Applying ISO 31000:2009 in Regulatory Work

Kevin W Knight *AM*
CPRM; Hon FRMIA; FIRM (UK); LMRMIA.

CHAIRMAN
ISO PROJECT COMMITTEE 262 - RISK MANAGEMENT

MEMBER
STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND
JOINT TECHNICAL COMMITTEE OB/7 – RISK MANAGEMENT

P 0 BOX 226, NUNDAH Qld 4012, Australia
E-mail: kknight@bigpond.net.au

Managing Risk

- **We all manage risk consciously or unconsciously**
  - but rarely systematically
- **Managing risk means forward thinking**
- **Managing risk means responsible thinking**
- **Managing risk means balanced thinking**
- **Managing risk is all about maximising opportunity and minimising threats**
- **The risk management process provides a framework to facilitate more effective decision making**

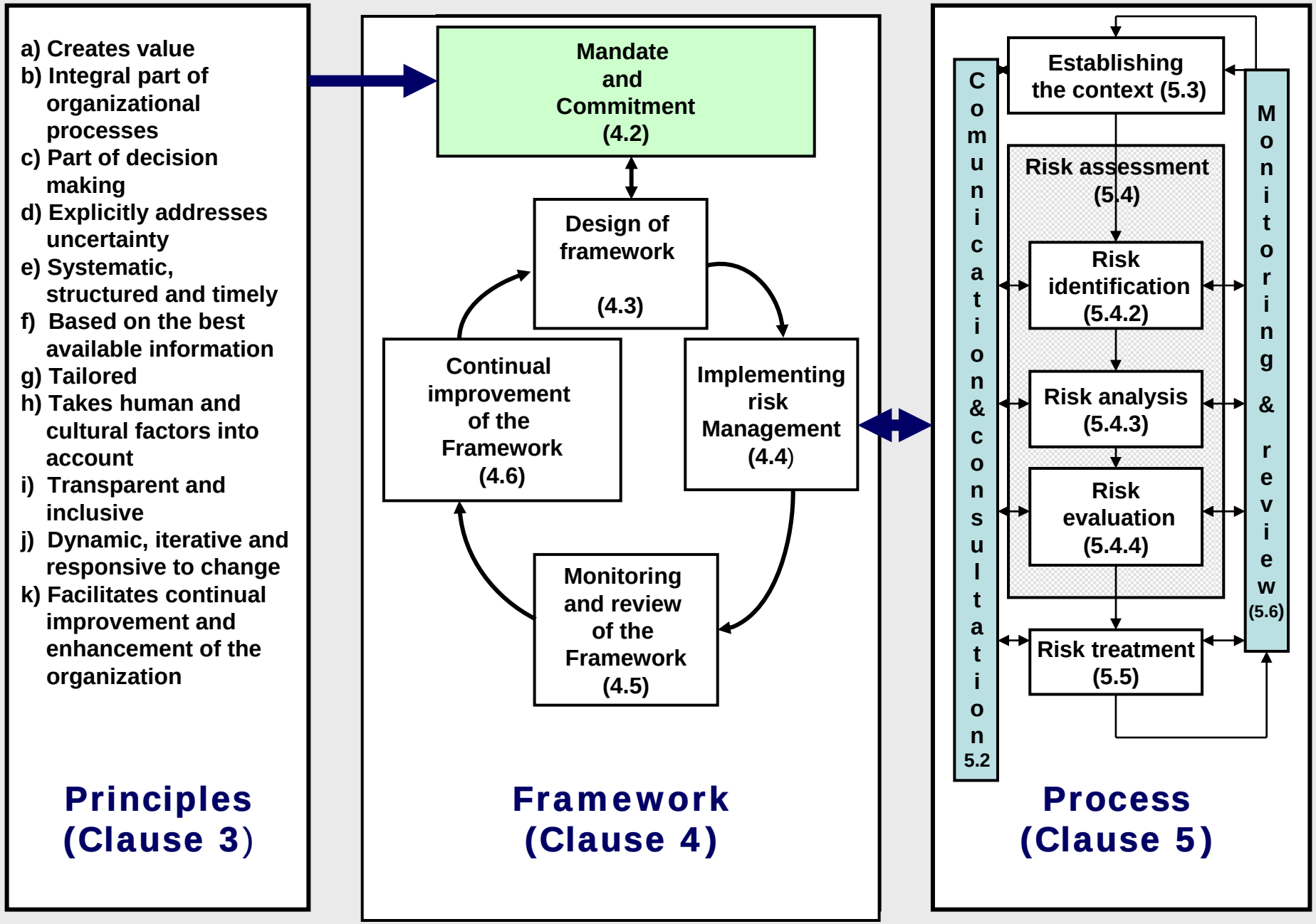
The Pivotal Definition

risk

effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected — positive and/or negative.
NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
NOTE 3 Risk is often characterized by reference to potential events and consequences, or a combination of these.
NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

[ISO Guide 73:2009]



ISO 31000:2009 Figure 1 – Relationship between the principles, framework and process

Business Principles Approach

ISO 31000:2009 Principles (Clause 3)

Risk management should….

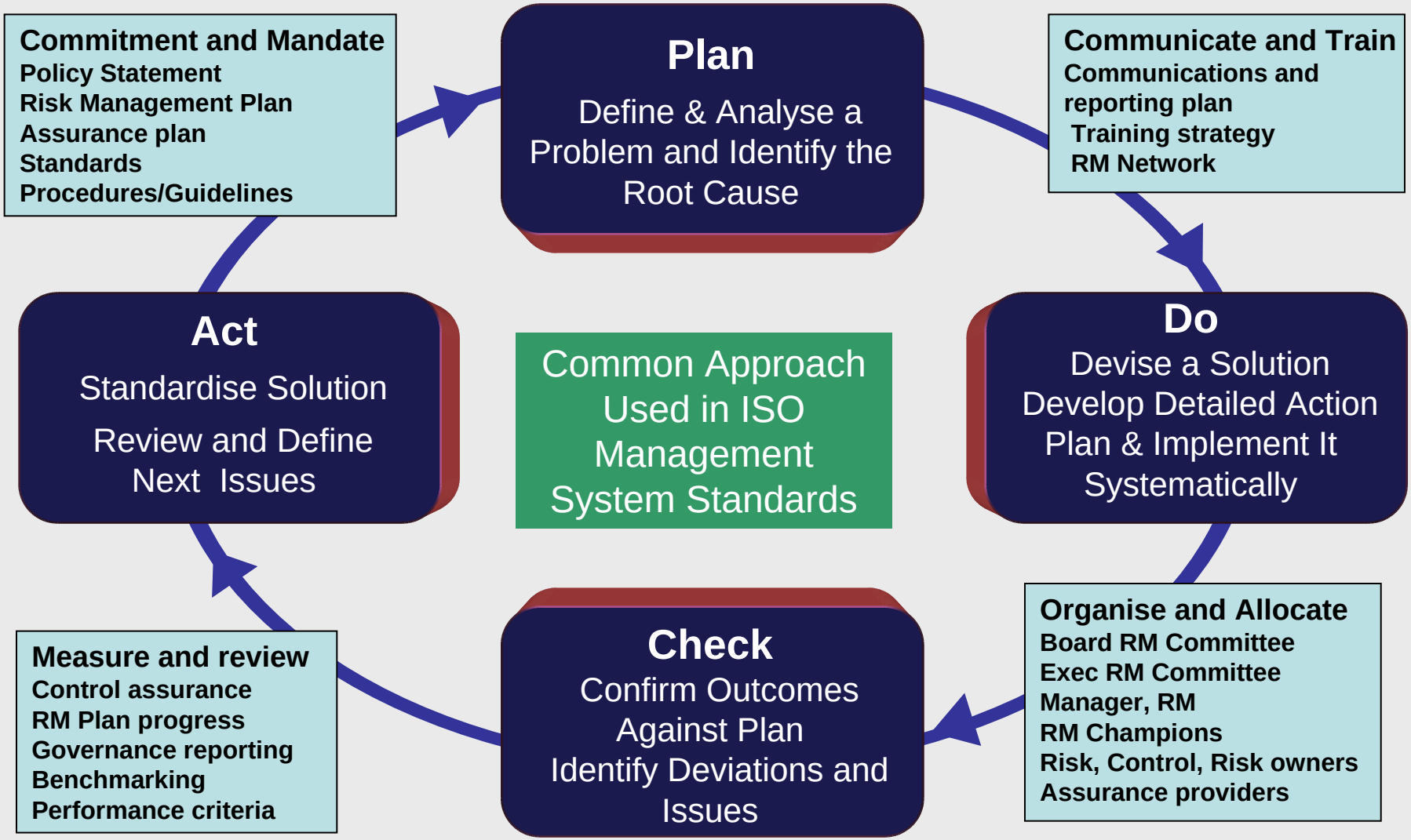
1. Create value
2. Be an integral part of organisational processes
3. Be part of decision making
4. Explicitly address uncertainty
5. Be systematic and structured
6. Be based on the best available information
7. Be tailored
8. Take into account human factors
9. Be transparent and inclusive
10. Be dynamic,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

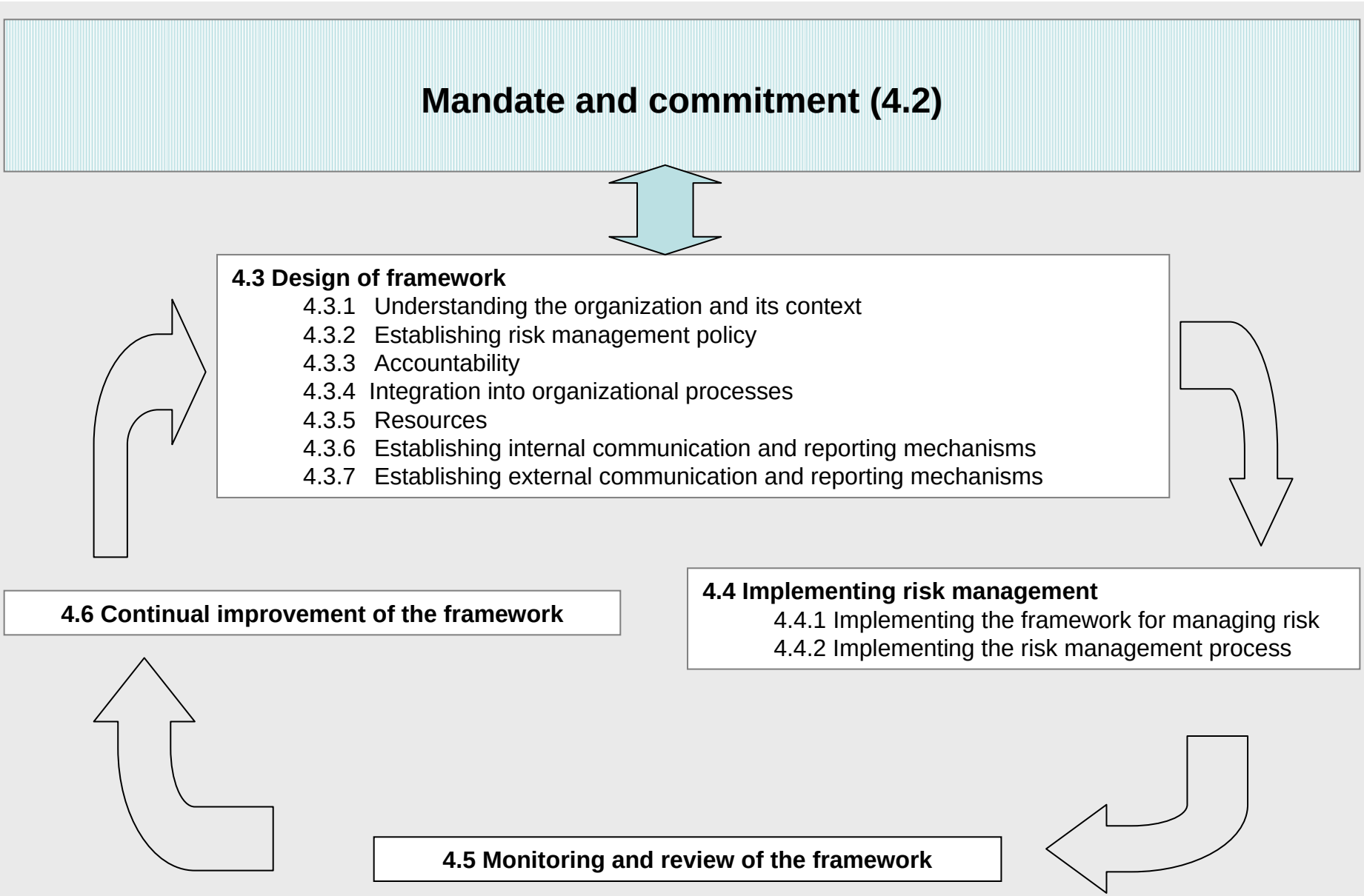
ISO 31000:2009 Risk management framework (Clause 4)

- **The framework in Clause 4 of ISO 31000:2009 is not intended to describe a management system; but rather, it is to assist the organization to integrate risk management within its overall management system.**

- **Therefore, organizations should adapt the components of the framework to their specific needs.**

PDCA – the starting point of any management system

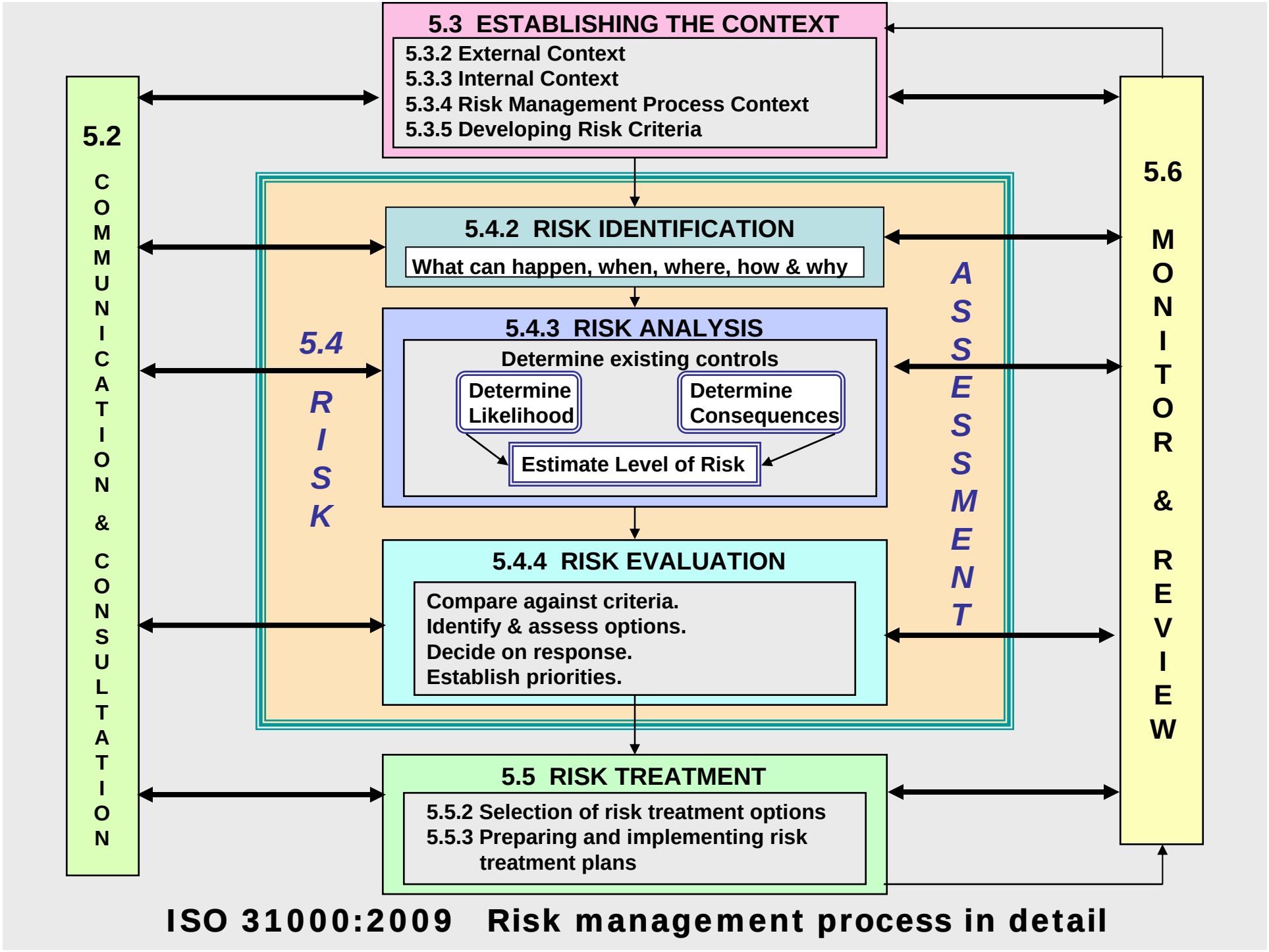




ISO 31000:2009 Figure 2 — Relationship between the components of the framework for managing risk

ISO 31000:2009 Risk management process (Clause 5)

- should be an integral part of management, be embedded in culture and practices and tailored to the business processes of the organization.
- includes five activities: communication and consultation; establishing the context; risk assessment; risk treatment; and monitoring and review.



ISO 31000:2009 Risk management process in detail

ISO / IEC 31010:2009

Risk Management - Risk Assessment Techniques

In particular, those carrying out risk assessments should be clear about

- **the context and objectives of the organization,**
- **the extent and type of risks that are tolerable, and how unacceptable risks are to be treated,**
- **how risk assessment integrates into organizational processes,**
- **methods and techniques to be used for risk assessment, and their contribution to the risk management process,**
- **accountability, responsibility and authority for performing risk assessment,**
- **resources available to carry out risk assessment,**
- **how the risk assessment will be reported and reviewed.**

And Finally!!

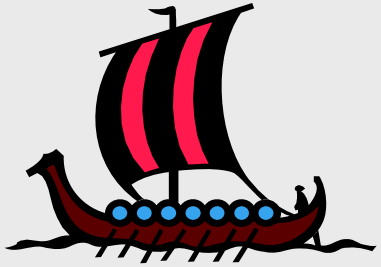
- **ISO 31000:2009 is the natural successor to AS/NZS 4360:2004**
- **Hopefully it will influence a revision of COSO**
- **It will fit 'ERM' requirements, but will also allow silo/project risk management**
- **Following ISO 31000:2009 will provide a low cost, high chance of success approach to ERM**
- **ISO 31000:2009 will add value and reduce risk in risk management**
- **Managing risk is about creating value out of uncertainty**

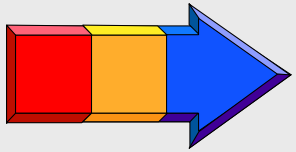
YOU DO NOT HAVE TO MANAGE RISK!!

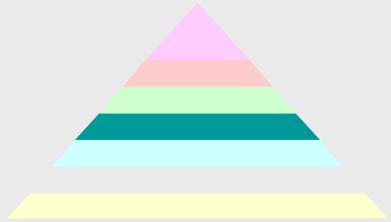
SURVIVAL IS NOT COMPULSORY

The greatest risk of all is to take no risk at all!

The Journey Continues



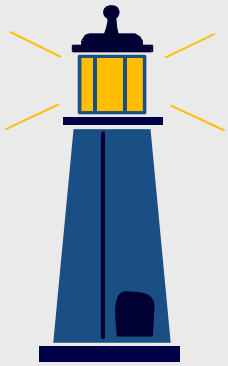




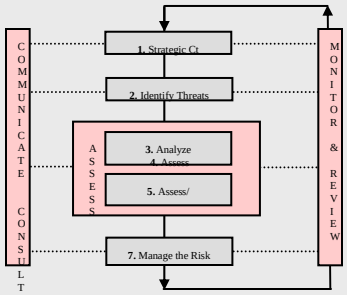
A journey ..... A race

In pursuit of performance Building Value

ISO 31000, ISO / IEC 31010 and ISO Guide 73 provide generic guidance on how to embrace the management of risk in order to maximise the opportunities and minimise the threats to the achievement of your objectives.

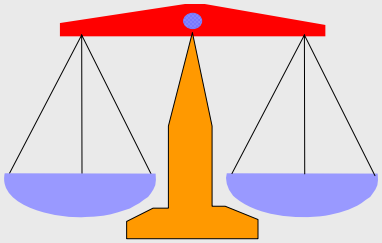


Structure Direction



Processes

Culture Communication



Opportunities Risks

The Next Step on the Journey

- February 2011 ISO/TMB approved the creation of Project Committee 262 - *Risk Management* with the scope of "Standardisation in the field of risk management".
- The Secretariat was allocated to BSI and the Chair to SA. Mr Mick Maghar (UK) and Mr Kevin Knight (Australia) have been appointed as Secretary and Chairman respectively
- The PC was set up to develop ISO 31004 *Risk Management — Guidance for the implementation of ISO 31000.* This standard is to provide implementation guidance to the risk management framework and processes defined in ISO 31000 – *Risk management – Principles and guidance.* This standard is not intended for certification purposes.
- Over 20 National Standards Bodies already indicated participation.
- UNECE is able to apply for liaison status with the PC and attend meetings. The first meeting planned for w/c 12.09.2011

The following documents are available online from: http://infostore.saiglobal.com/store/

ISO 31000:2009 Risk management — Principles and guidelines

ISO Guide 73:2009 Risk management — Vocabulary

ISO/IEC 31010:2009 Ed. 1.0: Risk Management - Risk Assessment Techniques

AS/NZS 5050:2010 Business continuity—Managing disruption related risk

AS 8000-2003 Corporate Governance Standards Set (Contains 8000, 8001, 8002, 8003 & 8004 and associated Handbooks). *Standards Australia*.

SAA HB 158 (Rev):2010 Delivering assurance based on ISO 31000:2009 Risk Management, *Standards Australia*, 16 November 2010

SAA/NZS HB 246 (Rev):2010 Guidelines for Managing Risk in Sport and Recreation, *Standards Australia/Standards New Zealand, 18 August 2010*

SAA HB 266:2010 Guide for managing risk in Not-For-Profit organisations, *Standards Australia,13 August 2010*

SAA/NZS HB 327:2010 Communicating and consulting about risk, *Standards Australia /Standards New Zealand, ISBN 978-0-7337-9346-2, Standards Australia, 2010*

The following Handbooks have been revised to bring them into harmonisation with AS/NZS ISO 31000:2009 and will eventually be available online from:
http://infostore.saiglobal.com/store/

SAA HB 141-201X Risk Financing Guidelines, *Standards Australia*.

SAA/NZS HB 203:201X Environmental risk management – Principals and process, *Standards Australia/Standards New Zealand.*

The following Handbooks are currently being revised to bring them into harmonisation with AS/NZS ISO 31000:2009: -

SAA HB 205-201X OHS Risk Management Handbook, *Standards Australia.*

SAA HB 436-201X Risk Management Guidelines – A Companion to AS/NZS ISO 31000:2009, *Standards Australia/Standards New Zealand.*

The following Handbooks based on the superseded AS/NZS 4360:2004 require revision to bring them into harmonisation with AS/NZS ISO 31000:2009: -

HB 167:2006 - Security risk management, *Standards Australia/Standards New Zealand.*

SAA HB 231:2004 Information Security Risk Management Guidelines, *Standards Australia.*

SAA HB 240-2004 Guidelines for Managing Risk in Outsourcing using the AS/NZS 4360:2004 Process, *Standards Australia.*

SAA HB 254-2005 Governance, risk management and control assurance, *Standards Australia.*

SAA/NZS 221:2004 Business Continuity Management,
Standards Australia/Standards New Zealand.

SAA HB 292:2006 A Practitioners Guide to Business Continuity Management
Standards Australia (2006)

SAA HB 293:2006 An Executive Guide to Business Continuity Management
Standards Australia (2006)

SA HB 296:2007 Legal Risk Management, *Standards Australia (2007), ISBN 0 7337 8295 7.*