

Une méthode pratique de gestion du risque informatique

A. Huet
Conseiller en chef de la sécurité de l'information
Fedict

Technofutur Security day
22/05/2008

Sommaire

- > **Famille ISO 270xx**
- > **ISO 27005**
- > **Méthodes et outils classiques**
- > **Méthode simplifiée**

Sommaire

- > **Famille ISO 270xx**
- > **ISO 27005**
- > **Méthodes et outils classiques**
- > **Méthode simplifiée**

> Famille ISO 270xx

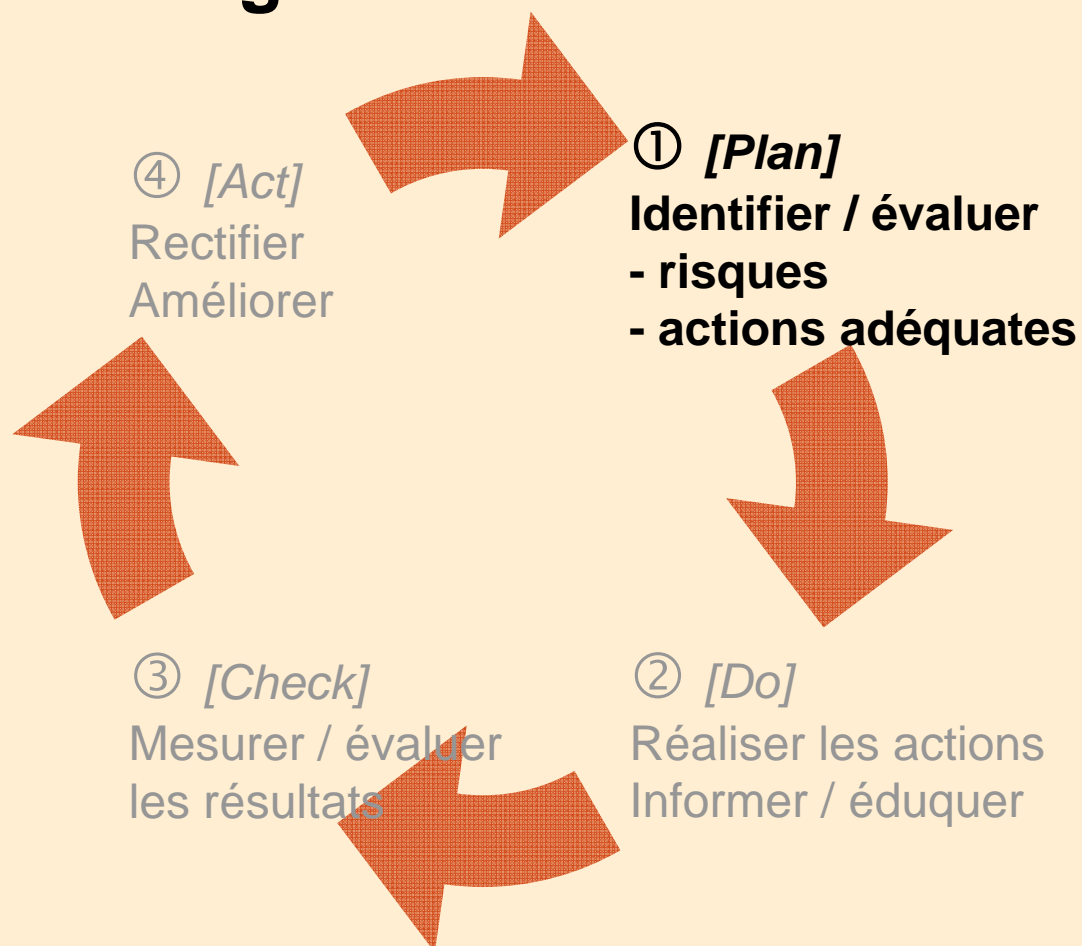
- > ISO 27000 Vue d'ensemble et vocabulaire
- > ISO 27001 Systèmes de gestion de sécurité de l'information (SGSI) : exigences (← BS7799-2)
- > ISO 27002 Code de pratique (= ISO17799 ← BS7799-1)
- > ISO 27003 Guide de mise en oeuvre
- > ISO 27004 SGSI : mesurage
- > **ISO 27005 Gestion du risque (← ISO 13335-3/4)**
- > ISO 27006 Organismes d'homologation
- > ISO 27007 Directives d'audit (SGSI)

Sommaire

- > Famille ISO 270xx
- > **ISO 27005**
- > Méthodes et outils classiques
- > Méthode simplifiée

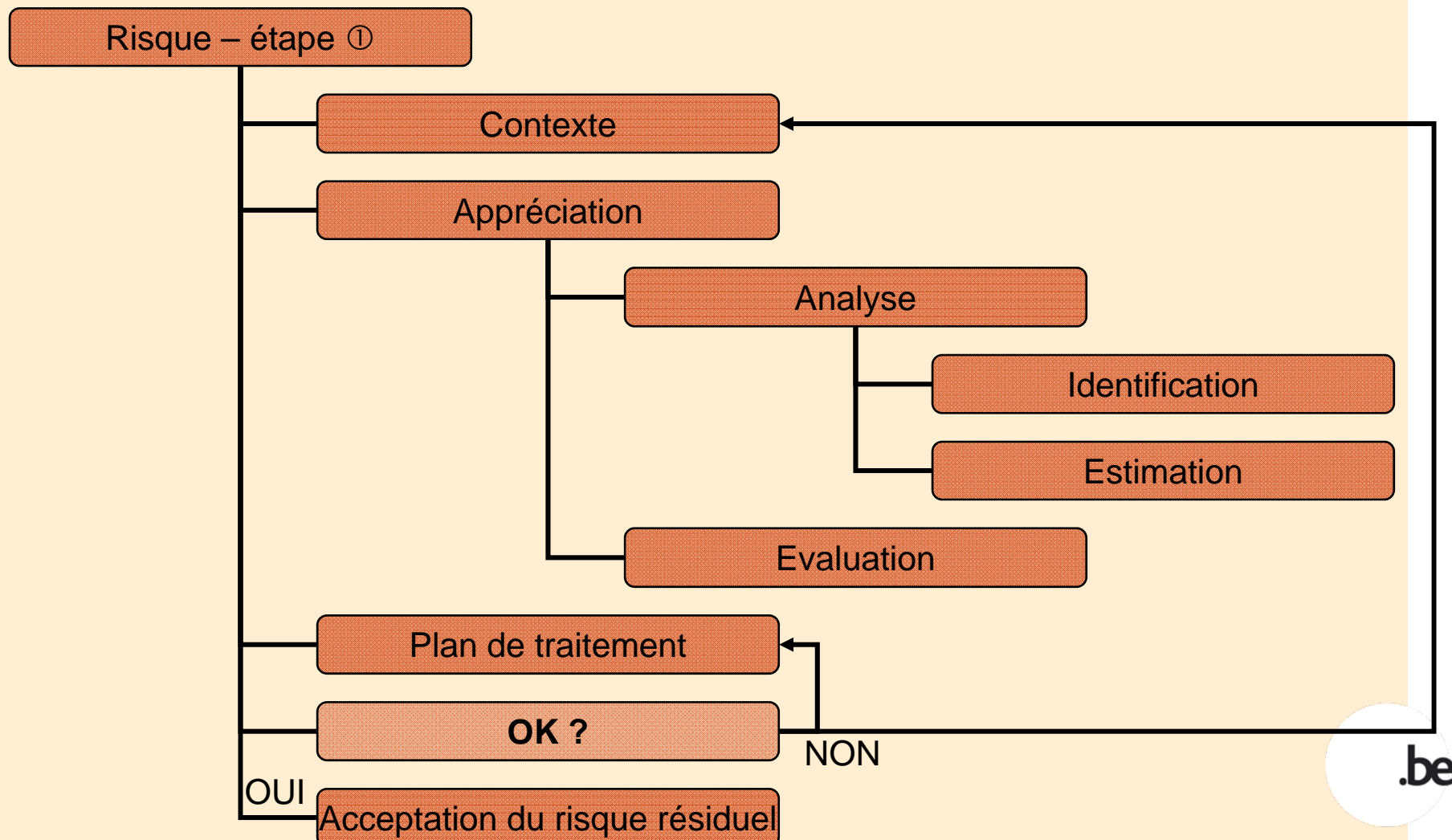
ISO 27005 (1)

> Roue de Deming



v ISO 27005 (2)

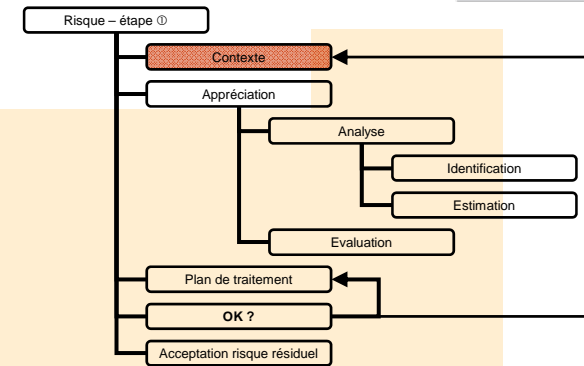
> Etape 1



ISO 27005 (3)

> Etablissement du contexte

- Objet
 - ? toute l'organisation → SGSI
 - ? 1 produit / service → spécifications du produit/service
- Critères de base
 - évaluation
 - impact
 - acceptation
- ...

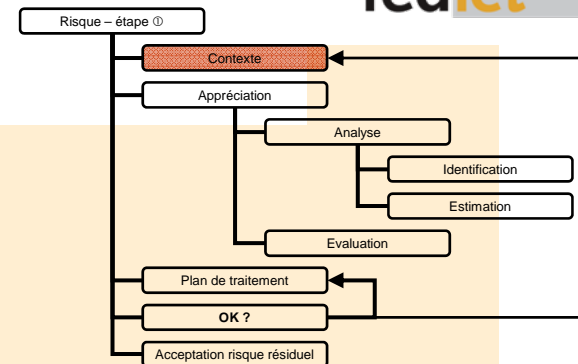


> Exemple

Métrique d'impact → services gouvernementaux

ISO 27005 (4)

> Exemple : métrique d'impact Services gouvernementaux



G r a v i t é	Nature des conséquences					
	Perte financière (millions €) F	Ordre public O	Juridique Judiciaire J	Image du service public I	Social et humain S	Classification C
0	< 0,001	-	-	-	-	-
1	0,001 – 1	Perturbation locale et momentanée	Sanctions internes	Plaintes occasionnelles	Divulgation de données personnelles	Diffusion restreinte
2	1 – 10	Menace pour l'ordre public	Actions en justice	Critiques occasionnelles dans les media	Divulgation de données personnelles sensibles	Confidentiel
3	10 – 100	Difficulté à maintenir l'ordre public	Condamnation de l'Autorité	Critiques graves dans les media	Atteinte sérieuse à l'intégrité ou à la réputation	Secret
4	> 100	Ordre public gravement en péril	Condamnation internationale de l'Autorité	Altération définitive	Perte de vie humaine Atteinte grave à la réputation	Très secret

ISO 27005 (5)

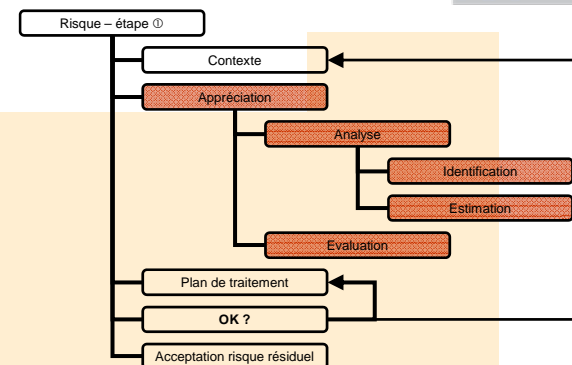
> Analyse des risques

- Actifs (← valeur)
- Menaces
 - origine
 - probabilité
 - motivation
 - impact
- Vulnérabilités

⇒ **Liste des risques et de leur niveau**

> Evaluation des risques

- Conséquences pour l'organisation



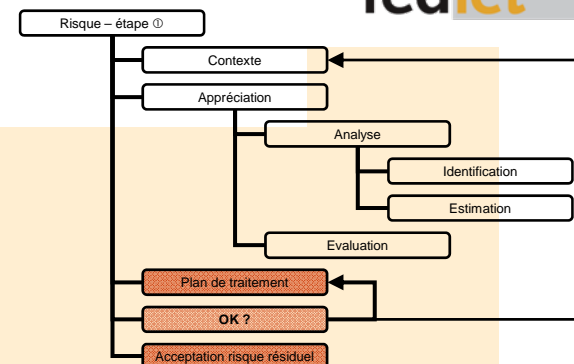
ISO 27005 (6)

> Plan de traitement

- Mesures de sécurité : bonnes pratiques (ISO 27002) + ...
 - prévention : probabilité ↘
 - protection : impact ↘
 - coût : initial / récurrent

- Décision
 - refus du risque : STOP
 - transfert du risque → assurance, exonération, ...
 - réduction du risque → mesures de sécurité

⇒ **Risque résiduel : à accepter par la direction**



Sommaire

- > Famille ISO 270xx
- > ISO 27005
- > **Méthodes et outils classiques**
- > Méthode simplifiée

> Méthodes et outils classiques (1)

> ISO 27005 : orientations méthodologiques méthode

> Méthodes et outils

Exemples

	Origine	Analyse	Évaluation	Traitement	Expertise *	Langue	Outil
CRAMM	UK	•••	•••		•••	EN NL	•
EBIOS	F	•••	•••	•••	••	EN FR DE ES	•
Grundschutz	D	•••	•••	•••	••	EN DE	•
Octave	USA	••	••	••	••	EN	

* Expertise nécessaire :

- base
- standard
- spécialiste

Source : ENISA

> Méthodes et outils classiques (2)

> Mise en œuvre assez lourde

- experts en sécurité
- charge de travail
- délai
- implication du propriétaire du système ?

Sommaire

- > Famille ISO 270xx
- > ISO 27005
- > Méthodes et outils classiques
- > **Méthode simplifiée**

Méthode simplifiée (1)

> Méthode simplifiée

■ Objectif

propriétaire du système

→ acteur principal de la gestion de risque

■ Simplifications

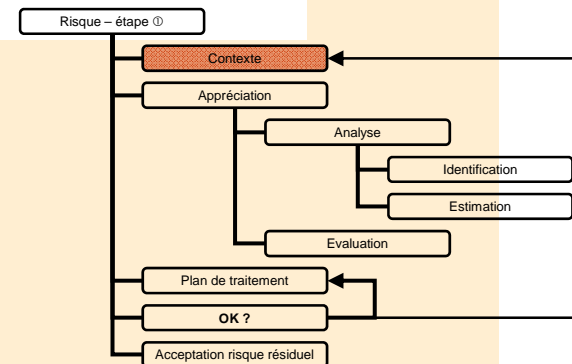
- métrique d'impact (→ l'organisation)
- métrique de défauts de sécurité
- probabilités : rôle secondaire
- socle de bonnes pratiques de base : pour toute l'organisation
- + mesures de sécurité spécifiques : par système

> Méthode simplifiée (2)

> Etablissement du contexte

- Métrique d'impact

Exemple ↓



G r a v i t é	Nature des conséquences			
	Perte financière (€) F	Commercial C	Juridique / Judiciaire J	Divulgarion D
1	1.000 – 10.000	Quelques plaintes	-	-
2	10.000 – 100.000	Nombreuses plaintes	-	Divulgarion de données personnelles
3	100.000 – 1.000.000	Perturbation sérieuse de la clientèle	Condamnation civile	Divulgarion de secret commercial
4	> 1.000.000	Altération sérieuse de l'image	Condamnation pénale	Divulgarion de secret industriel



> Méthode simplifiée (3)

> Appréciation des risques (1)

- Actifs

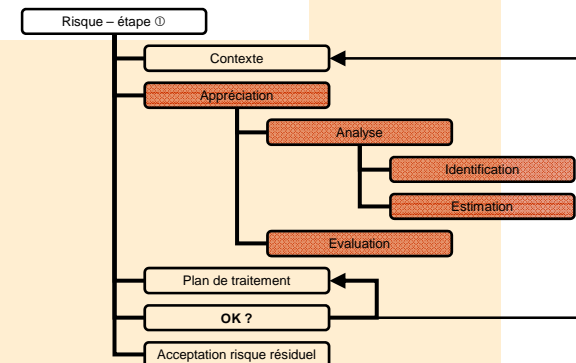
Informations

Processus / fonctions

Flux

- Métrique de défauts de sécurité

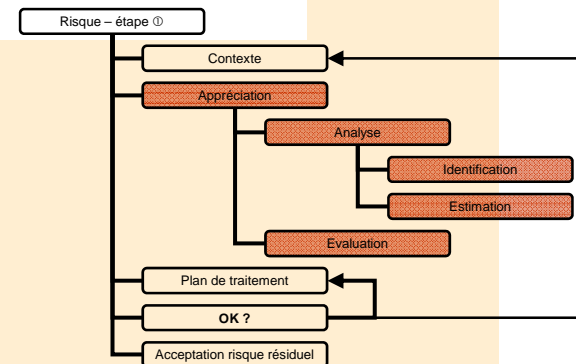
Disponibilité	Indisponibilité : 5 minutes 1 heure 1 jour 1 semaine > 1 semaine
Intégrité	Corruption accidentelle Corruption volontaire Transactions perdues : 1 10 100 1.000
Confidentialité	Divulgation
Preuve	Enregistrements non probants



Appliquée à
chaque actif

> Méthode simplifiée (4)

> Appréciation des risques (2)



- Modèle documentaire ↓

Actif :		F	C	J	D	Tot
Disponibilité	Indisponibilité : 5 minutes					
	1 heure					
	1 jour					
	1 semaine					
	> 1 semaine					
Intégrité	Corruption accidentelle					
	Corruption volontaire					
	Transactions perdues : 1					
	10					
	100					
	1.000					
Confidentialité	Divulgateion					
Preuve	Enregistrements non probants					



> Méthode simplifiée (5)

> Plan de traitement (1)

- **Mesures de base**

SGSI (← ISO 27001)

bonnes pratiques de base (← ISO 27002)

- **Mesures spécifiques**

au métier, à l'application, ...

- **Attributs des mesures**

- Mode d'action

PV : **p**révention (probabilité/opportunité ↘)

PT : **p**rotection (impact ↘)

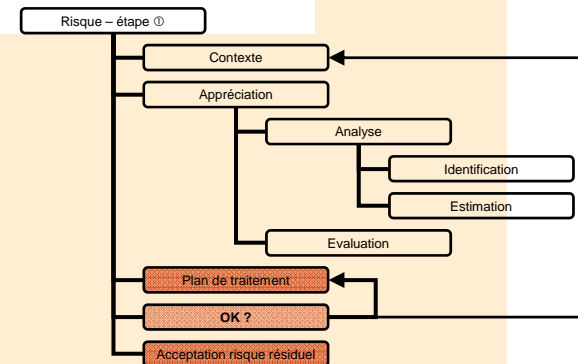
- Localisation

IT : **I**CT

US : end **u**ser

- Coût : initial / récurrent

- Attributs de sécurité améliorés : disponibilité, intégrité, ...

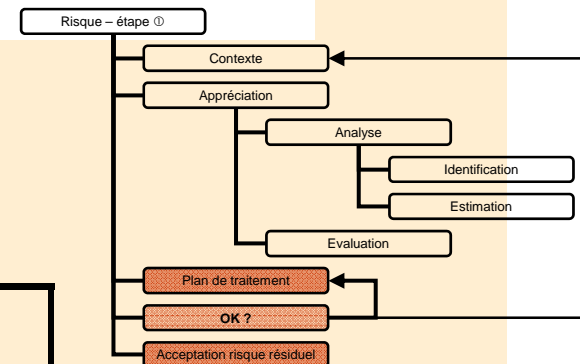


> Méthode simplifiée (6)

> Plan de traitement (2)

■ Modèle documentaire ↓

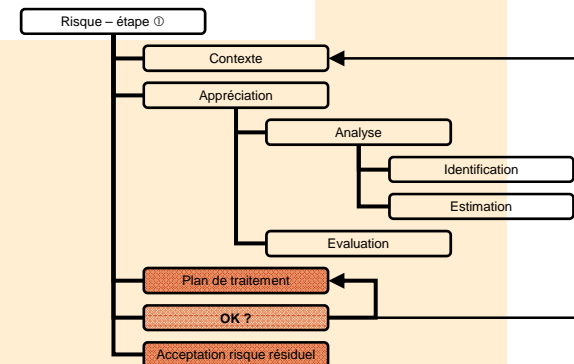
Mesure :		
Mode d'action		
Localisation		
Coût initial		
Coût récurrent		
Disponibilité	Indisponibilité : 5 minutes 1 heure 1 jour 1 semaine > 1 semaine	
Intégrité	Corruption accidentelle Corruption volontaire Transactions perdues : 1 10 100 1.000	
Confidentialité	Divulgation	
Preuve	Enregistrements non probants	



> Méthode simplifiée (7)

> Plan de traitement (3)

- **Risque résiduel**
après application des mesures



Actif :		F	C	J	D	Tot
Disponibilité	Indisponibilité : 5 minutes 1 heure 1 jour 1 semaine > 1 semaine					
Intégrité	Corruption accidentelle Corruption volontaire Transactions perdues : 1 10 100 1.000					
Confidentialité	Divulgation					
Preuve	Enregistrements non probants					



Questions ?