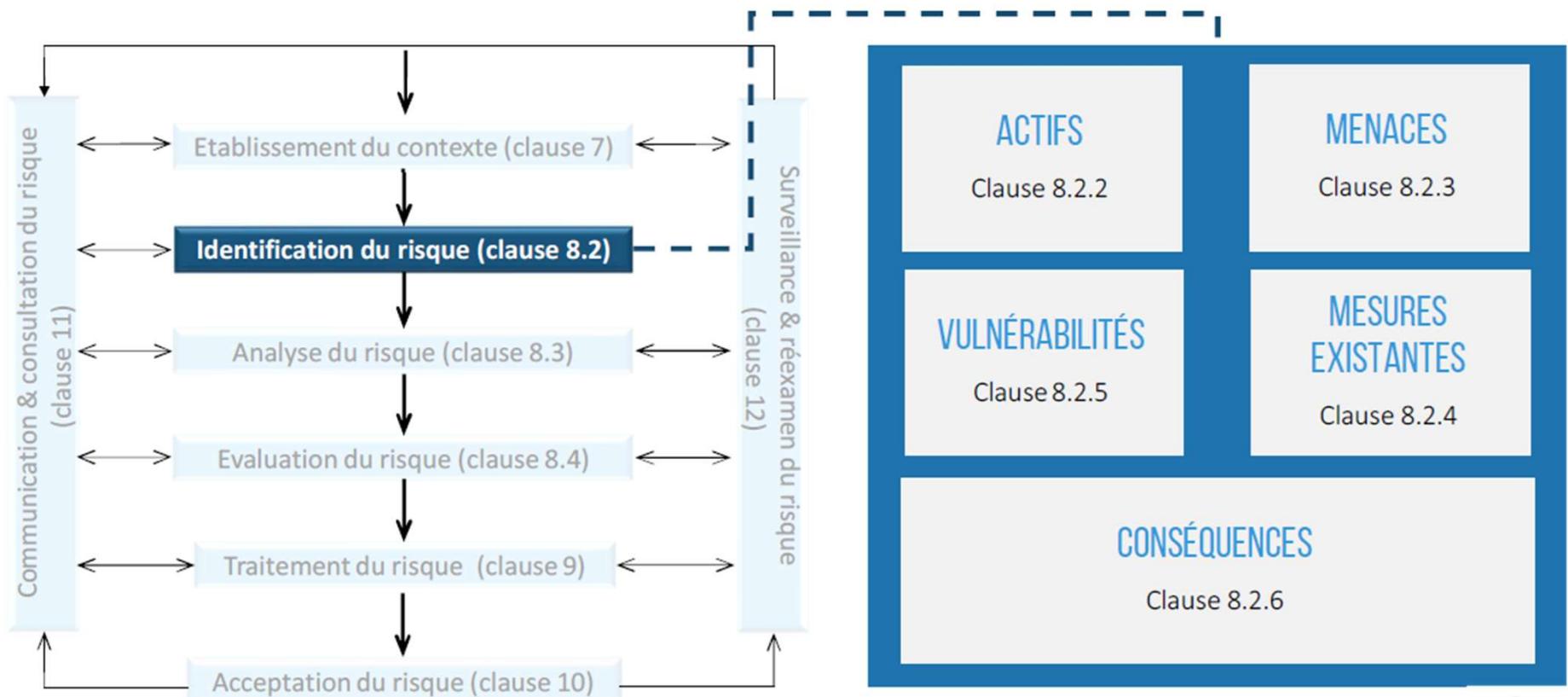
Seuil de tolérance au risque

Appréciation du risque

Etc...

# Étape 2

## Identification du risque



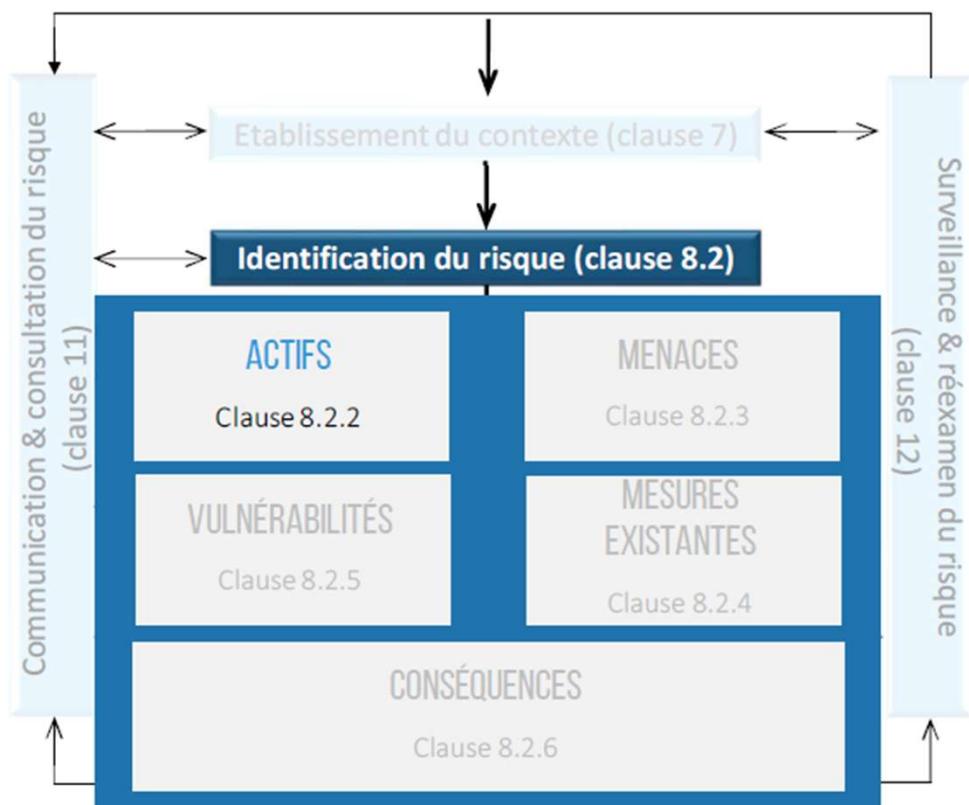


# Objectifs de l'identification

L'objectif de l'identification des risques est de déterminer les événements susceptibles de se produire causant une perte potentielle et de donner un aperçu de comment, où, et quand cette perte pourrait survenir.

Il convient que l'identification des risques inclue les risques dont la source est ou non sous le contrôle de l'organisme, même si la source n'est peut-être pas évidente.

# Identification des actifs



### Eléments d'entrée

Domaine d'application et limites de l'appréciation des risques à effectuer, liste des composants avec les propriétaires, emplacement, fonction, etc.

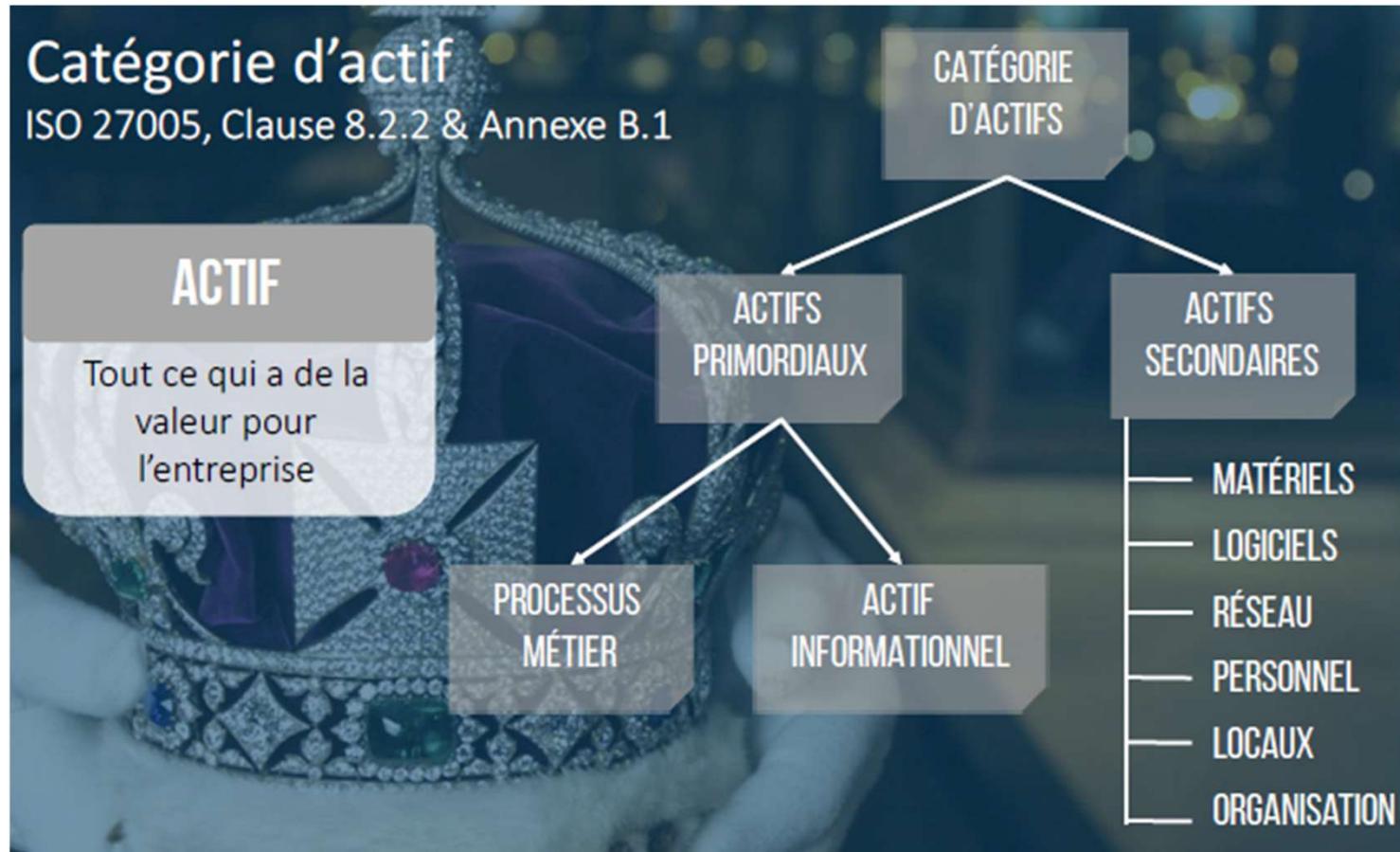
### Activités

Il convient d'identifier les actifs relevant du domaine d'application établi.

### Eléments de sortie

Liste des actifs dont les risques sont à gérer et liste des processus métier relatifs aux actifs et leur pertinence.

# Catégorie d'un actif



# **Identification des actifs informationnels**

Ce qu'il faut considérer:

Vitaux pour l'organisation et qui lui permettent de réaliser ses missions

Contiennent des informations qui ont une valeur économique, administrative ou légale pour l'organisation

Supportent des coûts importants pour leur collecte, leur acquisition ou leur conservation.

# Comment identifier et documenter les actifs de supports ?

## Bonnes pratiques

The screenshot displays the Lansweeper software interface, which is used for managing network assets and creating tickets.

**Left Panel (Ticket Creation Form):**

- Subject:** [Text input field]
- Type:** IT Support [Dropdown menu]
- Priority:** Medium [Dropdown menu]
- External reference ID:** [Text input field]
- Root cause known:**  No  Yes [Radio buttons]
- Approval for:** None selected... [Text input field]
- Assign to agent:** [Buttons: Select agent, Set self]
- Add subscribers:** [Buttons: Subscriber, Add CC user]
- Assets concerning:** [Asset icon]
- User concerning:** James Millard [User icon]
- Source:** Website [Dropdown menu]
- Agent initiated:** [Checkboxes]
- Set personal:** [Checkboxes]
- Add CC user:** [CC User icon]

**Right Panel (Asset Inventory Table):**

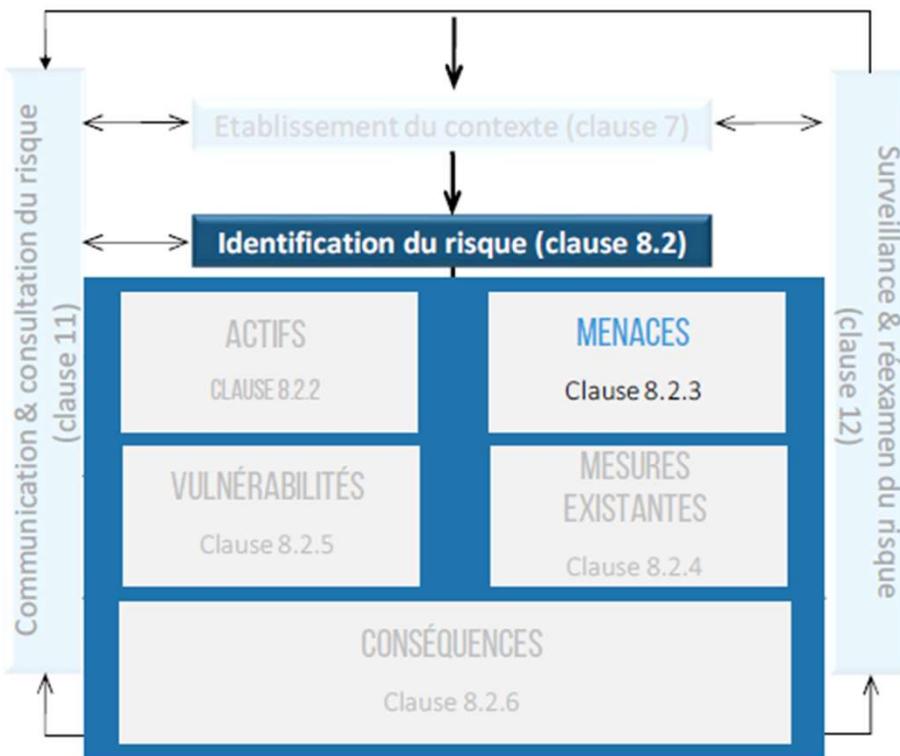
AssetName	Domain	Type	IP Address	Description	Manufacturer	Model	Location
Acer Monitor	Lansweeper	Monitor		Monitor on L004	Acer	P225HQL_Analog	
AOC International	Lansweeper	Monitor		Monitor on D005	AOC International (USA) Ltd.	AOC LM729	
Backup.lansweeper.local			102.169.1.104	VMware ESX 5.1.0 build-799733 VMware	VMware, Inc.		
				47 Cisco IOS Software, C2960X Software	Cisco		Server Room
				48 Cisco IOS Software, C2960X Software	Cisco		Server Room
				1.12 Windows Workstation Desk 01	Dell Inc.	OptiPlex 9020M	Lansweeper H
				1.13 Windows Workstation Desk 02	Dell Inc.	OptiPlex 9020M	Lansweeper H
				1.9 Windows Workstation Desk 03	Dell Inc.	OptiPlex 9020M	Lansweeper H
				1.36 Windows Workstation Desk 04	Dell Inc.	OptiPlex 9020M	Lansweeper H
				1.31 Windows Workstation Desk 05	Dell Inc.	OptiPlex 9020M	Lansweeper H
				Monitor on L004	Dell Inc.	DELL P2417H	
				Monitor on D002	Dell Inc.	DELL P170S	
				Monitor on D001	Dell Inc.	DELL P1911	
				.90 Dell 1130n Mono Laser Printer	Dell Inc.	Dell 1130n Mono Laser Printer	Lansweeper H
				Monitor on D003	Fujitsu Siemens	B22W-6 LED	Lansweeper H
					Hewlett-Packard	HP L1950 LCD Monitor	Stock
				.106	Dell Inc.		
				.107	Dell Inc.		
				.91 HP ETHERNET MULTI-ENVIRONMENT	Hewlett-Packard	HP LaserJet 300 colorMFP M375nw	Glass Room
				Monitor on D004	IBM	IBM 6331 ES4	Lansweeper H
				234 Video / Image Editing	Apple		Main Branch
				56 Desk 01	Cisco		Main Branch
				57 Desk 02	Cisco		Main Branch
				99 Desk 03	Cisco		Main Branch
				100 Desk 04	Cisco		Main Branch
				1.68 Laptop	Dell Inc.	Latitude 5580	Main Branch
				1.77 Laptop	Dell Inc.	Latitude 5580	Main Branch
				1.2 Laptop	Dell Inc.	Latitude 5580	Main Branch
					Lenovo	L197 Wide	Stock
					Server Monitor	Lenovo	Server Room
						L2250p Wide	Main Branch
				4 Linux Testmachine	Dell Inc.	20M35	Main Branch
				5 Linux Testmachine	Dell Inc.	IPS234	Main Branch
				6 Linux Testmachine	Dell Inc.		Main Branch
				7 Linux Testmachine	Dell Inc.		Main Branch



## Identification des propriétaires d'actif

- Il convient d'identifier un propriétaire pour chaque actif afin d'associer pour celui-ci une personne responsable et redevable.
- Quel est son rôle ?

Le propriétaire de l'actif ne jouit peut-être pas de droits de propriété sur l'actif mais est responsable de sa production, de son développement, de sa maintenance, de son utilisation et de sa protection selon le cas. Le propriétaire de l'actif est souvent la personne la plus à même de déterminer la valeur qu'il représente pour l'organisme (voir 8.3.2 pour la valorisation des actifs).



### Eléments d'entrée

Informations relatives aux menaces obtenues grâce à la revue des incidents, aux propriétaires des actifs, aux utilisateurs et à d'autres sources, y compris des catalogues de menaces externes.

### Activités

Il convient d'identifier les menaces et leurs sources

### Eléments de sortie

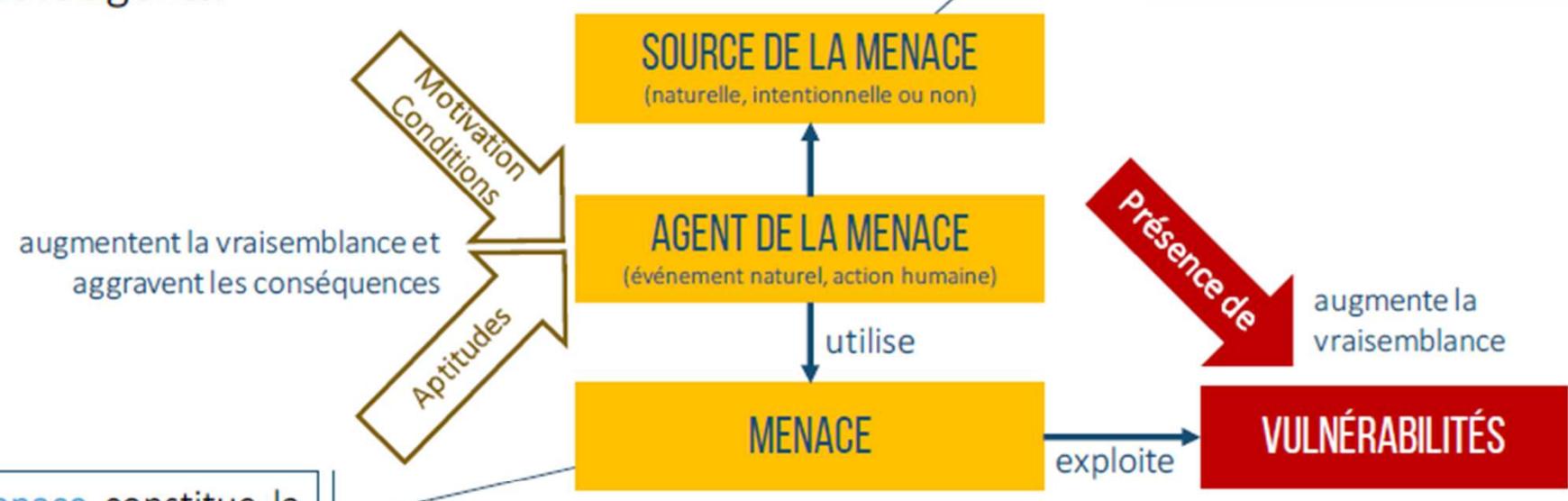
Liste de menaces avec identification du type et de la source de la menace.

# Identification des menaces

# Identification des menaces

ISO 27005, Clause 8.2.3

Il convient d'identifier les menaces, leurs sources et leurs agents.



La menace constitue la cause potentielle d'un incident indésirable pouvant affecter une organisation.

La source de la menace réfère à tout ce qui constitue l'origine possible de la menace, que ce soit à travers sa nature, sa motivation ou ses capacités.

# Bonnes pratiques pour identifier les menaces

Les éléments d'entrée de l'identification des menaces peuvent être obtenus auprès de différentes parties prenantes, internes ou externes à l'organisation, telles que :

- Propriétaires ou utilisateurs des actifs
- Personnel de l'organisation
- Expert en sécurité de l'information
- Avocats
- Compagnies d'assurance
- Autorités gouvernementales
- Catalogue d'une méthode de menaces
- Etc.

# Types de menaces

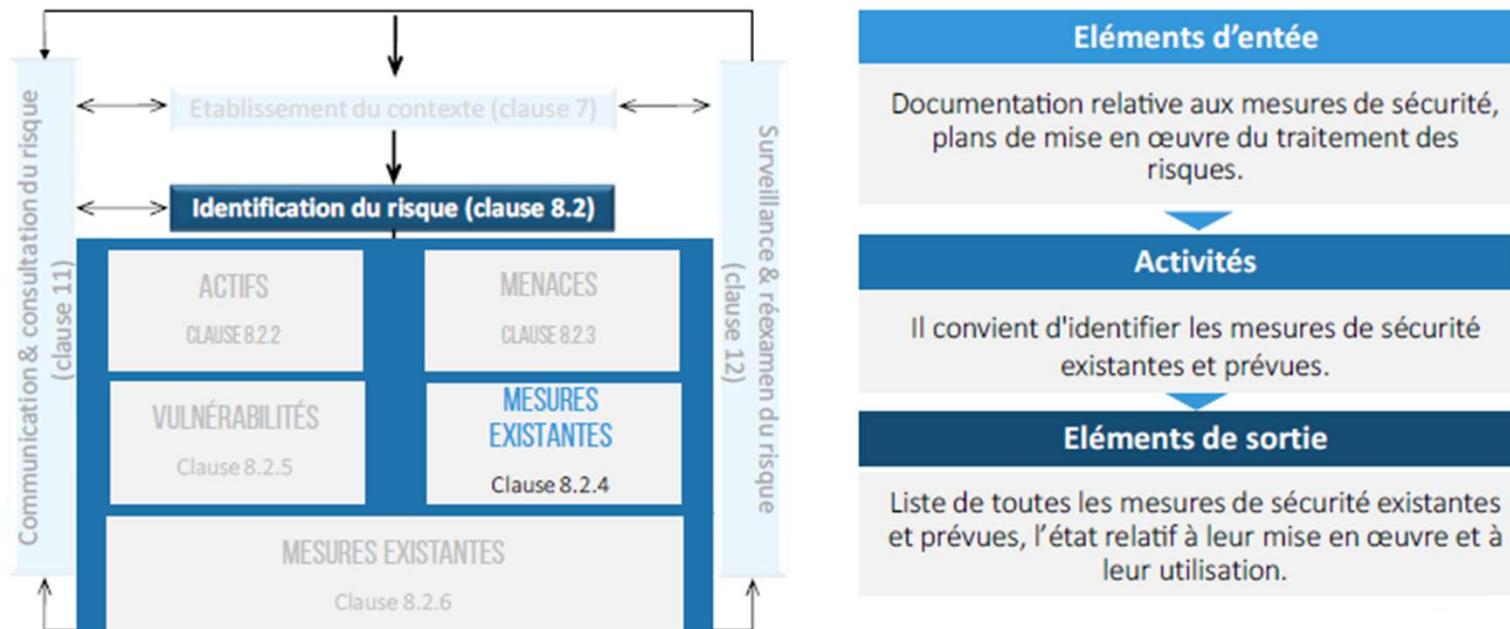
TYPE DE MENACES	EXEMPLES	
DOMMAGE PHYSIQUE	Pollution	Accident majeur
	Dégât des eaux	Incendie
CATASTROPHES NATURELLES	Phénomène climatique	Phénomène volcanique
	Phénomènes sismique	Phénomène météorologique
PERTE DE SERVICES ESSENTIELS	Panne d'électricité	Panne de la climatisation
	Panne du matériel de télécommunications	Perte d'alimentation en eau
PERTURBATION DUE À DES RAYONNEMENTS	Rayonnements électromagnétiques	Impulsions électromagnétiques
	Rayonnements thermiques	
COMPROMISSION D'INFORMATION	Divulgation	Espionnage à distance
	Piégeage de logiciel	Géolocalisation
DÉFAILLANCES TECHNIQUES	Panne de matériel	Dysfonctionnement du matériel
	Saturation du système d'information	Dysfonctionnement du logiciel
ACTIONS NON AUTORISÉES	Corruption de données	Traitemet illégal de données
	Reproduction frauduleuse de logiciel	Utilisation de contrefaçons
COMPROMISSION DES FONCTIONS	Erreur d'utilisation	Usurpation de droits
	Abus de droits	Renierement d'actions

Source: ISO 27005, Annexe C

## **Étape 2**

# **Identification des mesures existantes**

# Identification des mesures existantes



# Identification des mesures de sécurité existantes



Il convient de procéder à une identification des mesures de sécurité existantes pour éviter des travaux ou des coûts inutiles dûs, par exemple, à une redondance des mesures de sécurité.



En outre, tout en identifiant les mesures de sécurité existantes , il convient d'effectuer un contrôle afin de garantir que les mesures de sécurité fonctionnent correctement – il convient qu'une référence aux rapports d'audit du SMSI déjà existants limite le temps dédié à cette tâche. Si une mesure de sécurité ne fonctionne pas comme prévu, des vulnérabilités peuvent être engendrées.

# Collection d'information sur les mesures de sécurité existantes

- Revue et analyse documentaire

- Questionnaire de maturité

- Entretiens

- Visites sur sites

- Plans de mise en oeuvre de traitement des risques

- Processus de gestion de la sécurité de l'information

- Documentation sur les mesures existantes et leurs statuts de mise en oeuvre

- Résultats des audits internes

- Ateliers avec les utilisateurs et responsables

- Revue sur site des mesures existantes

# Évaluation de l'efficacité des mesures de sécurité

Quels sont les contrôles existants liés à un risque particulier ?

Ces contrôles sont-ils en mesure de traiter le risque de manière à le maintenir à un niveau tolérable ?

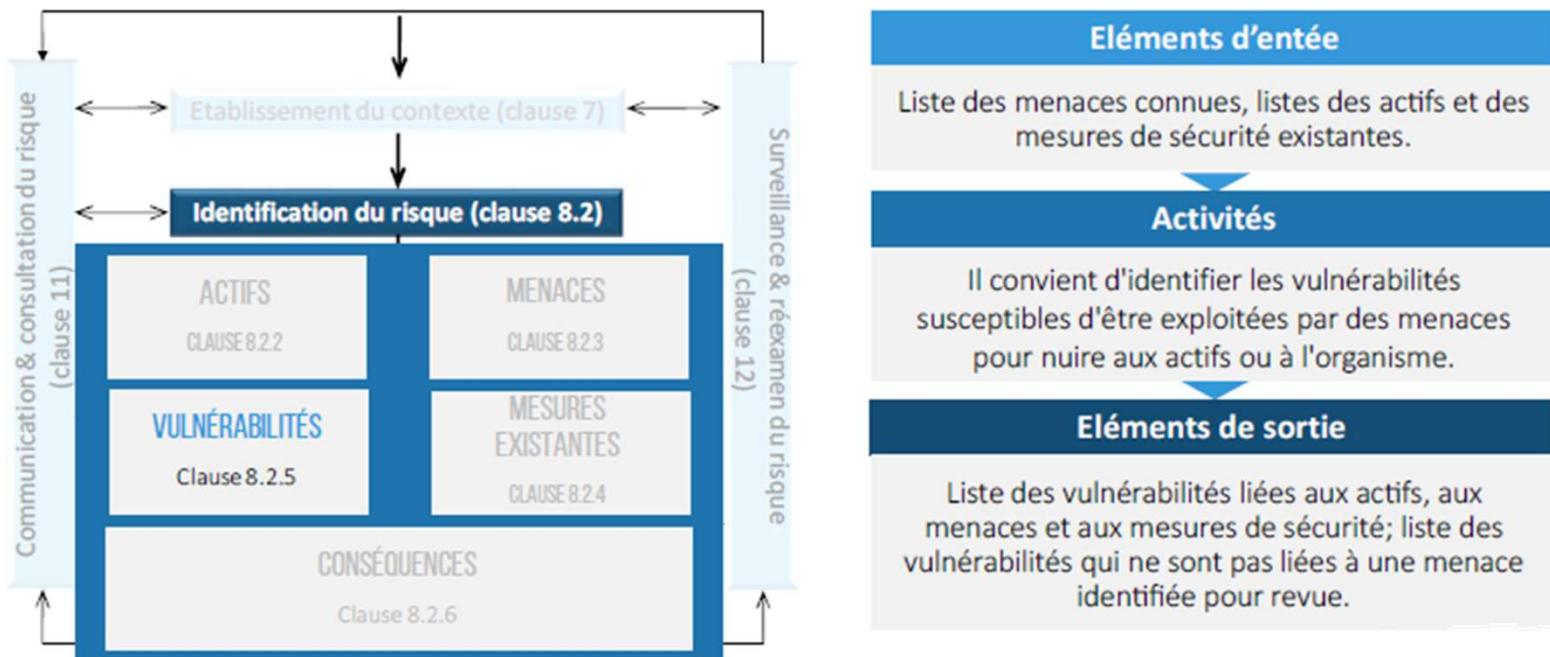
Dans la pratique, les contrôles fonctionnent-ils comme prévu ?

Est-ce que l'on peut démontrer l'efficacité des mesures avec des preuves ?

# Étape 2

## Identification des vulnérabilités

# Identification des vulnérabilités



# Identification des vulnérabilités

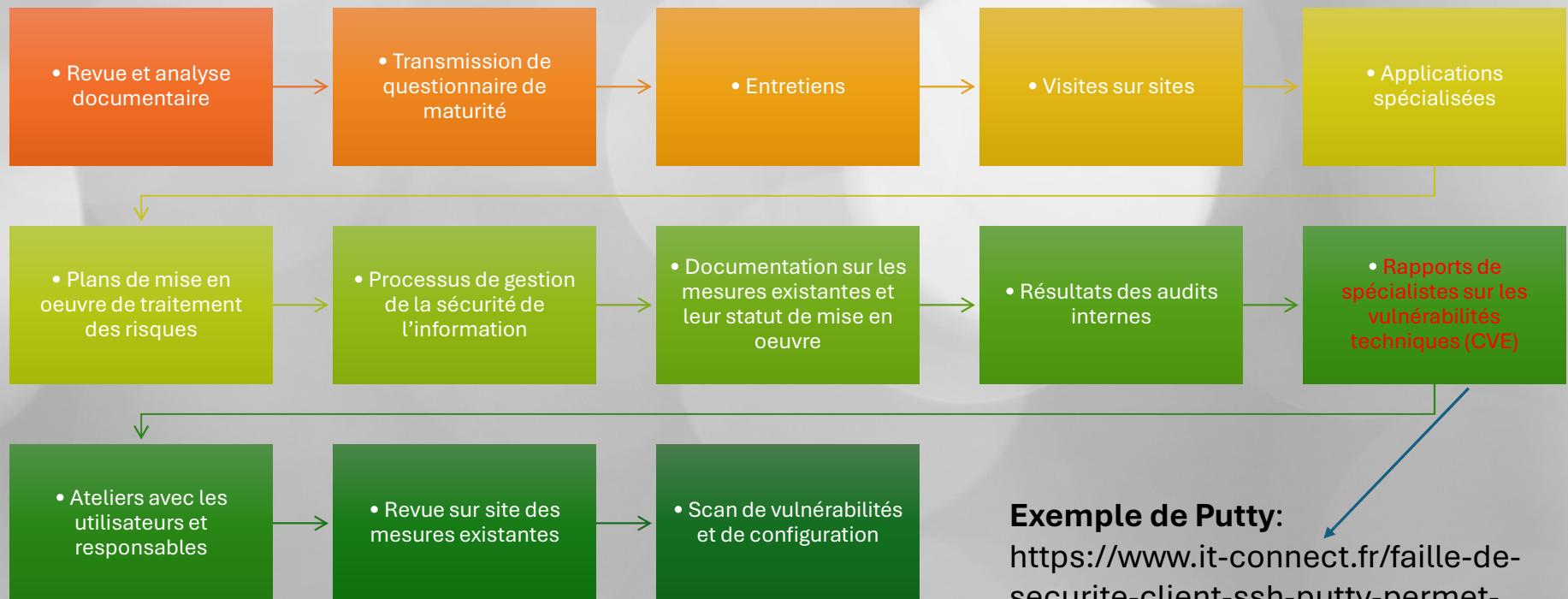


Il convient d'identifier les vulnérabilités susceptibles d'être exploitées par des menaces pour nuire aux actifs ou à l'organisme.



Il peut s'agir d'une faille d'un actif ou d'une mesure de sécurité qui pourrait être exploitée par une menace

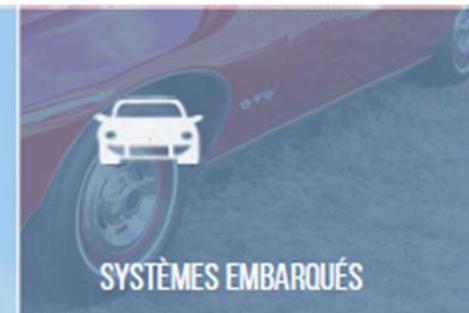
# Méthodes pour identifier les vulnérabilités



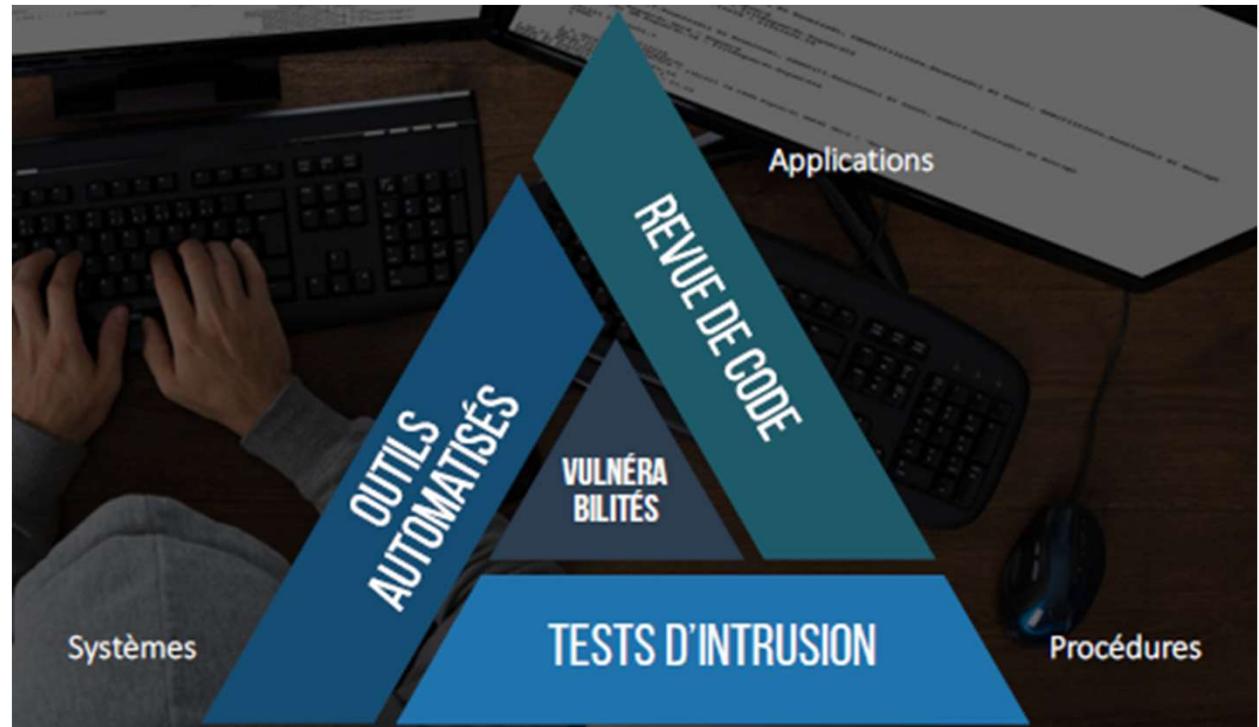
## Exemple de Putty:

<https://www.it-connect.fr/faille-de-securite-client-ssh-putty-permet-de-recuperer-les-cles-privees-cve-2024-31497/>

# Exemples de systèmes vulnérables



Méthodes  
d'identification  
des  
vulnérabilités  
techniques



# Source de vulnérabilités

---

Processus et procédures

---

Activités récurrentes de gestion

---

Environnement physique

---

Personnel

---

Configuration du système d'information

---

Matériels, logiciels et infra de communication

# Score de vulnérabilité (CVSS)

Le système CVSS (Common Vulnerability Scoring System) permet d'évaluer la gravité et les risques en matière de sécurité du système informatique.

CVSS est une infrastructure ouverte composée des groupes de métriques suivants :

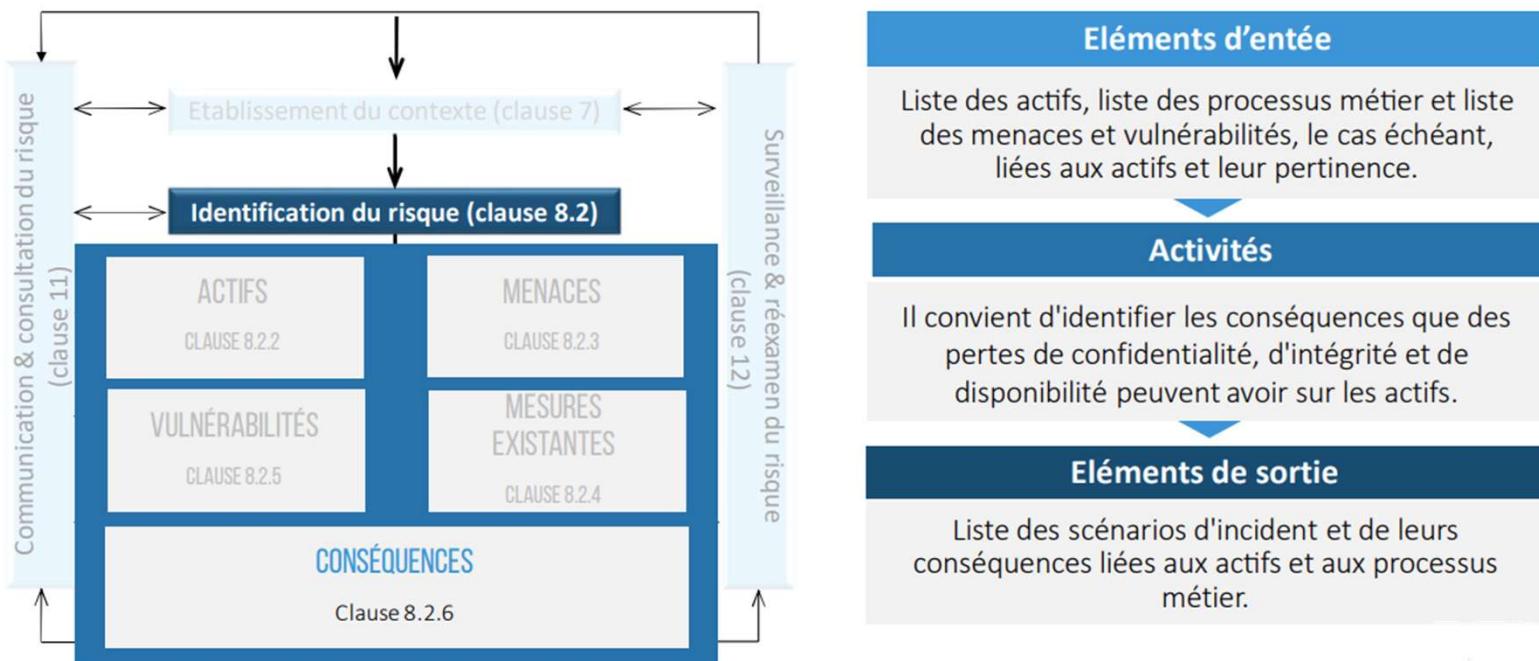
- Base
- Temporel
- Environnemental



4.0

# Identification des conséquences

# Identification des conséquences



# Identification des conséquences (suite)

Il convient d'identifier les conséquences que des pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les actifs.

Disponibilité	Intégrité	Confidentialité
<ul style="list-style-type: none"><li>▪ Dégradation des performances</li><li>▪ Interruption d'un service</li><li>▪ Inaccessibilité d'un service</li><li>▪ Perturbation des opérations</li></ul>	<ul style="list-style-type: none"><li>▪ Modification accidentelle</li><li>▪ Modification délibérée</li><li>▪ Résultats incorrects</li><li>▪ Résultats incomplets</li><li>▪ Perte de données</li></ul>	<ul style="list-style-type: none"><li>▪ Atteinte à la vie privée des usagers ou des clients</li><li>▪ Atteinte à la vie privée du personnel de l'organisme</li><li>▪ Fuite d'information confidentielle</li></ul>

# Évaluation d'une conséquence



Conséquence: Effet d'un événement affectant les objectifs



Une conséquence peut être certaine ou incertaine et peut avoir des effets positifs ou négatifs, directs ou indirects sur l'atteinte des objectifs.



Les conséquences peuvent être exprimées de façon quantitative ou qualitative



Toute conséquence peut déclencher des effets en cascade ou cumulatifs.

# Étape 3

## Analyse des risques

# Analyse de risques

## 1) **Methodologie d'analyse de risque**

Qualitative et/ou quantitative, à différents niveaux de détail, en plusieurs itérations selon les scénarios de risque.

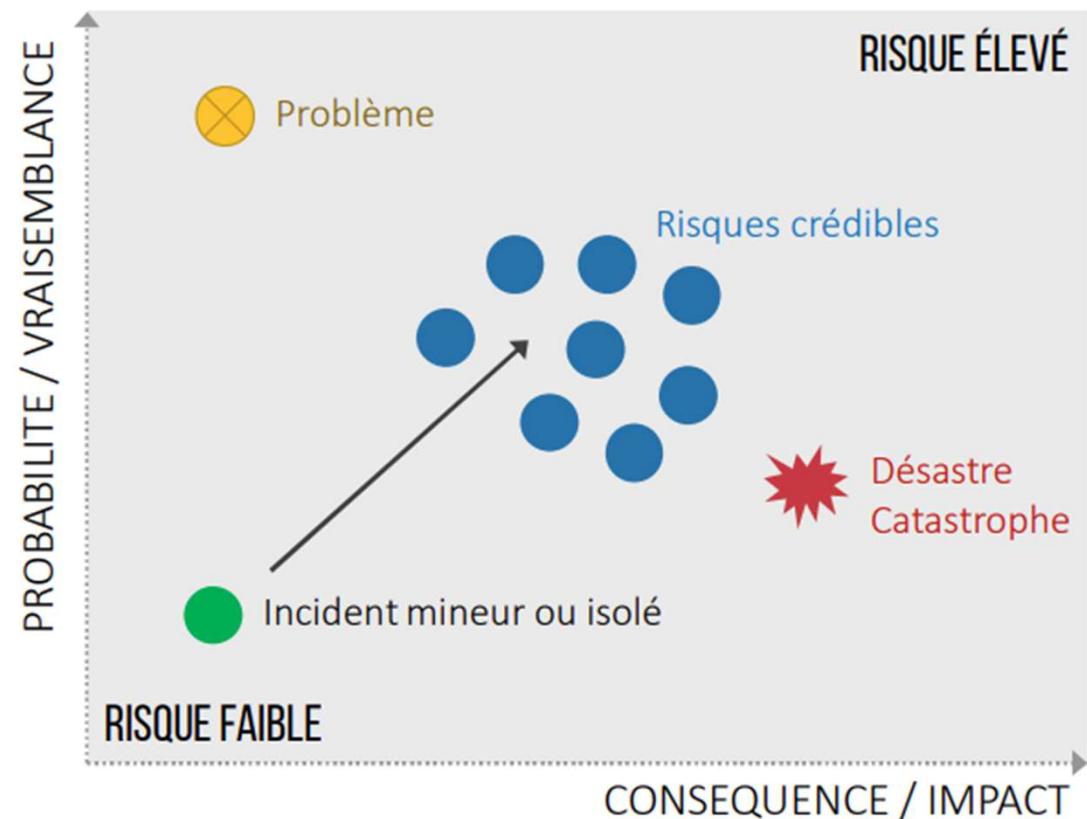
## 2) **Appréciation de la vraisemblance**

En tenant compte de la fréquence de survenance des menaces et la facilité d'exploitation des vulnérabilités

## 3) **Estimation du niveau de risque**

Estimer le niveau de risque de tout scénario pertinent

# Analyse du risque: approche générale



# Qualitative ou quantitative?



L'analyse des risques peut être effectuée à différents niveaux de détail selon la criticité des actifs, la portée des vulnérabilités connues et des incidents antérieurs expérimentés au sein de l'organisme.

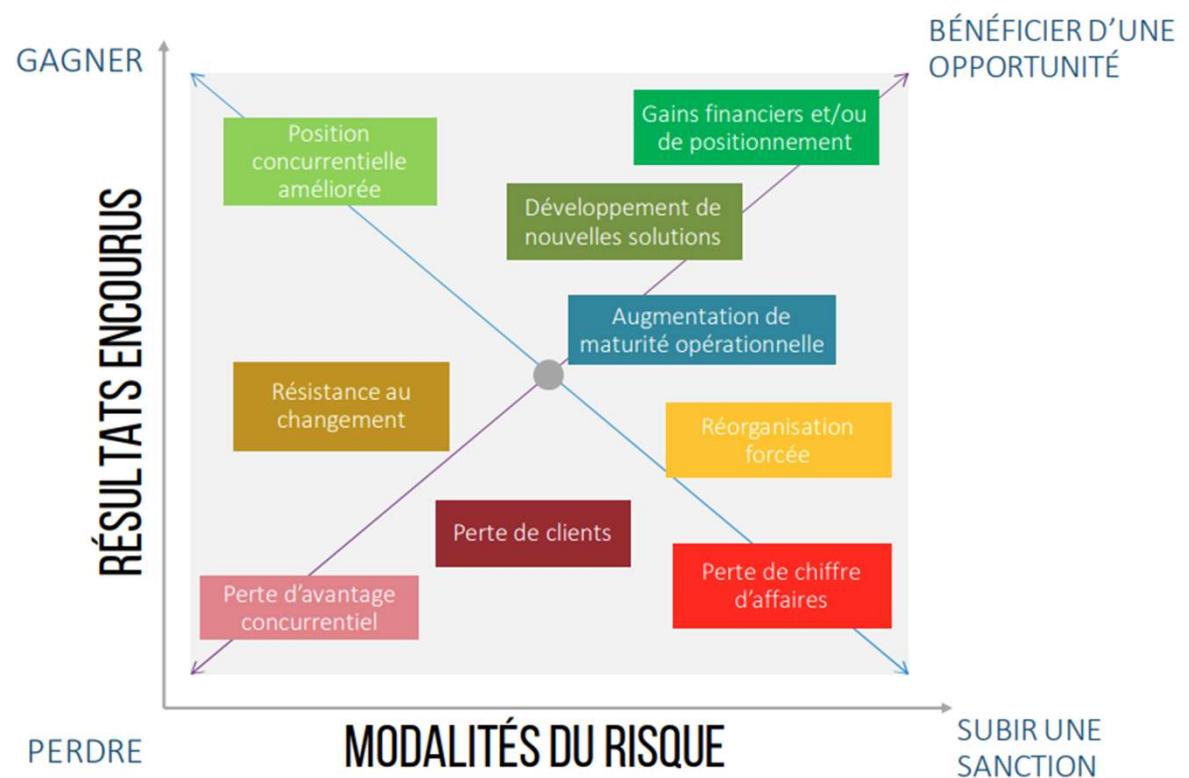


Selon les circonstances, une méthodologie d'analyse des risques peut être qualitative, quantitative ou une combinaison des deux. En pratique, l'analyse qualitative est souvent utilisée en premier lieu pour obtenir une indication générale du niveau des risques et pour mettre en exergue les principaux risques.

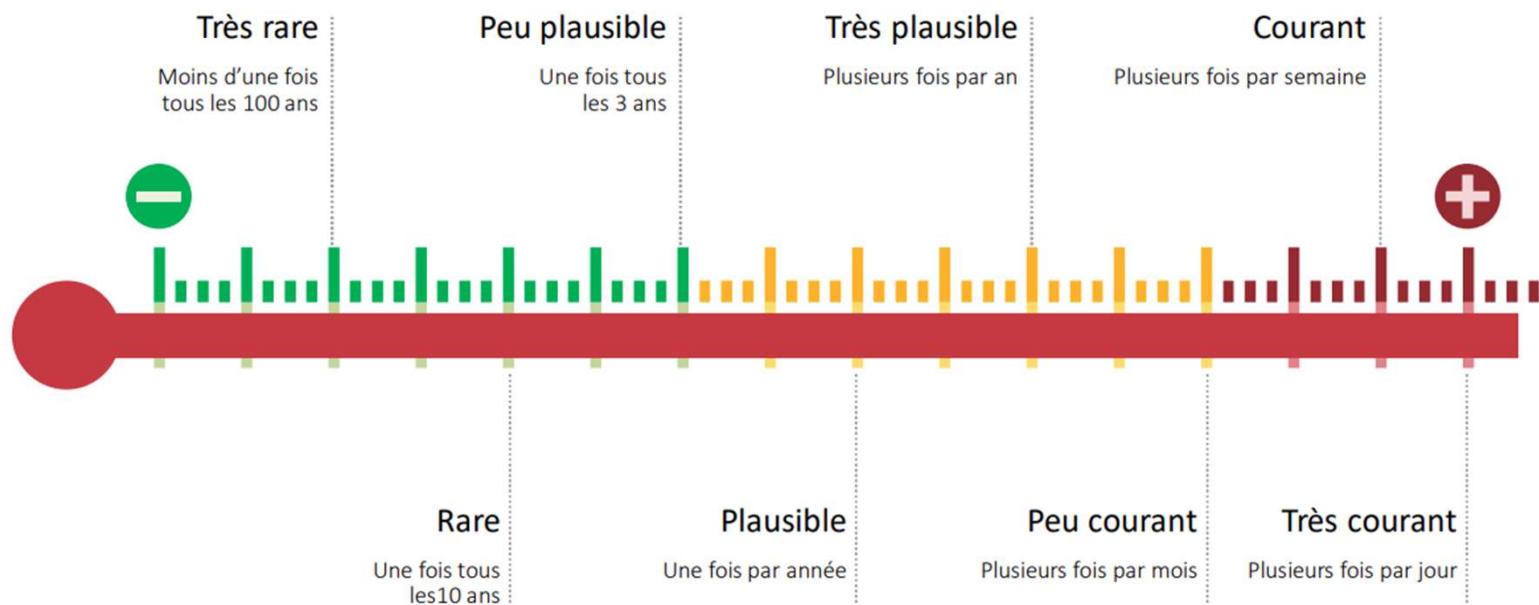


Il peut ensuite être nécessaire d'entreprendre une analyse plus spécifique ou quantitative des risques majeurs, étant donné qu'il est souvent moins complexe et moins onéreux d'effectuer une analyse qualitative qu'une analyse quantitative.

## Appréciation des conséquences



# Appréciation de la probabilité: Suivant une échelle



## Appréciation de la vraisemblance: méthode qualitative

Complexité			Niveau de complexité	
Connaissance de la société	Connaissance technique	Conditions		
Personne externe à la société Absence de connaissance spécifique requise	Absence de connaissance requise	Environnement extrêmement favorable (pas de mesure de sécurité implémentée)	Facile	1
Personne externe avec une bonne connaissance de la société	Connaissance ou recherche nécessaire	Environnement favorable (pas de mesure de sécurité implémentée)	Moyen	2
Personne externe avec une très bonne connaissance de la société. Un ancien employé par exemple	Connaissance et recherche nécessaires	Mesure de sécurité implémentée	Difficile	3
Complicité interne obligatoire	Connaissance avancée et recherche nécessaires	Mesure de sécurité implémentée et efficace	Très difficile	4

# Appréciation de la probabilité d'occurrence: exemple qualitatif

On parle de probabilité d'occurrence plutôt lorsque que l'analyse s'appuie sur des données numériques en nombre suffisant pour permettre d'assurer une statistique fiable et des résultats répétables à travers une méthode de calcul éprouvée.



# Exemple de tableau d'estimation des risques

PROBABILITÉ	FREQUENT				RISQUES ÉLEVÉS	
	PROBABLE					
	INCERTAIN					
	RARE	RISQUES	thumb up			
	EXTRAORDINAIRE	ACCEPTABLES				
		NEGLIGABLE	MINEUR	MODERE	MAJEUR	SEVERE

Le processus d'appréciation détaillée des risques en sécurité de l'information implique l'identification et la valorisation approfondie des actifs, l'appréciation des menaces par rapport à ces actifs et l'appréciation des vulnérabilités. Les résultats obtenus grâce à ces activités sont alors utilisés pour apprécier les risques, puis pour identifier le traitement des risques.

# Étape 4

## Evaluation des risques

# Evaluation des risques

L'évaluation des risques utilise la compréhension des risques obtenue par l'analyse des risques pour prendre des décisions concernant les actions futures. Les décisions devraient inclure :

- Le cas où une activité doit être entreprise ;
- Les priorités en matière de traitement des risques, compte tenu des niveaux de risques estimés.

# Validation de la cohérence des critères d'évaluation



## LES CRITÈRES D'ÉVALUATION DU RISQUE UTILISÉS POUR PRENDRE DES DÉCISIONS

- ✓ Sont cohérents avec le contexte interne et externe de gestion des risques en sécurité de l'information.
- ✓ Tiennent compte des objectifs de l'organisme, du point de vue des parties prenantes.



## LES DÉCISIONS PRISES LORS DE L'ÉVALUATION DU RISQUE

- ✓ Sont basées sur le niveau acceptable de risque.
- ✓ Considèrent les conséquences, la vraisemblance et le degré de confiance dans l'identification et l'analyse des risques.

# Déterminer les critères de risque

La matrice d'évaluation des risques utilise généralement deux critères qui se croisent :

- Probabilité : le niveau de probabilité que le risque se produira ou se réalisera.
- Impact : le niveau de gravité qu'aura le risque s'il se réalise.

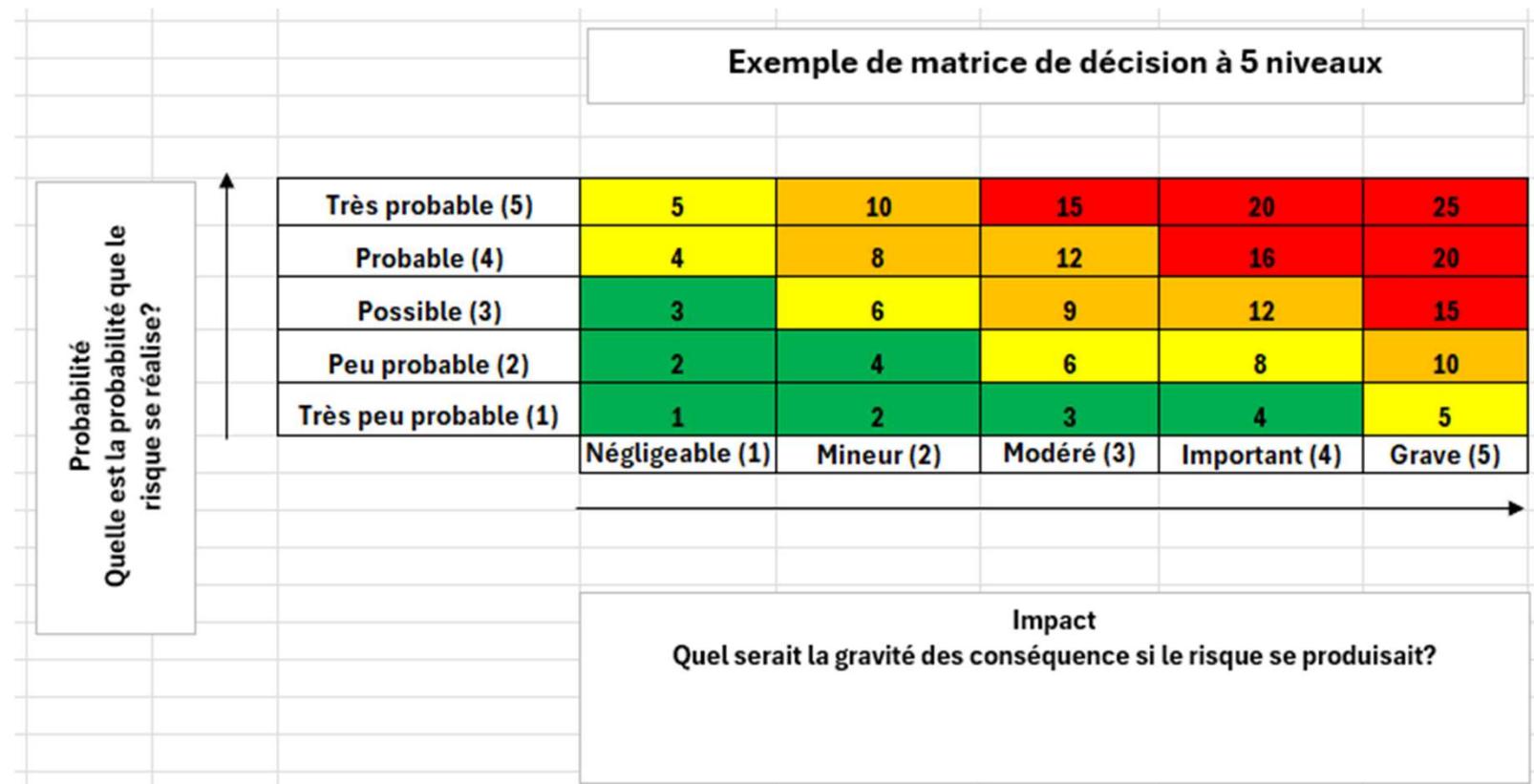
# Déterminer les critères de la probabilité

Niveau de probabilité	Description
Très probable (5)	Le risque se produira très certainement à un moment ou à un autre du projet.
Probable (4)	Il y a de fortes chances que ce risque se produise
Possible (3)	Le risque pourrait se produire, mais pas nécessairement
Peu probable (2)	Il y a peu de chances que ce risque se produise.
Très peu probable (1)	Il y a très peu de chances que ce risque se produise.

# Déterminer les critères de l'impact

Niveau de l'impact	Description
Négligeable (1)	Très faible impact sur les activités de l'organisation et la réalisation de ses objectifs
Mineur (2)	Faible impact
Modéré (3)	Impact moyen
Important (4)	Impact majeur
Grave (5)	Grave impact

## Estimation du niveau de risque: matrice à 5 niveaux



Source: MIL-STD-882E

# Exemple d'évaluation de risque

Exemple de scénarios	Valeur de l'impact	Probabilité/Vraisemblance	Mesure d'évaluation du risque	Priorité du risque
Scenario A	3	4	12	1
Scenario B	1	3	3	5
Scenario C	2	4	8	4
Scenario D	2	5	10	2
Scénario E	1	2	2	6
Scenario F	4	2	8	3

# Déterminer le niveau de gravité

Donner la priorité aux risques qui présentent la probabilité et l'impact les plus élevés, et créer un plan d'évaluation des risques pour les atténuer efficacement.

## Exemple de niveau de gravité

Niveau de gravité	
Acceptable	Acceptation du risque
Modéré	Surveillance à exercer
Significatif	Action à planifier
Critique	Action immédiate requise

# Exercice d'appréciation de risques

Le cas d'étude ci-joint présente une situation de risque assez fréquente en sécurité de l'Information que vous allez être amené à apprécier en vous basant sur les différents éléments présentés précédemment.

Le but de l'exercice est d'identifier les actifs, les mesures de sécurité existantes, les vulnérabilités qui y sont associées et d'analyser et évaluer les risques résultants de cette situation puis les prioriser en utilisant la matrice d'évaluation présentée précédemment.

# Exemple de cas

Utilisation d'un **ordinateur** portable par un chercheur de l'INRS lors de ses déplacements :

- Le disque dur contient des résultats de recherche et des informations stratégiques (**courriels échangés** avec des partenaires industriels, **rapport de recherche, projet de brevet**).
- Ce chercheur se déplace régulièrement à l'étranger et utilise son ordinateur dans des endroits publics exposés : aéroports, gares, hôtels...
- La seule protection utilisée est un simple couple identifiant / mot de passe pour s'authentifier à l'ordinateur.

# Questions ?



En avez-vous?



LAB NESSUS



Nessus  
vulnerability scanner

# Références

- <https://reciprocity.com/what-is-meant-by-risk-evaluation/>
- <https://www.eea.europa.eu/publications/GH-07-97-595-EN-C2/chapter8h.html>
- <https://www.vectorsolutions.com/resources/blogs/risk-matrix-calculations-severity-probability-risk-assessment/>
- <https://www.slideshare.net/mansoor765/risk-assessment-236466295>
- <https://www.haspod.com/blog/paperwork/5x5-risk-matrix>
- <https://www.ibm.com/docs/fr/qsip/7.4?topic=vulnerabilities-common-vulnerability-scoring-system-cvss>