La norme ISO 27005

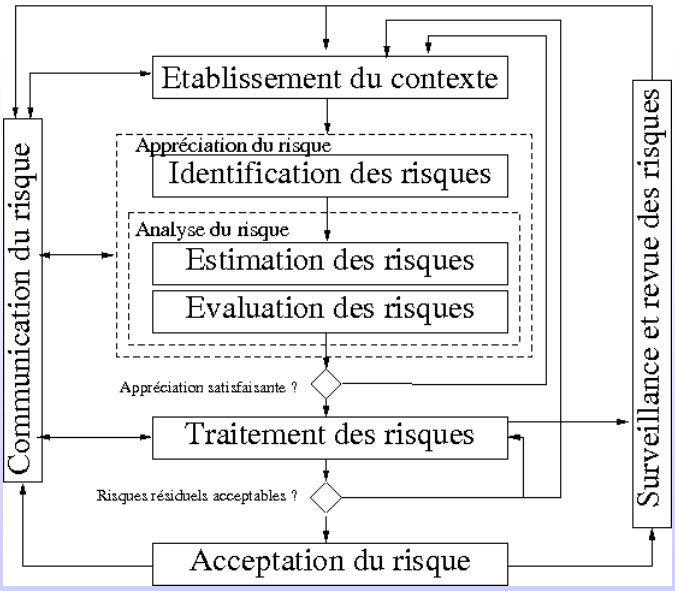
Information Security Risk Management

Pierre-Yves BONNETAIN
B&A Consultants
py.bonnetain@ba-consultants.fr
Certificat LSTI/RM27005/17

Mêmes principes que la qualité

- Cycle continu selon la roue de Deming (Plan, Do, Check, Act).
- De manière (très) simplifiée :
  - Identifier les actions à mener,
  - Réaliser les actions prévues,
  - Vérifier les résultats et l'efficacité des actions,
  - Adapter le processus pour l'itération suivante.

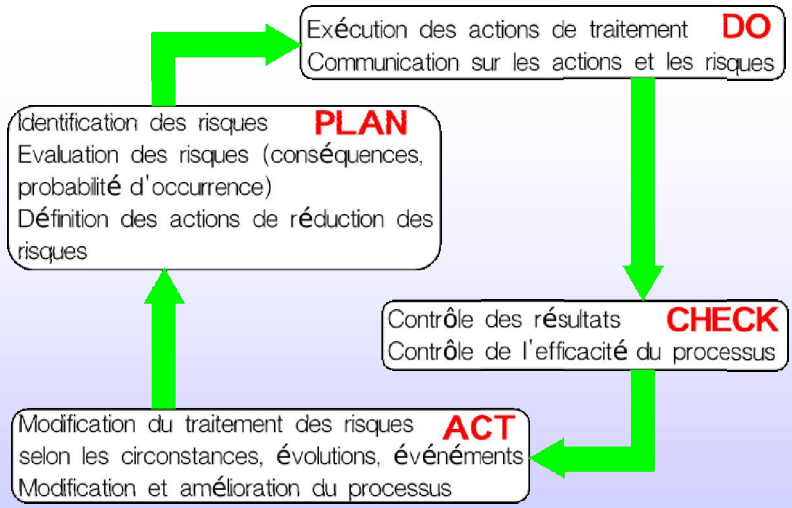
Processus ISO 27005



Terminologie

- Norme en anglais, traduite en francais
  - Risk analysis : Analyse du risque
  - Risk evaluation : Evaluation du risque
  - Risk estimation : Estimation du risque
  - Risk assessment : Appréciation du risque
- Attention à ne pas confondre
  - Appréciation du risque et
  - Analyse du risque

ISO 27005 et PDCA



ISO 27005

- Norme « non directive » :
  - Explicite comment faire (le processus général)
  - Tout en laissant l'entière liberté de comment on exécute chaque étape
- Peut couvrir des situations très diverses sans modification.
  - L'avantage d'une norme « consensuelle ».
  - Inconvénient, la première itération peut être « plus longue » (définition des critères, des règles, formules de calcul, etc).

Etablissement du contexte

- Définit « ce sur quoi va porter l'analyse de risques » et « comment on va mesurer... »
- Etape d'identification (actifs principaux, actifs supports, processus...)
- Peut être corrigée suite aux étapes ultérieures.
- Le contexte peut concerner un ensemble très large ou très resserré, par exemple :
  - Tout un système d'informations, ou
  - Juste un sous-composant du SI.

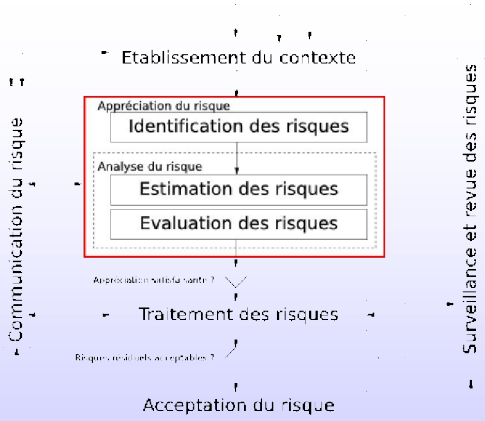
Etablissement du contexte

- Définition des critères et échelles
  - D'évaluation : seuil de traitement des risques
  - D'impact : seuil de prise en compte des risques.
  - D'acceptation : seuil d'acceptation d'un risque résiduel.
- Pas d'échelles standards, ce doit être “pertinent” pour l'entreprise.
- Les critères peuvent changer d'une itération à l'autre, ou être revus dans une itération.

Etablissement du contexte

- Définir
  - L'objectif du processus de gestion des risques (vision claire de ce sur quoi va porter la gestion des risques),
  - sa portée ainsi que ses limites,
  - l'environnement dans lequel il s'inscrit (organisation, contraintes...)
- Organiser et diriger la gestion des risques (intervenants, rôles, chemins de décision...)

Appréciation des risques



Identification des risques

- Identifier et évaluer
  - les actifs associés au contexte et leur propriétaire,
  - les menaces qui pèsent sur ces actifs,
  - les mesures de sécurité existantes,
  - les vulnérabilités possibles, et
  - les conséquences de celles-ci.
- Evaluation == donner une note.
- Elaboration de scénarii d'incidents

Identification des risques

- Que peut-il arriver aux actifs qui composent le contexte ?
  - Réunions, brainstorming,
  - Réflexions individuelles,
  - Approches scénarisées,
  - Entretiens,
  - Lectures
  - Expériences vécues...

Identifier les risques

- Critères d'évaluation pour les actifs, menaces, conséquences :
  - Qualitatifs,
  - Quantitatifs,
  - Financiers,
  - Etc.
- Les critères peuvent être quelconques.
- Obtenir une note pour les différents éléments.

Estimation des risques

- Estimer les conséquences de l'avénement d'un risque.
- Estimer la vraisemblance d'un scénario d'incident.
- Estimer le niveau de risque.
- Méthodes d'estimation qualitatives (coûts difficiles à mesurer), quantitatives (coûts mesurables), ou mixtes.

Exemple d'échelles

- Actifs : notés de 0 (jetable) à 4 (vital).
- Vraisemblance des menaces : 0 (peu vraisemblable) à 2 (très vraisemblable).
- Facilité d'exploitation : 0 (très difficile) à 2 (facile).
- Ce ne sont que quelques exemples simples, sur échelles resserrées.
- L'échelle peut être très large (1 à 100).

Estimation des risques

- Exemple classique : somme des pondérations des trois critères (probabilité, facilité, valeur)
- 0 à 2 : bénin ; 3 ou 4 : moyen ; supérieur à 5 : grave

	Probabilité d'occurrence du risque	Faible			Moyenne			Elevée		
	Facilité d'exploitation	F	M	E	F	M	E	F	M	E
Valeur de l'actif	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

Règles de calcul

- Absentes de la norme, donc à définir selon le projet, son contexte, la maturité de l'organisation.
- Commencer avec des règles simples.
- Faciliter la comparaison avec d'autres situations et d'autres projets.

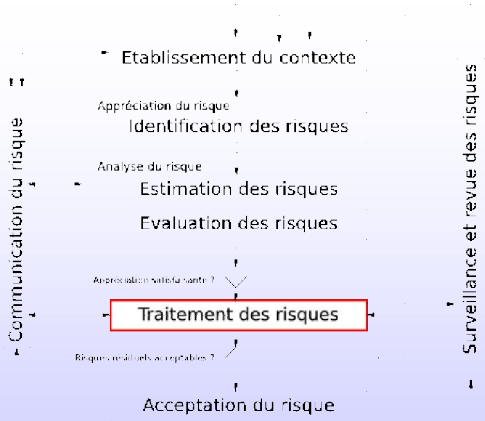
Evaluation des risques

- Etape de prise de décision :
  - Faut-il traiter le risque ?
  - Comment établir les priorités ?
- Analyse des risques => comprendre ceux-ci.
- On peut « redresser » les résultats de l'estimation des risques du fait de contraintes qualitatives difficiles à chiffrer (obligations contractuelles, réglementation, notoriété, etc.).

Prise de décision

- Niveau du risque (estimation des risques)
- Critères d'évaluation des risques (établissement du contexte)
- => priorisation des risques.
- Point de contrôle : l'appréciation est-elle satisfaisante ?
  - Oui, on passe à la définition du plan de traitement
  - Si non, on refait une itération

Traitement du risque



Définition du plan de traitement

- Pour définir les options de traitement :
  - Mettre en adéquation le risque et le coût de traitement/réduction.
  - Intégration possible d'éléments non rationnels (« 11 septembre »).
  - Intégration des parties concernées
    - Perception des risques par celles-ci
    - Communication avec elles.

Options de traitement

- Refus du risque : l'activité amenant le risque doit être éliminée.
- Réduction du risque : le risque doit être diminué.
- Transfert du risque : le risque sera transféré à une autre « entité » capable de le gérer.
- Conservation du risque : le risque est maintenu tel quel.
- Chaque option produit un risque résiduel à évaluer.

Acceptation du risque

Acceptation du risque

- Le plan de traitement des risques et les risques résiduels qui en découlent doivent être approuvés par la direction.
- Peut déroger aux règles d'évaluation des risques (critères d'acceptation)
  - Coût jugé trop élevé,
  - Avantages intéressants à maintenir un risque
  - etc.
- Dérogations justifiées et documentées.
- Prises en compte à la prochaine itération.

Au-delà de la 27005

- S'intègre normalement dans un SMSI
  - Par exemple un processus ISO 27001
  - Ou toute autre méthode d'organisation de la gestion de la sécurité informatique
- Peut fonctionner de manière autonome, hors SMSI
  - Attention à ne pas oublier d'appliquer le plan de traitement !

Vision à moyen et long terme

- Un processus comme ISO 27005 permet de garder un historique significatif :
  - Des risques, hypothèses, scénarii envisagés
  - Des analyses, évolutions du contexte et modifications associées des scénarii
  - Des plans de traitement, dérogations, contraintes spécifiques
- Donc, de maîtriser son existant.