KPMG

GOVERNMENT

Les outils pour mettre en place le management du risque

Expériences dans les collectivités publiques

AUDIT

Alain Guillaume
Senior manager
Neuchâtel
Septembre 2006

AUDIT ▪ TAX ▪ ADVISORY

Sommaire

1. La gestion des risques dans le contexte suisse
2. Outils de gestion des risques
3. Particularités des collectivités publiques en matière de gestion des risques
4. La gestion des risques informatiques
5. Autres apports de la gestion des risques

1. La gestion des risques dans le contexte suisse

Le contexte suisse

Art. 663b CO (complété)

«L'annexe contient les informations suivantes : 12. des informations sur la réalisation d'une évaluation du risque».

- **L'importance d'une bonne gestion des risques au sein des entreprises est reconnue par le législateur**
- **La plupart des grandes sociétés cotées en Suisse ont mis en place une structure de gestion des risques… les autres suivent**

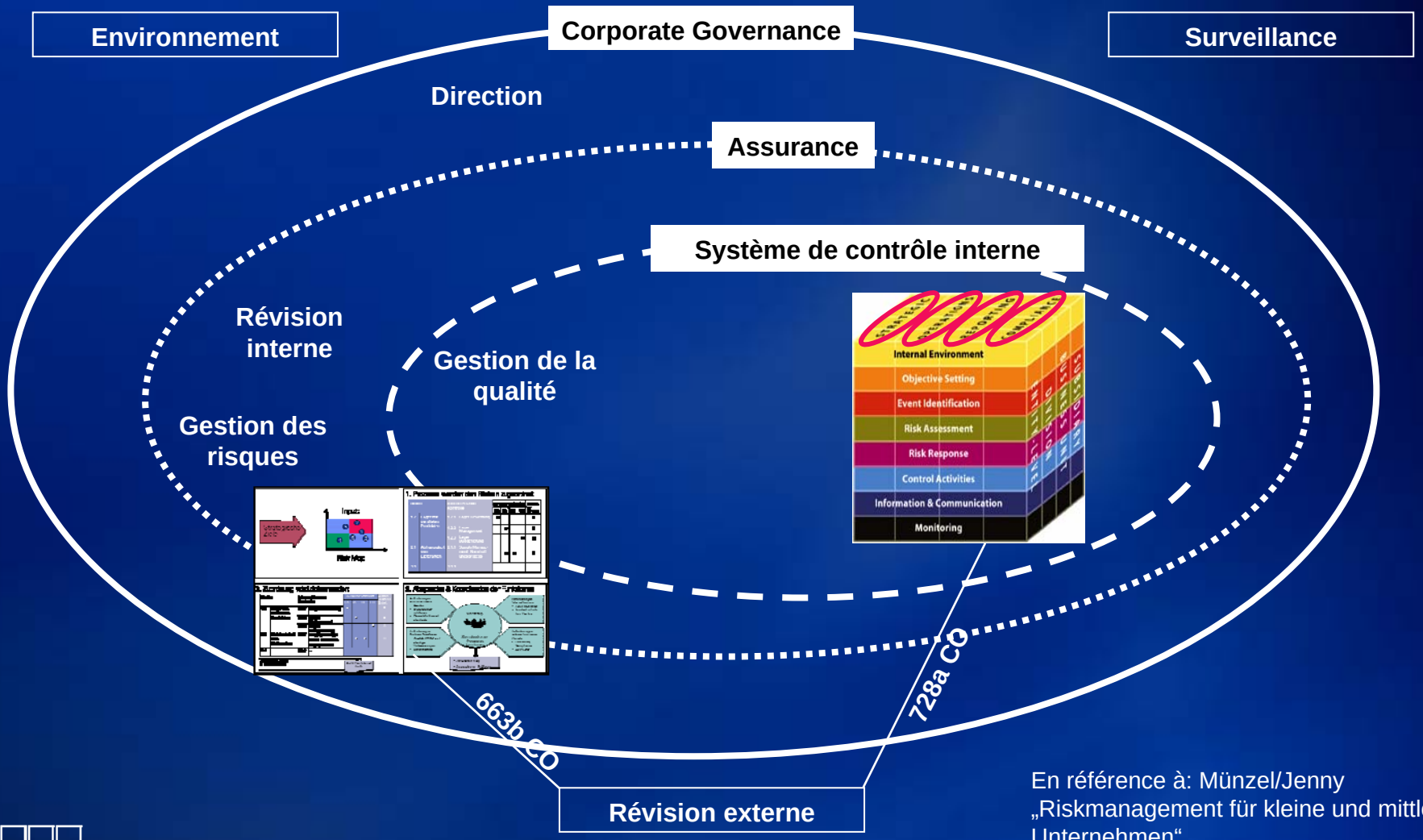
Le contexte suisse

Les collectivités publiques sont soumises elles aussi à des considérations de bonne gouvernance :

- **L'importance d'une bonne gestion des risques au sein des collectivités publiques est reconnue**

- **La plupart des collectivités publiques suisses considèrent que la gestion des risques est du ressort de la révision interne**

La gestion des risques et le contrôle interne comme éléments intégrés de la gouvernance d‘entreprise



En référence à: Münzel/Jenny „Riskmanagement für kleine und mittlere Unternehmen“

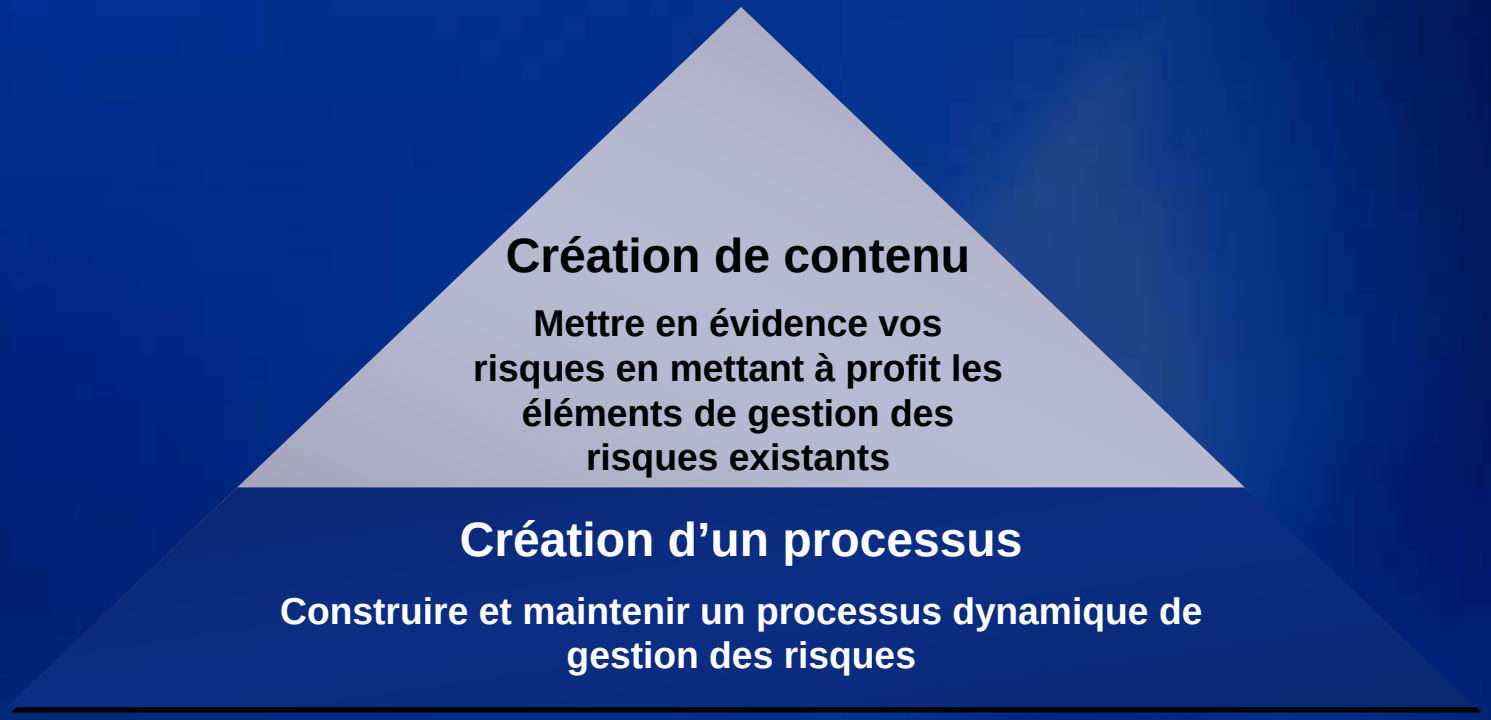
2. Outils de gestion des risques

Un exemple

Enterprise Risk Management – Gestion des risques d'entreprise

Enterprise Risk Management (ERM) est une solution basée sur une méthodologie éprouvée qui aide à définir et mettre en place une approche structurée au niveau de l'organisation pour identifier, évaluer et gérer les risques de manière efficace et à un coût supportable

Processus ou contenu



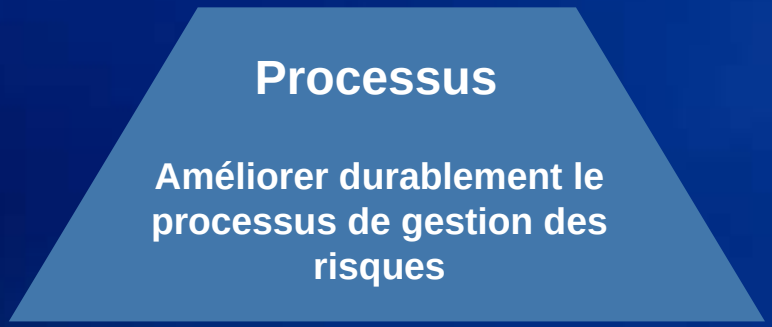
En pratique, qu'est-ce qui nous est demandé ?

ERM inclut de nombreuses activités, au travers de modèles conceptuels, pour intégrer et coordonner les activités de gestion des risques et de contrôle dans toute l'organisation

- Redéfinir et consolider des évaluations des risques existants pour obtenir une vue d'ensemble au niveau de l'organisation
- Intégrer des informations de toutes les branches qui traitent de la gestion des risques
- Présenter l'information relative à la gestion des risques de manière compréhensible et transparente

En pratique, qu'est-ce qui nous est demandé ?

ERM inclut de nombreuses activités, au travers de modèles conceptuels, pour intégrer et coordonner les activités de gestion des risques et de contrôle dans toute l'organisation



- Lier les activités de contrôles aux risques d'entreprise
- Mettre en place de nouveaux processus de gestion des risques transversaux
- Apporter une méthodologie / des outils pour faciliter la mise en place de la gestion des risques

Cadre conceptuel

- **Notre cadre conceptuel se compose de cinq éléments :**

Elément	Description
Gouvernance des risques	Mise en place d'une approche pour développer, soutenir et diffuser la stratégie de gestion des risques et les responsabilités
Evaluation des risques	Identification, évaluation et catégorisation des risques dans toute l'organisation (approche transversale)
Mesure des risques	Mesure, analyse et consolidation des risques de l'organisation
Suivi et reporting des risques	Reporting, suivi et activités de contrôle effectués pour fournir des informations sur les forces et les faiblesses de la gestion des risques
Optimisation des risques et contrôles	Utilisation des informations sur les risques et les contrôles pour améliorer la performance de l'organisation en matière de gestion des risques

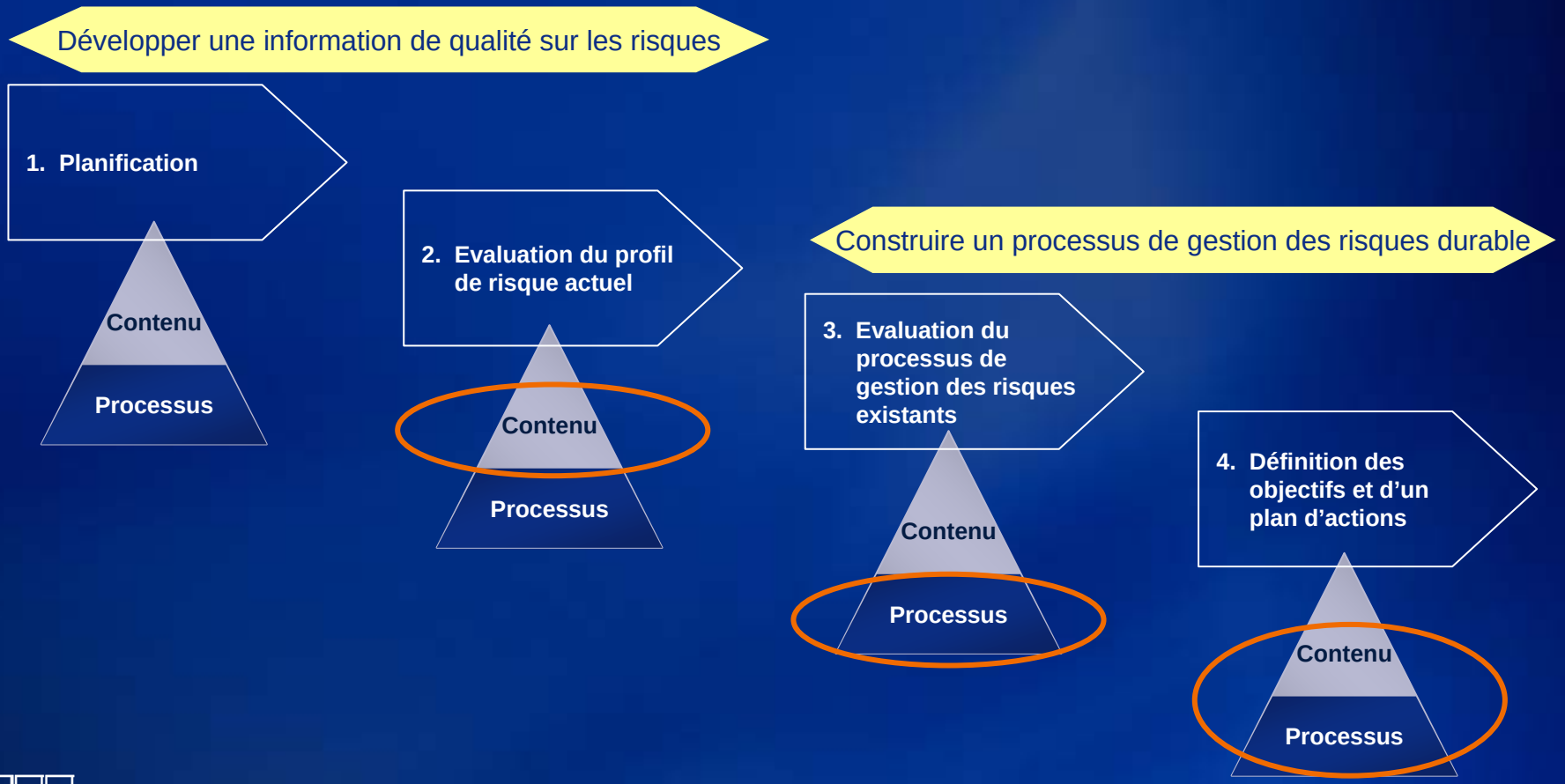
Le coeur de notre solution est la notion de maturité

- **ERM n'est pas une solution "prêt-à-porter". La clé est de déterminer le degré de maturité qui convient à l'organisation**

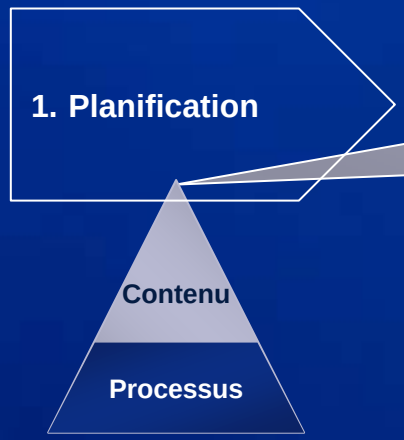
Elément du cadre conceptuel	BASIQUE *Respecter les lois et règlements*	MATURE *Un processus directionnel*	AVANCE *Un outil stratégique*
Gouvernance des risques	Principes de gestion des risques centralisés	Une structure de gestion des risques avec des responsabilités claires	La gestion des risques est intégrée dans la mesure de la performance
Evaluation des risques	Evaluation annuelle des risques avec une analyse limitée	Analyse des risques régulière et intégrée dans le reporting	Les activités de gestion et contrôle des risques sont intégrés dans les activités opérationnelles
Mesure des risques	Quantification de risques sélectionnés	Quantification des risques opérationnels; quantification anticipée de risques sélectionnés	Cumul des risques au travers de toute l'organisation
Suivi et reporting des risques	Reporting des risques destiné à fournir l'information requise	Reporting complet au Conseil d'adm. et au Comité d'audit sur les niveaux de risques existants et les risques futurs	Alignement de tous les reporting sur le risque pour donner une vision d'ensemble des risques
Optimisation des risques et contrôles	Moins de surprises grâce à la gestion des risques clés	Renforcement de la confiance des stakeholders et amélioration des stratégies de réduction des risques	La stratégie, l'évaluation de la performance et l'allocation des ressources sont ajustées aux risques

Une approche simple à comprendre

Quatre étapes



Evaluation ERM : 1ère étape

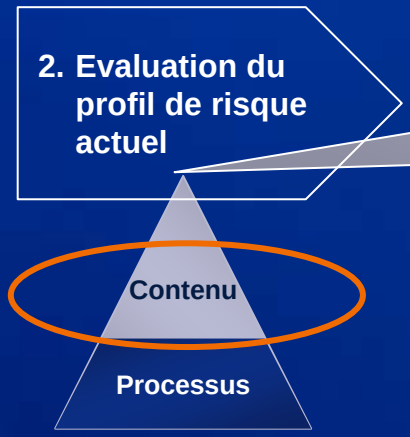


- Définir la structure du projet, le planning et la documentation
- Se mettre d'accord sur le catalogue des risques, les catégories et les critères
- Développer des fiches d'information
- Rassembler les informations et la documentation existantes

Documentation :

- Planning du projet détaillé
- Définitions des risques, des catégories, des critères de classement, etc.
- Fiches d'information sur le projet

Evaluation ERM : 2e étape

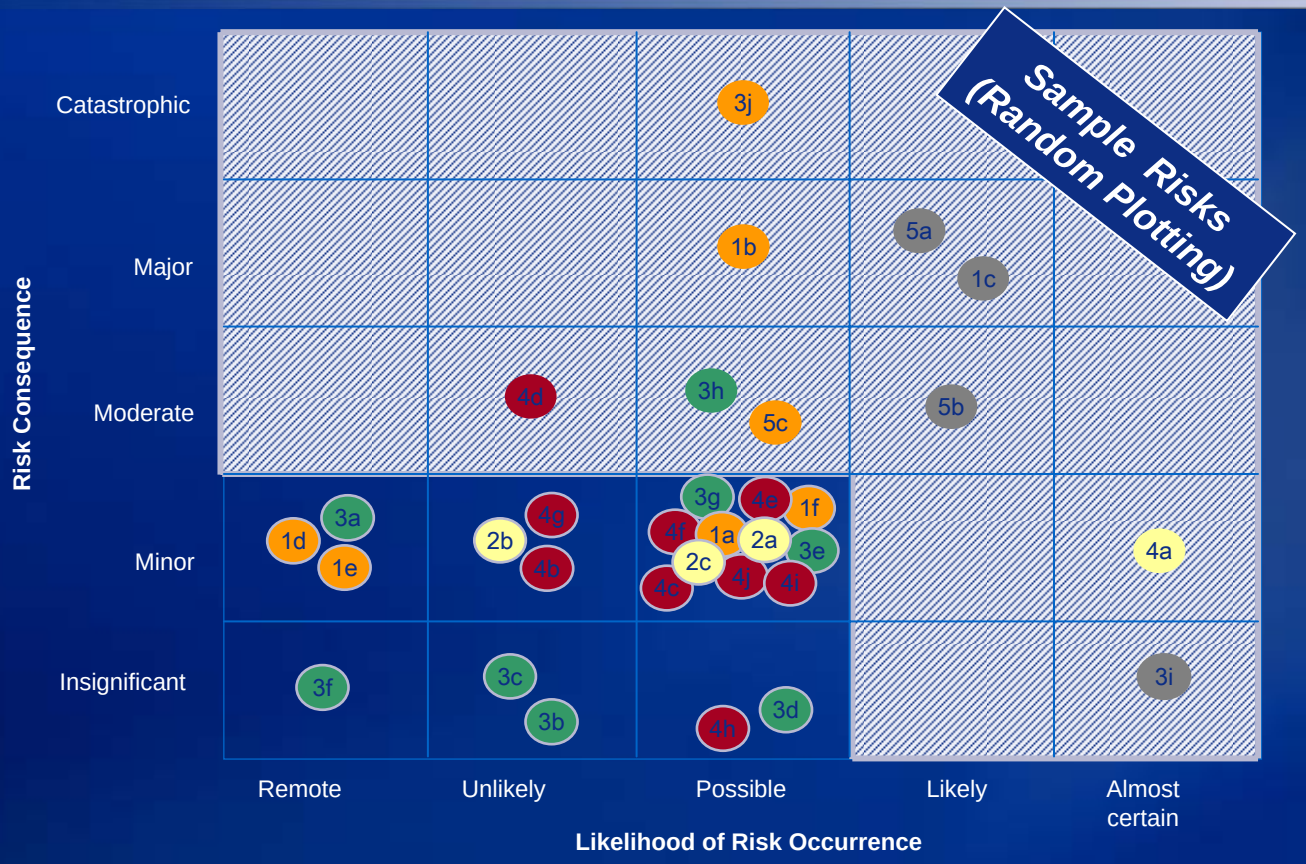


- Conduire les entretiens sur les risques
- Identifier, cumuler et analyser les risques
- Conduire des séances pour valider et classer les risques
- Conduire l'analyse de sensibilité
- Se mettre d'accord sur le profil de risque actuel

Documentation :

- Profil de risque
- Analyse de sensibilité
- Analyse des activités de gestion des risques

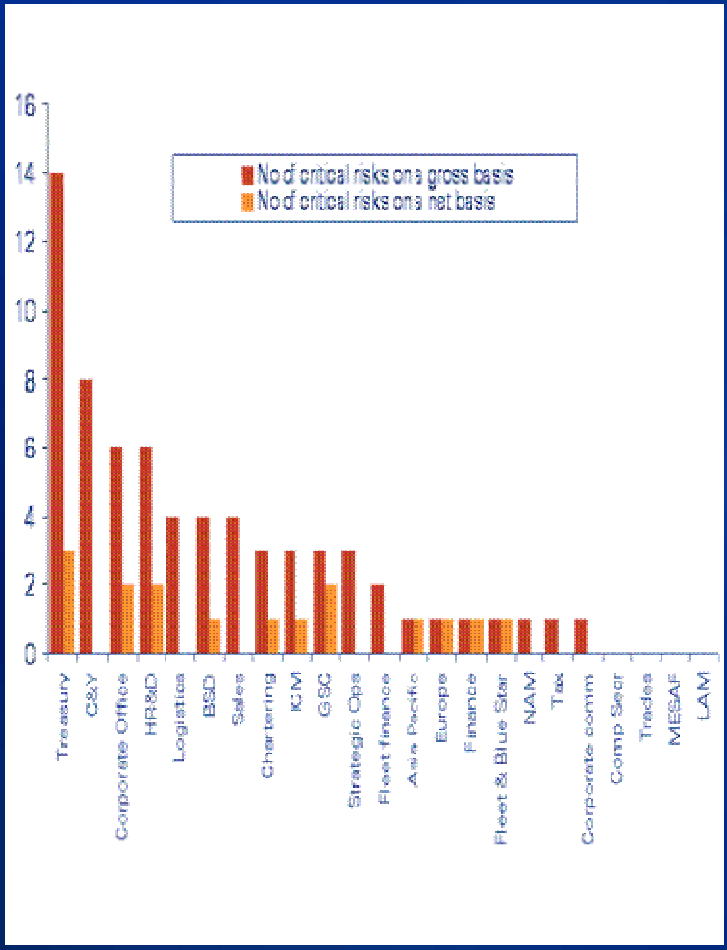
Exemple de documentation : Profil de risque



#	Top 10 Risks
1	**3j** Loss of building, together with key staff or technology infrastructure
2	**1c** Adverse changes in law and government affecting the company's business model
3	**5a** Loss of market share or revenue through competition or regulation
4	**5b** Introduction of competing products and technologies by other companies
5	**5c** Inability to attract and retain key employees
6	**1b** Failure to develop global management and information systems
7	**4d** Exposure to litigation related to the company's products/services
8	**3h** Deficient products/services provided, resulting in loss of reputation
9	**4a** Inability to react to changes in overseas legal, economic, or regulatory environment
10	**3i** Increased pricing pressure from competitors and/or customers

KPMG

Exemple de documentation : Utiliser l'information sur la gestion des risques pour planifier l'activité de contrôle interne



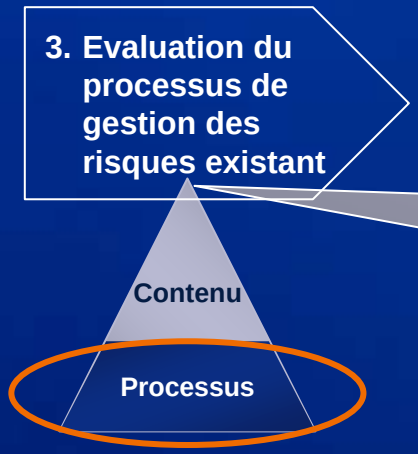
SAMPLE

Critical Risks on a gross basis in the current risk portfolio that are the best controlled (i.e. the largest difference between gross and net values)

Critical
Serious
Moderate
Minor

Risk	Source	Gross	Net	Gross risk reduced by %
Trustee / Chassis liability	Division X operations	25	10	60%
Huge shortage of tonnage	Chartering	32	18	44%
Exposure to increasing fx rates and increased exposure by not competing well against the market	Chartering	32	21	34%
High staff turnover. Low retention of competent staff.	HR&D	28	17	39%
Inability to attract competent, high quality staff.	HR&D	28	17	39%
Failure to implement XXX effectively	Europe	35	25	29%
Software vendors not able to support the system	Logistics	25	15	40%
Poor sales contract negotiations (& poor buying contract negotiations)	Sales	31	21	32%
Issue saturation across the global sales organisation	Sales	28	18	36%
CompanyX fail to meet the Time Charter limitation in the UK and Dutch Tonnage Tax Regimes.	Tax	28	18	36%

Evaluation ERM : 3e étape



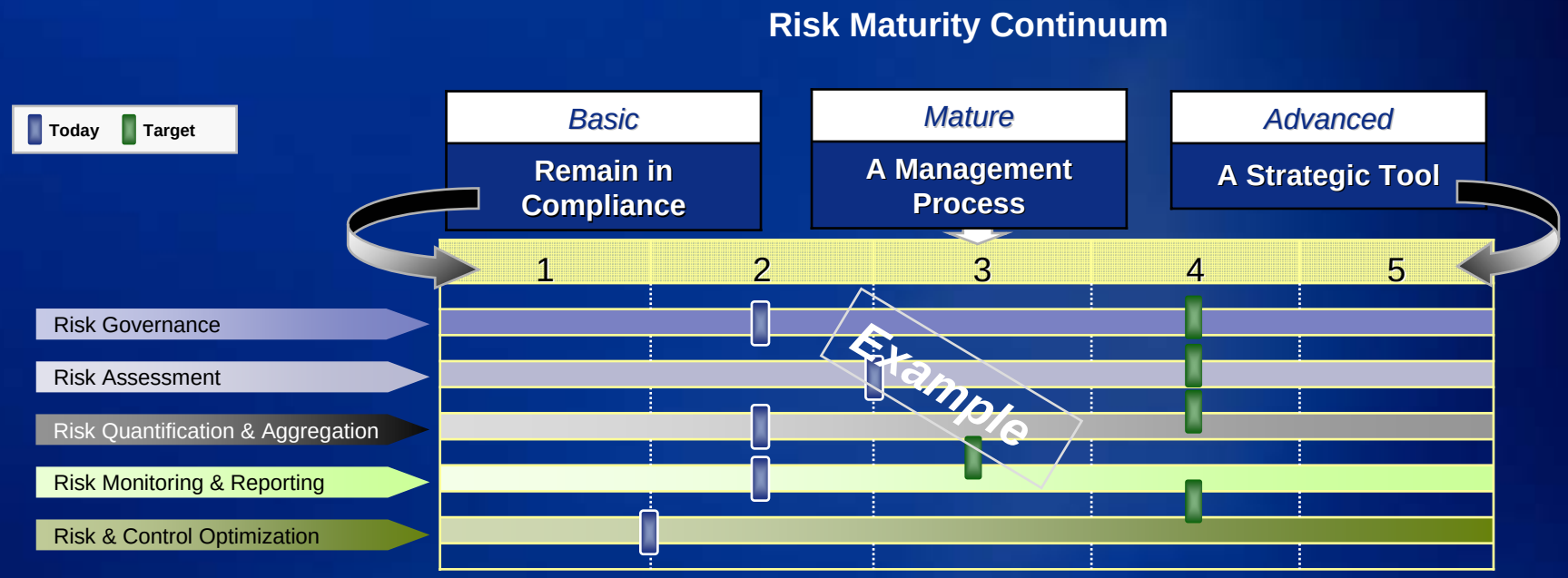
- Conduire des entretiens sur le processus de gestion des risques
- Analyser le processus et positionner l'organisation en terme de maturité
- Conduire des séances pour valider l'évaluation et le positionnement
- Se mettre d'accord sur l'évaluation

Documentation :

- Evaluation du processus de gestion des risques existants
- Observations et recommandations

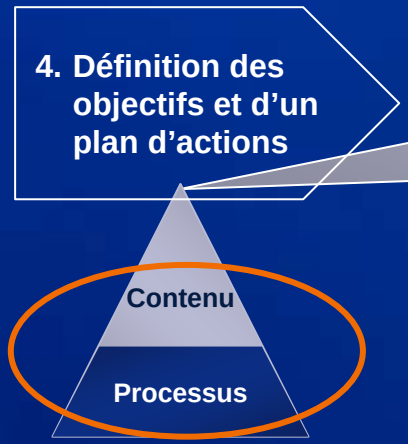
Evaluation de la maturité en matière de gestion des risques : Définir l'état actuel et souhaité

- **Une base de travail pour se poser les bonnes questions**



- **Et une approche sur mesure, incluant :**
  - **Un plan de travail pour la mise en place des améliorations en matière de gestion des risques**
  - **L'expression claire du niveau de maturité souhaité par l'organisation**

Evaluation ERM : 4e étape



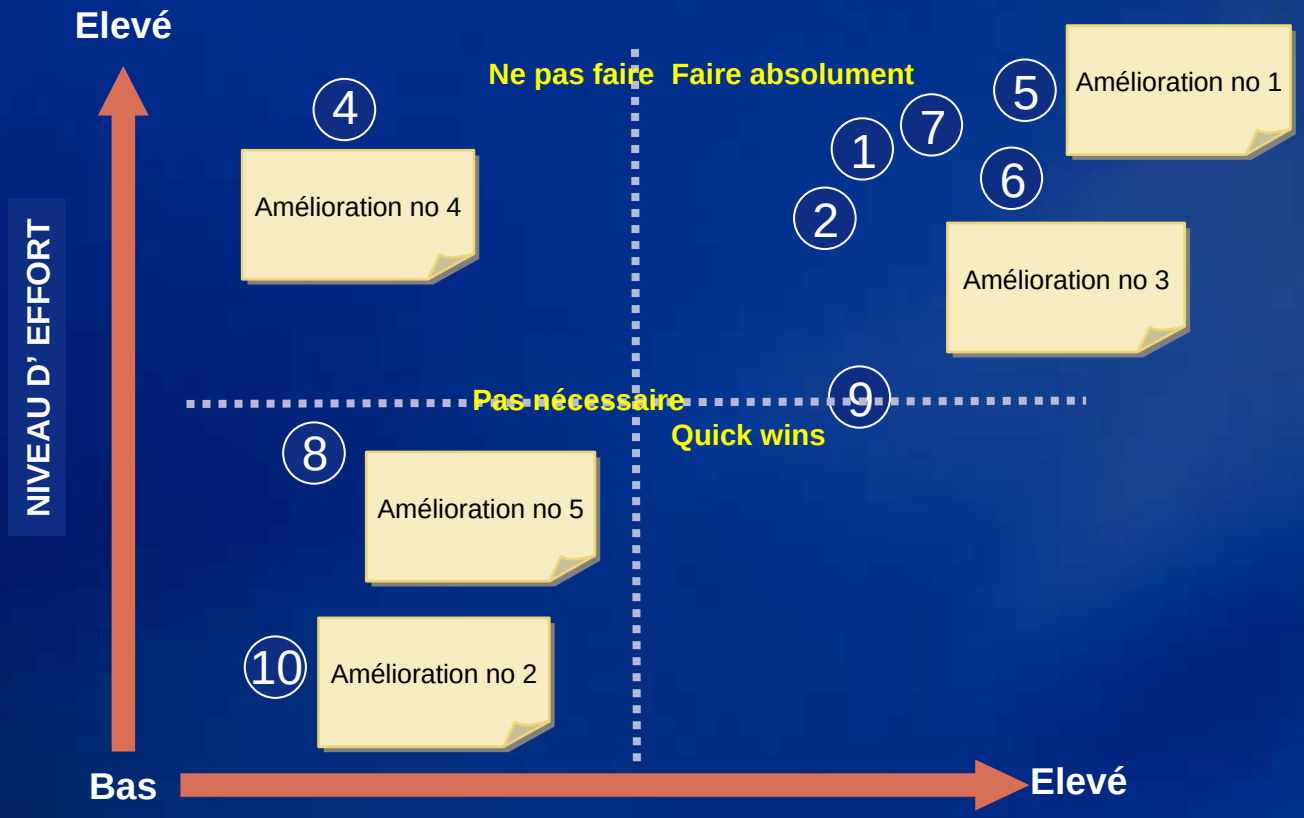
- Revoir et confirmer le profil de risques existants et le processus de gestion des risques
- Conduire des séances pour identifier le niveau souhaité (profil et processus)
- Participer à la définition des priorités et du plan d'actions
- Préparer la documentation

Documentation :

- Evaluation de l'état actuel et souhaité du profil des risques et du processus de gestion des risques
- Observations et recommandations
- Priorités et plan d'actions pour la mise en place

Le profil de risque peut être utilisé pour définir des priorités dans les propositions d'amélioration

- Priorisation en utilisant des facteurs tels que rapidité, impact sur les coûts et la qualité – et l'amélioration de l'efficacité des processus opérationnels



- Quels sont les avantages potentiels?
- Que faire en premier?
- Comment mettre en place chaque proposition?
- Quel est l'avis de la direction?
- Définir les étapes

Eléments clés pour la réussite d'un projet ERM

- Implication de la direction qui doit soutenir le projet activement
- Approche coordonnée top-down
- Définir le cadre de travail puis nommer le responsable du projet
- Passer du temps sur la formation :
  - N'a pas besoin d'être très long
  - Doit être complète au niveau de la direction et du conseil d'administration

3. Particularités des collectivités publiques en matière de gestion des risques

Particularités des collectivités publiques en matière de gestion des risques

Les collectivités publiques effectuent des tâches :

- très diverses
- dans un environnement complexe
- avec des ressources limitées

Les responsabilités en matière de gestion des risques ne sont souvent pas clairement attribuées

Le législatif réagit mais anticipe peu

La gestion des risques et le contrôle interne comme éléments intégrés de la gouvernance d'une collectivité publique

Environnement

Corporate Governance

Electorat

Conseil d'Etat

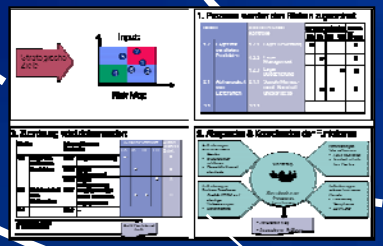
Assurance

Système de contrôle interne

Révision interne

Gestion de la qualité

Gestion des risques



Grand-conseil?
Commission?

En référence à: Münzel/Jenny „Riskmanagement für kleine und mittlere Unternehmen"

Particularités des collectivités publiques en matière de gestion des risques

Les réponses / nos expériences :

- **Des évaluations de risques (profil de risques) commencent à être réalisées au niveau des départements ou des directions**
- **Gestion des risques fractionnée (au niveau des services) car activités très diverses**
- **Pas de reporting global des risques**
- **Pas de gouvernance des risques**

Particularités des collectivités publiques en matière de gestion des risques

Les réponses / nos expériences (suite) :

- La révision interne (contrôle interne) effectue une analyse des risques (financiers) lors de ses vérifications
- La plupart des collectivités publiques considèrent que la gestion des risques est du ressort de la révision interne – celle-ci a-t-elle les compétences et les ressources disponibles ?
- Elle utilise cette analyse pour la planification de son travail (plan pluri-annuel)
- Pas de « consolidation » des risques, ni souvent de quantification des impacts
- La révision interne teste régulièrement le contrôle interne – donc vérifie le bon fonctionnement de certains contrôles internes destinés à réduire certains risques

- Recours fréquent à la délégation de tâches à des entités semi-autonomes qui gèrent leurs risques elles-mêmes

Le coeur de notre solution est la notion de maturité

- **ERM n'est pas une solution "prêt-à-porter". La clé est de déterminer le degré de maturité qui convient à l'organisation**

Elément du cadre conceptuel	BASIQUE *Respecter les lois et règlements*	MATURE *Un processus directionnel*	AVANCE *Un outil stratégique*
Gouvernance des risques	Principes de gestion des risques centralisés	Une structure de gestion des risques avec des responsabilités claires	La gestion des risques est intégrée dans la mesure de la performance
Evaluation des risques	Evaluation annuelle des risques avec une analyse limitée	Analyse des risques régulière et intégrée dans le reporting	Les activités de gestion et contrôle des risques sont intégrés dans les activités opérationnelles
Mesure des risques	Quantification de risques sélectionnés	Quantification des risques opérationnels; quantification anticipée de risques sélectionnés	Cumul des risques au travers de toute l'organisation
Suivi et reporting des risques	Reporting des risques destiné à fournir l'information requise	Reporting complet au Conseil d'adm. et au Comité d'audit sur les niveaux de risques existants et les risques futurs	Alignement de tous les reporting sur le risque pour donner une vision d'ensemble des risques
Optimisation des risques et contrôles	Moins de surprises grâce à la gestion des risques clés	Renforcement de la confiance des stakeholders et amélioration des stratégies de réduction des risques	La stratégie, l'évaluation de la performance et l'allocation des ressources sont ajustées aux risques

KPMG

4. La gestion des risques informatiques

La gestion des risques informatiques

- Les processus fonctionnels sont fortement dépendants des systèmes d'information
- Tendance au regroupement des services informatiques
- La plupart des administrations cherchent à faciliter l'accès aux informations via internet (guichet informatique)
- Certaines informations sont confidentielles (loi sur la protection des données)

La gestion des risques informatiques

Principaux risques informatiques :

- **Organisation et efficience du département informatique en charge de supporter les systèmes en termes de ressources et de compétences et notamment si ce service est partagé entre plusieurs entités (ville, canton, école, hôpitaux…)**
- **Adéquation des systèmes en place vis-à-vis des besoins fonctionnels des utilisateurs (environnement complexe, interfaces manuelles…)**
- **Support aux utilisateurs et gestion des problèmes non efficient car soit délocalisé soit partagé**

La gestion des risques informatiques

Principaux risques informatiques (suite) :

- **Contrôles informatiques en terme de sécurité, de continuité et de monitoring des systèmes (séparation des tâches, accès…)**
- **Manque de communication (départs ou changement de fonction)**
- **Priorisation, gestion des projets internes et des changements peu claire**

La gestion des risques informatiques

Domaines clés

- Gouvernance de l'IT
- Sécurité des systèmes et des informations
- Continuité des systèmes et plan de secours
- Gestion des changements et des développements

Assurance que les données sont intègres, fiables et confidentielles

Assurance que les contrôles en place sont en adéquation avec les meilleures pratiques, standards et législation en vigueur

La gestion des risques informatiques

Outils de gestion des risques

- Méthodologie de gestion des risques opérationnels (ERM)
- Audit informatique (interne ou externe)
- Standards ISO 1799/27001 pour les aspects sécurité
- CoBit
- NAS 402 pour les services outsourcés

Avoir une bonne connaissance des risques et des enjeux pour adopter des contrôles efficients

5. Autres apports de la gestion des risques

Un exemple

Autres apports de la gestion des risques

GESORBE – gestion intégrée de la plaine de l'Orbe

- **Groupe de travail multidisciplinaire**
- **Sélection entre plusieurs variantes possibles**
- **Calcul des impacts potentiels des débordements de cours d'eau en termes financiers**
- **Evaluation des scénarios en terme de rapport réduction du risque / coût des travaux**

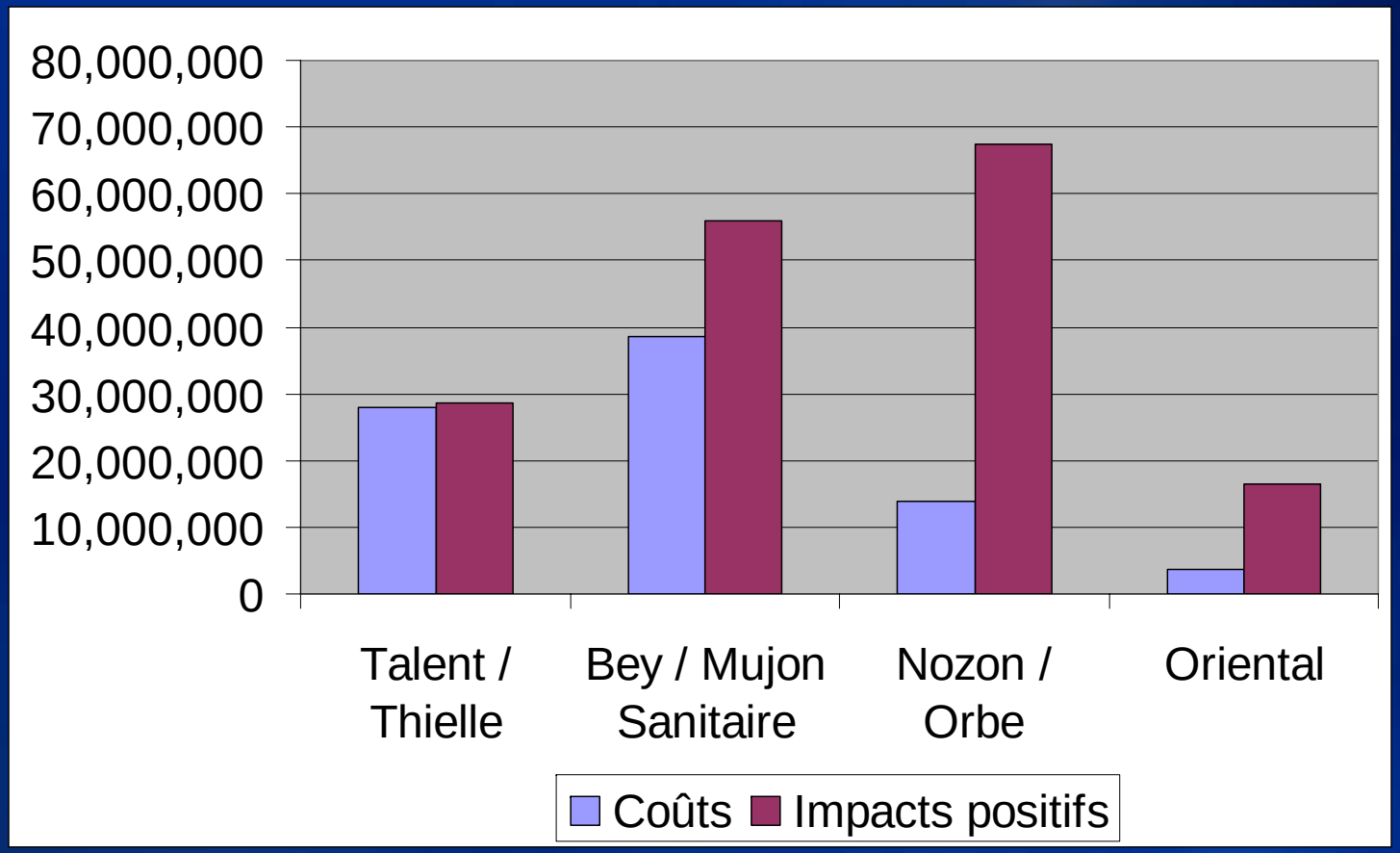
Autres apports de la gestion des risques

GESORBE – méthodologie

- **Estimation des dégâts potentiels :**
  - Méthodologie OFEV
  - Surfaces utilisées * valeur des biens
  - Avant et après mesures proposées
- **Estimation du coût des travaux :**
  - Calculés par les différents groupes d'études
- **Calcul du ratio d'efficacité :**
  - Si réductions des dégâts potentiels > coût des travaux => efficacité économique

Autres apports de la gestion des risques

GESORBE – Illustration des résultats



Discussion

Contacts

Alain Guillaume
Senior manager

KPMG Fides Peat
Rue du Seyon 1
2000 Neuchâtel

Tél. +41 32 727 61 38
Mobile +41 79 202 21 64
Fax +41 32 727 61 58
aguillaume@kpmg.com

Armin Haymoz
Sous-directeur

KPMG Fides Management AG
Hofgut
3073 Guemligen-Berne

Tél. +41 31 384 76 84
Mobile +41 79 416 29 40
Fax +41 31 384 76 17
ahaymoz@kpmg.com