

Atelier ANALYSE DE RISQUE

Conférence du réseau RELIER

*“management et maîtrise des risques
Quels enjeux et quels outils pour les universités”*

5 décembre 2014

Thierry BONTEMS
Resp. Qualité - UMR PACTE
CNRS



Sabine GOULIN
Directrice DAPEQ
Université de Lorraine



Attention ne pas confondre !

DANGER

~ **Capacité intrinsèque** d'un équipement, d'une substance ou d'une méthode de travail, **de causer un dommage.**

~ Source ou situation pouvant nuire par blessure ou atteinte à la santé, dommage à la propriété, à l'environnement du milieu de travail ou une combinaison de ces éléments (OHSAS 18001).

~ Exemple :

- un flacon d'alcool (dommage : incendie)
- Un virus (dommage : maladie)

~ **Survenue d'un danger**

~ **Combinaison** de la **probabilité** et de la (des) **conséquence(s)** de la survenue d'un événement dangereux spécifié (OHSAS 18001)

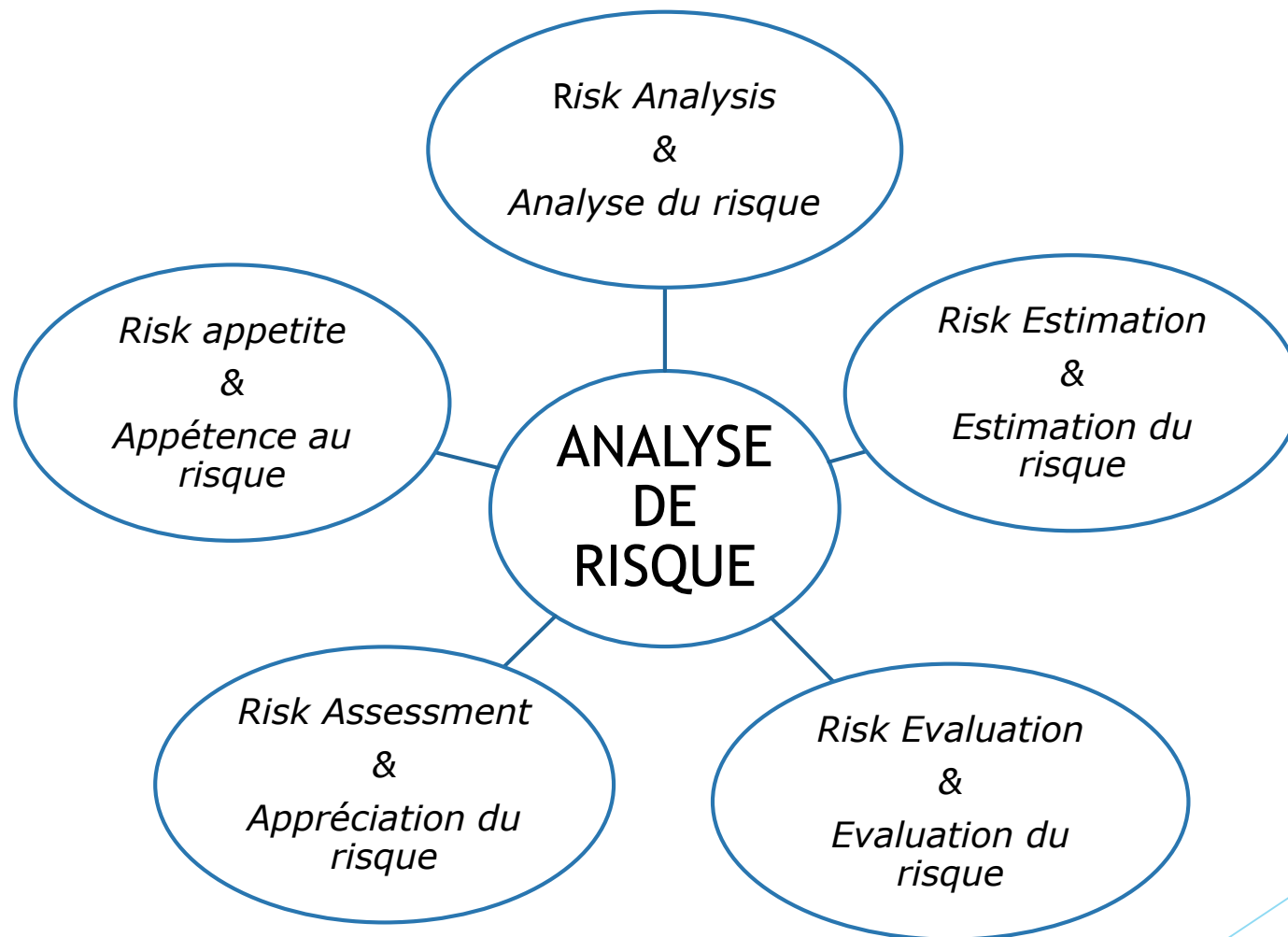
~ Exemple :

- L'incendie déclaré
- La maladie contractée

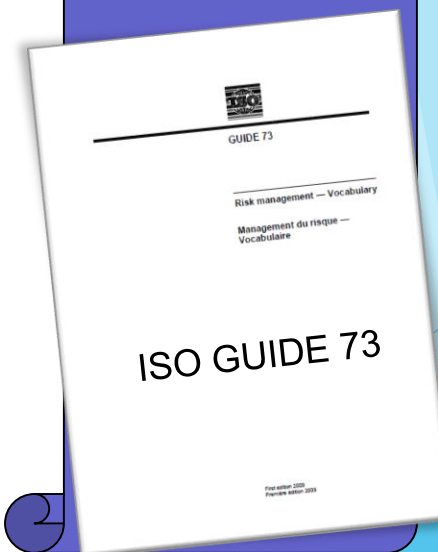
RISQUE

Ne pas confondre non plus !

Traduction normale et utilisée dans l'ISO 27001 et l'ISO 31000

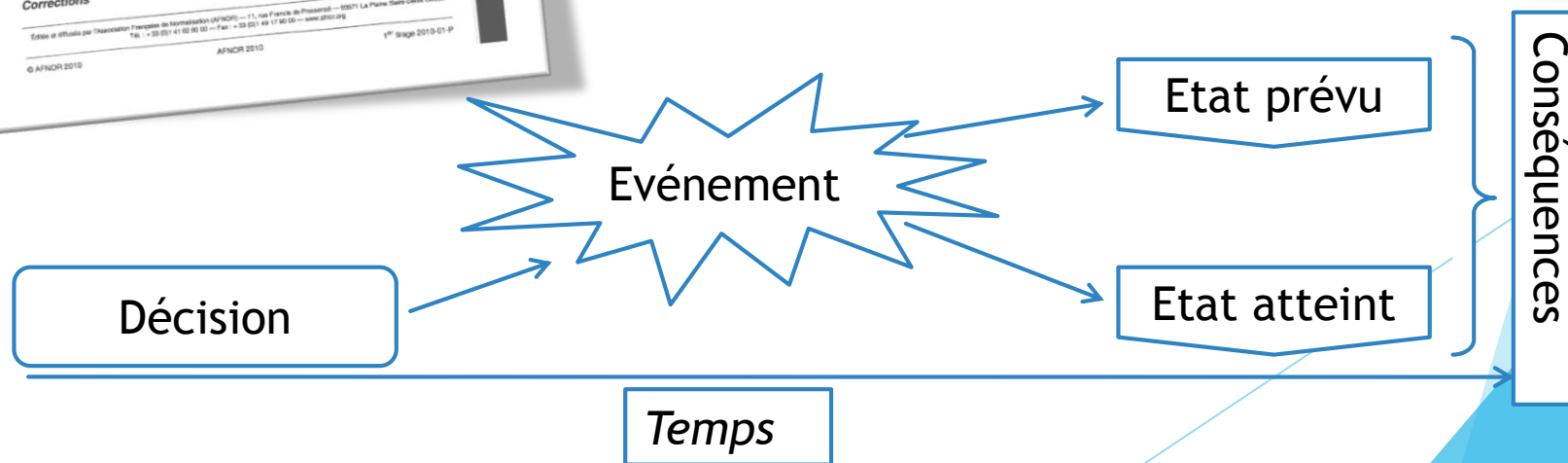
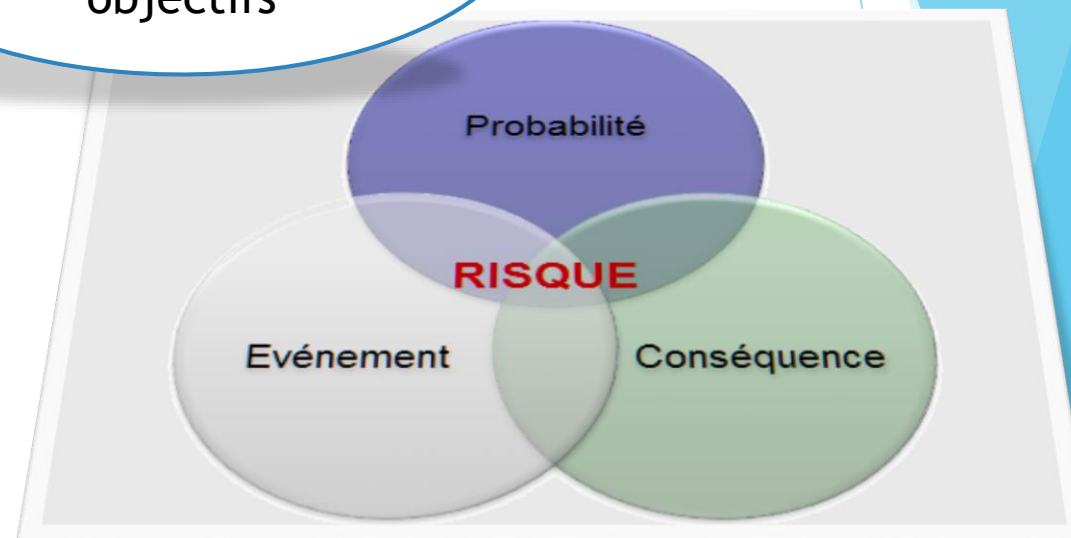
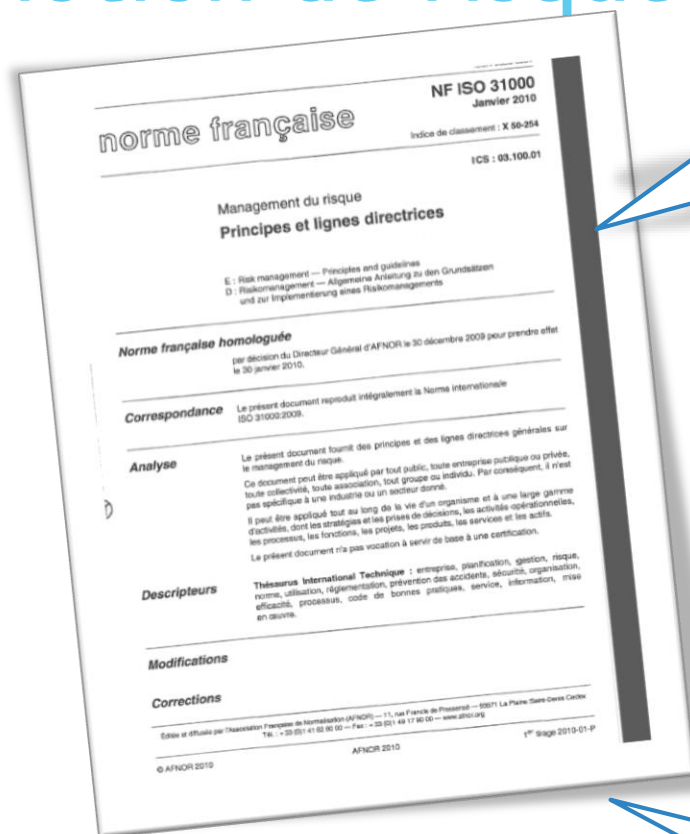


La bonne traduction :

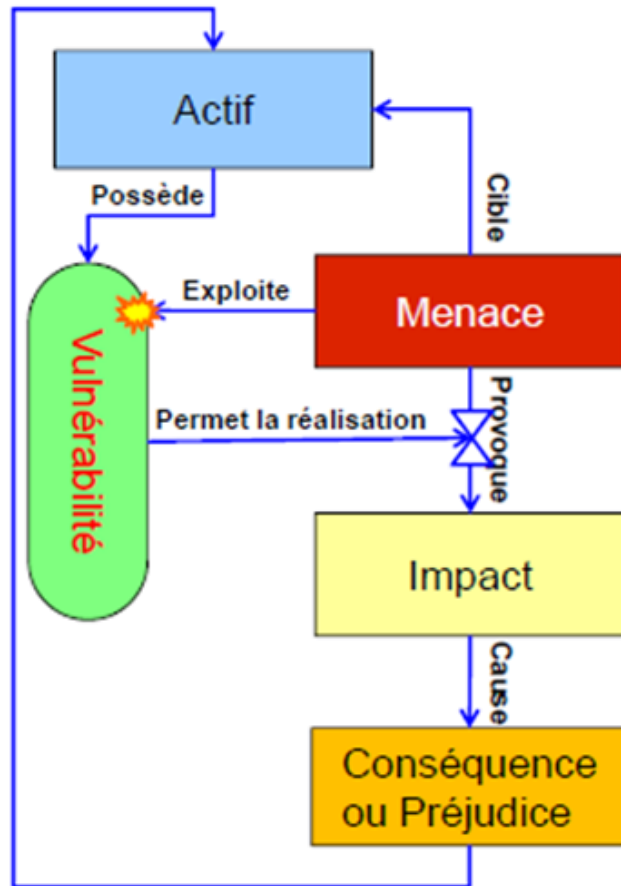


La notion de risque

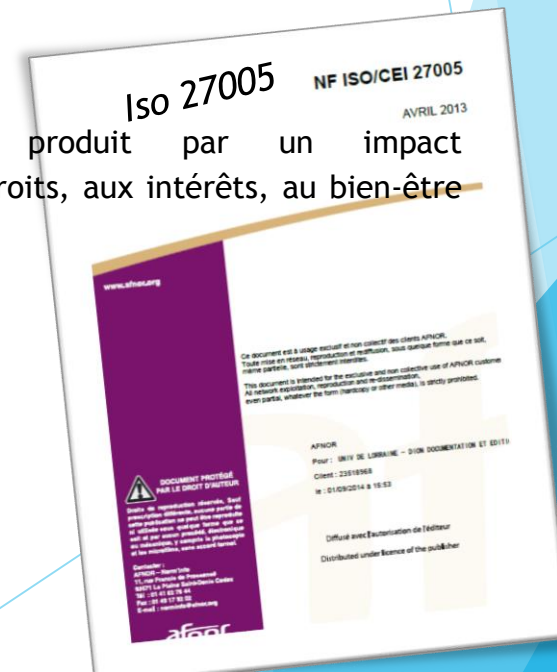
Risque : est l'effet de l'incertitude sur [la réalisation des] objectifs



Vocabulaire



- Un **actif** désigne tout élément ayant de la valeur pour l'organisation (ISO27005 §8.2.2)
- Une **menace** est [quelque chose] susceptible d'endommager les actifs tels que des informations, des processus et des systèmes et, par conséquent, des organisations (ISO27005 §8.2.3)
- les **vulnérabilités** [sont les propriétés d'un actif] susceptibles d'être exploitées par des menaces pour nuire aux actifs ou à l'organisation (ISO27005 §8.2.3)
- **Impact** : Effet produit par la menace
- **Conséquence** : ce qui est produit par un impact
Ou **Préjudice** : Atteinte portée aux droits, aux intérêts, au bien-être de quelqu'un, du fait d'un tiers



Processus de gestion du risque

Processus applicable

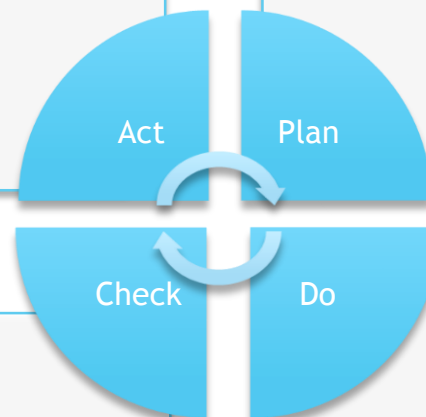
- A toute l'organisation
- A un sous ensemble
 - Ex : Service, site géographique, etc.
- A tout système
- A une mesure de sécurité ou un traitement existant ou planifié
 - Ex : continuité d'activité

- Rectifier le traitement du risque à la lumière des événements et des changements de circonstances
- Améliorer le processus de gestion du risque

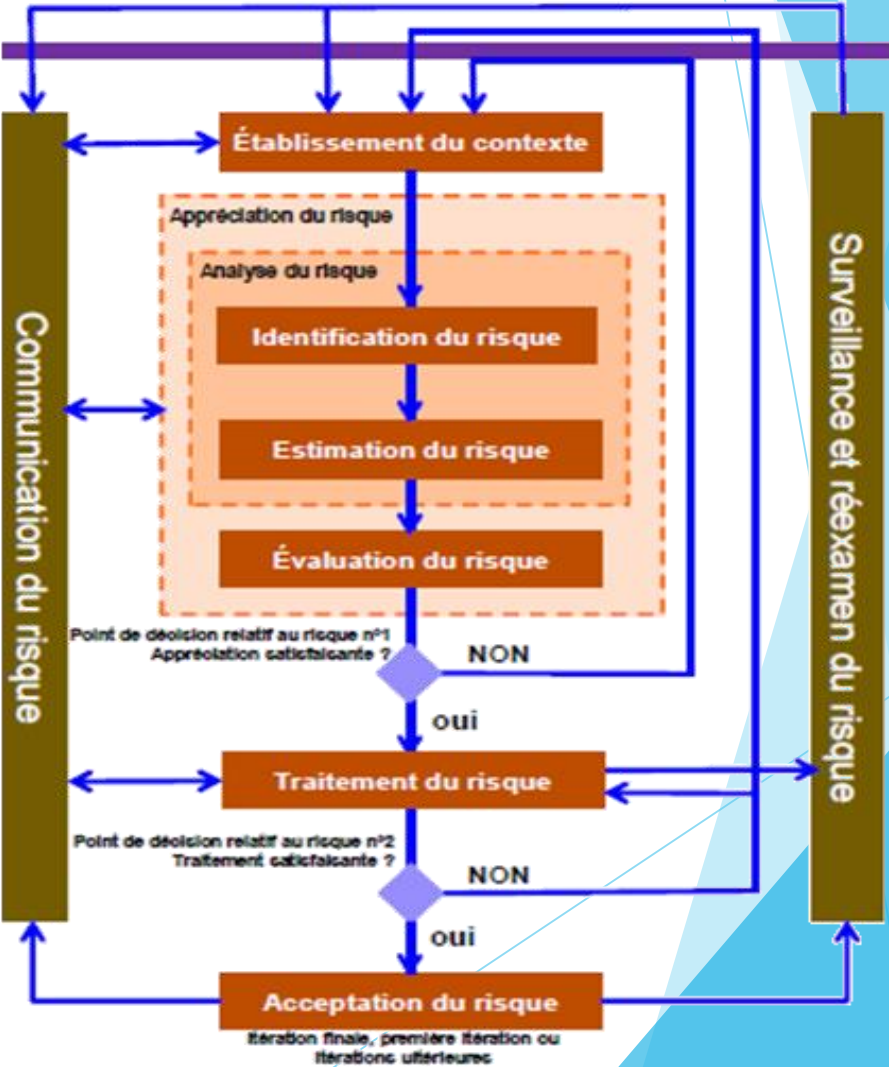
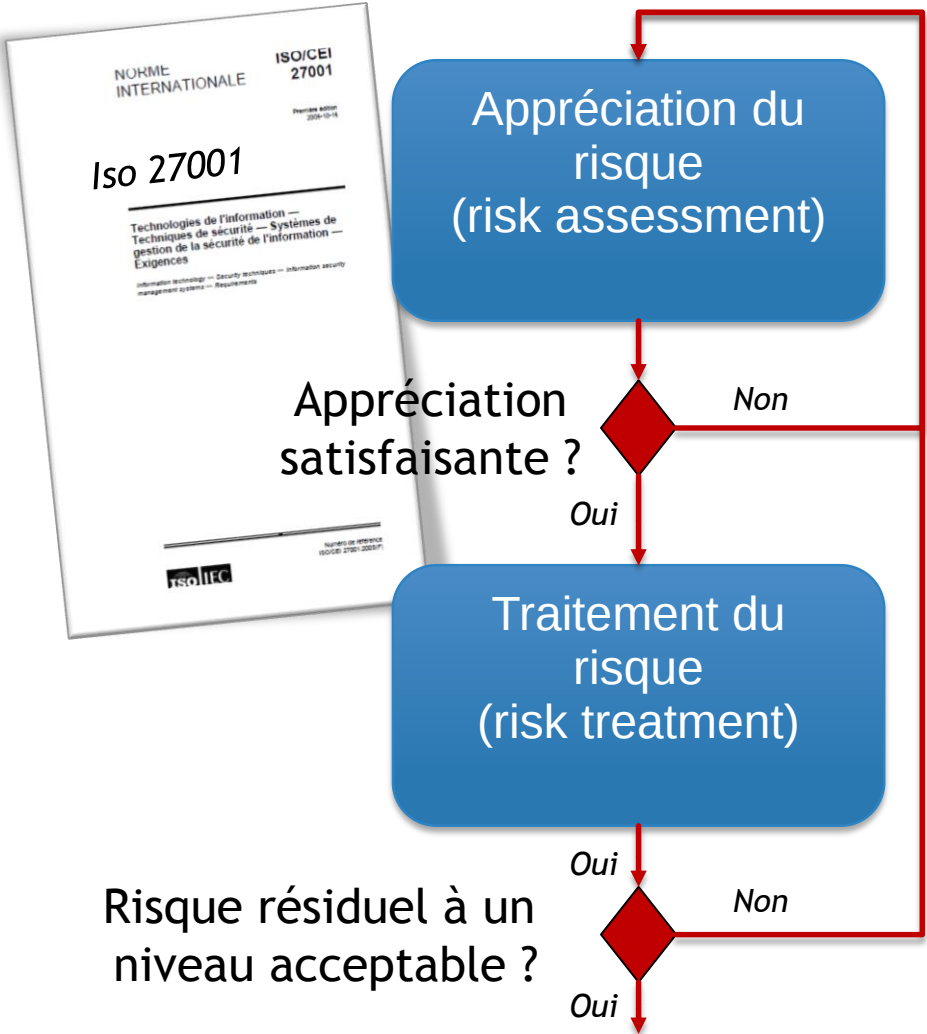
- Surveiller et réexaminer les résultats, l'efficacité, la conformité et l'efficacité du processus

- Établissement du contexte
- Appréciation du risque
- Élaboration du plan de traitement du risque
- Acceptation du risque

- Implémenter les actions pour réduire les risques
- Sensibiliser la direction et le personnel sur les risques et les actions prises pour les atténuer

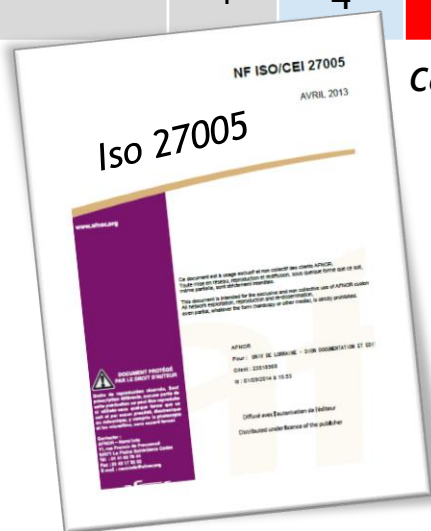


Risque et Qualité



Matrice d'évaluation des risques

Vraisemblance de la menace		Faible (1)			Moyenne (2)			Forte (3)		
Facilité de mise en œuvre		Basse (1)	Moy. (2)	Élevée (3)	Basse (1)	Moy. (2)	Élevée (3)	Basse (1)	Moy. (2)	Élevée (3)
Valeur de l'actif / niveau de l'impact	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8



Calcul : $Val + (Vrais - 1) + (Facil - 1)$



1. Risques nuls
(vert : 0)



2. Risques négligeables
(Jaune : 1-2)



3. Risques significatifs
(Rose : 3-4)



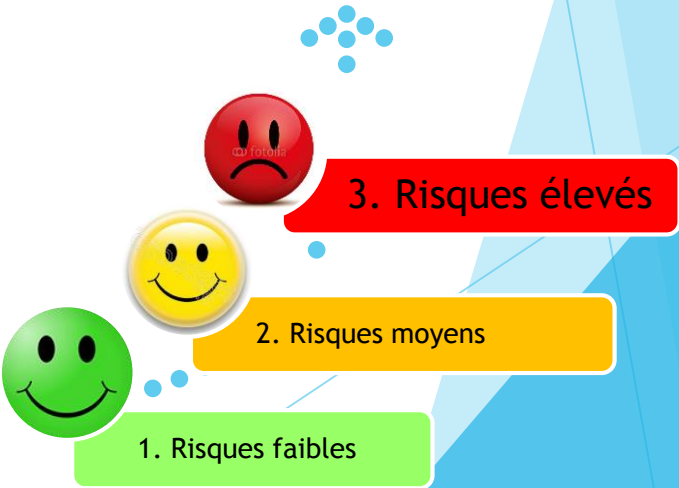
4. Risques graves
(Rouge : 5-6)



5. Risques vitaux
(Bordeaux : 7-8)

Classement des menaces par mesures des risques

	Vraisemblance d'un scénario d'incident	Très faible (Très peu probable)	Faible (Peu probable)	Moyenne (Possible)	Élevée (Probable)	Très élevée (Fréquente)
Impact sur l'activité	Très faible	0	1	2	3	4
	Faible	1	2	3	4	5
	Moyen	2	3	4	5	6
	Élevé	3	4	5	6	7
	Très élevé	4	5	6	7	8



Les étapes de la méthode

1. Établissement du contexte § 5.3 Iso 31000

- Interne: § 5.3.2
- Externe : § 5.3.3
- du processus : § 5.3.4

2. Définition des critères de risque § 5.3.5 Iso 31000

3. Appréciation des risques § 5.4 Iso 31000

4. Identification § 5.4.2 ISO 31000

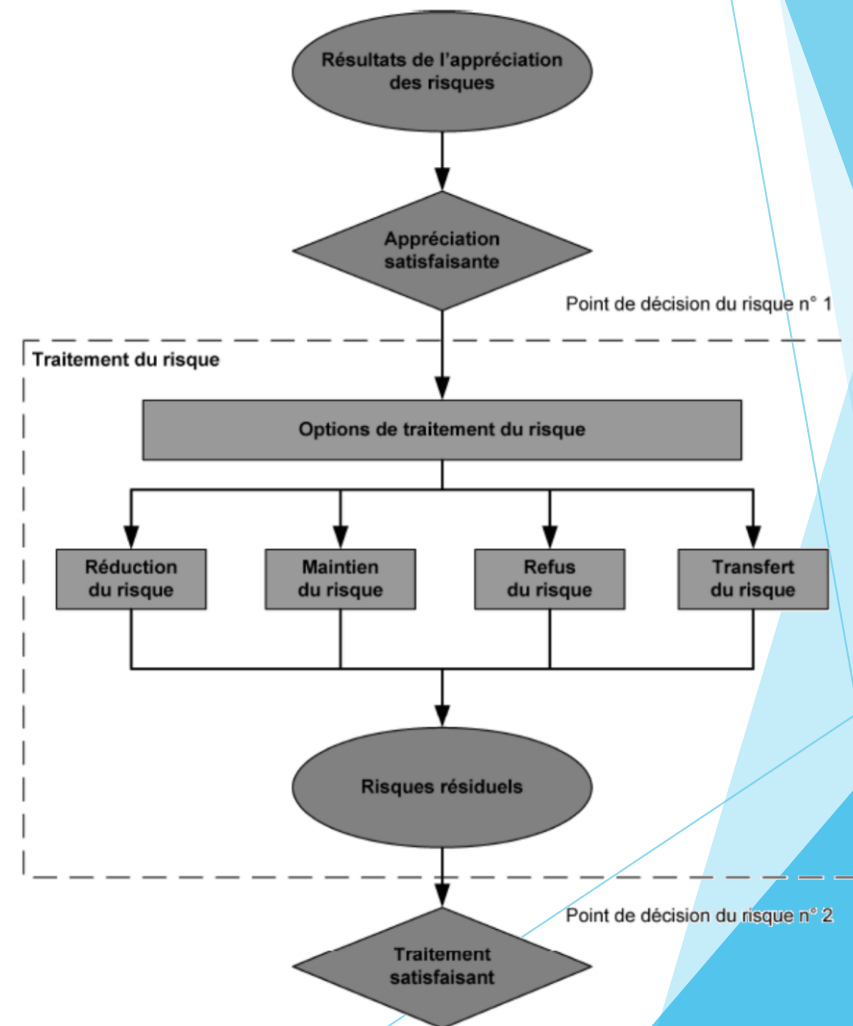
- Analyse § 5.4.3
- Evaluation § 5.4.4

5. Traitement du risque § 5.5 Iso 31000

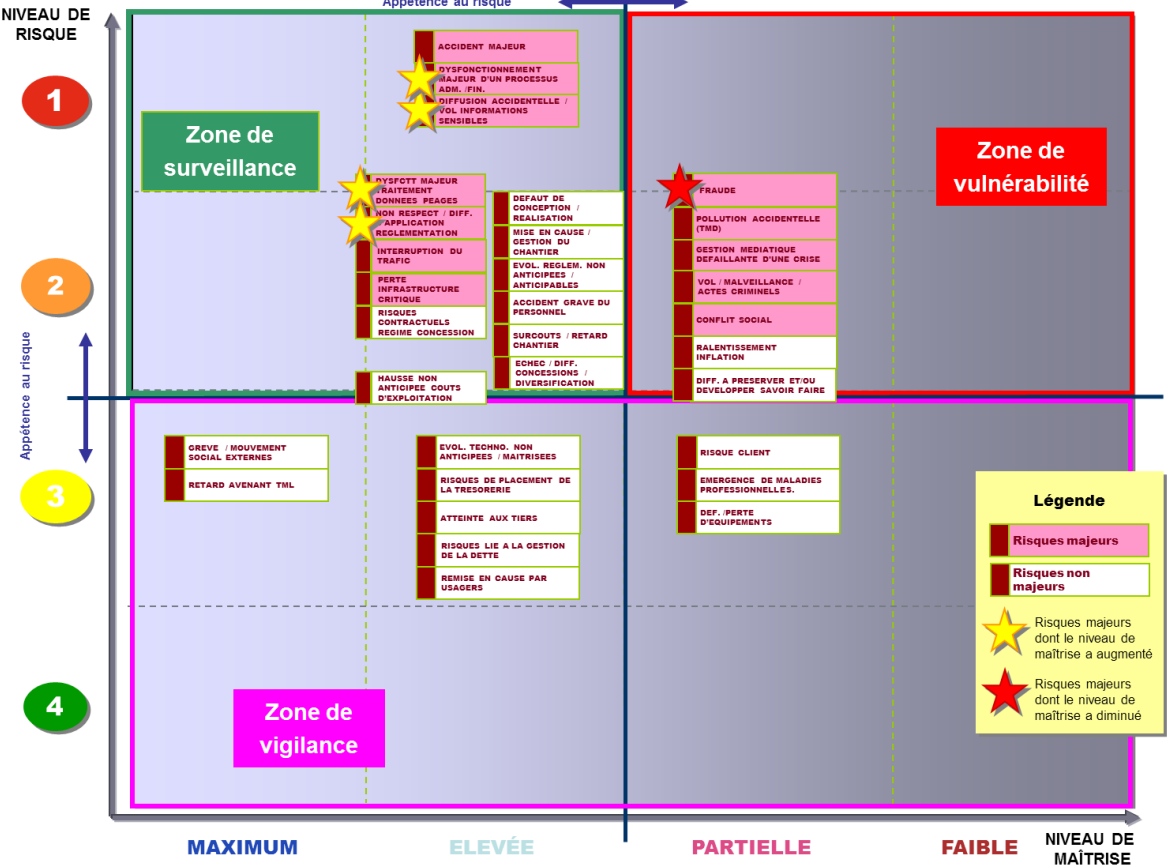
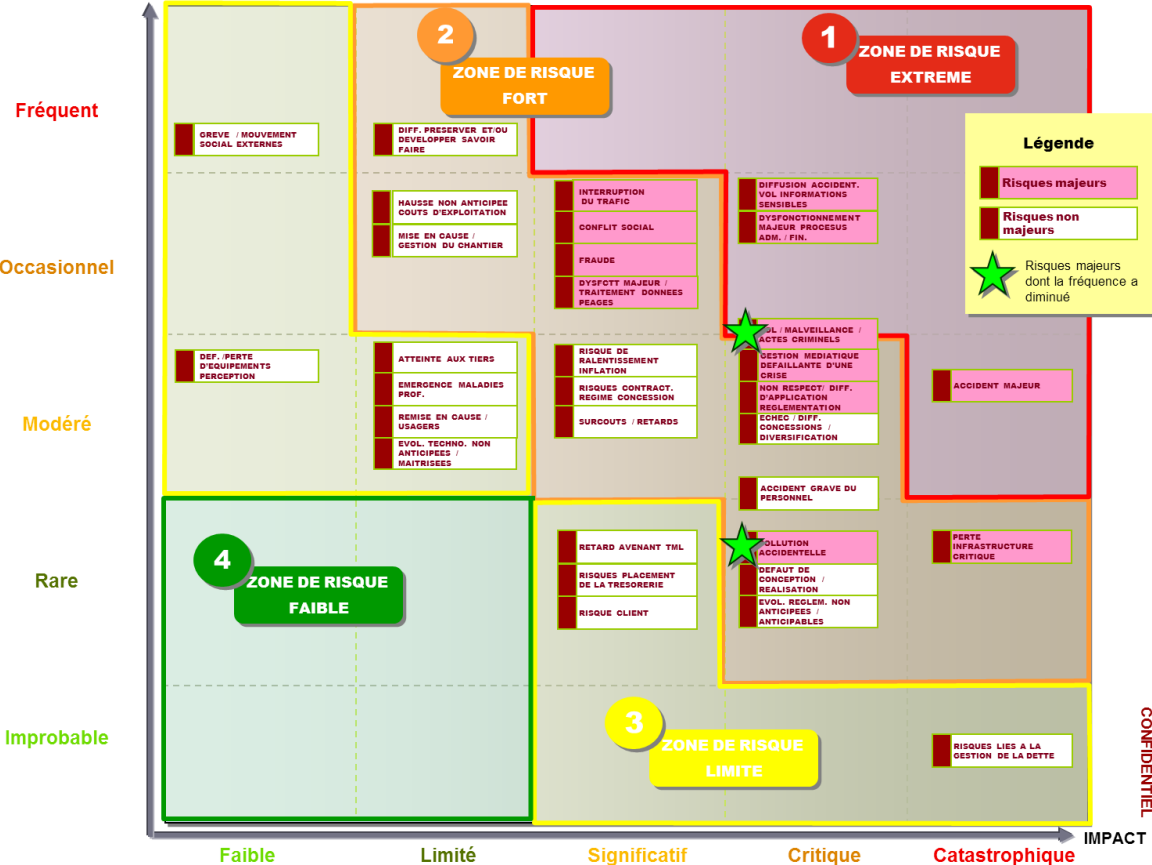
6. Acceptation du risque ISO 27005

Passer à la notion de risque résiduel

4 solutions pour passer d'un risque avéré à un risque résiduel



Cartographie des risques



L'atelier

A vous de jouer !