Techniques d'évaluation des risques

norme ISO 31010

www.pr4gm4.com

Gestion des risques

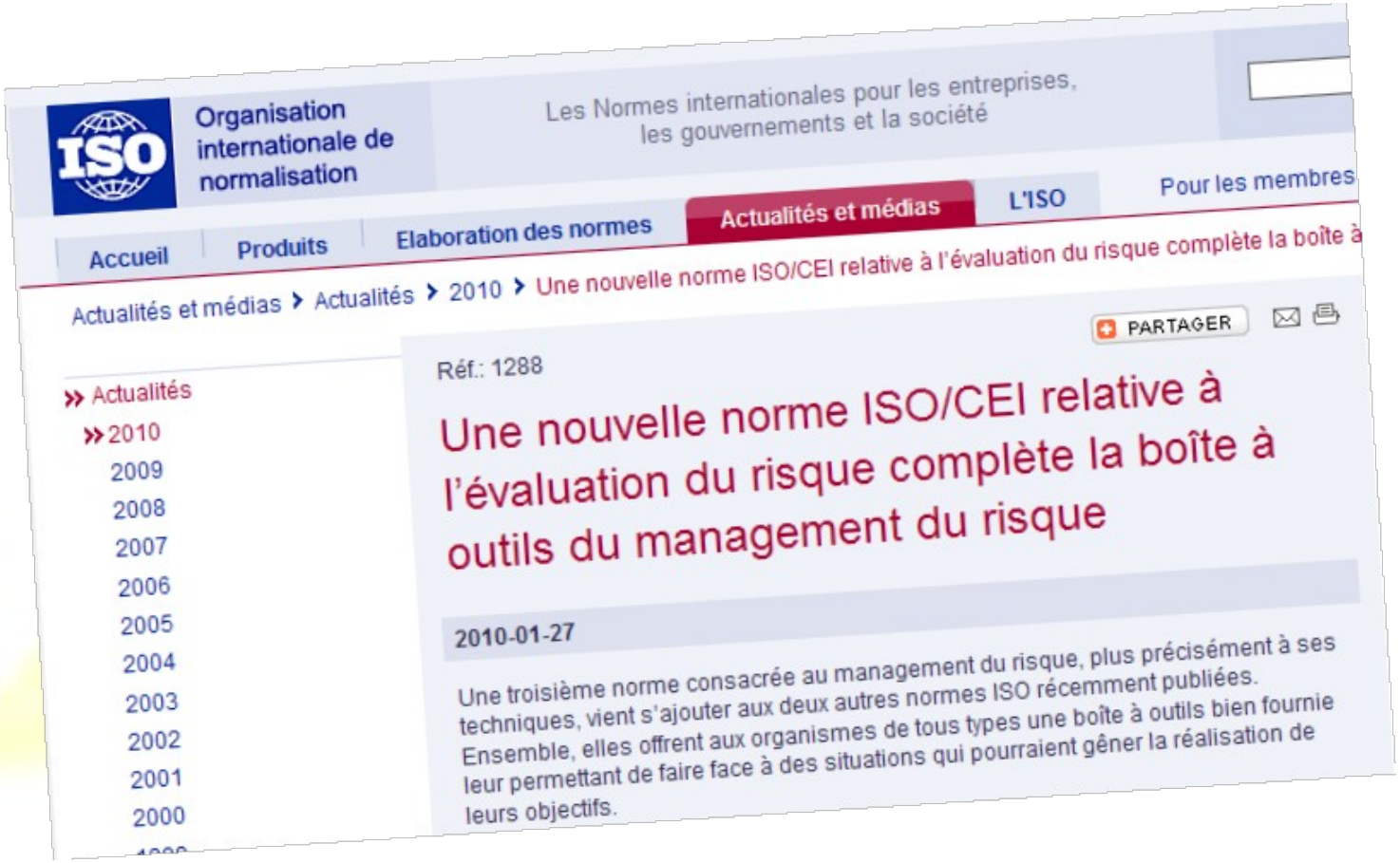
Présentation

Mars 2010

PR4GM4

Services conseils en sécurité de l'information

Actualité du 27 janvier 2010



Actualité du 11 février 2010

OH&S
OCCUPATIONAL HEALTH & SAFETY

Home Magazine News Calendar Community Products Resource Center Industry Directory Services / A

10 HALLMARKS of GREAT WEB CONTENT
DOWNLOAD NOW

HOT TOPICS
H1N1 Flu
AEDs CPR
Behavioral Safety
Confined Spaces
Construction Safety
Disaster Preparedness
Emergency Response
Enforcement

Home > Articles > News

Canada Adopts ISO 31000 Risk Management Standard

It will "help [users] incorporate internationally recognized best practices for identifying and managing risks across financial, strategic, and operational areas," said Doug Morton, director of Life Sciences & Business Management for CSA Standards.

Feb 11, 2010

Canada has adopted the ISO 31000 Risk Management standard, CSA Standards announced Feb. 4. CAN/CSA ISO 31000 *Risk Management – Principles and Guidelines* provides a framework and process for managing risk in any country or industry sector. It may be used by any public, private, or community organization, association, or individual. Following approval by the Standards Council of Canada, it is now a National Standard of Canada.

"These principles and guidelines in ISO 31000 Risk Management serve as an overarching guide for organizations and individuals to help incorporate internationally

Domaine d’application

La présente Norme internationale est une norme **d’accompagnement de l’ISO 31000.**

Elle fournit des lignes directrices permettant de choisir et d'appliquer des techniques systématiques d'évaluation des risques. Elle contribue ainsi à la gestion des risques.

…n’est pas destinée à être utilisée à des fins de certification

…ne fournit pas de critères particuliers permettant d'identifier s'il est nécessaire de procéder à une évaluation des risques

…ne privilégie aucune méthode

…ne traite pas spécifiquement de la sécurité

Domaine d’application

Cela peut être pour:

- Évaluer la fiabilité humaine
- Définir un arbre d’évènements
- Analyser un arbre de pannes
- Analyser des défaillances
- Analyser des impacts sur l’activité
- Faire de la maintenance basée sur la fiabilité
- Faire une analyse coût/bénéfice

…dans les domaines:

- des technologies de l’information
- études des dangers liés aux usines chimiques et pétrochimiques
- des sciences naturelles (végétaux, animaux, humain)
- de l’aéro-spacial
- systèmes de productions

Références normatives

Les documents de référence sont:

- Guide ISO/CEI 73, *Management du risque – Vocabulaire – Principes directeurs pour l'utilisation dans les normes*

- ISO 31000, *Management du risque – Principes et lignes directrices*

Raison d’être

Toute activité d'une organisation implique des risques qu’il convient de gérer.

Le processus de gestion des risques facilite donc la prise de décision.

Il s'agit en effet de tenir compte de l'incertitude, d'éventuels événements ou de certaines circonstances (prévus ou imprévus) et de leurs effets sur les objectifs fixés.

Qu’est-ce que l’évaluation des risques?

L'évaluation des risques tente de répondre aux questions essentielles suivantes:

- que se passe-t-il et pourquoi (par identification des risques) ?
- quelles sont les conséquences ?
- quelle est la probabilité d'occurrence ?
- existe-t-il des facteurs permettant de limiter la conséquence du risque ou de réduire la probabilité d’occurrence du risque ?

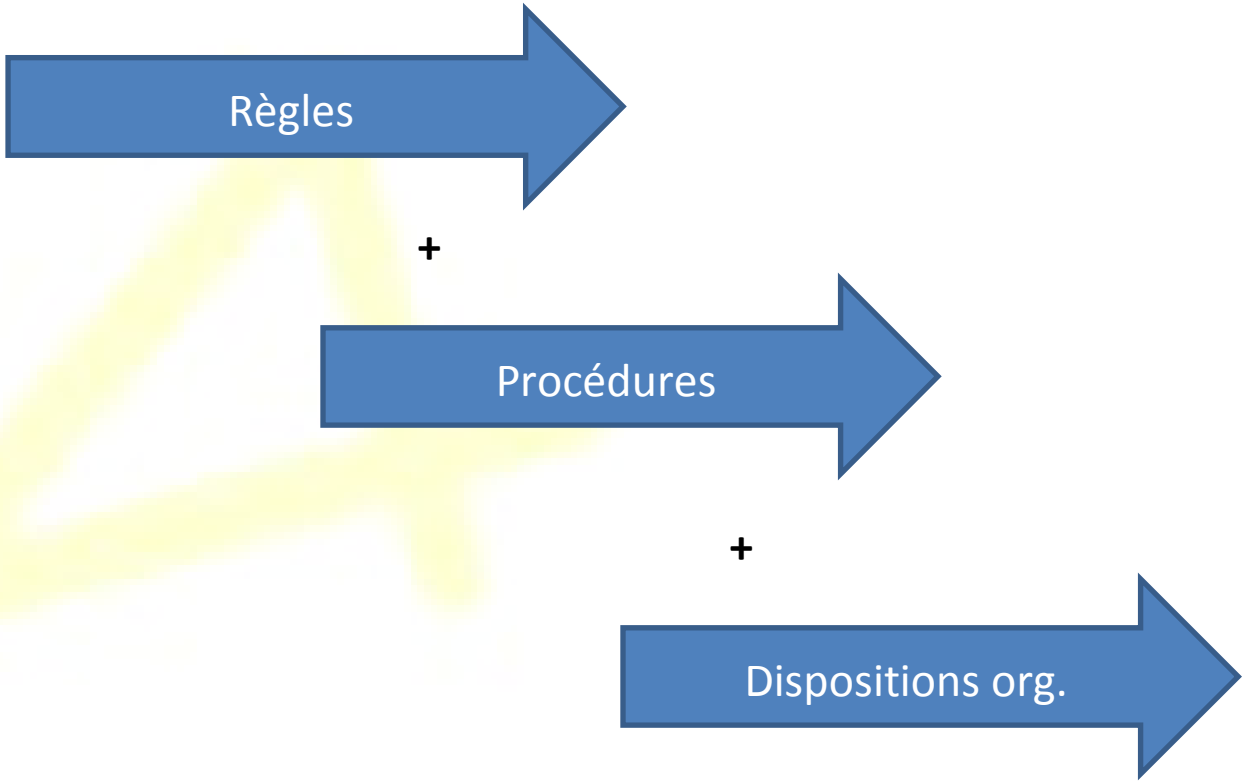
Concepts d’évaluation des risques

Avantages

- compréhension du risque et de son impact potentiel sur les objectifs;
- apport d'informations pour la prise de décision;
- participation à la compréhension des risques afin de faciliter la sélection des options de traitement;
- identification des principaux facteurs contribuant aux risques et des maillons faibles d'un système ou d'une organisation;
- comparaison des risques avec ceux d'autres systèmes, technologies ou approches;
- communication sur les risques et incertitudes;
- aide à l'établissement de priorités;

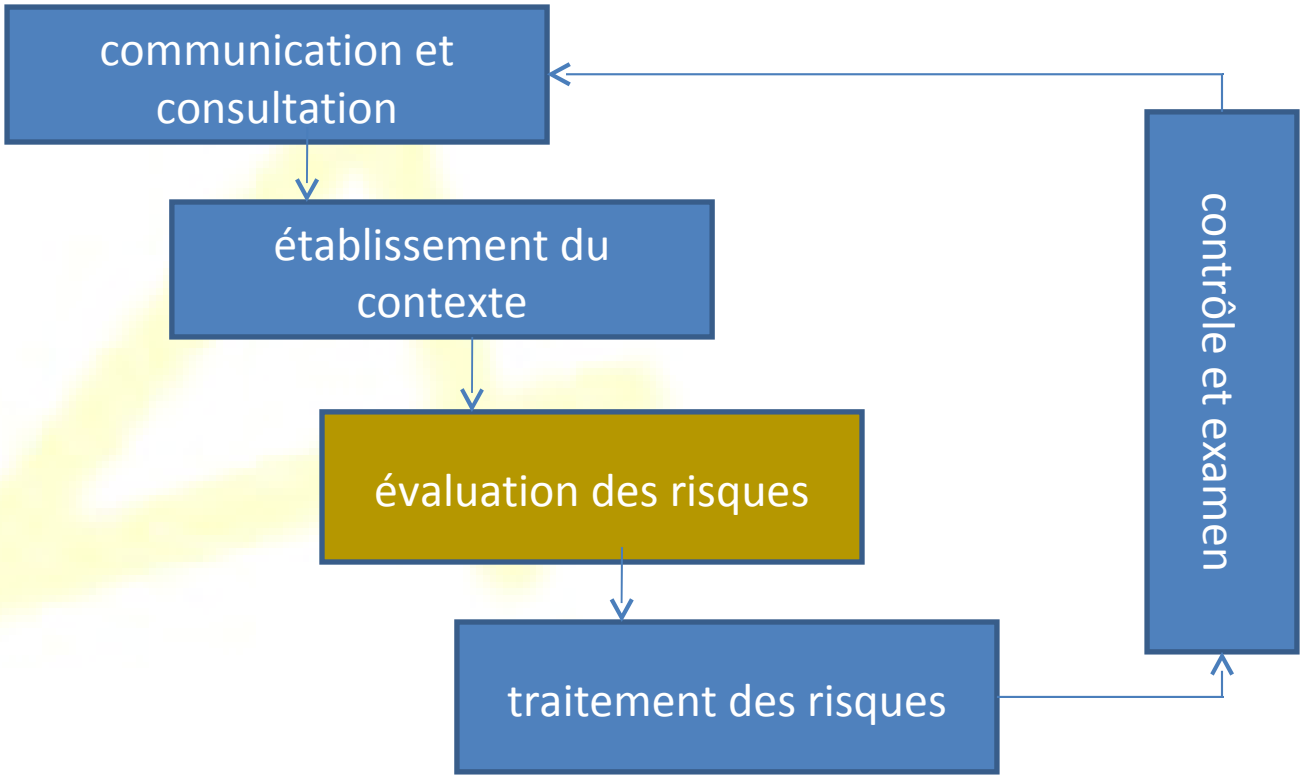
Concepts d'évaluation des risques

Cadre de gestion des risques



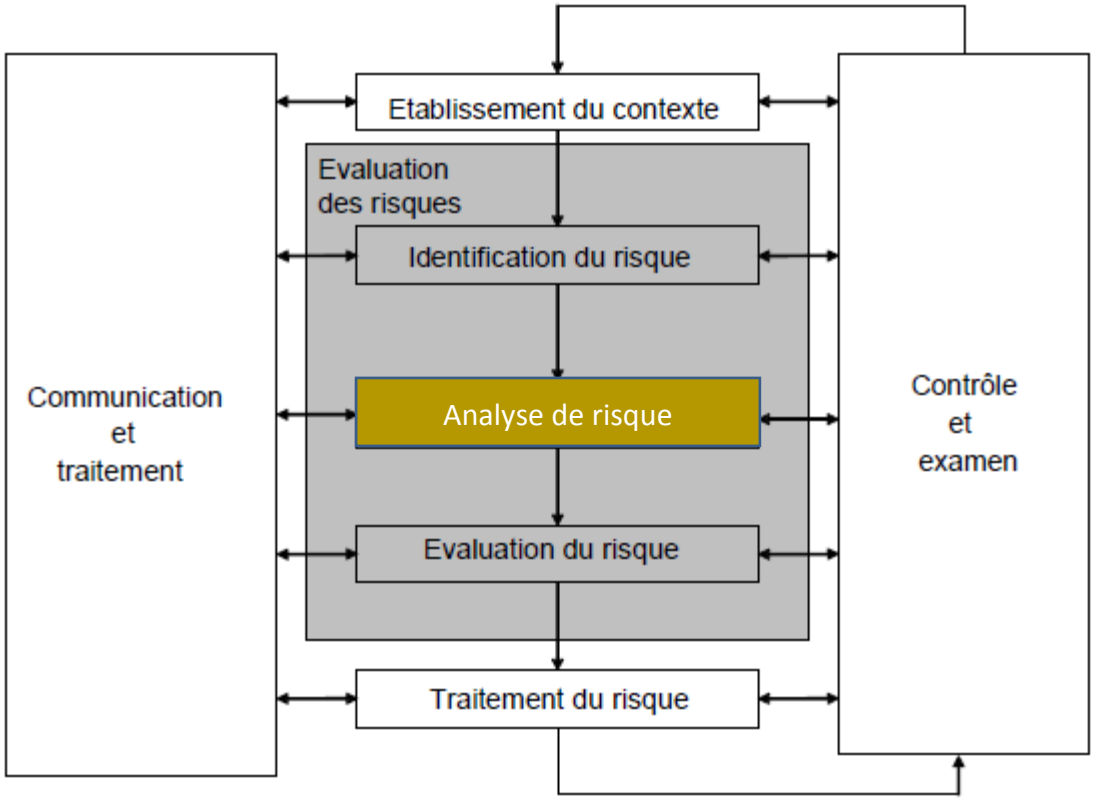
Concepts d'évaluation des risques

Processus de gestion des risques



Processus d'évaluation des risques

Vue d'ensemble



Processus d’évaluation des risques

Identification des risques

L'identification des risques est le processus de recherche, de reconnaissance et d'enregistrement des risques.

causes

origines

BUT: Identifier les raisons pour lesquelles les objectifs du système ou de l'organisation pourraient ne pas être atteints.

Processus d’évaluation des risques

Analyse des risques - Généralité

L'analyse des risques consiste à déterminer les **conséquences et les probabilités** pour les risques identifiés en tenant compte de la présence (ou non) et de l'efficacité des contrôles existants.

Elle peut être:

- Qualitative
- Semi-quantitative
- quantitative

Donne une estimation de l’ensemble des conséquences

Processus d'évaluation des risques

Analyse de risques - Évaluation des contrôles

- Le niveau de risque dépend de **l'adéquation et de l'efficacité des contrôles existants**. Cela implique de répondre aux questions suivantes:
  - quels sont les contrôles existants liés à un risque particulier?
  - ces contrôles sont-ils en mesure de traiter le risque de manière à le maintenir à un niveau tolérable?
  - dans la pratique, les contrôles fonctionnent-ils comme prévu et leur efficacité peut-elle être démontrée, le cas échéant?

Processus d'évaluation des risques

Analyse de risques – conséquences

L'analyse des conséquences **permet de déterminer la nature et le type d'impact susceptible de se produire** par l'affecte d'un ensemble d'objectifs et d'acteurs différents.

Processus d’évaluation des risques

Analyse de risques – vraisemblance et probabilité

3 approches:

a) Utilisation de données historiques pertinentes afin d'identifier des événements ou des situations qui se sont produits dans le passé et ainsi extrapoler la probabilité de leur occurrence dans le futur.

b) Prévision des probabilités à l'aide de techniques prédictives telles que l'analyse par arbre de panne et l'analyse par arbre d'événements.

c) L'avis d'un expert peut être utilisé dans un processus systématique et structuré pour estimer la probabilité.

Processus d’évaluation des risques

Analyse de risques – dépistage des risques

Il convient que le dépistage repose sur des critères définis dans le contexte. L’analyse préliminaire permet de déterminer l'une des suites d'actions suivantes:

- décision de traiter les risques sans évaluation supplémentaire;
- définition de risques non significatifs collatéraux ne justifiant pas de traitement;
- poursuite par une évaluation plus détaillée des risques.

Il convient de documenter les hypothèses initiales et les résultats.

Processus d’évaluation des risques

Analyse de risques – incertitude et sensibilité

Il est nécessaire de bien cerner ces incertitudes pour interpréter et **communiquer de manière efficace les résultats** de l'analyse des risques.

Processus d’évaluation des risques

Évaluation des risques, 3 « bandes »:

niveau de risque est considéré comme intolérable
le traitement du risque est primordial quel que soit son coût

niveau de risque est considéré comme « gris »
les coûts et avantages sont pris en compte

niveau de risque est considéré comme négligeable
aucun traitement n'est envisagé

Processus d’évaluation des risques

Documentation

la documentation peut comporter:

- les objectifs et le domaine d'application;
- la description des parties correspondantes du système et leurs fonctions;
- les critères de risque appliqués et leur justification;
- les limitations, hypothèses et la justification des hypothèses;
- la méthodologie d'évaluation;
- les résultats d'identification des risques;
- les données, hypothèses, leurs sources et la validation;
- les résultats de l'analyse des risques et leur évaluation;
- l'analyse de sensibilité et d'incertitude;
- les hypothèses critiques et autres facteurs devant faire l’objet d’une surveillance;
- la discussion des résultats;
- les conclusions et recommandations;
- les références.

Processus d’évaluation des risques

Contrôle et examen de l’évolution des risques

Il convient également de contrôler et de documenter l’efficacité des contrôles pour fournir des données à utiliser pour l’analyse des risques. Il convient de définir les responsabilités pour ce qui concerne la création et l’examen des preuves et de la documentation.

Processus d’évaluation des risques

Application de l’évaluation des risques

Les risques peuvent être évalués à **toutes les étapes du cycle de vie**. D'une manière générale, ils le sont plusieurs fois à différents niveaux de détail, de manière à faciliter la prise de décision à chaque phase.

Sélection des techniques d'évaluation

Généralité

Nous allons répondre à la question: comment sélectionner une ou des techniques d'évaluation des risques?

Annexe: outils et techniques.

Sélection des techniques d’évaluation

Sélection des techniques

Il convient qu’une technique adaptée possède les caractéristiques suivantes:

- convient qu’elle soit justifiée et adaptée à la situation ou à l'organisation considérée;
- il convient que les résultats obtenus se présentent sous une forme permettant une meilleure compréhension de la nature des risques et de la manière dont ils peuvent être traités;
- il convient qu’elle soit utilisée de telle sorte qu'elle soit traçable, reproductible et vérifiable.

Sélection des techniques d’évaluation

Sélection des techniques

il convient de choisir la ou les techniques sur la base de facteurs applicables, tels que :

- les objectifs de l'étude;
- les besoins des décideurs;
- le type de risques devant être analysés;
- l'amplitude potentielle des conséquences.
- le degré de compétence et les besoins en RH;
- la disponibilité de l’information;
- exigences réglementaires et contractuelles.

Sélection des techniques d’évaluation

Disponibilité des ressources

- les compétences, l'expérience, la capacité et les aptitudes de l'équipe d'évaluation des risques;
- les contraintes liées au temps et aux autres ressources de l'organisation;
- le budget disponible si des ressources externes sont requises.

Sélection des techniques d’évaluation

Nature et degré d’incertitude

- qualité médiocre des données ou de l'absence de données essentielles et fiables;
- être inhérente au contexte externe et interne de l'organisation.

Sélection des techniques d’évaluation

- Complexité

  Les impacts importants et dépendances du risque doivent être compris pour s'assurer que de la gestion d'un seul risque **ne découle pas une situation intolérable ailleurs.**

Sélection des techniques d’évaluation

- Application de l’évaluation des risques

L'évaluation des risques permet:

- d'assurer que les risques liés au système sont tolérables,
- de participer au processus d'amélioration de la conception,
- de participer aux études de rentabilité,
- d'identifier les risques ayant un impact sur les phases suivantes du cycle de vie.

Sélection des techniques d’évaluation

- Types de techniques d’évaluation des risques
  - l'Annexe A: met en corrélation les techniques potentielles et ces catégories;
  - l'Annexe B : Approfondissement de chaque technique.

Sélection des techniques d'évaluation

- techniques d'évaluation des risques

  + de 30 outils et techniques (Delphi, HAZOP, SWIFT, etc.)

  Facteurs influents

  - Ressources et aptitudes
  - Degré d'incertitude
  - complexité

Conclusion

- 31010 n’est pas une certification;
- L’air actuel oblige les organisations de faire de la gestion de risques;
- N’est pas spécifique à la sécurité mais plutôt la gestion des risques dans son ensemble;
- Atteindre la réalisation des objectifs corporatifs;
- A chaque organisation son contexte et donc sa (ses) méthode(s) d’analyse de risques appropriée(s).

Reproduction de ce document

Bibliographie

- ISO/IEC 31010:2009 PDF version (EN/FR)
- CSI-ISO31000-10-questions.pdf
- Tribune_ISO31000.pdf
- ISO31010Draft8-09.pdf
- ICSI-fiche-ISO31000.pdf
- Standard_ISO31000-CARM-slides.pdf
- risk_ims_09-4.pdf
- 02_evaluation_gestion_risques.pdf
- info_ieciso31010{ed1.0}b.pdf

- http://www.iso27001security.com/html/others.html
- http://www.sarma-wiki.org/index.php?title=ISO_31010_(DRAFT)
- http://www.business-wissen.de/controlling-buchhaltung/iso-norm-31010-zur-risikobewertung/
- http://www.nieuwsbank.nl/inp/2010/02/09/H100.htm
- http://ohsonline.com/articles/2010/02/11/canada-adopts-iso-31000-risk-management-standard.aspx?admgarea=
- http://www.qhseclub.com/fr/content/view/4489/104/
- http://www.iso.org/iso/fr/pressrelease.htm?refid=Ref1288