BROADLEAF CAPITAL INTERNATIONAL PTY LTD

ABN 24 054 021 117

23 Bettowynd Road
Pymble
NSW 2073
Australia

www.Broadleaf.com.au

Tel: +61 2 9488 8477
Mobile: 0419 433 184
Fax: + 61 2 9488 9685
Cooper@Broadleaf.com.au

Specialists in Strategic, Enterprise and Project Risk Management

Cura Webcast on ISO 31000, 10 December 2008

1 Introduction

Grant Purdy, an Associate Director of Broadleaf, featured in a live web-based briefing about the new ISO 31000 Risk Management standard on 10 December 2008. The briefing was hosted by risk management software solutions provider Cura and attended by over 100 delegates worldwide.

This note contains the Cura white paper with a synopsis of the questions raised and the answers given during the presentation, as well as the PowerPoint slides that were used.

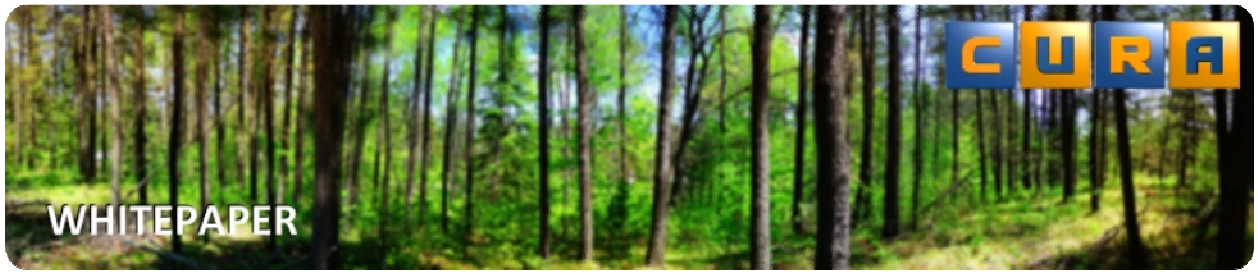
2 Broadleaf's Services in Implementing ISO 31000:2009

Broadleaf is working with many large organisations in the development and implementation of approaches to risk management that comply with ISO 31000:2009. We help organisations to achieve and sustain tailored approaches to risk management that suit them and that can adapt as their structure and strategic objectives change.

We are particularly conversant with current risk management thinking: three of our team are members of the committee that wrote AS/NZS 4360 and one is a nominated expert to the ISO Working Group that wrote ISO 31000:2009 and ISO/IEC Guide 73:2009.

Our practical experience base is unique. Our many service offerings include:

- Risk management planning;
- Gap and maturity analysis against ISO 31000:2009;
- Framework development;
- Policy, Standard and Guideline drafting;
- Risk management information system specification, procurement and deployment;
- Risk assessment facilitation;
- Development and delivery of risk management training;
- Risk based audit and assurance planning;
- Risk management performance management;
- Governance reporting and assurance;
- Risk management framework benchmarking and review;
- Training and mentoring of risk management specialists in all aspects of risk management and its implementation.



ISO 31000: The New Global Risk Management Standard

As part of Cura's continuing Executive Briefing Series on Enterprise Risk Management, we hosted a live Web based presentation and open Q&A session on December 10, 2008 for our clients and friends. This month's session featured Mr. Grant Purdy, a nominated expert on the ISO working group which recently wrote ISO 31000, the new global standard for Risk Management.

Developed in concert over the last 3½ years by over 30 ISO member organizations worldwide, ISO 31000 is arguably the most concise, clear, flexible set of guidelines ever developed for risk management. Mr. Purdy discussed with our audience how ISO 31000 represents a durable, flexible framework for developing a solid risk management culture in all forms and sizes of organizations.

Incidentally, in our experience, we have never seen a more lively, attentive and engaged online audience for any topic like we had for this one. Officials from a broad array of industries were treated to a thoroughly informative dialogue. Here we present some of the fascinating highlights of the Q&A session with Mr. Purdy and our audience. We hope you find it helpful.

Q: How has our understanding of risk and how to manage it changed?

GP: The way we think about risk and how we define it has changed greatly over the last 30 years. Even today, some professions and organizations define risk almost strictly in terms of adverse events, hazards and negative outcomes. Over the most recent decade, and exemplified in one of the most broadly adopted current standards, the Australia/New Zealand (AS/NZ) 4360, the definition has broadened to: "The chance of something happening that will have an impact on objectives." Now, with ISO 31000, we have defined Risk as: "Effect of uncertainty on objectives." Risk is simply concerned with the juxtaposition between objectives and the factors of the environment (both internal and external to the organization) in which they are pursued.

In the past risk has been equated solely with hazardous events and was often regarded as something that you tried to transfer away. Now we appreciate that risk is inherent to business and life and that you need to take risk to prosper, derive benefit and obtain enjoyment. Transferring risks is not easy and is often not the most cost effective form of risk treatment as in most cases you just get a different type of risk transferred back. This is why we call that approach to risk treatment 'risk sharing' – which is really just a way to change consequences. Risk is about the uncertainty inherent in any worthwhile endeavor, in whatever we want to achieve. Risk should not be described as either negative or positive, but the consequences can be positive and/or negative – it all just depends on your point of view. The context for risk is always our objectives – what we seek to achieve and therefore, critically, to be effective risk management must be regarded by senior managers as essential for the achievement of the organization's objectives. Managers must be proficient in the management of risk to ensure that their organization achieves that which it sets out to do.

Q: What differentiates ISO 31000 from other standards?

GP: I've worked in risk management for over 32 years, and have seen a considerable evolution in standards. Some were risk silo-specific, some have been written just to suit particular agendas or specific legislative environments. The Australian and New Zealand Risk Management Standard AS/NZS 4360 has existed for 13 years now and has become a de facto global standard used by many thousands of organizations of all shapes and sizes around the world. We have revised that standard on three occasions taking into account all the practical lessons learnt in the many organizations that have based their approach to risk management on it. ISO 31000 is based on AS/NZS 4360:2004 but has been improved further by the risk management experts representing over 30 countries on the ISO working group. The resulting set of guidelines are authoritative, a paramount standard of the same standing as ISO 9000 or 14000, which is applicable to all types of risks and to all types and sizes of organizations – from small non-profit to complex global corporations.

Q: Describe some features of the ISO 31000 Standard that make it so appealing?

GP: The ISO standard is succinct comprising only about 20 or so pages. It represents an easier, more accessible, more immediately applicable document. The standard not only describes the core, stepwise risk management process but precedes this with a practical guide as to how risk management should be established within the organization and integrated with its key processes to ensure that it is successful and so that it is sustained and remains relevant and appropriate to the organization, its context and its needs. The standard is associated with a standard vocabulary of terms whose adoption is mandated by all standards writers throughout the world. For once, we will now all have one set of definitions and one simple approach to the implementation and practice of risk management.

Q: Is there a certification process?

GP: No. The standard has been written so that you cannot certify against it. This is specifically precluded in the scope of the standard. The reason for this is that the experts on the working group felt that organizations should not waste their efforts just seeking to gain a certificate. As the first principle of good risk management given by the standard says: risk management must add value. Certification can lead to a 'compliance culture' attitude to managing risk and we know that this is very detrimental, dilutes ownership and accountability, and significantly reduces the effectiveness of the risk management process.

Q: What are the key take-aways for companies?

GP: ISO 31000 will be a natural and worthy successor to legacy standards like that from Australia and New Zealand. It will fit ERM (Enterprise Risk Management) requirements, but also will allow silo/project risk management if that is what you want to do. In the spirit of risk management being concerned with the seeking and realization of opportunity (as well as the avoidance of loss) organizations should now start planning how they will benefit most from the new standard. They should start now and use the draft standard as an opportunity to benchmark their current approaches to risk management and develop their risk management improvement plans. I am convinced that ISO 31000 will help organizations treat the risk in risk management.

Q: If companies want to get acquainted with ISO 31000, what is the best way to go about it?

GP: Get a copy of the draft Standard and Guide from the ISO31000 Downloads at http://www.curasoftware.com/Downloads/ISO31000-Draft.pdf . Contact Cura for the accompanying Guide. Compare your approach to risk management against the Principles of Good Risk Management (Clause 4) and the Attributes in the Annex. See if your framework matches that described in Clause 5 and see if your risk management process follows Clause 6. If not, create a risk management plan! You probably won't find a more effective model, whatever your goals, needs or risk appetite.

About Grand Purdy

Grant Purdy is an Associate Director of Broadleaf Capital International. Grant has specialized in the practical application of risk management for over 30 years, working across a wide range of industries and in many countries. He is a recognized expert on enterprise and strategic risk management, specializing in the tactics for the take-up, customization and embedding of 'bespoke' risk management frameworks and systems. Prior to working with Broadleaf, Grant was manager of risk management for BHP Billiton, the world's largest resource company. He led the team that implemented a global ERM framework that is recognized as world best practice in the resources sector.

Grant is Chairman of the Standard Australia and Standards New Zealand Risk Management Committee responsible for the Risk Management Standard AS/NZS 4360 and co-author of the 2004 version of the Standard and the associated Handbooks of best practice. He is the nominated expert representing Australia in the ISO Working Group on Risk Management

About Cura Software

Cura software solutions enable businesses around the world to quickly achieve the bottom line benefits of enterprise-wide governance, risk management and compliance (GRC), coupled with performance management. Cura does this through fast implementation, easier configurability and true enterprise architecture.

Cura is used by over 200 customers such as BHP Billiton plc, Westfield, Allianz, Old Mutual plc, GlaxoSmithKline, Standard Bank, Virgin Blue, Vodacom, as well as governments and consulting firms world-wide. Cura has offices in New York, London, Sydney, Melbourne and Johannesburg, and has distributors in 10 countries (South America, Middle East and Asia). For more information, visit http://www.CuraSoftware.com .

About Cura's Executive Briefing Series

This series has been recognized as a leading resource for Risk Management dialogue worldwide. If you would like to join the invitation list, contact Ed Alexander, Director, Client Development at eda@curasoftware.com .


CURA
CURA WEBINAR SERIES
Speakers
Grant Purdy – Associate Director, Broadleaf
Avi Eyal – CEO, Cura Software Solutions
Host: Ed Alexander
Please use Q&A panel on Webex to submit questions
The Smarter Choice in Governance, Risk and Compliance Software Solutions


Broadleaf
CURA
software solutions
ISO 31000:2009
treating the risk in risk management
Grant Purdy
Associate Director
Chair Standards Australia and Standards New Zealand
Risk Management Committee
Nominated Expert ISO TMB Risk Management Working Group
© Broadleaf Capital International Pty Ltd, 2008
www.Broadleaf.com.au

Broadleaf

CURA software solutions

Risk – the changing definition

"Measurable uncertainty"

Risk Uncertainty and Profit; Frank Knight, 1921

"Probability that a particular adverse event occurs during a stated period of time, or results from a particular challenge."

Royal Society Study Group on Risk Assessment, 1983

"Chance of something happening that will have an impact upon objectives"

AS/NZS 4360:1995

"Combination of the probability of an event and its consequences"

ISO/IEC Guide 73:2002

 www.Broadleaf.com.au 3

Broadleaf

CURA software solutions

Perceptions of risk

Risk is bad! – associated with "hazards"

Risk is something you try to transfer!

There are risks that have upsides and downsides ("*speculative*") and those that only have downsides ("*pure*")

Risk is inherent in business (and life)

You need take risks to make money (and to live)

Risks are about uncertainty in what we want to achieve

 www.Broadleaf.com.au 4

Broadleaf

CURA software solutions

Current views

- Risk is not just about events. It is also associated with situations and circumstances.
- Risk is associated with uncertainty in what we want to achieve
- Risk is not negative or positive
- The consequences can be positive and/or negative – it all depends on our point of view!
- The context for risk is always our objectives

 www.Broadleaf.com.au 5

Broadleaf

CURA software solutions

Risk (the new definition)

"effect of uncertainty on objectives"

ISO 31000:2009, ISO/IEC Guide 73:2009

 www.Broadleaf.com.au 6

Broadleaf

CURA software solutions

Control (the new definition)

"measure that is modifying risk"

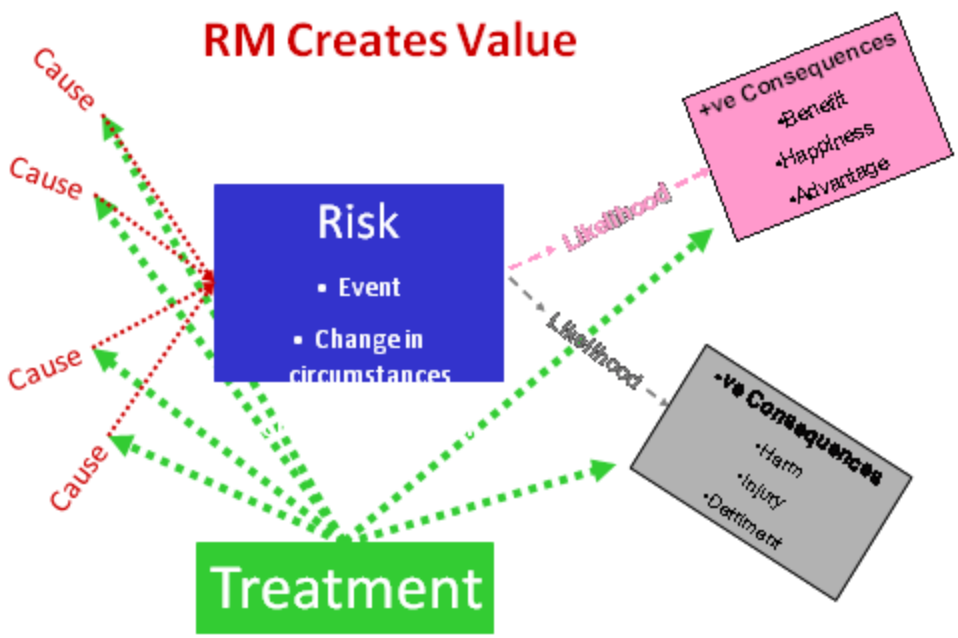
ISO 31000:2009, ISO/IEC Guide 73:2009

 www.Broadleaf.com.au 7

Broadleaf

CURA software solutions

RM Creates Value



 www.Broadleaf.com.au 8

Broadleaf

CURA software solutions

History of the ISO Standard on Risk Management?

ISO

1. Over 60 separate ISO and IEC committees address aspects of risk management
2. 27th June 2002, ISO "Guide 73, Risk Management - Vocabulary"
3. ISO TMB
   - 2004, approached by Australia and Japan
   - AS/NZS 4360:2004 to be adopted by ISO?
4. June 2005, TMB sets up WG
   - Standard for the harmonisation of other standards
   - 6 Meetings so far, final was in November 2008
   - ISO WG should also re-write Guide 73
   - ISO 31000 will be a paramount standard
5. ISO 31000 and Guide 73 published in 2009

 www.Broadleaf.com.au 9

Broadleaf

CURA software solutions

Status of ISO 31000 and Guide 73

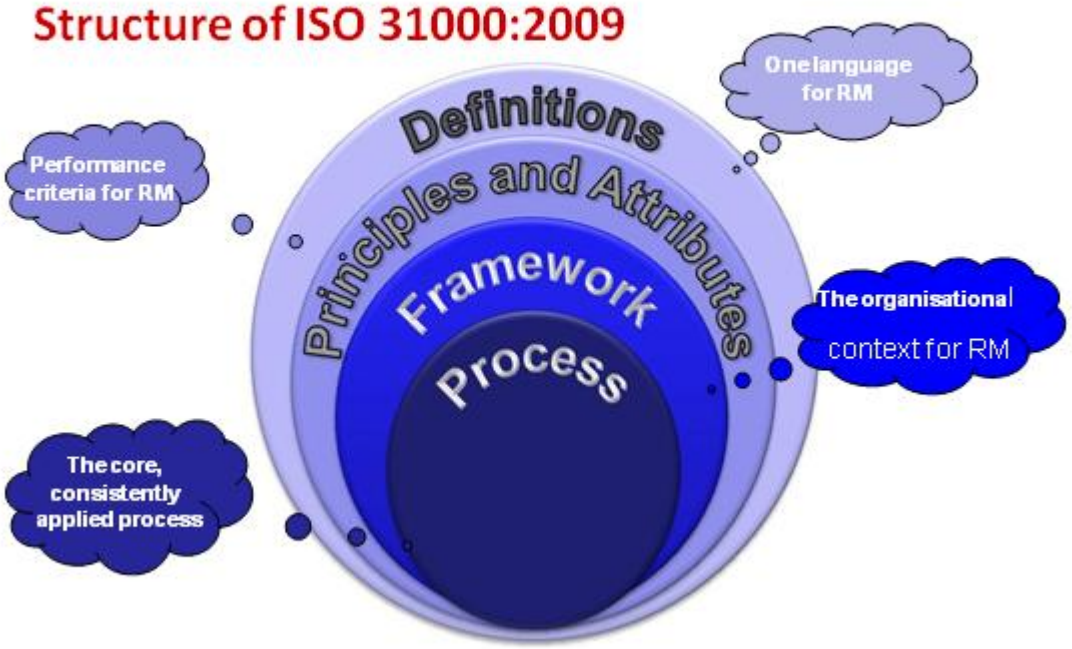
- Next, final version of standard is "FDIS"
- International vote on DIS 31000 and Guide 73
  - Passed at 90%
  - Only USA, Belgium and Italy voted against
- Final meeting of Working Group
  - 24-28th November 2008 in Singapore
- FDIS is to be published early next year which goes to a final vote before publication

 www.Broadleaf.com.au 10

Broadleaf

CURA software solutions

Structure of ISO 31000:2009



 www.Broadleaf.com.au 11

Broadleaf

CURA software solutions

Principles (Clause 4)

risk management should....

1. Create value
2. An integral part of organisational processes
3. Part of decision making
4. Explicitly address uncertainty
5. Be systematic and structured
6. Be based on the best available information
7. Be tailored
8. Take into account human factors
9. Be transparent and inclusive
10. Be dynamic, iterative and responsive to change
11. Be capable of continual improvement and enhancement

 www.Broadleaf.com.au 12

Broadleaf

CURA software solutions

Annex A – Attributes of excellence in risk management

1. A **pronounced emphasis on continuous improvement** in risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources and capability/skills.
2. **Comprehensive, fully defined and fully accepted accountability** for risks, controls and treatment tasks.

   Named individuals fully accept, are appropriately skilled and have adequate resources to check controls, monitor risks, improve controls and communicate effectively about risks and their management to interested parties.

 www.Broadleaf.com.au 13

Broadleaf

CURA software solutions

Annex A – Attributes of excellence in risk management

3. **All decision making within the organization**, whatever the level of importance and significance, involves the explicit consideration of risks and the application of the risk management process to some appropriate degree.
4. **Continual communications** and highly visible, comprehensive and frequent reporting of risk management performance to all "interested parties" as part of a governance process.

 www.Broadleaf.com.au 14

Broadleaf

CURA software solutions

Annex A – Attributes of excellence in risk management

5. **Risk management is always viewed as a core organizational process** where risks are considered in terms of sources of uncertainty that can be treated to maximize the chance of gain while minimizing the chance of loss.

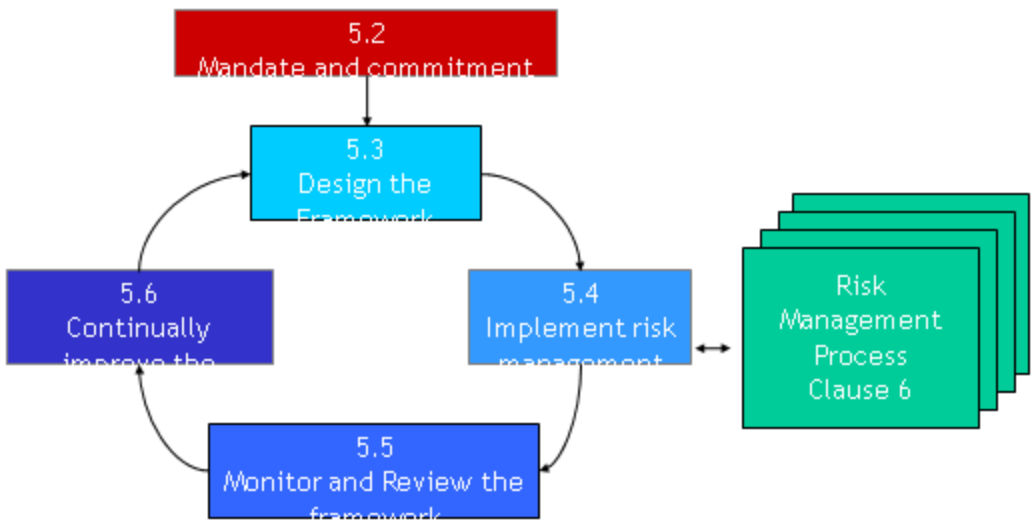
   Critically, effective risk management is regarded by senior managers as essential for the achievement of the organization's objectives. The organization's governance structure and process are founded on the risk management process.

 www.Broadleaf.com.au 15

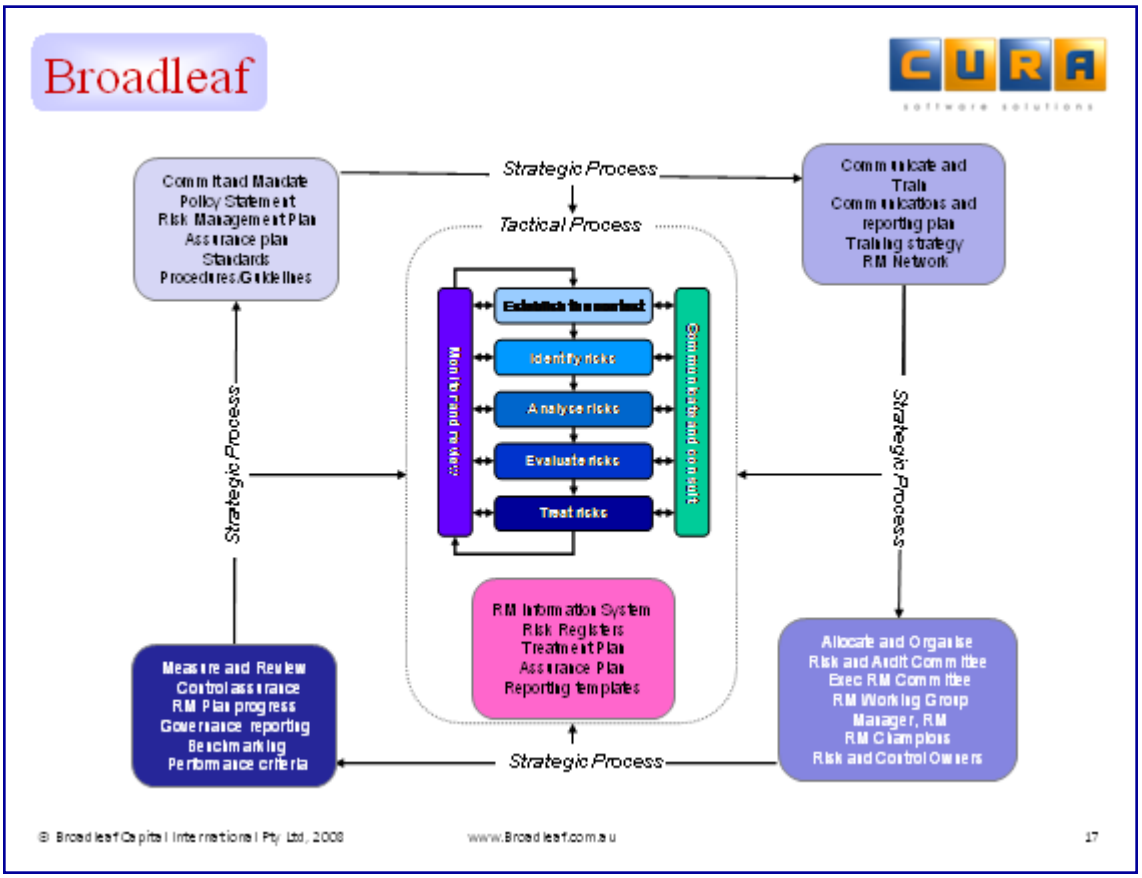
Broadleaf

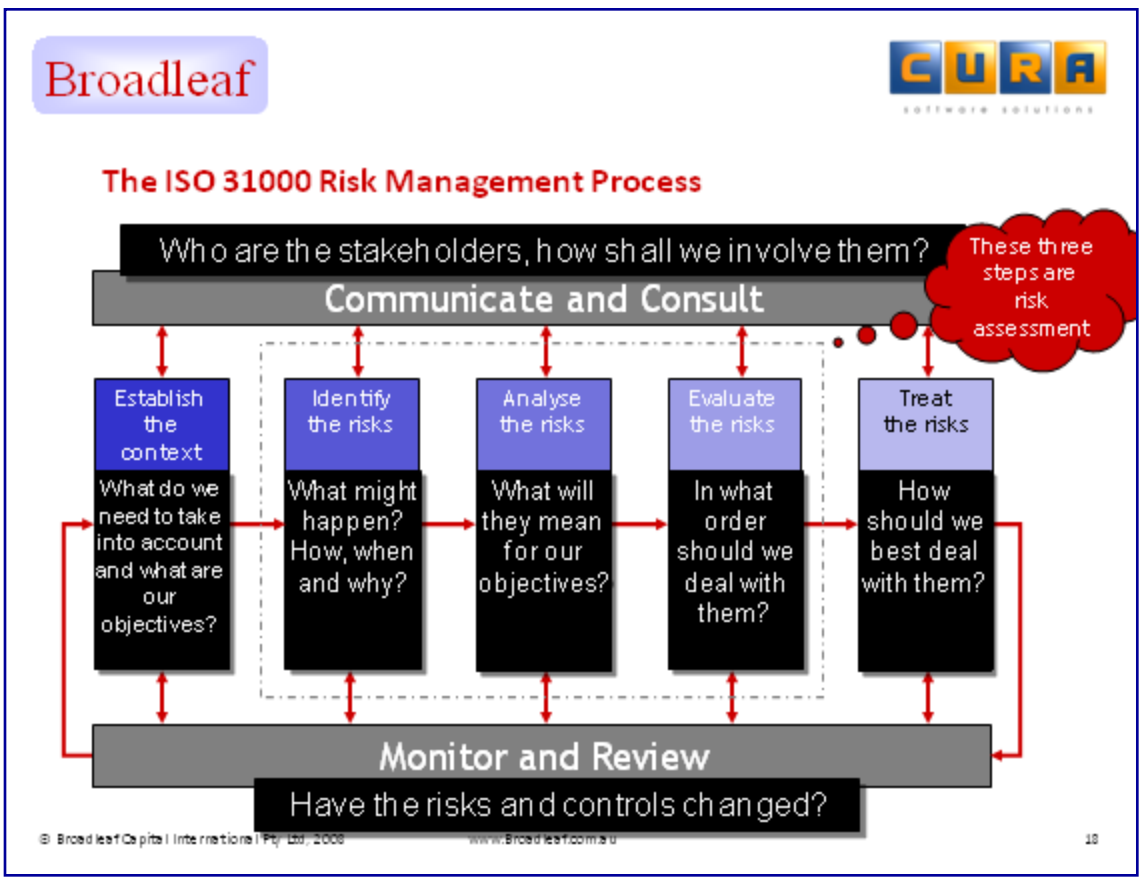
CURA software solutions

ISO 31000 Framework for Managing Risk



 www.Broadleaf.com.au 16


Broadleaf
CURA
software solutions
Commit and Mandate
Policy Statement
Risk Management Plan
Assurance plan
Standards
Procedures/Guidelines
Strategic Process
Tactical Process
Communicate and Train
Communications and reporting plan
Training strategy
RM Network
Establish the context
Identify risks
Analyse risks
Evaluate risks
Treat risks
Monitor and review
Communicate and consult
Strategic Process
Strategic Process
RM Information System
Risk Registers
Treatment Plan
Assurance Plan
Reporting templates
Measure and Review
Control assurance
RM Plan progress
Governance reporting
Benchmarking
Performance criteria
Strategic Process
Allocate and Organise
Risk and Audit Committee
Exec RM Committee
RM Working Group
Manager, RM
RM Champions
Risk and Control Owners
© Broadleaf Capital International Pty Ltd, 2008
www.Broadleaf.com.au
17


Broadleaf
CURA
software solutions
The ISO 31000 Risk Management Process
Who are the stakeholders, how shall we involve them?
Communicate and Consult
These three steps are risk assessment
Establish the context
What do we need to take into account and what are our objectives?
Identify the risks
What might happen? How, when and why?
Analyse the risks
What will they mean for our objectives?
Evaluate the risks
In what order should we deal with them?
Treat the risks
How should we best deal with them?
Monitor and Review
Have the risks and controls changed?
© Broadleaf Capital International Pty Ltd, 2008
www.Broadleaf.com.au
18

Broadleaf

CURA software solutions

What can you do now?

1. Get a copy of the draft Standard and Guide
2. Compare your approach to risk management to the Principles (Clause 4) and Attributes (Annex)
3. See if your framework matches that described in Clause 5
4. See if your risk management process follows Clause 6
5. If not, create a risk management plan!

 www.Broadleaf.com.au 19

Broadleaf

CURA software solutions

ISO 31000 and Guide 73 – Treating the Risk in Risk Management

- Avoid organisations re-inventing the wheel
  - And consultants doing it for them!
- Allow all to benefit from proven best practice
- Practical and clear (~20 pages)
- Provide a universal benchmark and a universal vocabulary
- Reduce barriers to trade
- Advise exactly what you need to do and how you need to do it – no wasted effort and no false starts
- Scalable – works for all sizes of organisation

 www.Broadleaf.com.au 20

Broadleaf

Conclusions

- ISO 31000 will be a natural successor to legacy standards
- It will fit 'ERM' requirements, but also will allow silo/project risk management if that is what you want to do
- You need to start planning now how you will adopt the new standard
- Use it as an opportunity to benchmark your risk management and develop your improvement plan
- ISO 31000 will treat the risk in risk management

 www.Broadleaf.com.au 21

Broadleaf

Uncertainty is the human paradox:

we fear it, but we need it!

 www.Broadleaf.com.au 22


CURA
CURA WEBINAR SERIES
ISO 31000 – The New Risk Standard
For more information visit:
www.curasoftware.com
or e-mail:
eda@us.curasoftware.com
The Smarter Choice in Governance, Risk and Compliance Software Solutions