Risk assessment techniques

ISO 31010

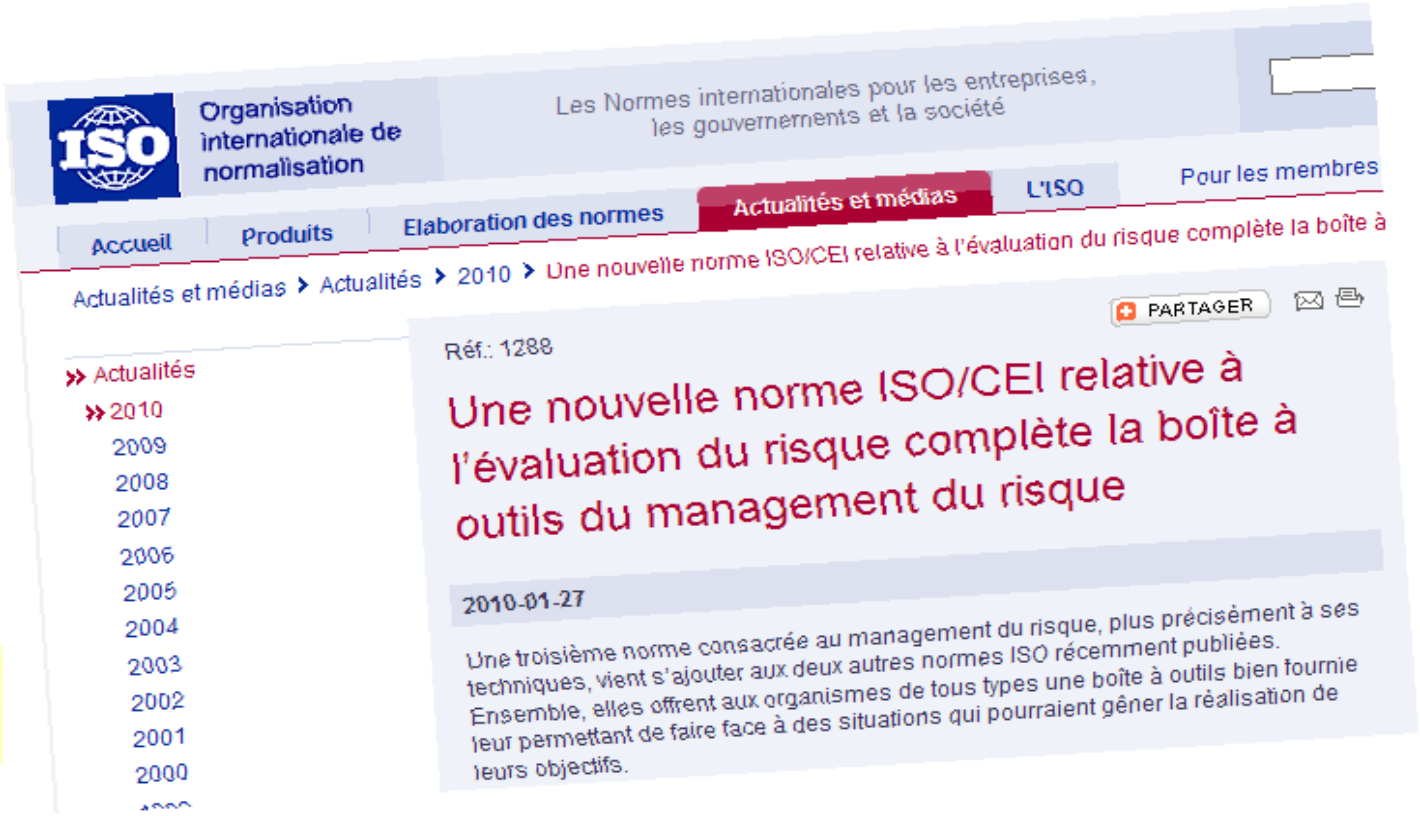
www.pr4gm4.com

Risk management

Aout 2011

PR4GM4
Services conseils en sécurité de l'information

News, January 27 2010



News, February 11 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

Scope

This International Standard is a **companion standard ISO 31000**.

It provides guidelines for choosing and applying techniques of systematic risk assessment. It thus contributes to risk management.

... Is not intended to be used for certification

... Does not provide specific criteria for identifying the need to conduct a risk assessment

... Does not recommend any method

... Does not specifically address security

Application fields

This can be for:

- Assessing human reliability
- Define a tree of events
- Analyze a fault tree
- Failure Analysis
- Analyze the impact on activity
- To the reliability-based maintenance
- Make a cost / benefit analysis

... In the fields:

- of information technology
- study of hazards of chemical and petrochemical plants
- natural sciences (plant, animal, human)
- aero-spacial
- production systems

Normative references

The reference documents are:

- ISO / IEC Guide 73, Risk management - Vocabulary
- ISO 31010, Risk management – Risk assessment techniques

To be reason

Any activity of an organization involves risks should be managed.

The process of risk management therefore facilitates decision-making.

It is indeed to take into account the uncertainty of any events or circumstances (intended or unintended) and their effects on targets.

What is risk assessment?

Risk assessment attempts to answer the following key issues:

- What's going on there and why (risk identification)?
- what are the consequences?
- what is the probability of occurrence?
- Are there any factors to limit the impact of the risk or reduce the likelihood of risk occurring?

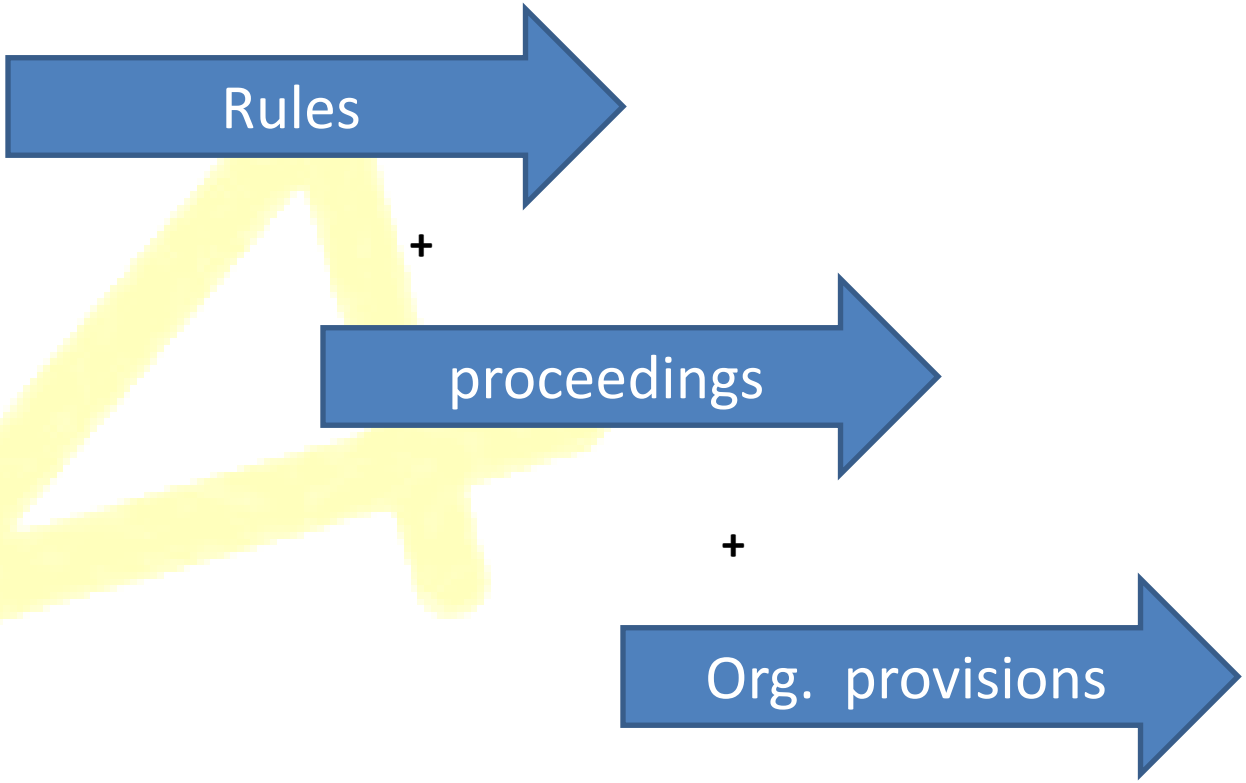
Concepts of risk assessment

Benefits:

- understanding of risk and its potential impact on objectives;
- providing information for decision-making;
- participation in the understanding of risks to facilitate the selection of treatment options;
- identification of the main factors contributing to risk and weak links of a system or organization;
- risk comparison with other systems, technologies or approaches;
- communication about risks and uncertainties;
- help set priorities;

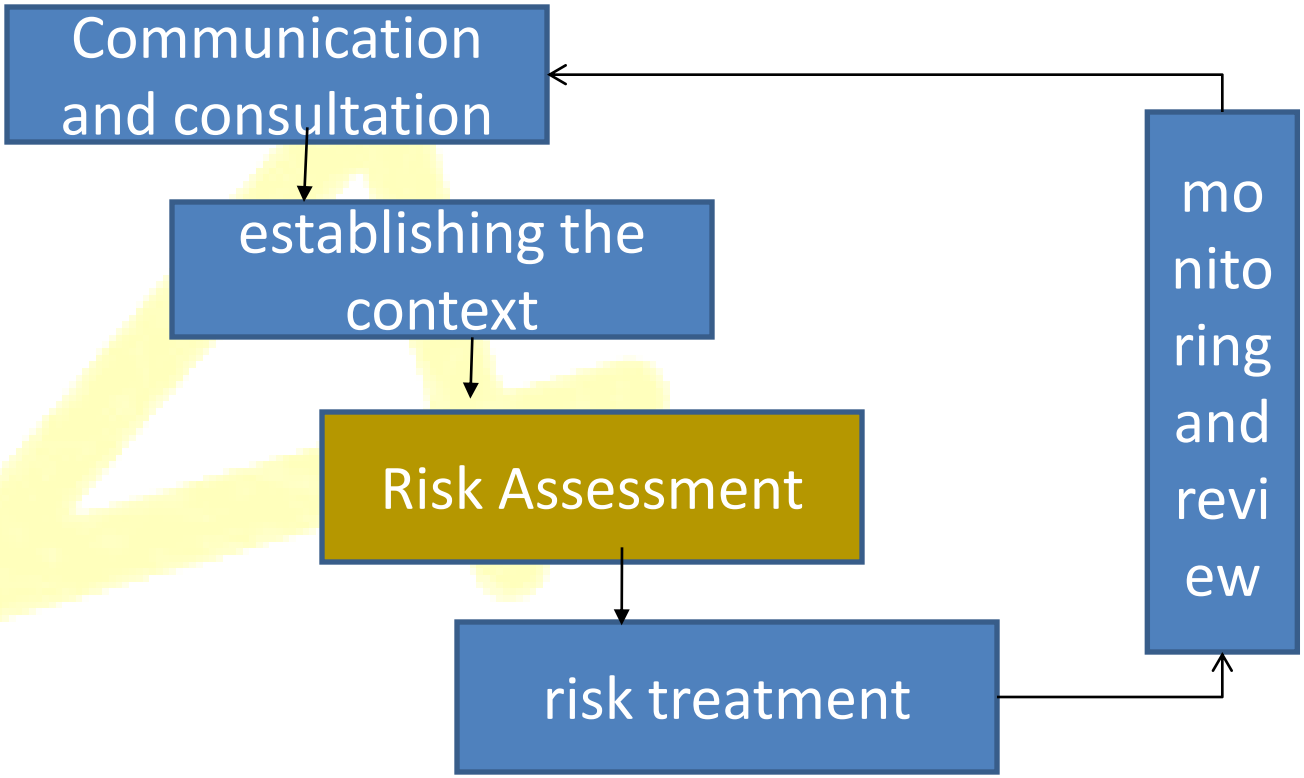
Concepts of risk assessment

Risk Management Framework:



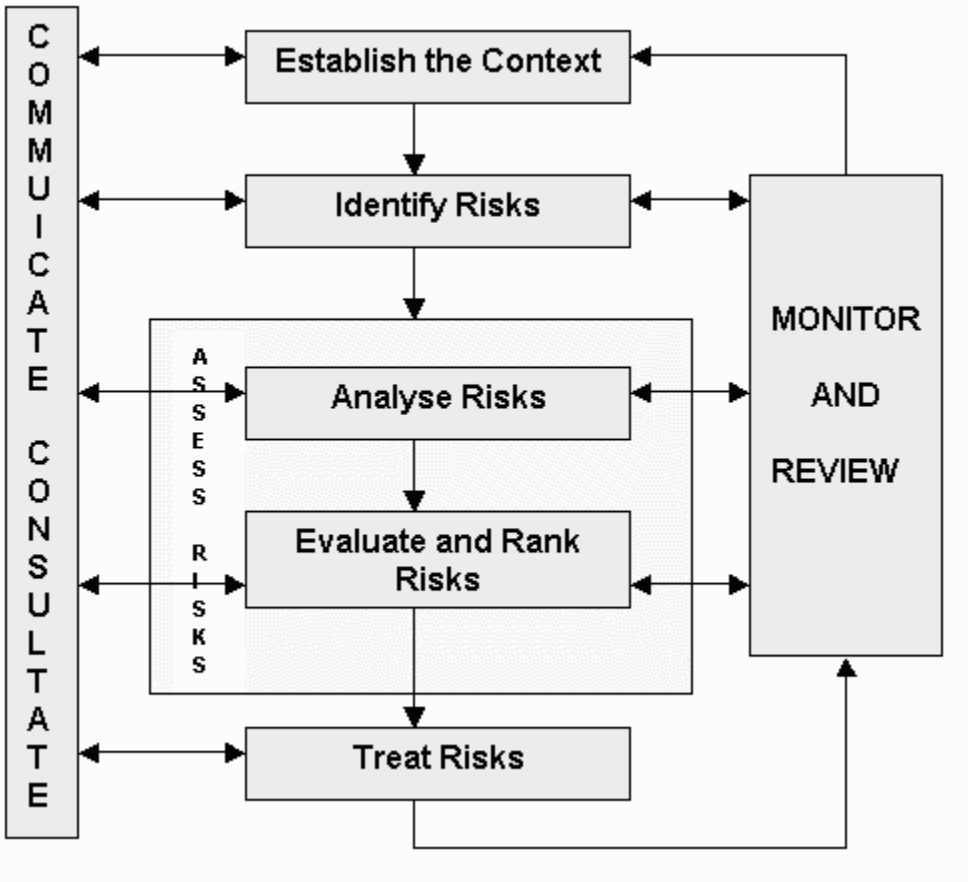
Concepts of risk assessment

Process risk management:



Process risk management

Overview:



Process risk management

Risk Identification:

Risk identification is the process of research, recognition and registration of risk.

causes

origins

GOAL: To identify the reasons why the objectives of the system or organization may not be achieved.

Process risk management

Risk Analysis - Generality:

Risk analysis is to determine **the consequences and probabilities** for the risks identified, taking into account the presence (or not) and the effectiveness of existing controls.

It can be:

- qualitative
- Semi-quantitative
- quantitative

Provides an estimate of all the consequences

Process risk management

Risk Analysis - Assessment of Controls:

The level of risk depends on **the adequacy and effectiveness of existing controls**. This involves answering the following questions:

- what are the existing controls related to a particular risk?
- these controls are they able to handle the risk so as to maintain a tolerable level?
- in practice, the controls do they work as expected and their effectiveness can be demonstrated, if any?

Process risk management

Risk analysis - implications:

The analysis of the consequences **to determine the nature and type of impact that may occur** by assigning a set of objectives and actors.

Process risk management

Risk analysis - probability and probability:

3 approaches:

a) Use of relevant historical data to identify events or situations that have occurred in the past and extrapolate the probability of their occurrence in the future.

b) Forecast probabilities using predictive techniques such as fault tree analysis and event tree analysis.

c) The expert opinion may be used in a systematic and structured process to estimate the probability.

Process risk management

Risk analysis - risk screening:

Screening should be based on criteria defined in the context. Preliminary analysis to determine one of the suites of the following:

- decision to treat the risk without further assessment;
- definition of non-significant collateral risk did not warrant treatment;
- continued by a more detailed assessment of risks.

It should document the initial assumptions and results.

Process risk management

Risk analysis - uncertainty and sensitivity:

It is necessary to clearly identify these uncertainties to interpret and **effectively communicate the results** of risk analysis.

Process risk management

Risk assessment, 3 "bands":

level of risk is considered intolerable
treatment of risk is essential regardless of cost

risk level is considered "gray"
the costs and benefits are taken into account

level of risk is considered negligible
no treatment is considered

Process risk management

Documentation:

Documentation may include:

- the objectives and scope;
- description of the corresponding parts of the system and their functions;
- risk criteria applied and their justification;
- the limitations, assumptions and justification of assumptions;
- the evaluation methodology;
- results of risk identification;
- the data, assumptions, their sources and validation;
- results of risk analysis and evaluation;
- sensitivity analysis and uncertainty;
- critical assumptions and other factors to be monitored;
- discussion of results;
- conclusions and recommendations références

Process risk management

Control and examination of the development risk:

It should also monitor and document the effectiveness of controls to provide data for use in risk analysis. It should define the responsibilities for the creation and review of evidence and documentation.

Process risk management

Application of risk assessment:

Risks can be assessed at **all stages of the life cycle**. In general, they are many times at different levels of detail, so as to facilitate decision making at every stage.

Selection of evaluation techniques

Generality:

We will answer the question: how to select one or more techniques of risk assessment?

Appendix: Tools and Techniques.

Selection of evaluation techniques

Selection techniques:

It should be a suitable technique has the following characteristics:

- it should be justified and appropriate to the situation or organization concerned;
- should the results come in a form that allows a better understanding of the nature of the risks and how they can be treated;
- should it be used so that it is traceable, repeatable and verifiable.

Selection of evaluation techniques

Selection techniques:

It should be chosen and the techniques based on relevant factors such as:

- the objectives of the study;
- the needs of decision makers;
- the type of risk to be analyzed;
- the magnitude of potential consequences.
- the degree of competence and HR needs;
- availability of information;
- regulatory and contractual requirements.

Selection of evaluation techniques

Availability of resources:

- skills, experience, ability and skills of the team risk assessment;
- the constraints of time and other resources of the organization;
- the budget available if external resources are required.

Selection of evaluation techniques

Nature and degree of uncertainty:

- Poor data quality or lack of essential data and reliable;
- be inherent in the external and internal organization.

Selection of evaluation techniques

Complexity:

Significant impacts and dependencies of the risk must be understood to ensure that the management of one risk **does not follow an intolerable situation elsewhere.**

Selection of evaluation techniques

Application of risk assessment:

The risk assessment provides:

- to ensure that the system risk is tolerable
- to participate in the process of improving the design,
- to participate in feasibility studies,
- identify risks that impact on the subsequent phases of the life cycle.

Selection of evaluation techniques

Types of risk assessment techniques:

- Appendix A: correlates and potential technical class;
- Appendix B: Further development of each technique.

Selection of evaluation techniques

Technical risk assessment:

30 + tools and techniques (Delphi, HAZOP, SWIFT, etc.).

factors influencing

- Resources and skills
- Uncertainty
- complexity

Conclusion

- 31010 is not a certification;
- The air current requires organizations to make risk management;
- Is not specific to security but rather risk management as a whole;
- Achieve corporate objectives;
- Every organization and therefore its context (its) way (s) appropriate risk assessment (s).

Reproduction

Bibliography

- 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=news
- http://www.qhseclub.com/fr/content/view/4489/104/
- http://www.iso.org/iso/fr/pressrelease.htm?refid=Ref1288