ISO 31000

La futur norme ISO en gestion des risques ?

Alex Dali, ARM, EFARM

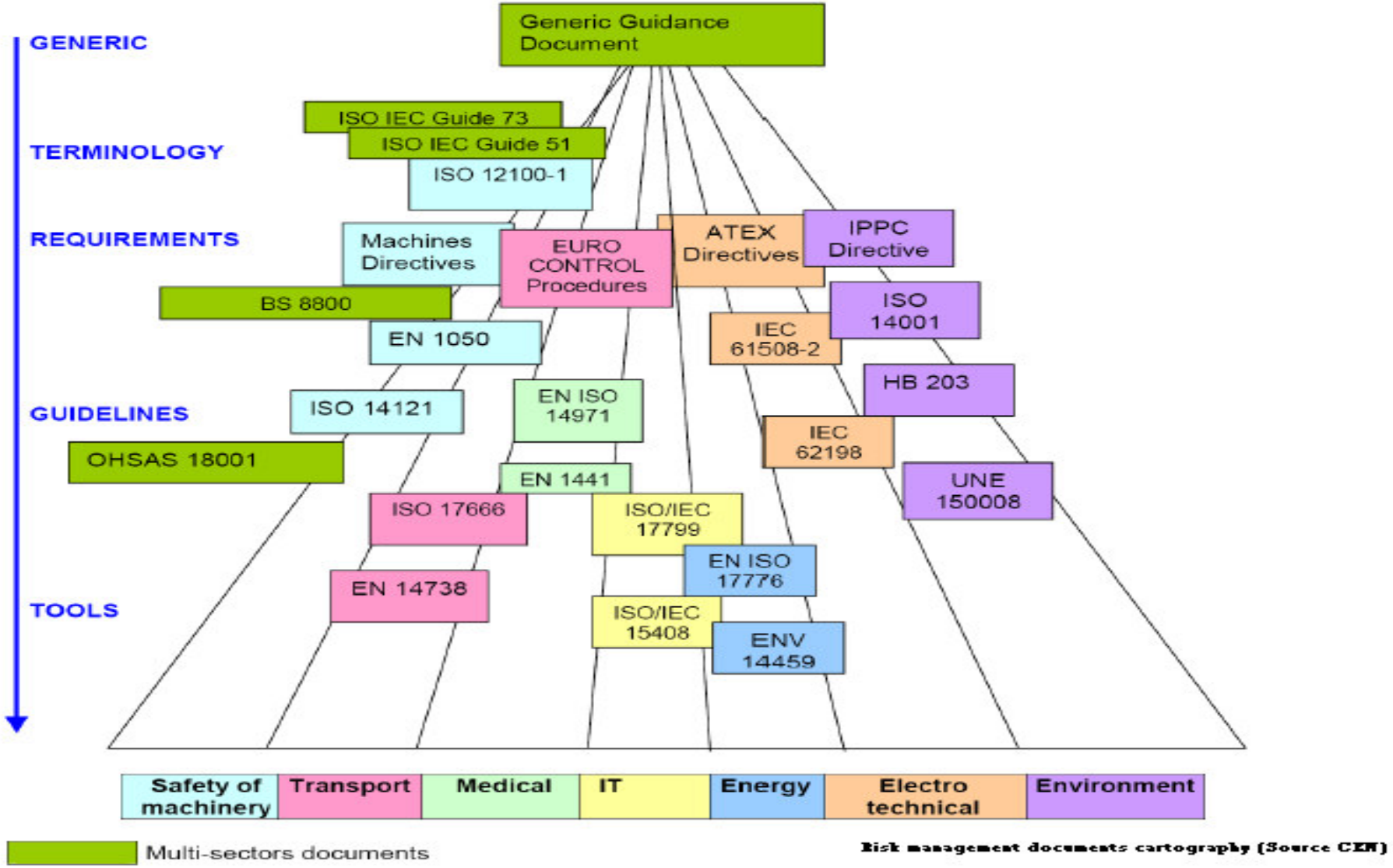
Directeur associé - ATLASCOPE

Email : dali@atlascope.com

Contenu de la présentation

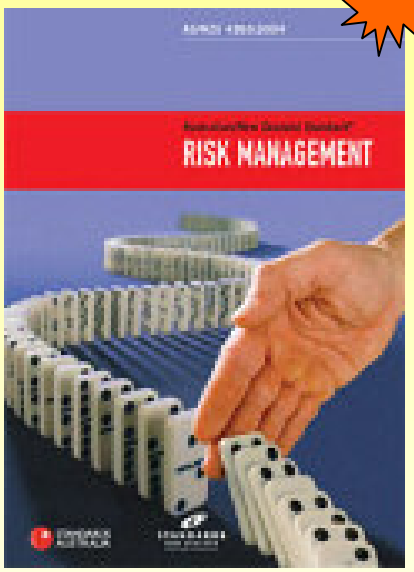
1. Historique de sa conception
2. Apports / bénéfices
3. Objectifs – Utilisateurs - Vocabulaire
4. Méthodologie
   - Principes
   - Cadre organisationel
   - Processus
5. Impact de la norme
6. Recueil des avis et opinions

Petit historique…

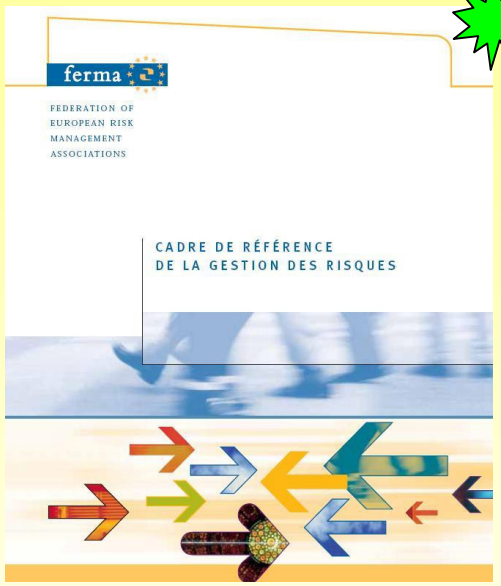


Risk management documents cartography (Source CEN)

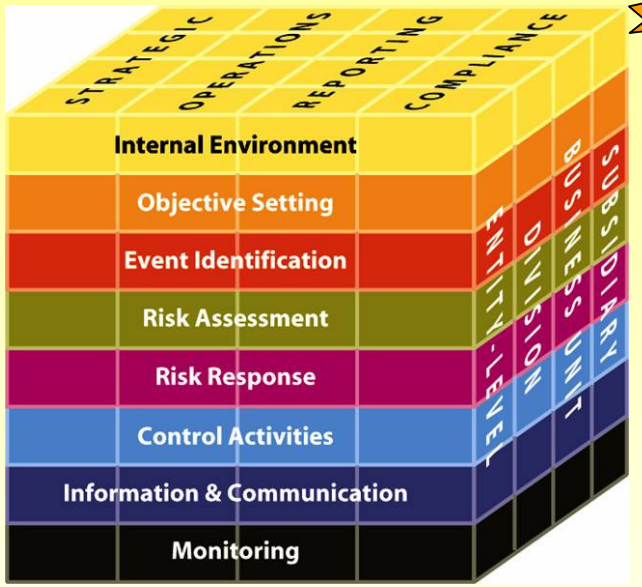
Trois "standards" importants...



AS/NZS4360
95/99/04
Australie



FERMA:2004
Europe



COSO 2 (ERM) : 2004
USA

JIS Q 2001
Japan

CAN/CSA-Q850-1997
Canada

ONR 49000:2008
Autriche
(Allemagne/Suisse)

BS 6079-3
BSI PAS 56:2003
AIRMIC, ALARM, IRM:2002
Royaume-Uni.

Historique de la norme ISO 31000

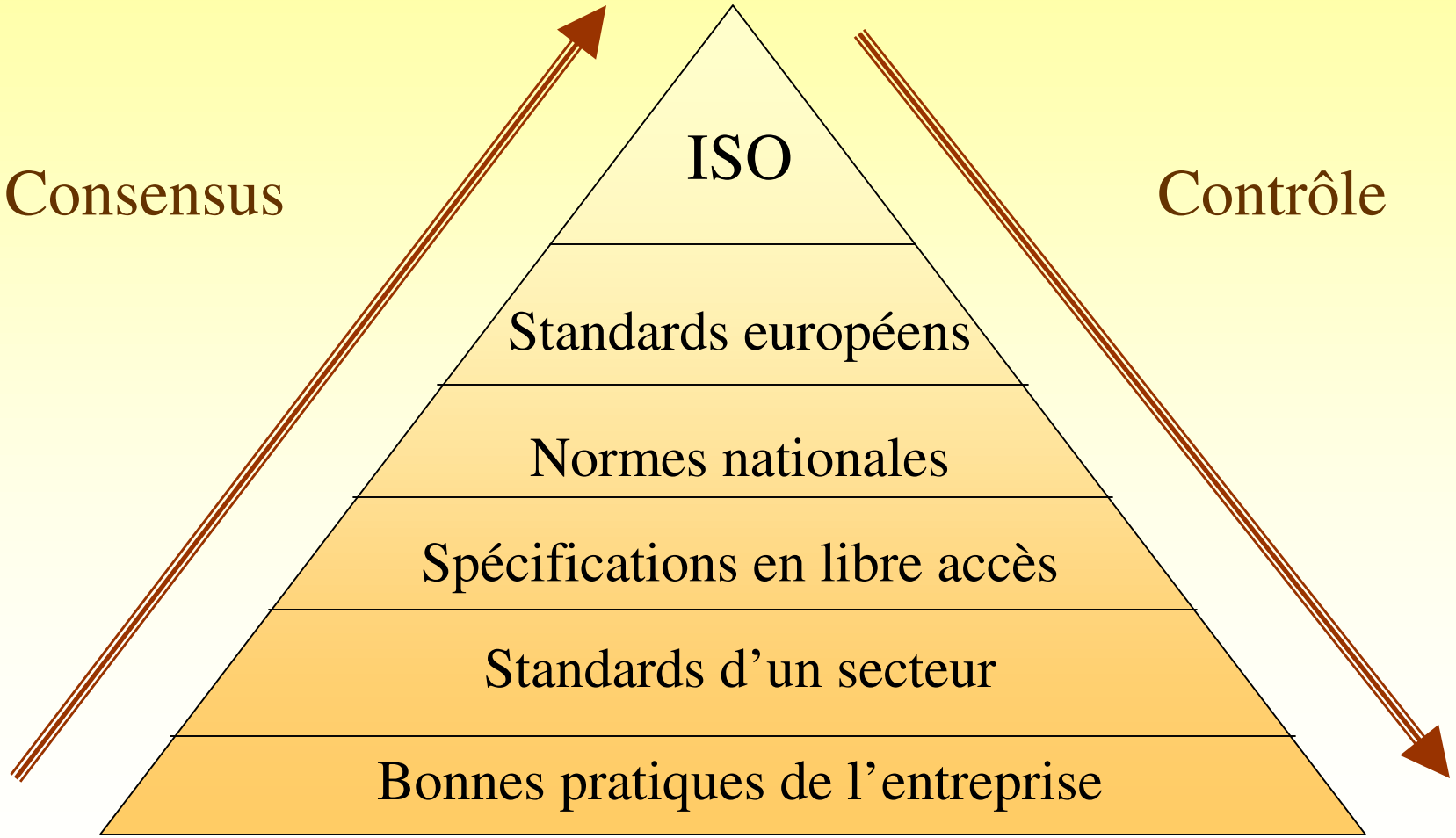
- Juin 2004 : Demande de reprise « fast-tract » de l'AS/NZS4360 en ISO – **refusé**
- Juin 2005 : Lancement de la procédure ISO
- Sept. 2005 : ISO = Guideline ≠ Certification
- Fév. 2006, Sept.2006, Mai 2007, Déc. 2007
- Avril 2008 : Rédaction du DIS et enquête
- Déc. 2008 : Final draft et vote comité
- Début 2009 : Vote des membres
- « Juin 2009 » : Publication

Représentants ISO et experts

Apports et bénefices

1. Standard = **consensus** (≠compromis)
2. Standards ≠ réglementation ➔ **adhésion**
3. Apports mutuels ≠ un seul point de vue
4. Application multi-domaines et approche **intégrée**
5. Niveau d'abstraction élevé ➔ **lignes directrices**
6. Mise à jour régulière
7. Faire reconnaître ses pratiques

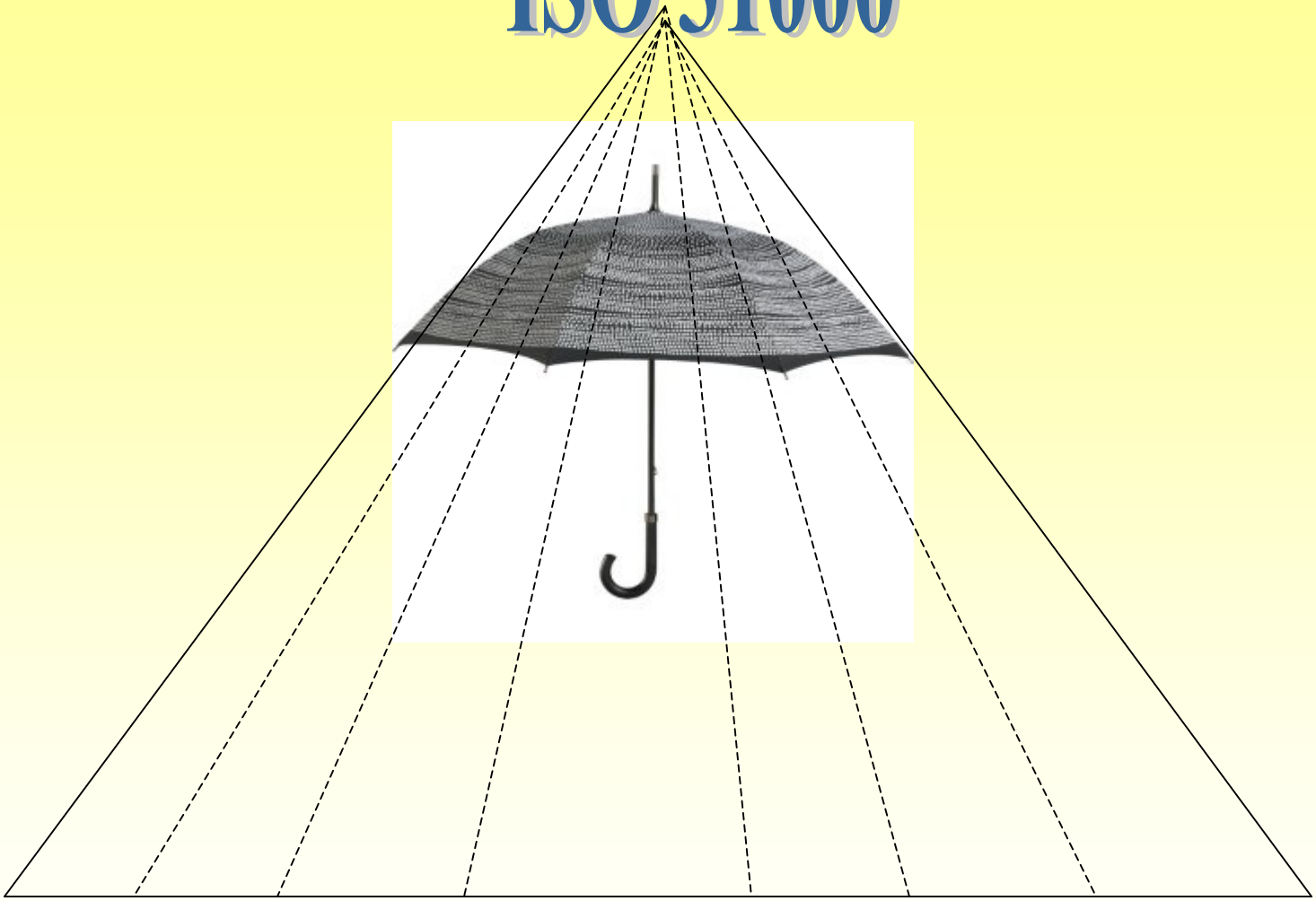
Apports et bénefices



Objectifs de l'ISO 31000

- **Principes** et lignes directrices de mise en œuvre pour le management des risques
- Organisations de **tout** secteur, de toute taille
- **Tout** type de risque
- **Générique** → harmoniser les processus
- Outil efficace pour la **formation**
- **Profession** renforcée

ISO 31000



Qualité OH&S Finance Appro Sécurité de l'information Sûreté des équipements

Environnement Sécurité alimentaire

Utilisateurs

- ✓ Manager : personnes définissant les objectifs et approches
- ✓ Opérationnels : personnes chargées de la gestion des risques comme outil d'aide à la décision
- ✓ Rédacteurs : Personnes définissant les pratiques
- ✓ Auditeurs : Personnes chargées d'évaluer les pratiques

Vocabulaire

Ingénieur	➔ risque = danger
Modéliste	➔ risque = événement
Manager objectifs	➔ risque = incertitude par rapport aux
Santé négatif)	➔ risque = menace (fondamentalement
Finance	➔ risque = rendement

Secteur public ➔ risque = interruption de service ou perte d'emploi

- *Les organismes sont confrontés à divers* ***risques***

- *Les organismes sont confrontés à diverses* ***combinaisons de probabilités d'évènements et de leurs conséquences !!!***

- *Les organismes sont confrontés à divers* ***effets d'incertitude sur l'atteinte de leur objectif***

Vocabulaire

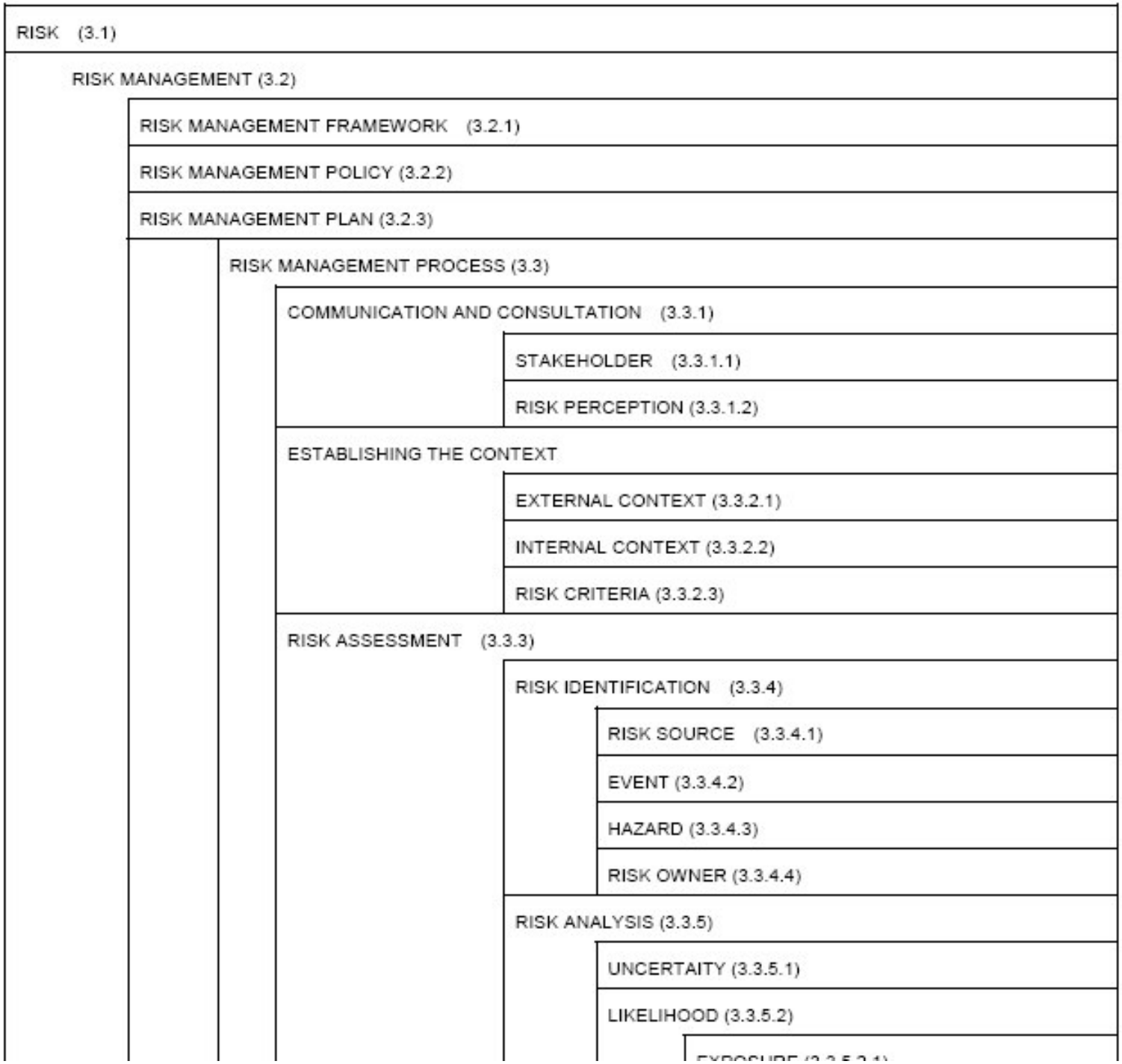
Vocabulaire ISO/IEC Guide 73 **non inséré**

- Beaucoup de termes de la version actuelle contiennent des techniques ➔ à supprimer / à adapter
- Terminologie est plus large que celle utile à l'ISO 31000
- Concepts, idées à revoir dans une approche générique

➔ Committee draft (CD2) : juin 2008

➔ Draft International Standard (DIS) : 2009

➔ **Sortira en même temps que la publication de l'ISO 31000**



ISO IEC Guide 73

Stade CD2

Juin 2008

Risque = Incertitude sur les objectifs

Impact négatif =		Impact positif =
▪ Dommages aux biens	⟺	▪ Construction nouvelle,
▪ Pertes de revenu,	⟺	▪ Profit, bénéfices,
▪ Blessures, Décès	⟺	▪ Santé, emploi
▪ Engagement de RC	⟺	▪ Opportunités

Menace ⟺ Opportunités

Structure : 3 éléments

- **Principes** : Pourquoi fait-ton du management des risques ?
- **Cadre opérationnel** : Comment intégrer le management des risques dans la stratégie de l'organisation ?
- **Processus de management** : Comment intégrer, au niveau opérationnel, le management des risques de la stratégie de l'organisation?

Principes du management des risques

- Crée de la valeur….*encourage à la création de valeur*
- Est intégré au processus organisationnels *(opérationnels)*
- Est intégré aux processus de prise de décision
- Doit être taillé sur mesure….*en fonction des ressources disponibles…et du contexte*
- Intégre les facteur humains et culturels
- Est transparent et participatif
- etc.

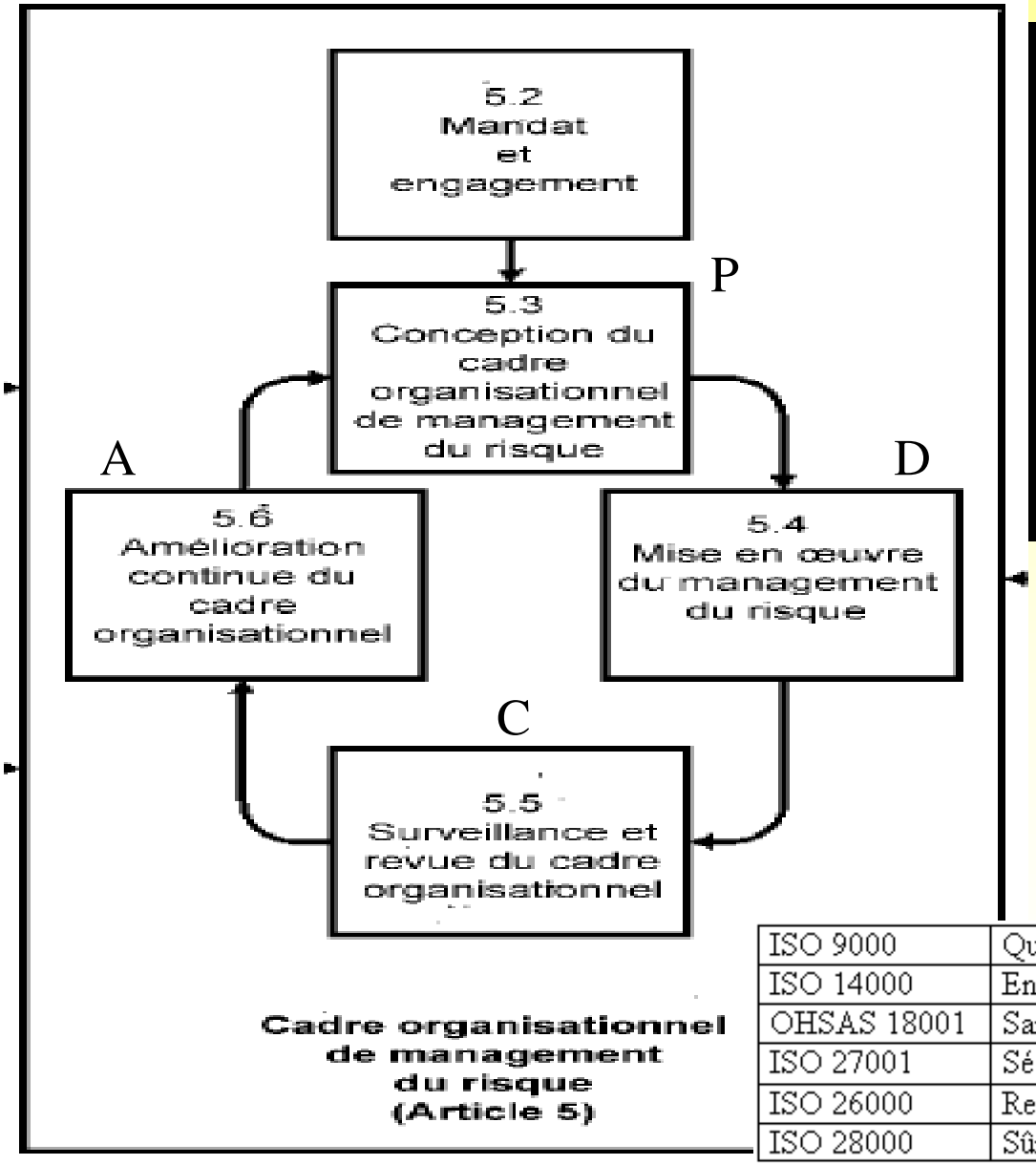
(Extrait)

Cadre organisationnel

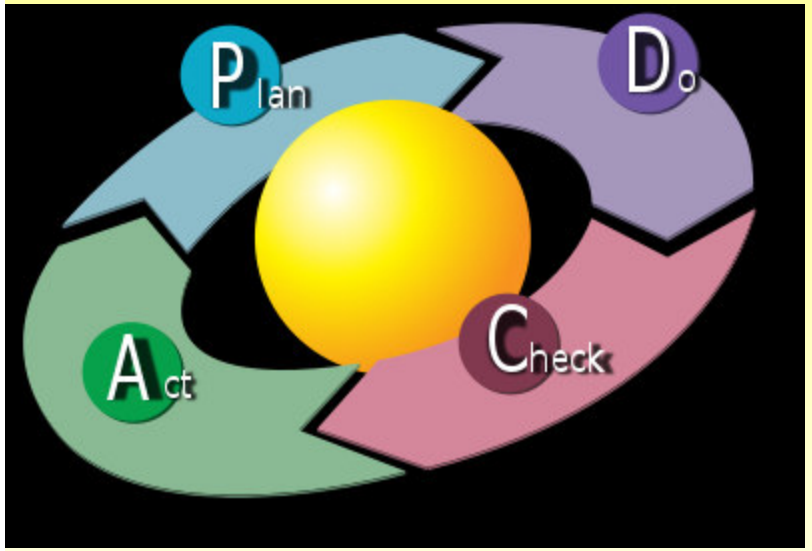
Objectifs

- ✓ Intégrer le management du risque au sein de son propre système global de management
- ✓ ≠ système de management ➔ = aide à la mise en place et à son évolution
- ✓ Si existant, *révision sérieuse*….
- ✓ Composants à adapter par rapport à ses besoins spécifiques

Cadre organisationnel



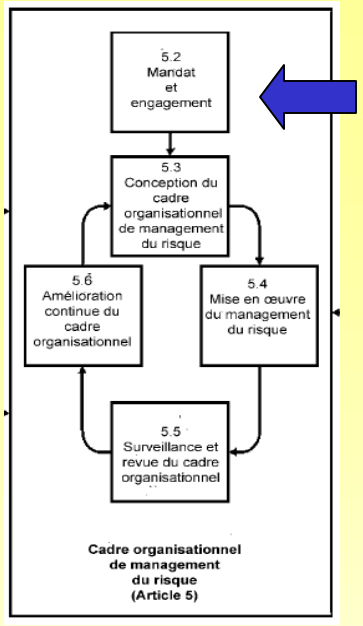
Cadre organisationnel de management du risque (Article 5)



ISO 9000	Qualité	2008	PDCA
ISO 14000	Environnement	2004	PDCA
OHSAS 18001	Santé & sécurité	1999	PDCA
ISO 27001	Sécurité de l'information	En cours	PDCA
ISO 26000	Responsabilité sociétale des entreprises	En cours	
ISO 28000	Sûreté de la chaîne d'approvisionnement	2007	PDCA

Cadre organisationnel

Mandat et engagement

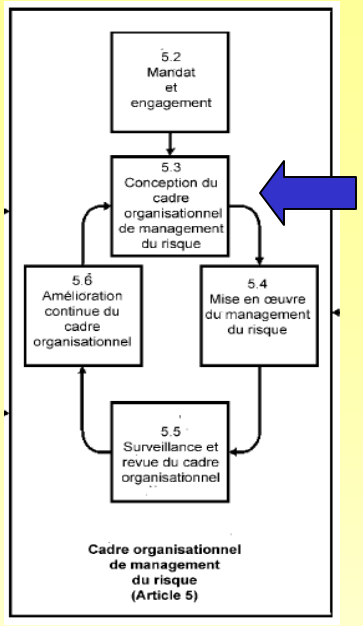


- Implication de la Direction
- Définition des indicateurs de risques
- Affectation des responsabilités
- Décision sur l'allocation des ressources
- Communication

Cadre organisationnel

Conception

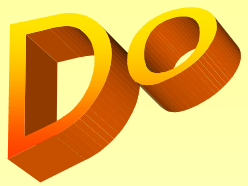
Plan

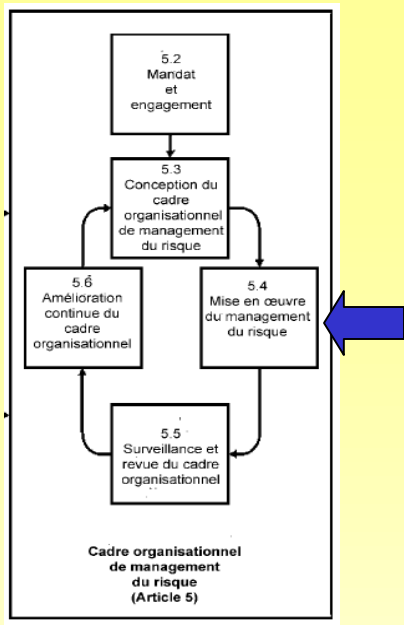


- Compréhension de l'organisme et de son **contexte**
- Politique de management des risques
- Intégration aux processus organisationnels
- Responsabilité… *en charge de et non au sens juridique*
- Ressources

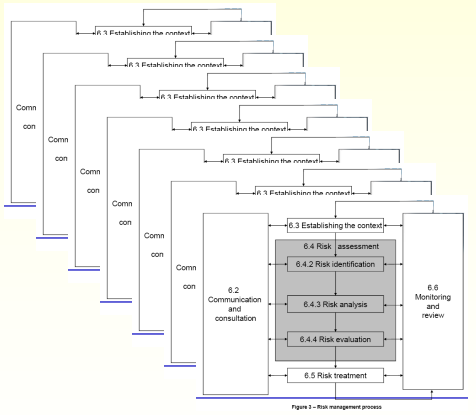
Cadre organisationnel

Mise en oeuvre





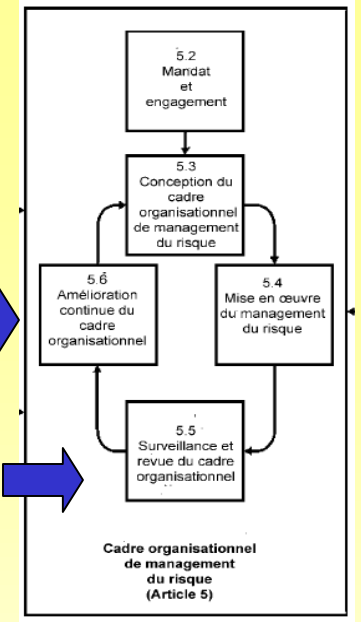
- Définir un calendrier et une politique
- Appliquer la politique et le processus MR au processus organisationnels (voir plus loin)
- Respect des obligations légales
- Reporting



Cadre organisationnel

Surveillance et revue

Check



- Etablir des KRI et mesurer les écarts au plan
- Vérifier l'adéquation du contexte externe et interne et Reporting

Amélioration continue

Act

Processus

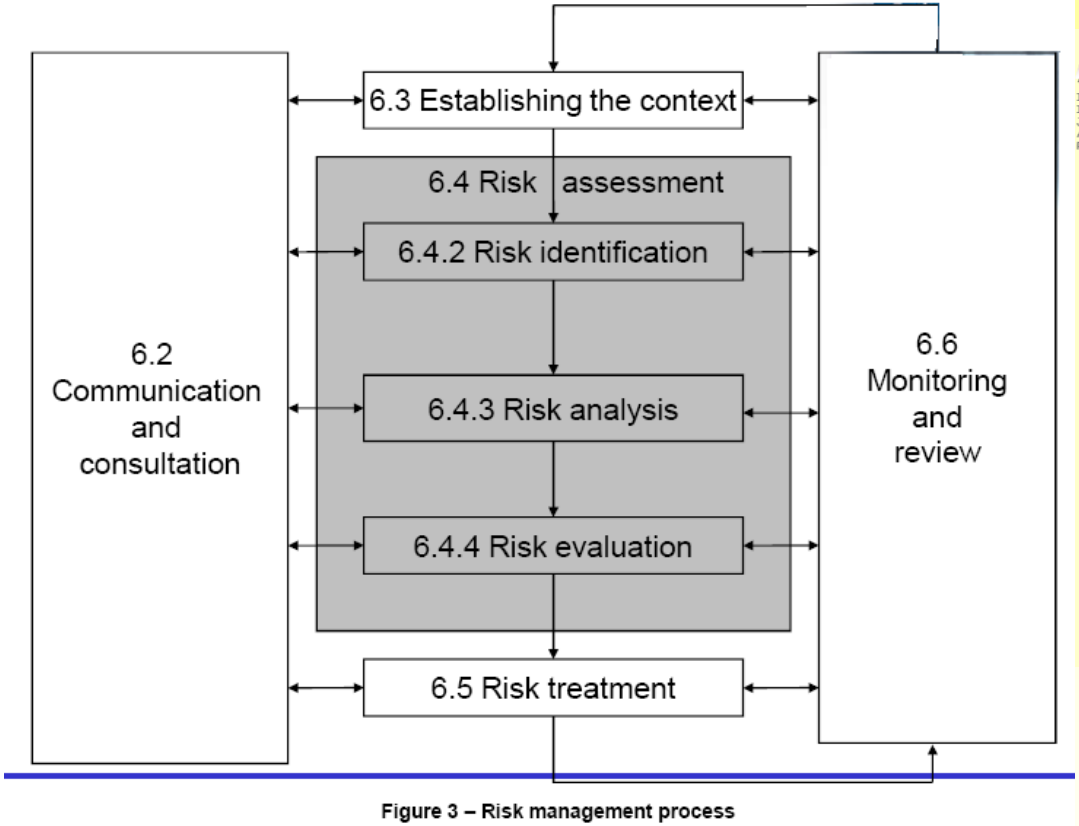
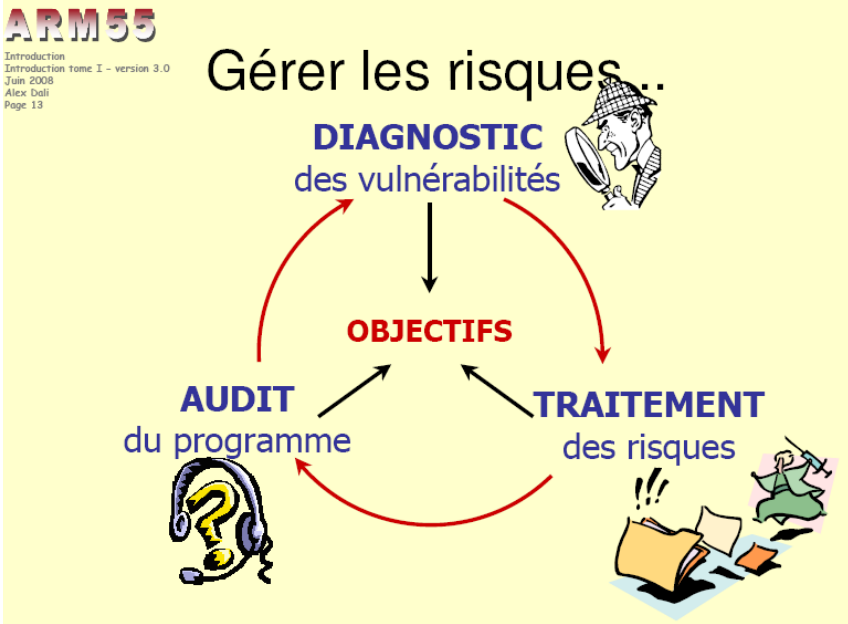
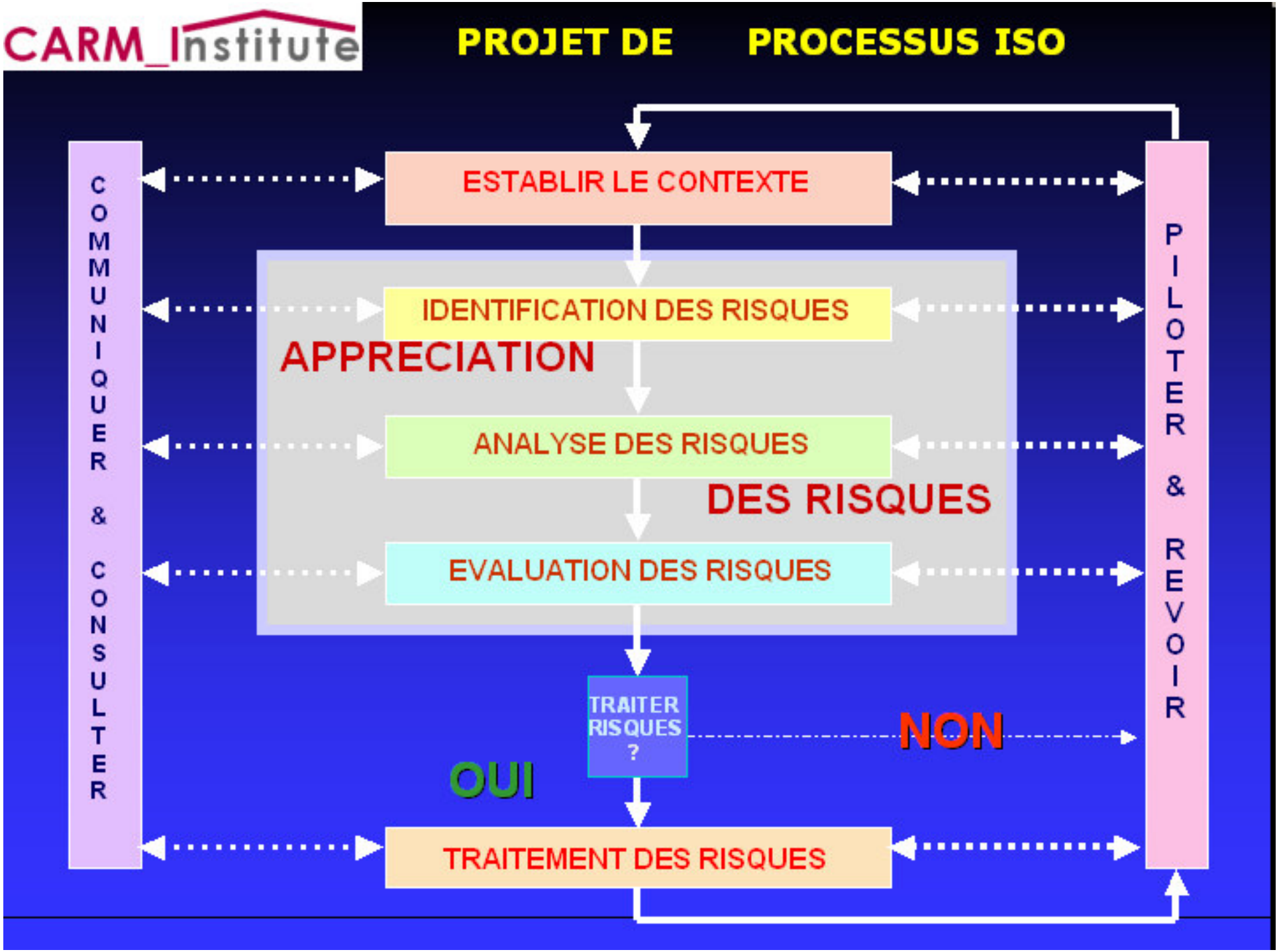


Figure 3 – Risk management process

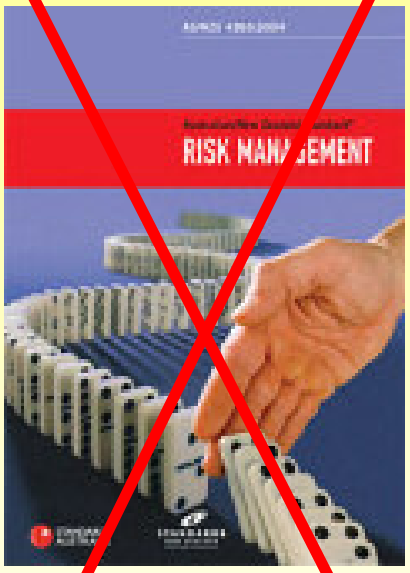


- **Etablir le contexte**
- **Communication et consultation**


CARM_Institute
PROJET DE PROCESSUS ISO
COMMUNIQUER & CONSULTER
ESTABLIR LE CONTEXTE
IDENTIFICATION DES RISQUES
APPRECIATION
ANALYSE DES RISQUES
DES RISQUES
EVALUATION DES RISQUES
TRAITER RISQUES ?
NON
OUI
TRAITEMENT DES RISQUES
PILOTER & REVOIR

Impact de la norme ISO 31000

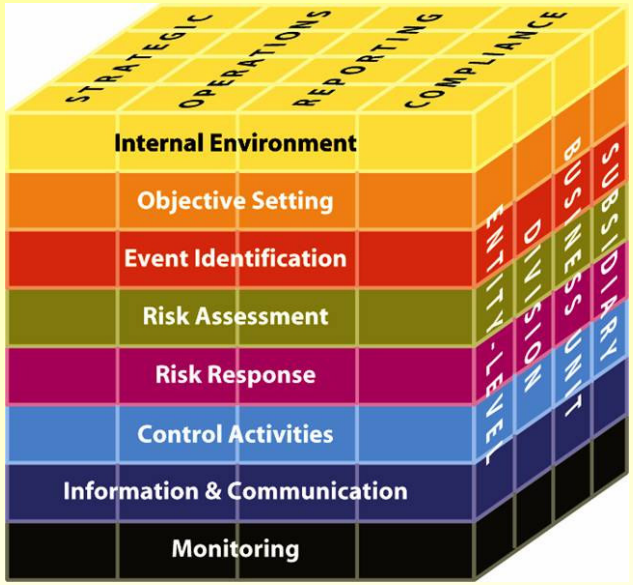
Certification



AS/NZS4360
95/99/04
Australie

FERMA:2004
Europe

Conservé



COSO ERM
USA

JIS Q 2001

Japan ?

~~CAN/CSA-Q850-1997~~

Canada

Intégré et certification

ONR 49000:2008

Autriche

(Allemagne/Suisse)?

Certification

BSI 31100

~~AIRMIC, ALARM, IRM:2002~~

Royaume-Uni.

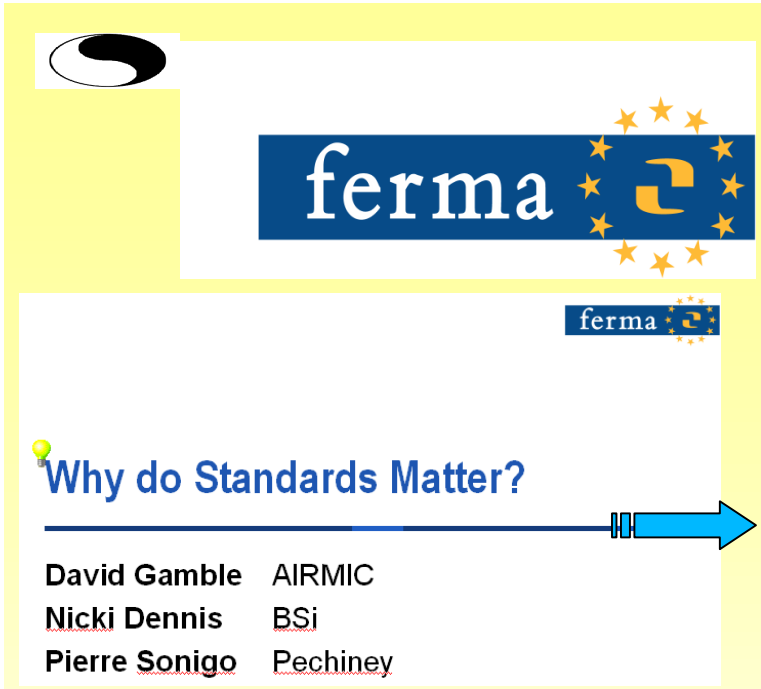
Certification des standards

Avantages

- Validation du standard par une certification et un audit externe accrédité
- Validation des décisions de management
- Lien rapide et cohérent avec une législation formalisée
- Confiance accrue des partenaires externes et clients à une norme internationale ISO

Inconvénients

- Rarement objectif et souvent disparate entre pays
- Contrainte supplémentaire sur les ressources et sans contre-partie garantie
- Les performances des entreprises certifiées pas supérieures
- Sentiment de fausse sécurité
- Incorporé dans la législation
- En cas de procès légal, négligence aggravée en cas de non-adoption
- Focalisation sur l'audit et non le processus !



FERMA – 4 octobre 2005

The Risk Management Standard

- High Level ✓
- Not prescriptive ✓
- Used the ISO/IEC73 guide vocabulary ✓
- Short ✓
- Provided Free X

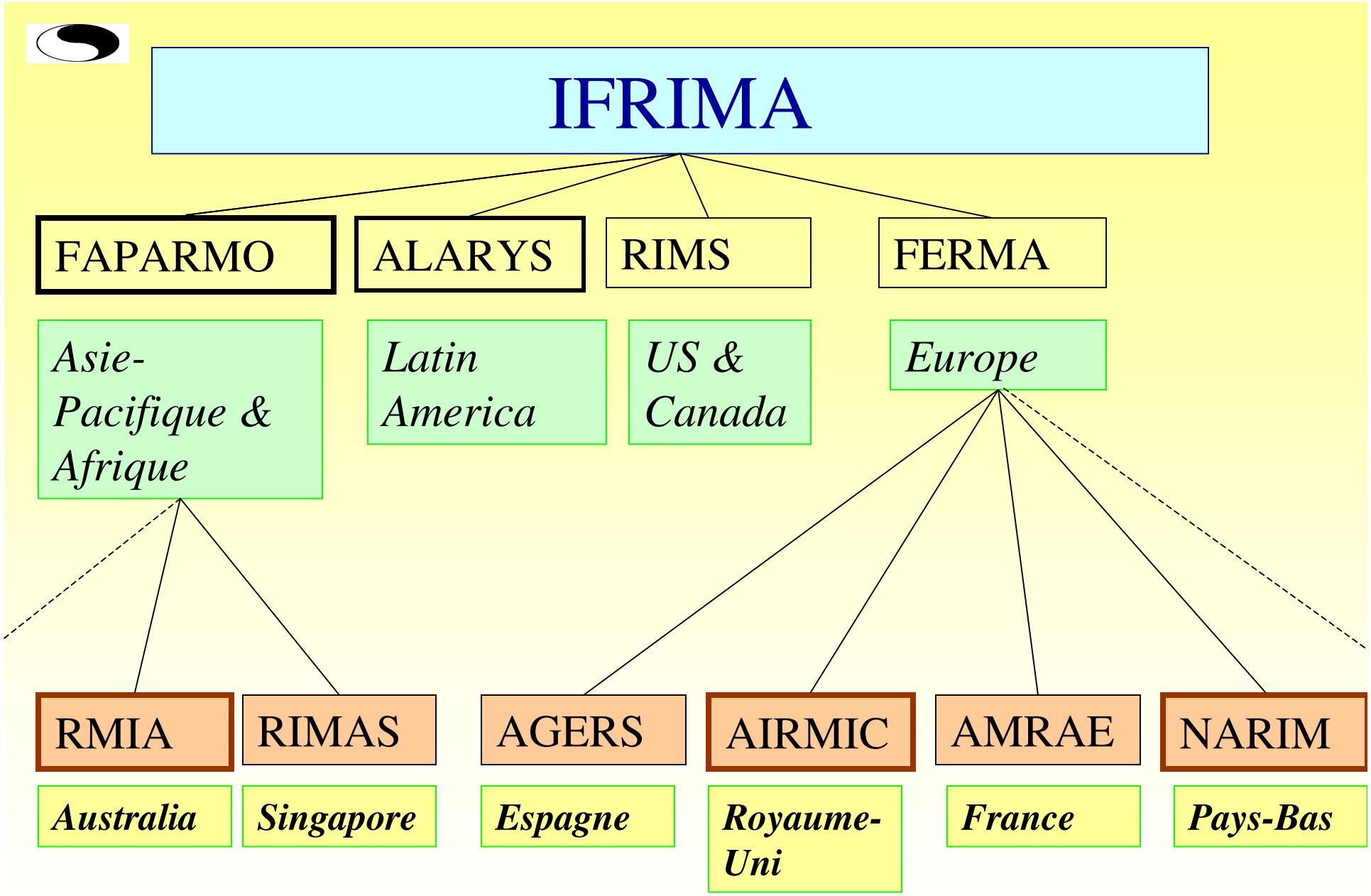
"ISO risk management standard not needed", says FERMA

Strategic risk – Juillet 2007

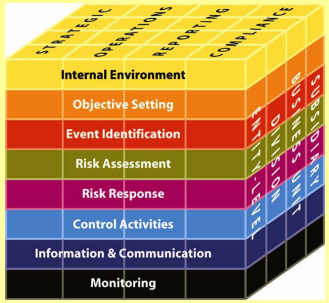
FERMA would support a generic guide entitled "Risk management : essential principles and terminology"

Position paper FERMA – 22 juin 2007

La présidente actuelle est Marie-Gemma Dequae

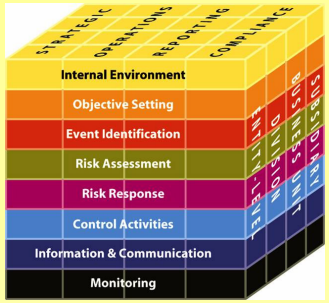


COSO - ERM



1. **Risque non défini clairement** → Risque incertitude et lien avec les objectifs ?
2. **Risque = évènements à effets négatifs** → Situations/circonstances changent
3. **Risque défini séparément** → Interdépendances, corrélation ?
4. **Risques homogènes à travers le business** → Silo, projets, business unit ? Matrice ?
5. **Pas de contexte externe** → Autorité, clients, marché, compétition (idem interne : manque culture, formation,)
6. **Risk assessment « fixé » ou négligé** → Complexe et dynamique. Type de risque change

COSO - ERM



« ERM is effective if management has reasonable assurance that they understand the following :

- *Strategic objective are being achieved*
- *Operational objectives are being achieved*
- *Reporting is reliable*
- *Laws and regulations are being complied with »*

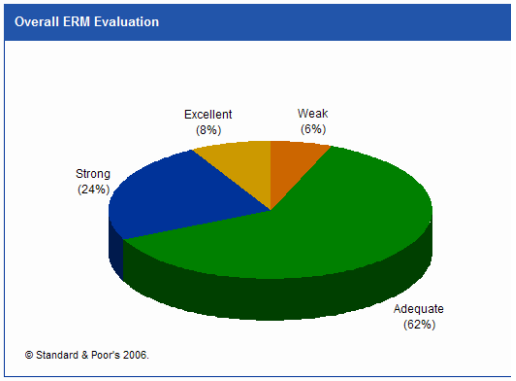
Est-ce du risk management ou de la conformité ?

Standards & Poors

new

STANDARD &POOR'S

Création d'une analyse ERM pour évaluer les ICR de :



- Assurance et réassurance – 78 assureurs évalués
- Mais aussi : Corporate (non-financier)
  - Démarrage : Septembre 2008
  - 4 catégories : Excellent/Strong/adequate/weak
  - Référence acceptée : COSO ERM, AS/NZS 4360 et autres
  - Points d'intérêts : Stratégie, vision de la direction, diagnostic, communications
  - Exclusions : Traitement (risk-control measures)

Standards & Poors

new

STANDARD &POOR'S

Création d'une analyse ERM pour évaluer les ICR de :

- Assurance et réassurance – 78 assureurs evalués
- Corporate (non-financier) - 2009

<u>Quelques critères négatifs selon S&P</u>

o No formal ERM infrastructure

o No formal ERM program

o Existing ERM processes not very formalized

o A decentralized ERM organization

o Underfunded and underintegrated ERM

o Exposing too much competitive information

o Weak ERM culture and strategic risk management

o

Corporates

Overview | Services | News & Commentary | Ratings Actions Press Releases | Reports

· Description · Definitions · Credit Ratings List

All | 0-9 | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

11-20 of 91 View 10 Per page

Entity	Local Currency	Foreign Currency	National Scale	Type
GCI Inc.	BB-/Negative/--	BB-/Negative/--		ICR
GenCorp Inc.	B+/Negative/--	B+/Negative/--		ICR
Genentech Inc.	AA-/Stable/A-1+	AA-/Stable/A-1+		ICR
General Cable Corp.	BB-/Stable/--	BB-/Stable/--		ICR
General Dynamics Corp.	A/Stable/A-1	A/Stable/A-1		ICR
General Electric Co.	AAA/Stable/A-1+	AAA/Stable/A-1+		ICR
General Maritime Corp.	BB/Negative/--	BB/Negative/--		ICR
General Mills Cereals LLC	BBB+/Negative/--	BBB+/Negative/--		ICR
General Mills Inc.	BBB+/Negative/A-2	BBB+/Negative/A-2		ICR
General Motors Corp.	CCC+/Negative/NR	CCC+/Negative/NR		ICR

<u>General Electric</u> : AAA

<u>General Motors</u> : CCC+

Development of an ISO and British Standard for Risk Management

Nicki Dennis
Head of Market Development
Risk, Quality, Health & Safety, Security & Fire
British Standards Institution
nicki.dennis@bsi-global.com

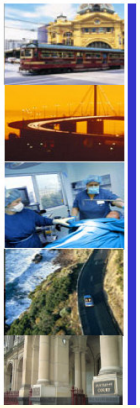
ISO 31000 Risk Management Principles & Guidlines

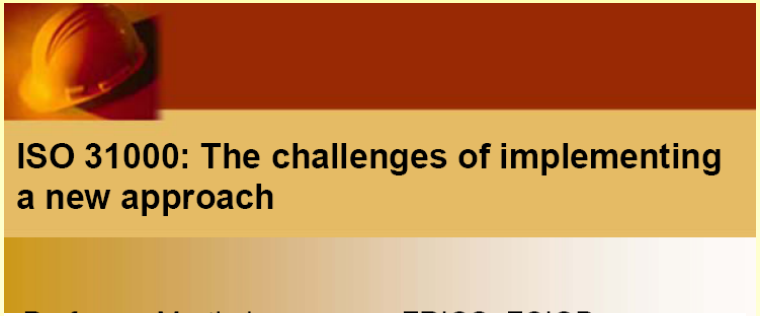
1. ISO proces
2. ISO 31000.
3. Guide 73.
4. Hoe verder.

VICTORIAN MANAGED INSURANCE AUTHORITY
Taking care of risks

ISO 31000
"Raising the standard of risk management"

Grant Purdy
Associate Director,
Broadleaf Capital International
Chair, Standards Australia and New Zealand Risk Management Committee
Nominated Australian "Expert" on ISO Working Group





CHEMIEKARRIERE.NET **Veranstaltungskalender**

Seminar/Schulung
Was ist Risikomanagement und wie funktioniert es? Die heutigen Anforderungen und der Standard von morgen
20.11.2007-20.11.2007

Risk management best practice is ISO 31000

John Shortreed
Director, Institute for Risk Research
University of Waterloo

IMPLEMENTING RISK MANAGEMENT IN 2008
Toronto May 9, 2008

Pengenalan ISO 31000 Manajemen Risiko

By Informasi Training

3 Desember 2008 | Hotel Millennium, Jakarta | RP. 1,850,000 (115 euros)

談 ISO 31000 風險管理標準之發展 (上)

來源：Committee Draft of ISO 31000

1. 前言

從國外發展的總體趨勢來看，進行整合性的風險管理已經成為一種趨勢，其目標是把所有系統面臨的風險整合至一個有條理、一致

Recueil des avis et commentaires

Merci de votre attention…

www.ISO31000.fr
prochainement

Alex Dali

Directeur Associé

Conseil en gestion des risques

ATLASCOPE sarl.

116 rue de Charenton, 75012 Paris

Email : dali@atlascope.com