

# ISO 31000 – Risk Management Standard

Ottawa February 27, 2008

John Shortreed, Director, Institute for Risk Research

University of Waterloo

([shortree@uwaterloo.ca](mailto:shortree@uwaterloo.ca))

- 1. What is ISO 31000?**
- 2. What are the key components of 31000?**
- 3. Questions**

**workshop format to understand ISO 31000 by examining  
key components**

# What is ISO 31000?

## Guide for principles and implementation of risk management

- More or less final - will be issued in 2009 along with Guide 73 (terms), and 31010 (revised IEC risk analysis standard - originally Canadian eh!)
- Can review 31000 and have input by asking after April 1 for the latest draft (free but must read, [shortree@uwaterloo.ca](mailto:shortree@uwaterloo.ca) )
- Will replace CSA Q850, Treasury Board, RIMS, etc. etc. and become the recognized international framework for risk management everywhere – good stuff, no fooling

# first a few things about risk and 31000

- **risk** ; “effect of uncertainty on objectives”
  - positive and negative consequences
  - safety, compliance, strategy, anything under the sun
- **risk management**; “coordinated activities to direct and control and organization with regard to risk”
- **risk management framework**; “set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organization”
- **risk management process**; “systematic application of management policies, procedures and practices to the tasks of communication, consultation, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk”

# Is this your organization?

- Name Brand has been tarnished
- Continually in crisis management mode due to the absence of Quality Assurance mechanisms
- Repeated cases of:
  - Overspending
  - Delays
  - Non compliance with policies and regulations

Self assessment by a Canadian Government department (good start!!)

Quality assurance must follow & be coordinated with risk management

# Your Organization and 31000

- Every organization is unique, yours might be a regulator, a deliverer of services, a policy analysis shop, an enforcer of laws, a facilitator of industry and commerce, support for education or literacy or rights, etc.
- So implementation of risk management in every organization is different but instantaneously recognized as 31000 risk management framework, process, terminology, and other best practices.
- So your organization's risk management could be reviewed and evaluated by any other risk management literate person from any organization to mutual advantage.

Workshop will rate your organization against  
key components in ISO 31000  
In the process you will learn what is in 31000

Scorecard

1. Risk Register	____/10
2. Accountability	____/6
3. RM Process	____/14
4. RM Framework	____/14
5. Integration	____/6
6. Terminology	____/5 (bonus)
Total	____/50

## Key components Workshop – **Risk Register (RR)**


**risk register;** “ record of information about identified risks”

1. **risk owner;** “person or entity with the accountability and authority”
2. **risk evaluation** – use **risk analysis** to compare risk against **risk criteria** and find **level of risk** – is it **acceptable?**
3. **risk treatment;** “process of developing, selecting, and implementing measures to modify risk”  
(control is “measures to modify risk” )
4. **risk trends, performance measures for risk and risk controls**
5. **record for every risk in the organization**

The following three slides provide illustrations of **risk registers** that have been found to be useful in organizations with successful ERM

1. A bow tie diagram used by Broadleaf Capital, used for design of risk treatment but also a risk register

2. An illustrative example of the approach used by  , and

3. An illustrative example of how  use their risk register for monitoring and review



# Bow-Tie Risk Treatment Tool

**1. Risk**

2. Causes
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

3. Impacts
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Existing Likelihood affecting controls		Control Owner
1.		
2.		
3.		
4.		
5.		
6.		

Tasks (future controls)	Task Owner	Due Date
1.		
2.		
3.		

Existing Consequence affecting Controls		Control Owner
1.		
2.		
3.		
4.		
5.		
6.		

Tasks (future controls)	Task Owner	Due Date
1.		
2.		
3.		

6. Risk Control Effectiveness

7. Consequence factor

8. Likelihood factor

9. RISK RATING

10, Potential exposure

11. Risk Owner

Example risk register for a specific Objective – illustration only  
 Courtesy of Larry Warner of **MARS** the Food Company



1. Identify initiatives and their associated descriptions with measurable objectives

6. Management Team evaluates the probability of success in achieving this initiative's overall objectives

2. Prioritize order of the key initiatives based on their contribution to achieving the overall financial and strategic objectives within the OP

3. Document the individual in charge of the given initiative

7. Document the immediate next steps for effective initiative execution

<b>Ready-to-Heat</b>		Risk Profile	
Aggressively grow and build the ready-to-heat business by expanding the product line (15% NSV growth & maintain shares above 30%) and broaden the availability of the product.		Priority	
		Owner	
Risks		Mitigation Activities	
1	Increase of aggressive competition from Rice Master and Fast Rice Aggressive year for growth target for the segment & brand	1,2,3	Accelerate innovation
2	Achieve new product growth targets	1	Conduct competitor analysis session
3			
<b>Action Plan</b>			
4. List of risks that could hinder the ability to meet the initiative's objectives		5. List of planned activities that will mitigate the risks – match the mitigation strategies to risk through the reference numbers	

4. List of risks that could hinder the ability to meet the initiative's objectives

5. List of planned activities that will mitigate the risks – match the mitigation strategies to risk through the reference numbers



**Business units are required to review and update a dashboard on a quarterly basis which allows tracking of performance over time**

Initiative	Risk Profile				Trend	Comments
	Q3 '05	Q4 '05	Q1 '06	Q2 '06		
<b>Re-launch of Pedigree</b> Effectively execute the re-launch of Pedigree to achieve the growth targets (10%)	Yellow	Green			Improving	Shipments started in P2 to meet advertising schedule. Advertising on air (P2W3). Massive presentation to all customers was executed during P1 with excellent customer participation.
<b>Direct-to-store (DTS)</b> Increase DTS operations by 10% and add 500 points of sale per cell	Green	Green			Stable	DTS operation is improving however there are still some areas that need to improve further. We will expand when we have a holistic strategy.
<b>Associate engagement</b> Increase associate engagement score from 85% to 90% within the factory	Blue	Green			Improving	Shift managers have been provided associate engagement training. All managers have held meetings with their team members.
<b>Bring Pet Dry plant online</b> Make the Dry plant fully operational by P13	Red	Blue			Stable	On track, construction permit granted. Plant will be ready by P13
<b>Launch of Dove</b> Successfully launch Dove into the mass market and achieve 65% distribution	Blue	Yellow			Stable	Increased risk due to current demand exceeding supply. We have re-phased the roll-out for the mass market to ensure current supply is adequate.



## Key components Workshop – Risk Register (RR)

discuss at table, then rate your organization out of 10

**risk register;** “ record of information about identified risks”

### **Rate each item out of 2**

1. **risk owner;** “person or entity with the accountability and authority”
2. **risk evaluation** – use **risk analysis** to compare risk against **risk criteria** and find **level of risk** – is it **acceptable?**
3. **risk treatment;** “process of developing, selecting, and implementing “measures to modify risk””  
(**control** is “measures to modify risk” )
4. **risk trends, performance measures for risk and risk controls**
5. **record for every risk in the organization**

## Key components Workshop – Accountability

discuss, rate organization out of 6

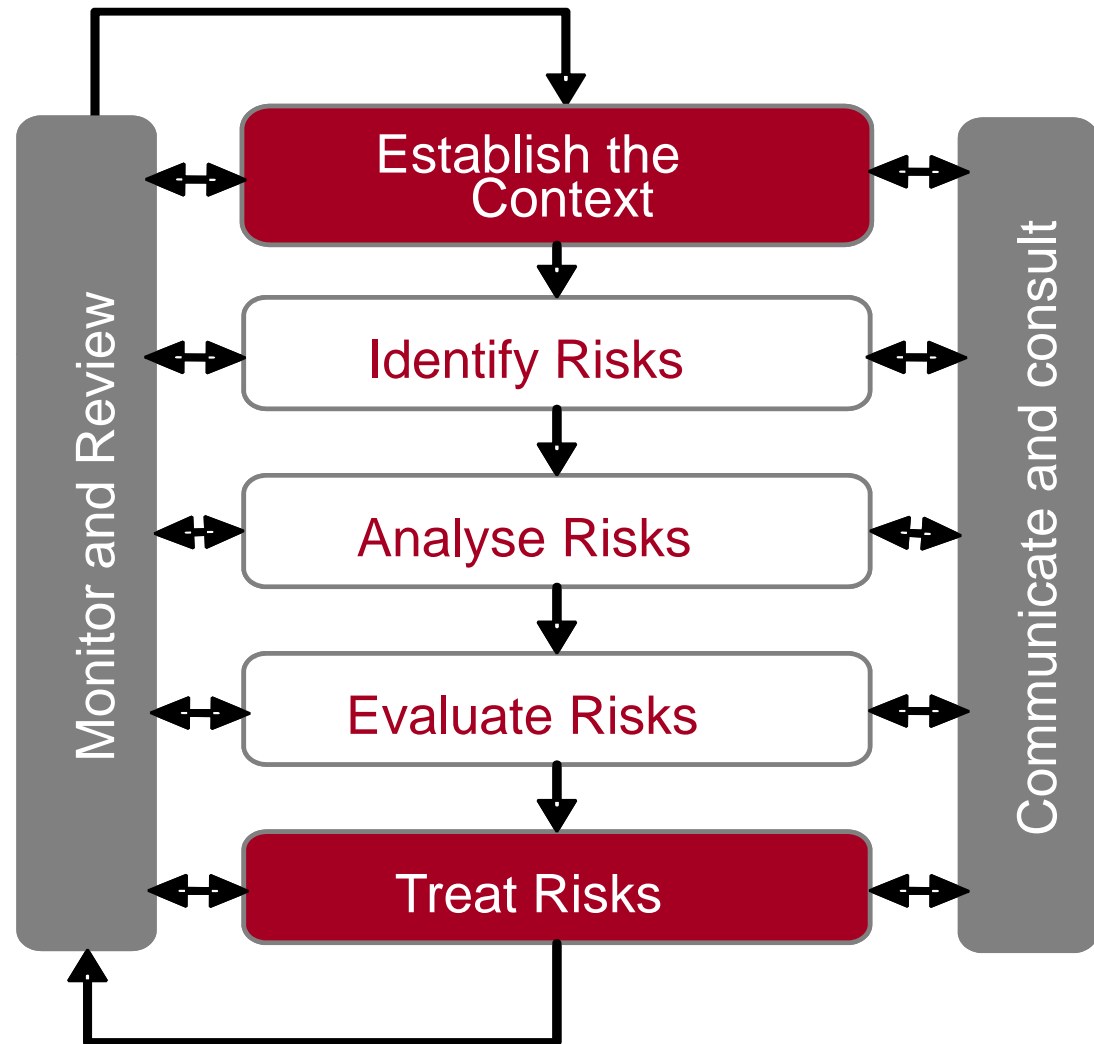
- Policy that states each risk owner is accountable for that risk, the associated controls and monitoring of risk
- Accountability is assessed at manager's annual performance review where evidence is expected
- Culture of accountability is such that everyone knows what risks they own and who owns risks that impact them

# Key components Workshop – Risk Management Process

discuss, rate organization out of 14

## Notes

- Risk assessment is the white boxes
- Process is for every manager for every project, program, decision
- 2 points-have box, 1- being done
- We will not spend much time here since this should be well known

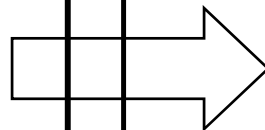


Key components Workshop –Risk Management Framework  
discuss, rate organization out of 14

- Framework; “set of components that provide the foundations and organizational arrangement for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organization” (wow a mouthful)
- Framework is new to 31000, follows Plan-Do-Check-Act quality model and must follow principles outlined in 31000
- Next two slides show
  - 1) relationship of of framework, process and principles
  - 2) details of framework implementation

- a) Creates value
- b) Integral part of organizational processes
- c) Part of decision making
- d) Explicitly addresses uncertainty
- e) Systematic, structured and timely
- f) Based on the best available information
- g) Tailored
- h) Takes human and cultural factors into account
- i) Transparent and inclusive
- j) Dynamic, iterative and responsive to change
- k) Facilitates continual improvement and enhancement of the organization

**Principles for managing risk**  
**(Clause 4)**



5.2  
Mandate  
and  
commitment

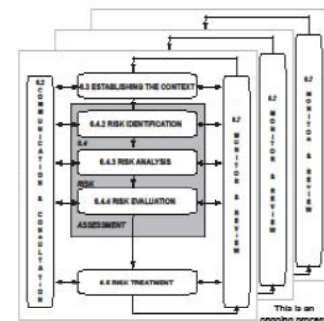
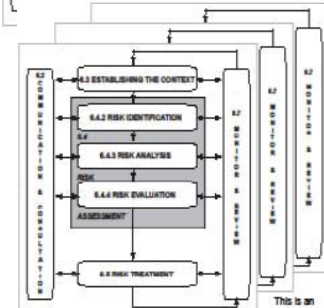
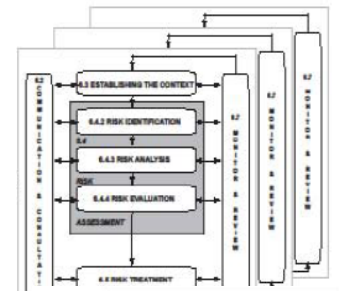
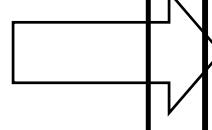
5.3  
Design of  
framework  
for managing  
risk

5.6  
Continual  
improvement  
of the  
framework

5.4  
Implementing  
risk  
management  
framework

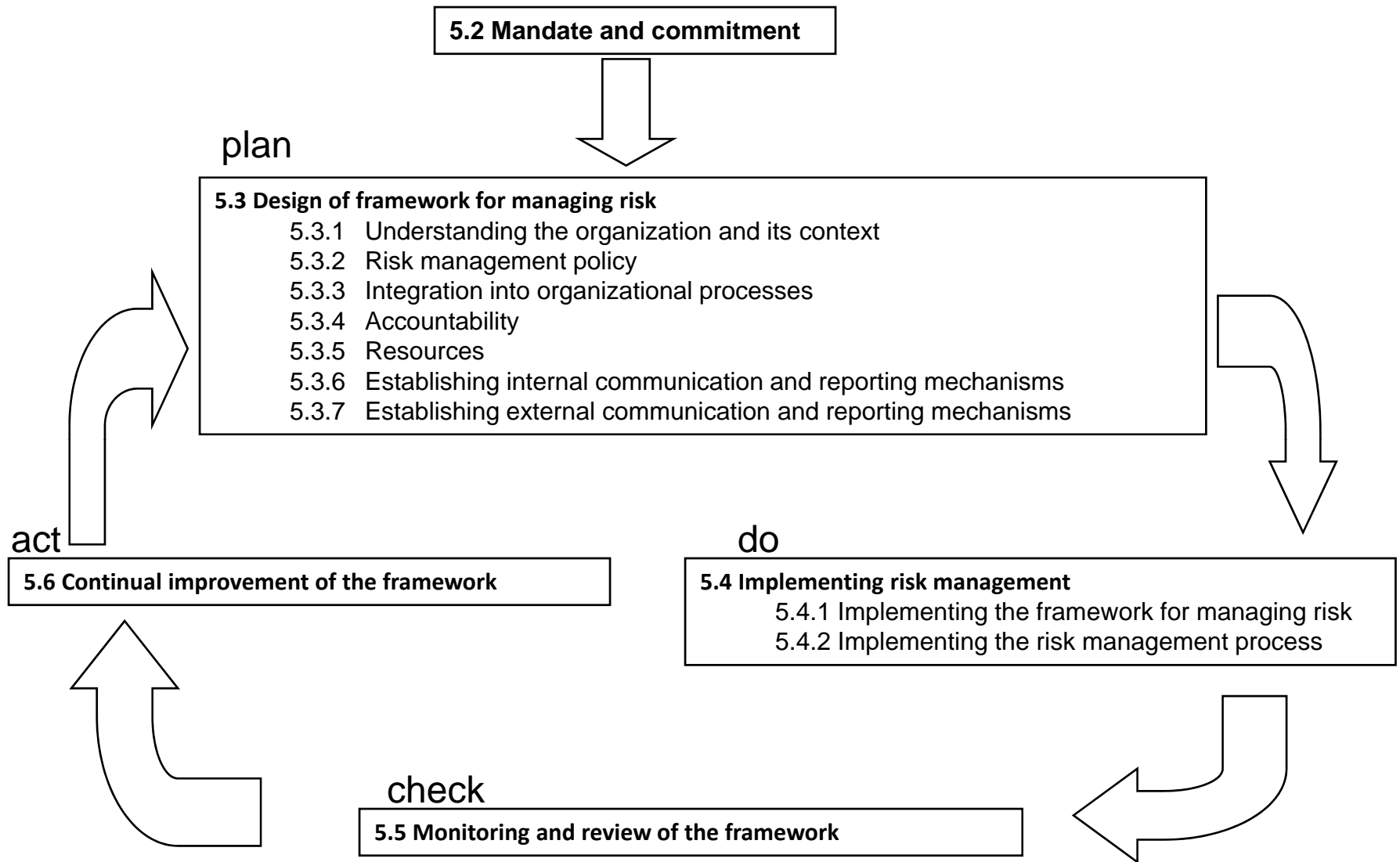
5.5  
Monitoring  
and review  
of the  
framework

**Framework for managing risk**  
**(Clause 5)**



**Processes for managing risk**  
**(Clause 6)**





Continuous Improvement of the ISO 31000 Framework for risk management

## Key components Workshop Risk Management Framework

discuss, rate organization out of 14 as follows

- Proclaimed commitment & policy (2)
- Framework well known & communicated (2)
- Continuous improvement of framework (2)
- Principles – ½ point each to max of (4)
- Champion and implementation plan (2)
- Framework facilitated by a small risk group of 2-4 people, with processes and application the responsibility of managers in every unit in the organization's hierarchy (2)

## Key components Workshop Integrated Risk Management

discuss, rate organization out of 6

- Integrated approach to all risk silos from strategic to new projects to workplace safety (2)
- Integrated risk management by individual managers with other aspects of decision making, oversight of activities, etc. Not a separate task (2)
- Risk management considered a core activity, referred to in annual reports, major topic in strategic and all decisions, etc. Opportunity focus as well as prevention of negative risks (2)

Key components Workshop – Terminology/concepts  
discuss, have a term for \_\_\_\_\_ 5 (bonus points)  
may currently use other than ISO 31000 terms

- risk is “impact of uncertainty on objectives”, must be either positive or negative (1)
- risk management framework for whole organization (1)
- risk management process for individual manager everywhere in organization (1)
- risk control as result of risk treatment, it is basis for risk owner’s actions to modify risk (1)
- context, internal and external as the source of objectives, and risk criteria used in risk evaluation (1)

*please see next slide for full list of 31000 terms*

**Terms in  
ISO 31000  
& Guide 73**

**risk management**-coordinated activities to direct and control an **organization** with regard to risk

<b><u>risk management policy</u></b>	<b><u>external context</u></b>	<b><u>internal context</u></b>	<b><u>risk profile</u></b>
<b><u>risk management framework</u></b>	<b><u>risk management plan</u></b>	<b><u>risk appetite</u></b>	<b><u>risk attitude</u></b>
<b><u>risk owner</u></b>	<b><u>risk management audit</u></b>	<b><u>exposure</u></b>	<b><u>resilience</u></b>

- risk** – effect of uncertainty on objectives
- event**
- consequence**
- likelihood**
- uncertainty**
- probability**
- frequency**
- level of risk**
- risk source**
- hazard**
- vulnerability**

**risk evaluation**-process of comparing the results of risk analysis against risk criteria to determine whether the level of risk is acceptable or tolerable (**part of risk management process**)

<b><u>risk criteria</u></b>	<b><u>risk tolerance</u></b>	<b><u>risk aversion</u></b>
<b><u>risk matrix</u></b>	<b><u>risk aggregation</u></b>	

**stakeholder** those people and organizations who can affect, be affected by, or perceive themselves to be affected by a decision or activity

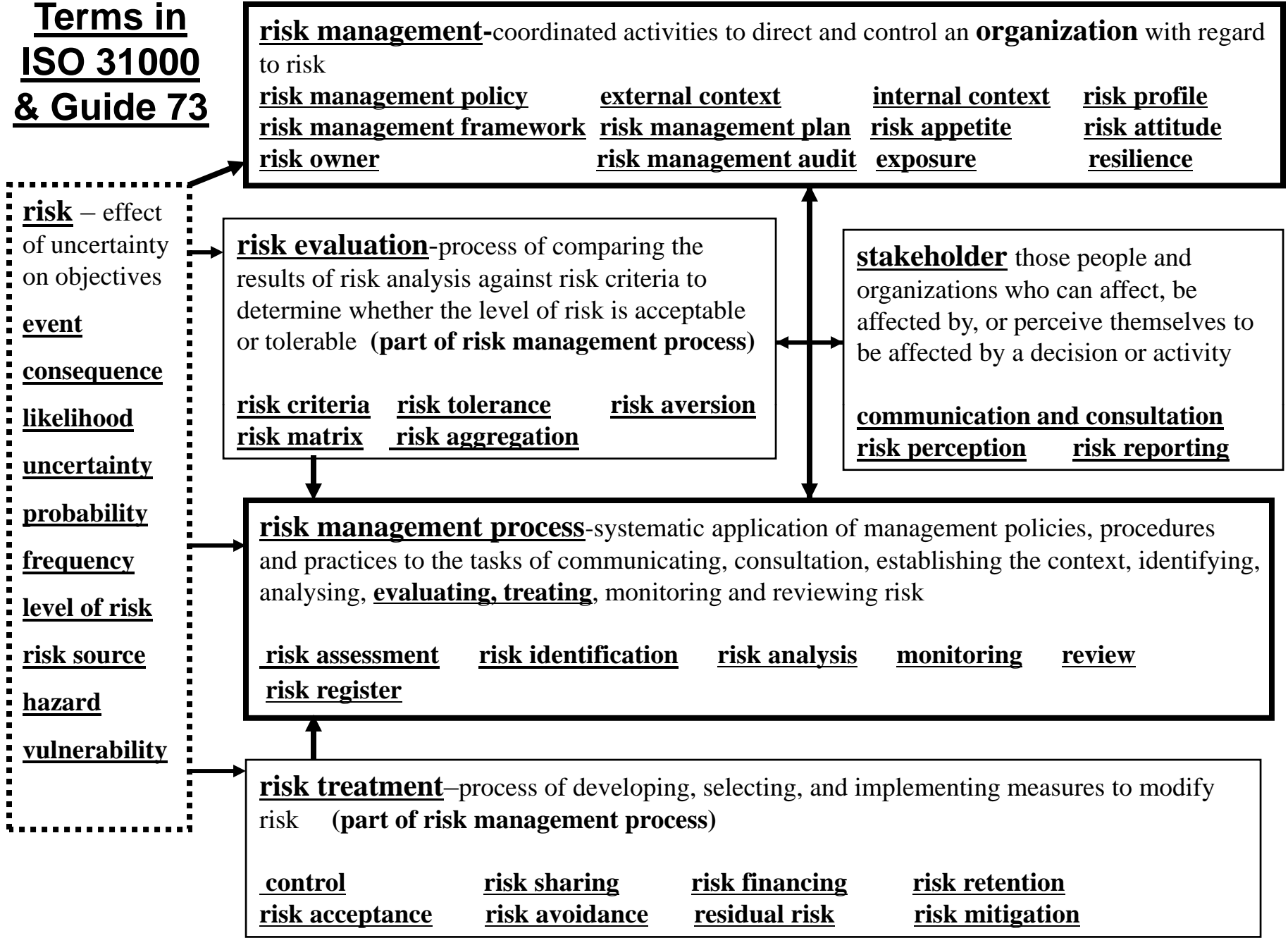
**communication and consultation**  
**risk perception**      **risk reporting**

**risk management process**-systematic application of management policies, procedures and practices to the tasks of communicating, consultation, establishing the context, identifying, analysing, **evaluating**, **treating**, monitoring and reviewing risk

<b><u>risk assessment</u></b>	<b><u>risk identification</u></b>	<b><u>risk analysis</u></b>	<b><u>monitoring</u></b>	<b><u>review</u></b>
<b><u>risk register</u></b>				

**risk treatment**-process of developing, selecting, and implementing measures to modify risk (**part of risk management process**)

<b><u>control</u></b>	<b><u>risk sharing</u></b>	<b><u>risk financing</u></b>	<b><u>risk retention</u></b>
<b><u>risk acceptance</u></b>	<b><u>risk avoidance</u></b>	<b><u>residual risk</u></b>	<b><u>risk mitigation</u></b>



# **Broadleaf Capital's 10 point approach to Implementation of Risk Management**

*If Time topic* - Continued on next slide with 10 steps for implementation

## Approach Rational

Rather than use a “design build” contractor with a pre-packaged approach to ERM it is preferred to have a consultant who partners with the organization in developing a customized framework, tools and methods that reflect the organization’s needs, risk profile, and organization structure. Risk management champions are found within the organization and trained to implement and roll out the framework in a top-down engagement process.

This seems to achieve the most rapid take-up and long term ownership of risk management in the organization, by working with the organisation’s line managers and risk management specialists, and building on their skills and experience risk management processes are more relevant to business needs and this also creates early and visible risk management benefits.

([Purdy@broadleaf.com.au](mailto:Purdy@broadleaf.com.au)) for more information

## Broadleaf's 10 point approach to implementation of RM

1. Achieve an unequivocal Executive and Board mandate with a full appreciation of the changes required at all levels of the organisation.
2. Undertake a gap analysis and maturity evaluation.
3. Develop a carefully tailored framework, based on ISO 31000 risk management framework, principles, and process as well as the organisation's context and structure necessary for ERM to be implemented and sustained.
4. Workshop and develop a strategic risk management plan to implement the framework utilizing practical tools and best practice methods
5. Develop and gain senior management agreement on a set of performance-base standards to codify the framework and its implementation plan.
6. Create a tailored risk management information system, that enforces accountability for risks, controls and tasks, supports control assurance and enables risk management performance management and reporting.
7. Cause Champions to be appointed within the organisation and trained to create the confidence, skills and local management support needed for roll-out
8. Help Champions engage local management and implement the framework and risk management plan, generating risk registers, etc.
9. Establish a process and structure for RM performance management and reporting, including committees and review groups, and performance measures.
10. Periodically, review, benchmark, and revise the framework.

Questions please

20 sec questions

30 sec answers

Also ask

[shorttree@uwaterloo.ca](mailto:shorttree@uwaterloo.ca)