TRANSITIONING TO THE NEW RISK MANAGEMENT STANDARD

AS / NZS / ISO 31000:2009

Kevin W Knight AM

CPRM; Hon FRMIA; FIRM (UK); LMRMIA.

CHAIRMAN
ISO WORKING GROUP - RISK MANAGEMENT STANDARD

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

08/2009

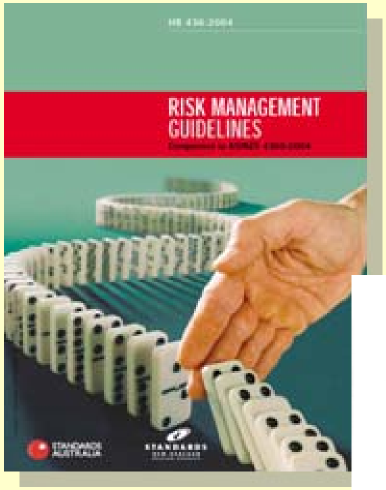
Why a new standard?

AS/NZS 4360:2004

- Was due for update in 2009
- The most widely used global RM Standard

ISO 31000 is a paramount standard

- Like 9000 and 14000
- Will guide all other ISO/IEC standards with respect to RM process
- Will replace national RM standards



HB 436:2004

RISK MANAGEMENT GUIDELINES

Companion to AS/NZS 4360:2004

GUIDE 73

Risk management — Vocabulary — Guidelines for use in standards

Management du risque — Vocabulaire — Principes directeurs pour l'utilisation dans les normes

ISO Guide 73

- Global vocabulary of risk management terms
- Being re-written by same WG, in parallel with ISO 31000

IEC 31010 Risk Management - Risk Assessment Techniques

- Reflects current good practices in selection and utilisation of RM techniques
- Being written in with the involvement of the same WG, in parallel with ISO 31000 and ISO Guide 73

Terms of Reference

(as approved by ISO TMB)

- **The Working Group develop a document which provides principles and practical guidance to the risk management process.**
- **The document is applicable to all organisations, regardless of type, size, activities and location and should apply to all type of risk.**
- **The document should establish a common concept of risk management process and common related concepts.**

Terms of Reference, as approved by ISO TMB (Continued)…

- **The document should provide practical guidelines to:**
  - **Understand how to implement risk management**
  - **Identify and treat all types of risk**
  - **treat and manage the identified risks,**
  - **improve an organisation's performance through the management of risk,**
  - **maximize opportunities and minimize losses in the organisation;**
  - **raise awareness of the need to treat and manage risk in organisations.**

- **Type of deliverable**

  The standard to be developed is a Guideline document, *and is NOT to be used for the purpose of certification.*

ISO Guide 73 - Scope

- Provides a basic vocabulary of the definitions of generic terms related to risk management

- Aims to encourage a mutual and consistent understanding, a coherent approach to the description of activities relating to the management of risk, and use of risk management terminology in processes and frameworks dealing with the management of risk.

Terms included in ISO Guide 73

- COMMUNICATION & CONSULTATION
- CONSEQUENCE
- CONTROL
- ESTABLISHING THE CONTEXT
- EVENT
- EXPOSURE
- EXTERNAL CONTEXT
- FREQUENCY
- HAZARD
- INTERNAL CONTEXT
- LEVEL OF RISK
- LIKELIHOOD
- MONITORING
- PROBABILITY
- RESIDUAL RISK
- RESILIENCE
- REVIEW
- RISK
- RISK ACCEPTANCE
- RISK AGGREGATION
- RISK ANALYSIS
- RISK APPETITE
- RISK ASSESSMENT
- RISK ATTITUDE
- RISK AVERSION
- RISK AVOIDANCE
- RISK CRITERIA
- RISK EVALUATION
- RISK FINANCING
- RISK IDENTIFICATION
- RISK MANAGEMENT
- RISK MANAGEMENT AUDIT
- RISK MANAGEMENT FRAMEWORK
- RISK MANAGEMENT PLAN
- RISK MANAGEMENT POLICY
- RISK MANAGEMENT PROCESS
- RISK MATRIX
- RISK OWNER
- RISK PERCEPTION
- RISK PROFILE
- RISK REGISTER
- RISK REPORTING
- RISK RETENTION
- RISK SHARING
- RISK SOURCE
- RISK TOLERANCE
- RISK TREATMENT
- STAKEHOLDER
- VULNERABILITY

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, organisation-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]

		KNOWLEDGE ABOUT OUTCOMES	
		Well-defined outcomes	Poorly defined outcomes
KNOWLEDGE ABOUT LIKELIHOODS	Some basis for probabilities	risk	ambiguity
		“INCERTITUDE”	
	No basis for probabilities	uncertainty	ignorance

O’Riordan, T, and Cox, P. 2001. Science, Risk, Uncertainty and Precaution.

Senior Executive’s Seminar – HRH the Prince of Wales’s Business and the Environment Programme.

University of Cambridge.

Key Definitions

- **RISK OWNER: person or entity with the accountability and authority to manage risk.**

- **RISK ATTITUDE: organisation's approach to assess and eventually pursue, retain, take or turn away from risk.**

- **RISK APPETITE: amount and type of risk that an organisation is prepared to pursue, retain or take.**

- **RISK TOLERANCE: organisation's or stakeholder's readiness to bear the risk after treatment in order to achieve its objectives**

  Note: Risk tolerance can be influenced by legal or regulatory requirements.

- **RISK AVERSION*:* attitude to turn away from risk.**

[ISO CD Guide 73:2009]

Key Definitions (Continued)…

- **RISK AGGREGATION: consideration of risks in combination.**

- **RISK ACCEPTANCE: informed decision to take a particular risk.**

  Note 1: Risk acceptance can occur without risk treatment or during the process of risk treatment

  Note 2: Accepted risks are subject to monitoring and review

- **CONTROL: measure that is modifying risk.**

  Note 1: Controls include any process, policy, device, practice, or other actions which modify risk.
  Note 2: Controls may not always exert the intended or assumed modifying effect.

[ISO CD Guide 73:2009]

Key Definitions (Continued)…

- **RISK RETENTION: acceptance of the potential benefit of gain, or burden of loss, from a particular risk.**

  Note 1: Risk retention includes the acceptance of residual risks
  Note 2: The level of risk retained can depend on risk criteria.

- **RESIDUAL RISK: risk remaining after risk treatment.**

  Note 1: Residual risk can contain unidentified risk

  Note 2: Residual risk can also be known as "retained risk"

- **RESILIENCE: adaptive capacity of an organisation in a complex and changing environment.**

- **RISK PROFILE: description of any set of risks.**

  Note: The set of risks can contain those that relate to the whole organisation, part of the organisation, or as otherwise defined.

[ISO CD Guide 73:2009]

Yet to be defined…

- **ACCOUNTABLE: liability for the outcomes of actions or decisions.**

  NOTE: includes failure to act or make decisions

OR

- **ACCOUNTABLE: being obligated to answer for an action.**

- **RESPONSIBLE: obligation to carry out duties or decisions, or control over others**

OR

- **RESPONSIBLE: having the obligation to act.**

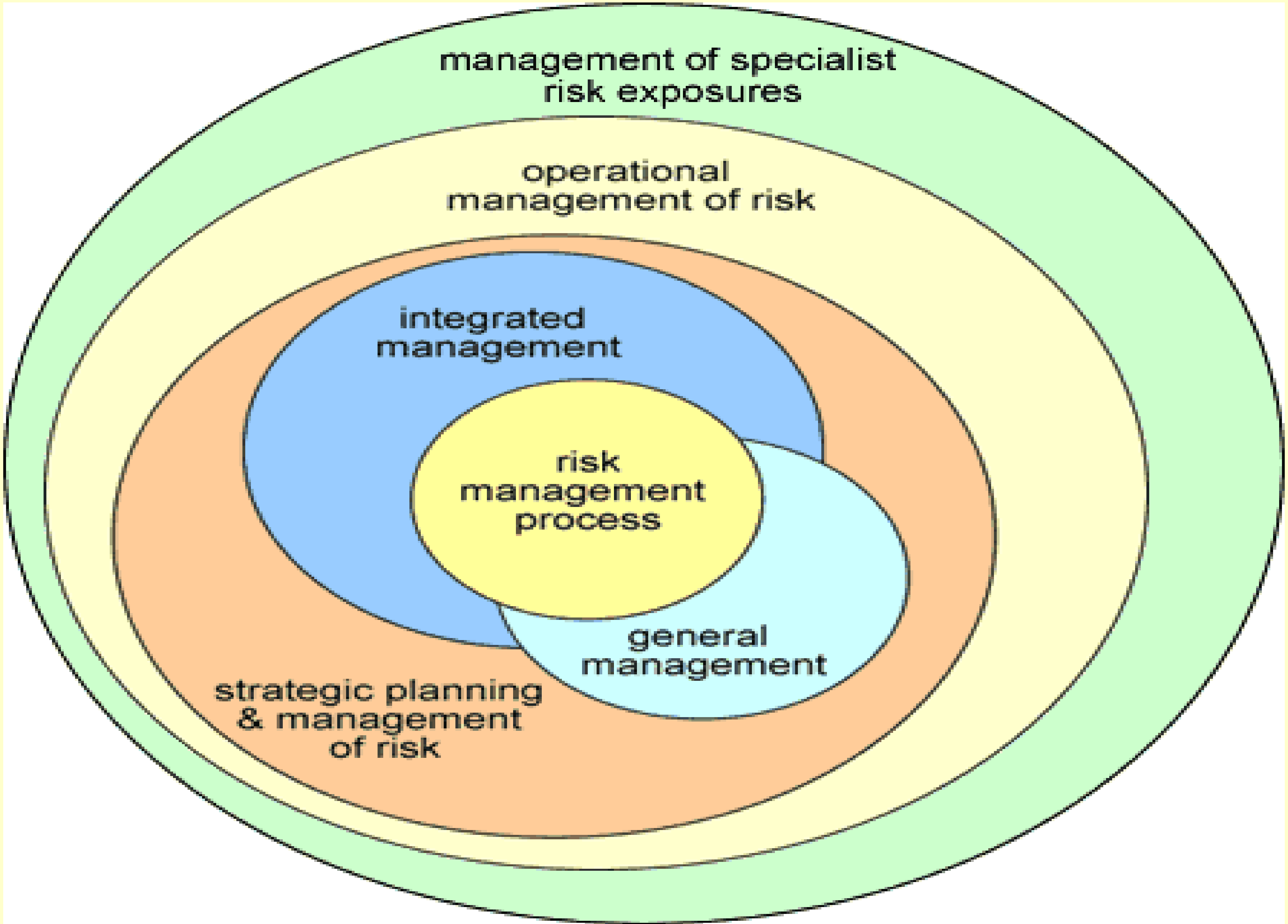
ISO 31000:2009 - Scope

- **Provides principles and generic guidelines on principles and implementation of risk management.**
- **Can be applied to any kind of organisation, and not specific to any industry or sector.**
- ***Is NOT intended to be used for the purpose of certification.***

ISO 31000:2009 - Users

- **ISO 31000:2009 is intended to be used by a wide range of stakeholders including:**
  - those responsible for implementing risk management within their organisation;
  - those who need to ensure that an organisation manages risk;
  - those who need to manage risk for the organisation as a whole or within a specific area or activity;
  - those needing to evaluate an organisation's practices in managing risk; and
  - developers of standards, guides, procedures, and codes of practice that in whole or in part set out how risk is to be managed within the specific context of these documents.

A Business Principles Approach to Risk Management


management of specialist risk exposures
operational management of risk
integrated management
risk management process
general management
strategic planning & management of risk

Business Principles Approach

AS/NZS/ISO 31000:2009 Principles (Clause 3)

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

Attributes of enhanced risk management

AS/NZS/ISO 31000:2009
Annex A
(Informative)

- **A pronounced emphasis on continuous improvement in risk management through the setting of organisational performance goals, measurement, review and the subsequent modification of processes, systems, resources and capability/skills.**

Attributes of enhanced risk management (Continued)

- **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.**

Attributes of enhanced risk management (Continued)

- **All decision making within the organisation, 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.**

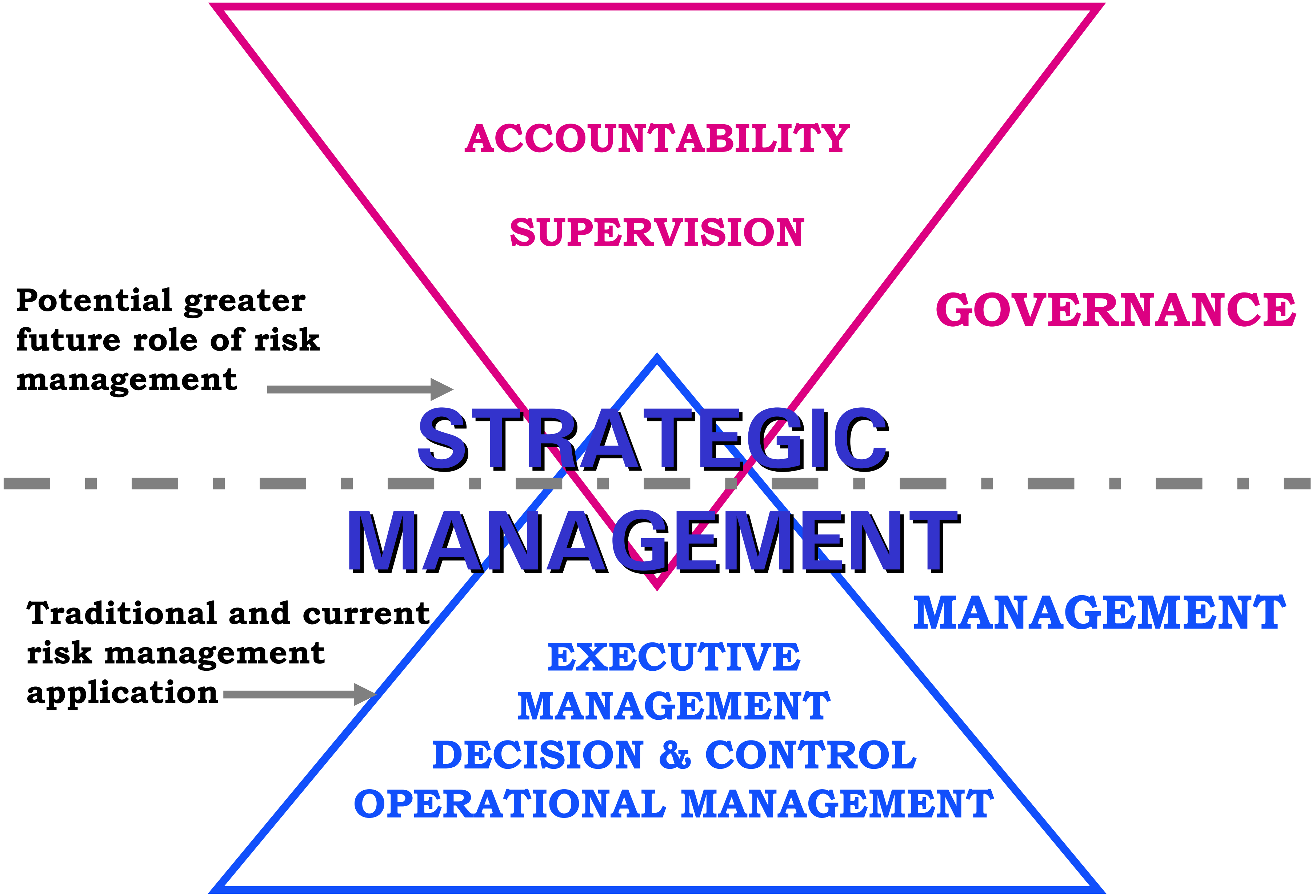
Attributes of enhanced risk management (Continued)

- **Continual communications and highly visible, comprehensive and frequent reporting of risk management performance to all "interested parties" as part of their accepted governance processes.**

Attributes of enhanced risk management (Continued)

Risk management is always viewed as a core organisational 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 organisation’s objectives. The organisation’s governance structure and process are founded on the risk management process.



ACCOUNTABILITY

SUPERVISION

GOVERNANCE

Potential greater future role of risk management

STRATEGIC MANAGEMENT

Traditional and current risk management application

MANAGEMENT

EXECUTIVE MANAGEMENT

DECISION & CONTROL

OPERATIONAL MANAGEMENT

Risk Management's Role in Corporate Governance

Enterprise-wide Risk management Framework

(AS/NZS/ISO 31000:2009 Clause 4)

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

Therefore, organisations should adapt the components of the framework to their specific needs.

DISCUSSION

Considering what we have discussed so far, what do you think you are going to need to do to align your current framework (based on AS/NZS 4360:2004) to AS/NZS/ISO 31000?

Risk Management Framework

Set of components that provide the foundations and organisational arrangements for designing, implementing,
monitoring, reviewing and continually improving risk management throughout the organisation

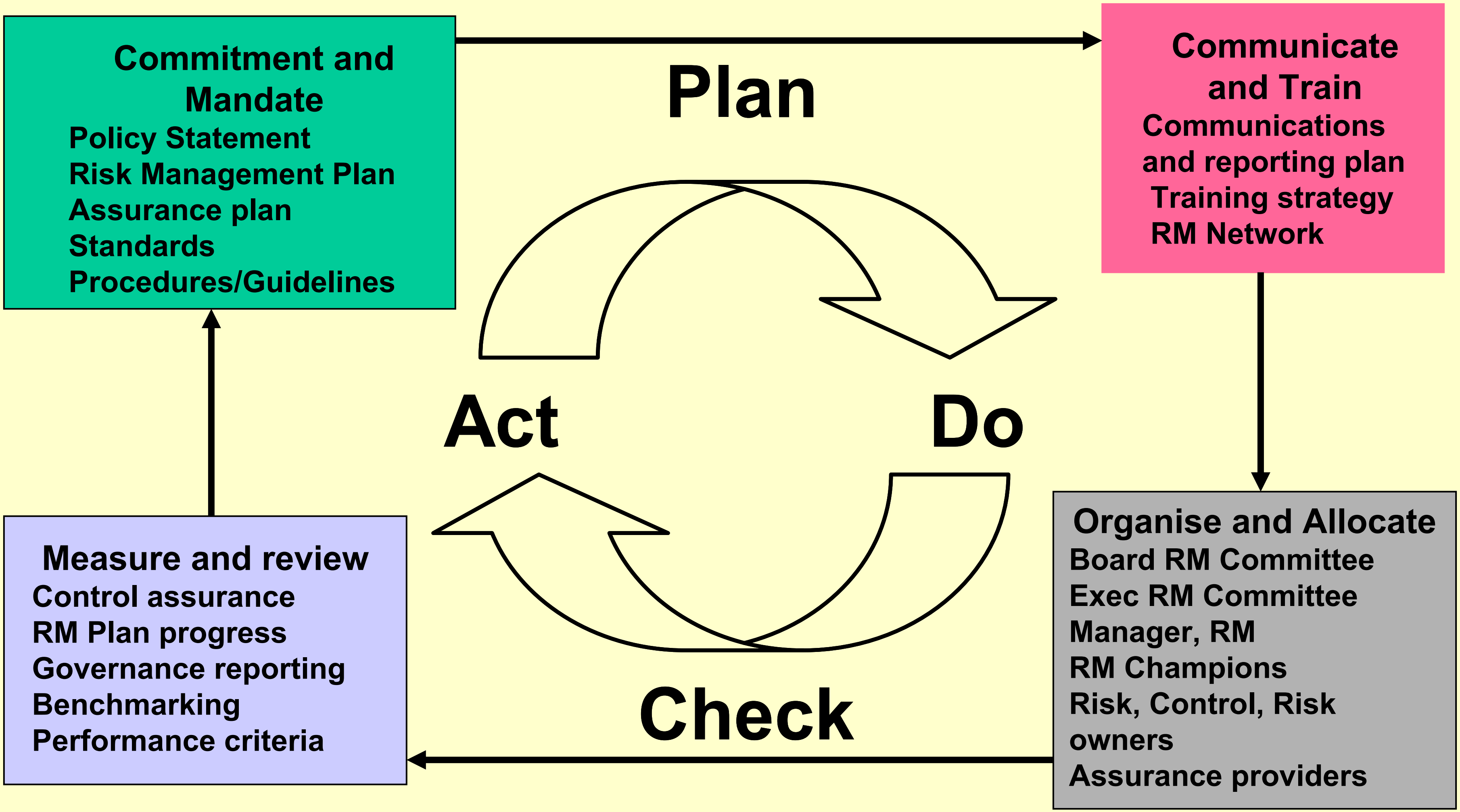
NOTE 1 The foundations include the policy, objectives, mandate and commitment to manage risk.

NOTE 2 The organisational arrangements include plans, relationships, accountabilities, resources, processes and activities.

NOTE 3 The risk management framework is embedded within the organisation's overall strategic and operational policies and practices.

[ISO Guide 73:2009]

PDCA – a starting point for a Business Improvement focused Risk Framework



Commitment and Mandate
Policy Statement
Risk Management Plan
Assurance plan
Standards
Procedures/Guidelines

Plan

Communicate and Train
Communications and reporting plan
Training strategy
RM Network

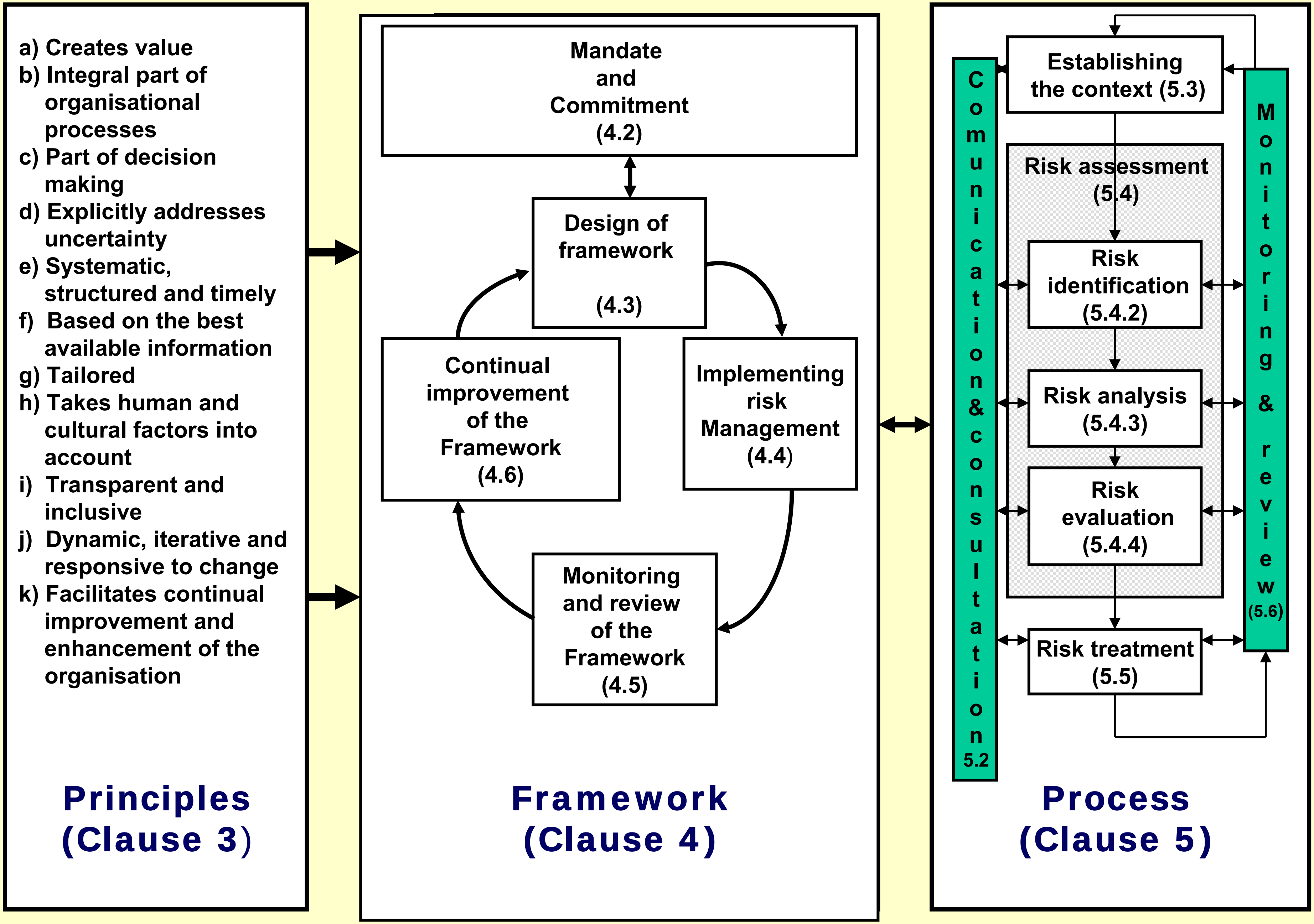
Do

Organise and Allocate
Board RM Committee
Exec RM Committee
Manager, RM
RM Champions
Risk, Control, Risk owners
Assurance providers

Check

Measure and review
Control assurance
RM Plan progress
Governance reporting
Benchmarking
Performance criteria

Act



a) Creates value
b) Integral part of organisational 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 organisation

Principles (Clause 3)

Mandate and Commitment (4.2)

Design of framework (4.3)

Implementing risk Management (4.4)

Monitoring and review of the Framework (4.5)

Continual improvement of the Framework (4.6)

Framework (Clause 4)

Communication & consultation 5.2

Establishing the context (5.3)

Risk assessment (5.4)

Risk identification (5.4.2)

Risk analysis (5.4.3)

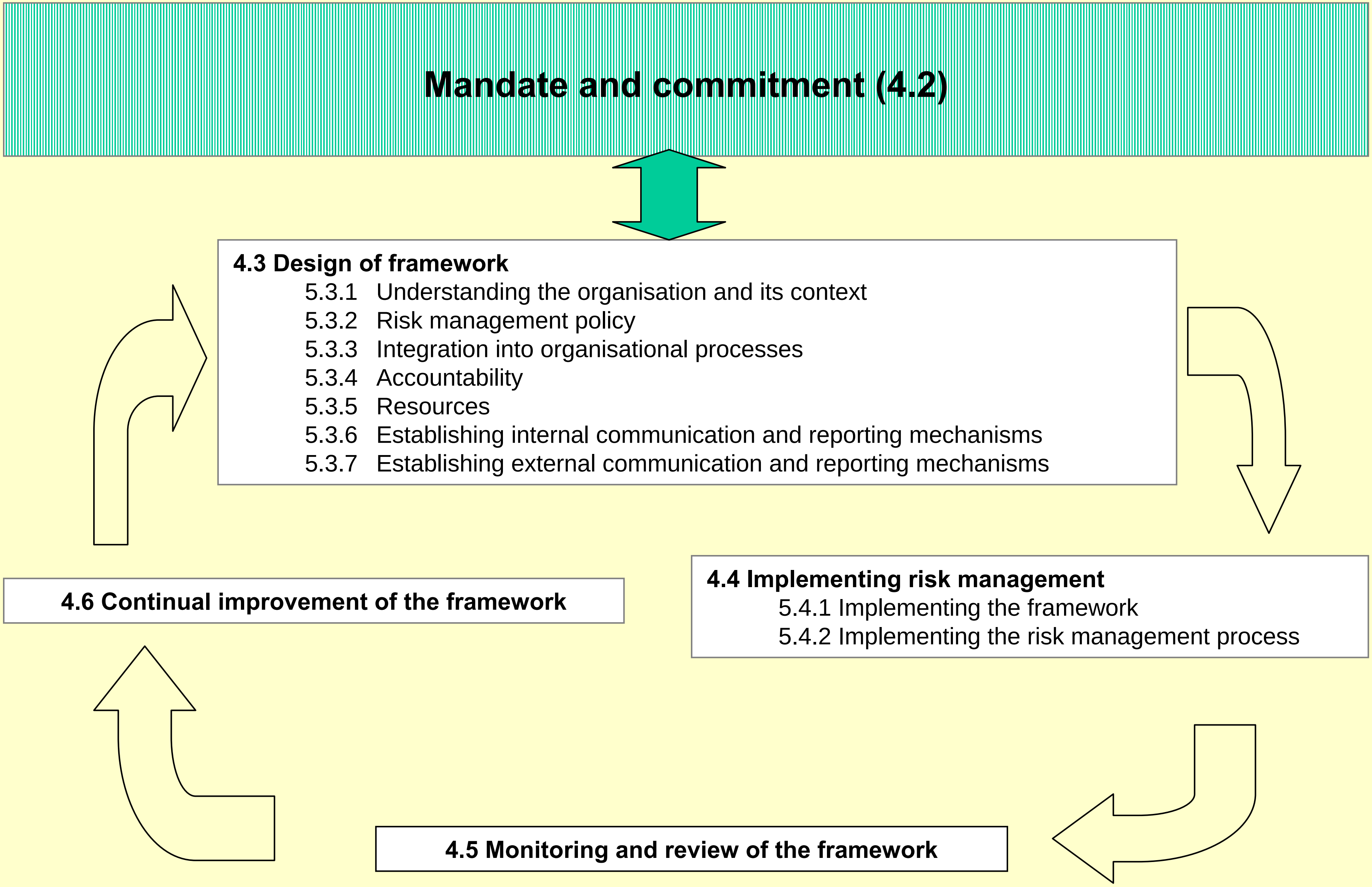
Risk evaluation (5.4.4)

Risk treatment (5.5)

Monitoring & review (5.6)

Process (Clause 5)

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



Mandate and commitment (4.2)

4.3 Design of framework

5.3.1 Understanding the organisation and its context
5.3.2 Risk management policy
5.3.3 Integration into organisational processes
5.3.4 Accountability
5.3.5 Resources
5.3.6 Establishing internal communication and reporting mechanisms
5.3.7 Establishing external communication and reporting mechanisms

4.4 Implementing risk management

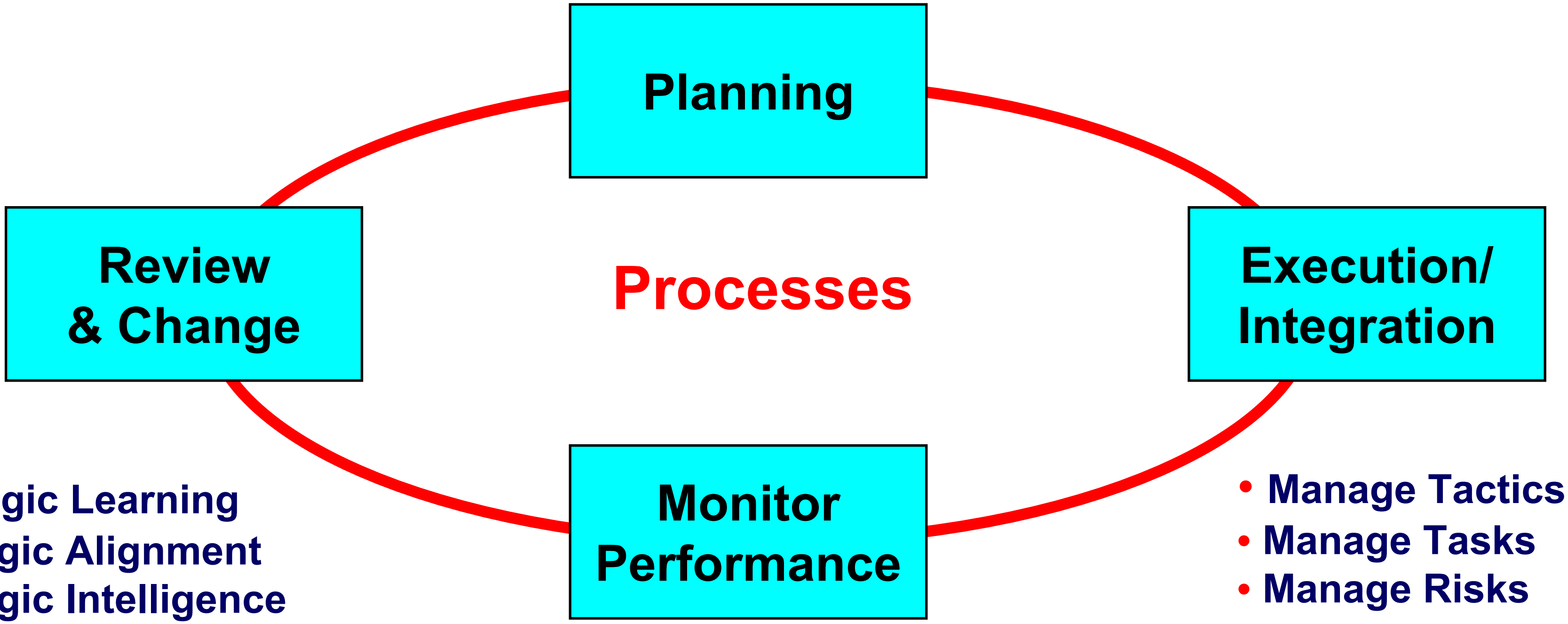
5.4.1 Implementing the framework
5.4.2 Implementing the risk management process

4.5 Monitoring and review of the framework

4.6 Continual improvement of the framework

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

- Future State/ End Vision
- SWOT, Opportunities and Risks
- Strategy & Tactics



Planning

Review & Change

Processes

Execution/ Integration

Monitor Performance

- Manage Tactics
- Manage Tasks
- Manage Risks

- Strategic Learning
- Strategic Alignment
- Strategic Intelligence

- Performance
- Capability
- External Environment

Hierarchical Objectives

- **Strategic:** designed to provide the direction required to achieve strategic goals. These are usually long-term plans with a minimum timeframe of three to five years.
- **Tactical:** designed to further the implementation of the strategic plan, addressing tactical goals, following a shorter timeframe of generally one to three years
- **Operational:** designed to further the implementation of tactical plans and addressing operational goals. These plans have a much shorter timeframe of usually less than one year, sometimes with a timeframe of months, weeks or days.

Organisational Objectives

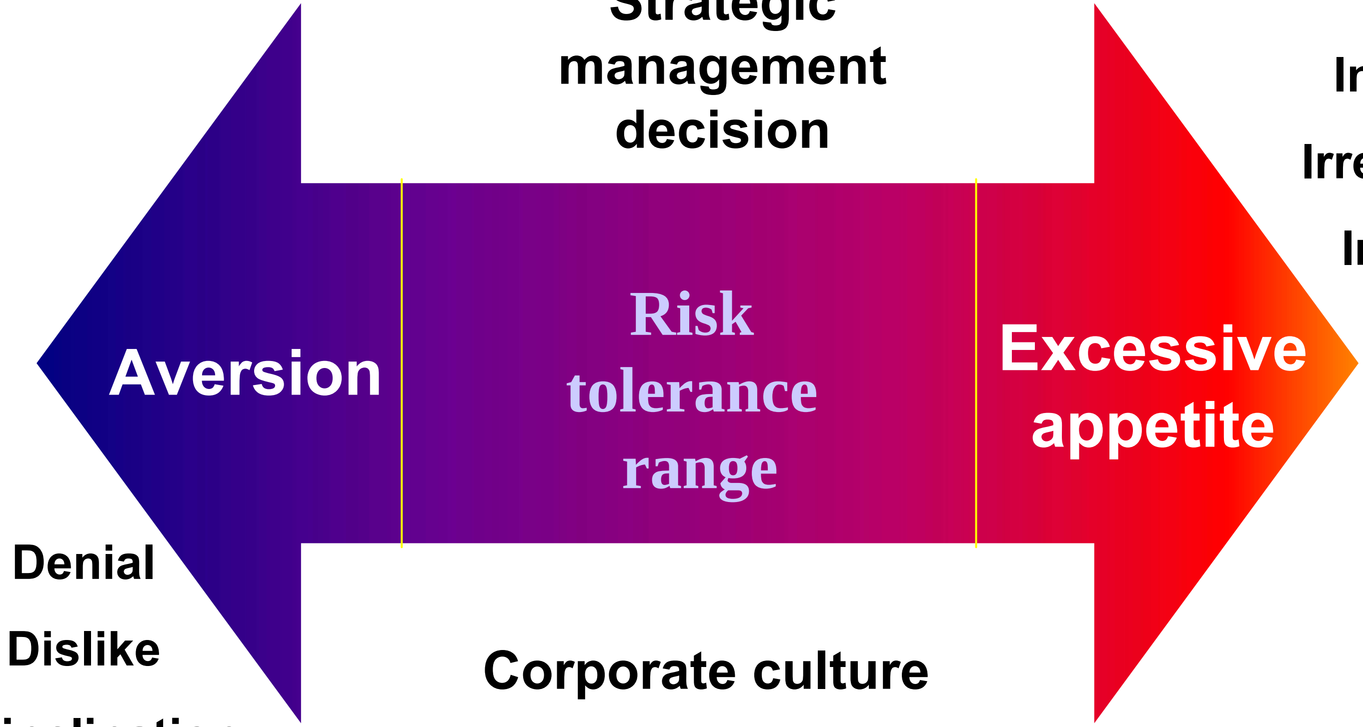
There are generally three levels of objectives in any organisation, which align to the type of plan that will be implemented to help attain them:

- Strategic objectives are usually very general by nature describing future results which have been determined by management. These generally describe the vision/mission for ensuring the success of the organisation.

- Tactical objectives are set by middle management for specific departments or business units. They are aligned to the strategic objectives and articulate what each department or business unit must do to achieve higher level objectives.

- Operational objectives are more specific in nature set by lower management to address the requirements set by tactical objectives.

Organisational Risk Criteria



Strategic management decision

Indecision

Irresponsible

Impulsive

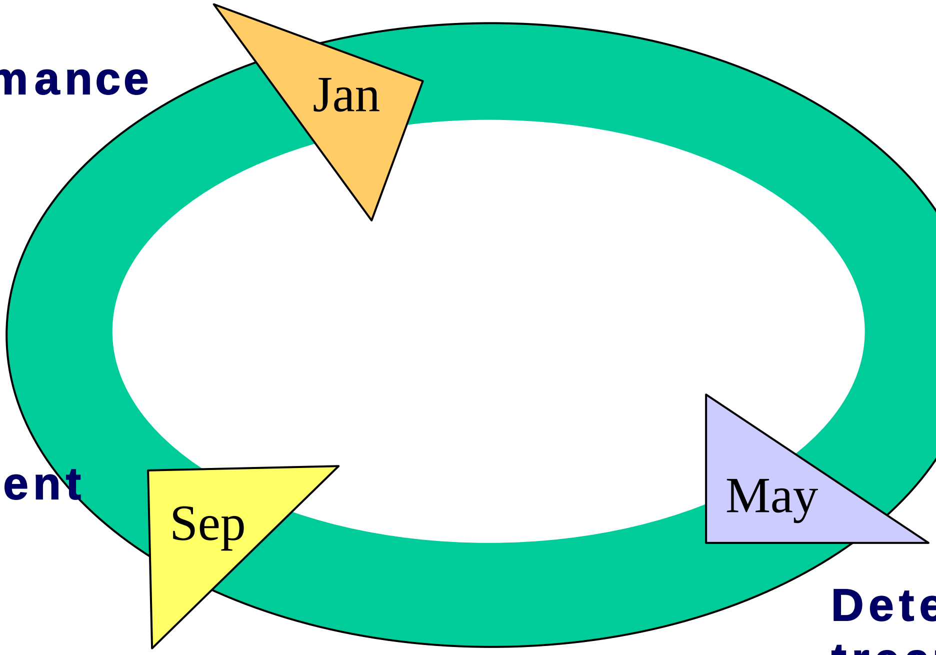
Denial

Dislike

Disinclination

Corporate culture

Operational Risk Management Cycle



Conduct risk profiling

Strategic planning

Determine risk treatment actions

Budget and business planning

Implement and monitor treatment actions

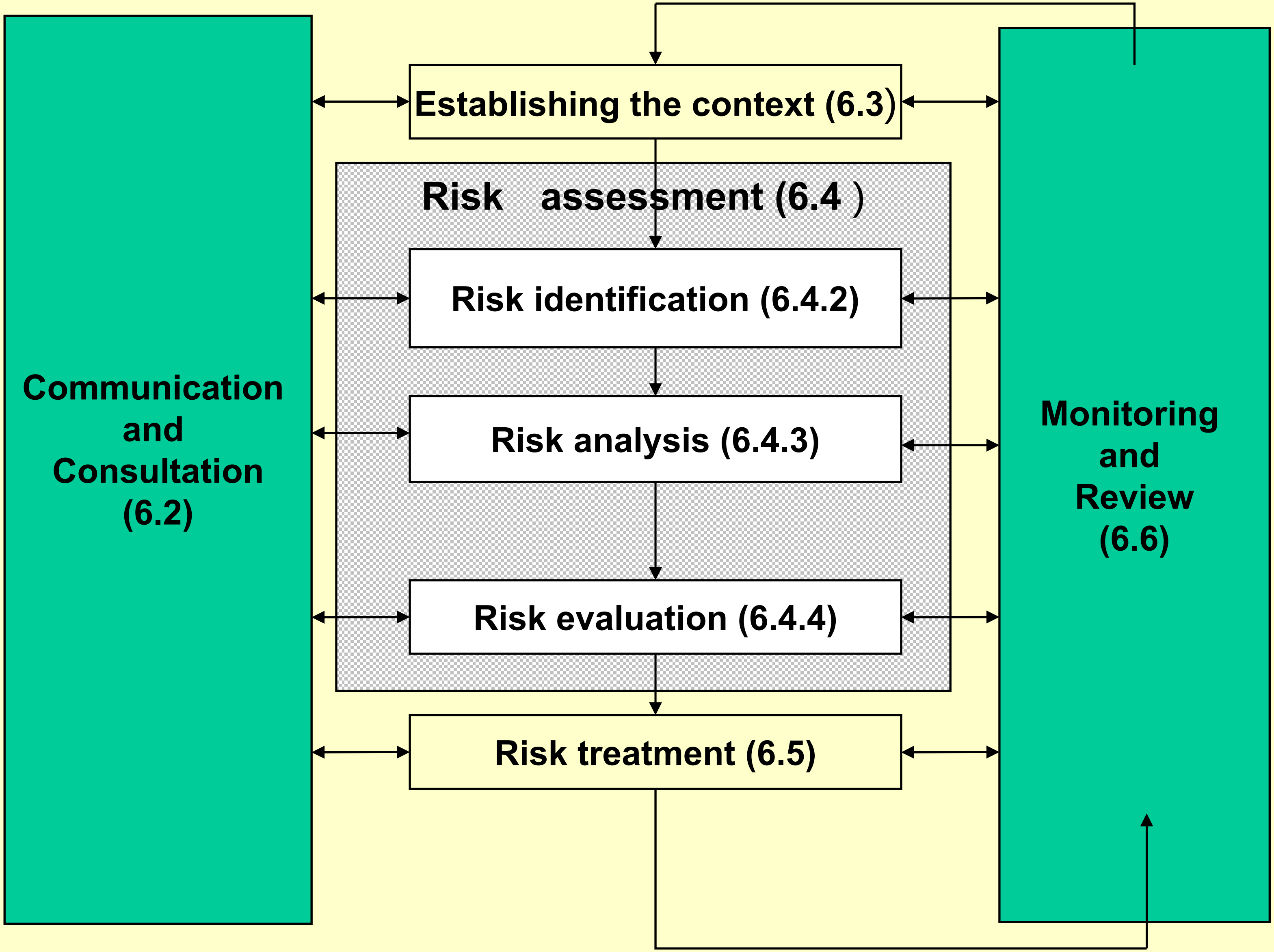
Review performance

DISCUSSION

How will you align the current objectives of your agency’s risk management framework to address the following objectives of AS/NZS/ISO 31000:

- **Strategic;**
- **Tactical; and**
- **Operational.**

A Process for Reviewing Risk Management Strategies (AS/NZS/ISO 31000)



Establishing the context (6.3)

Risk assessment (6.4)

Risk identification (6.4.2)

Risk analysis (6.4.3)

Risk evaluation (6.4.4)

Risk treatment (6.5)

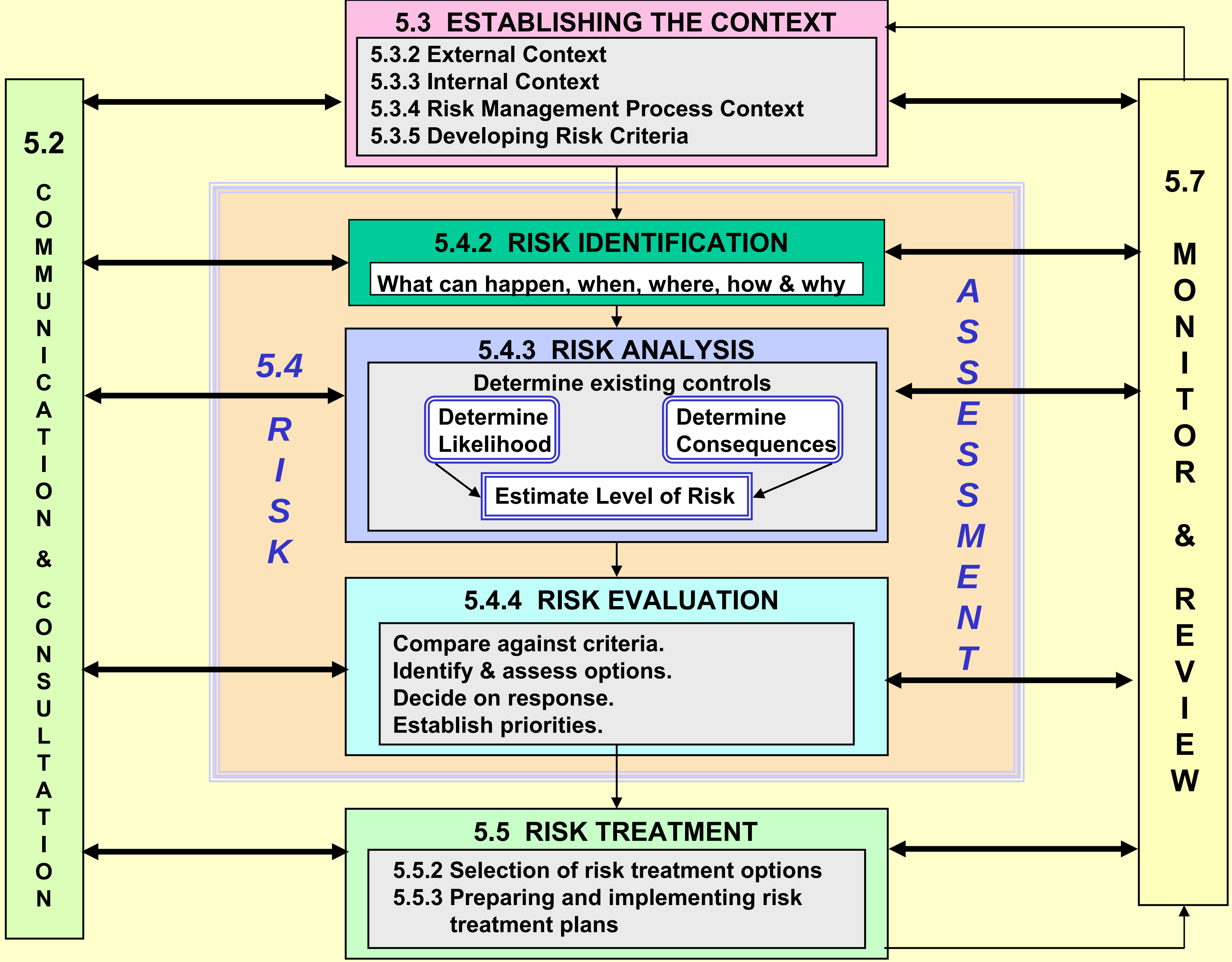
Communication and Consultation (6.2)

Monitoring and Review (6.6)

AS/NZS/ISO 31000:2009 (Clause 6) Risk management process

- Should be an integral part of management, be embedded in culture and practices and tailored to the business processes of the organisation.

- Includes five activities:
  - communication and consultation;
  - establishing the context;
  - risk assessment;
  - risk treatment; and
  - monitoring and review.



5.3 ESTABLISHING THE CONTEXT

5.3.2 External Context
5.3.3 Internal Context
5.3.4 Risk Management Process Context
5.3.5 Developing Risk Criteria

5.2 COMMUNICATION & CONSULTATION

5.4 RISK ASSESSMENT

5.4.2 RISK IDENTIFICATION

What can happen, when, where, how & why

5.4.3 RISK ANALYSIS

Determine existing controls

Determine Likelihood

Determine Consequences

Estimate Level of Risk

5.4.4 RISK EVALUATION

Compare against criteria.
Identify & assess options.
Decide on response.
Establish priorities.

5.5 RISK TREATMENT

5.5.2 Selection of risk treatment options
5.5.3 Preparing and implementing risk treatment plans

5.7 MONITOR & REVIEW

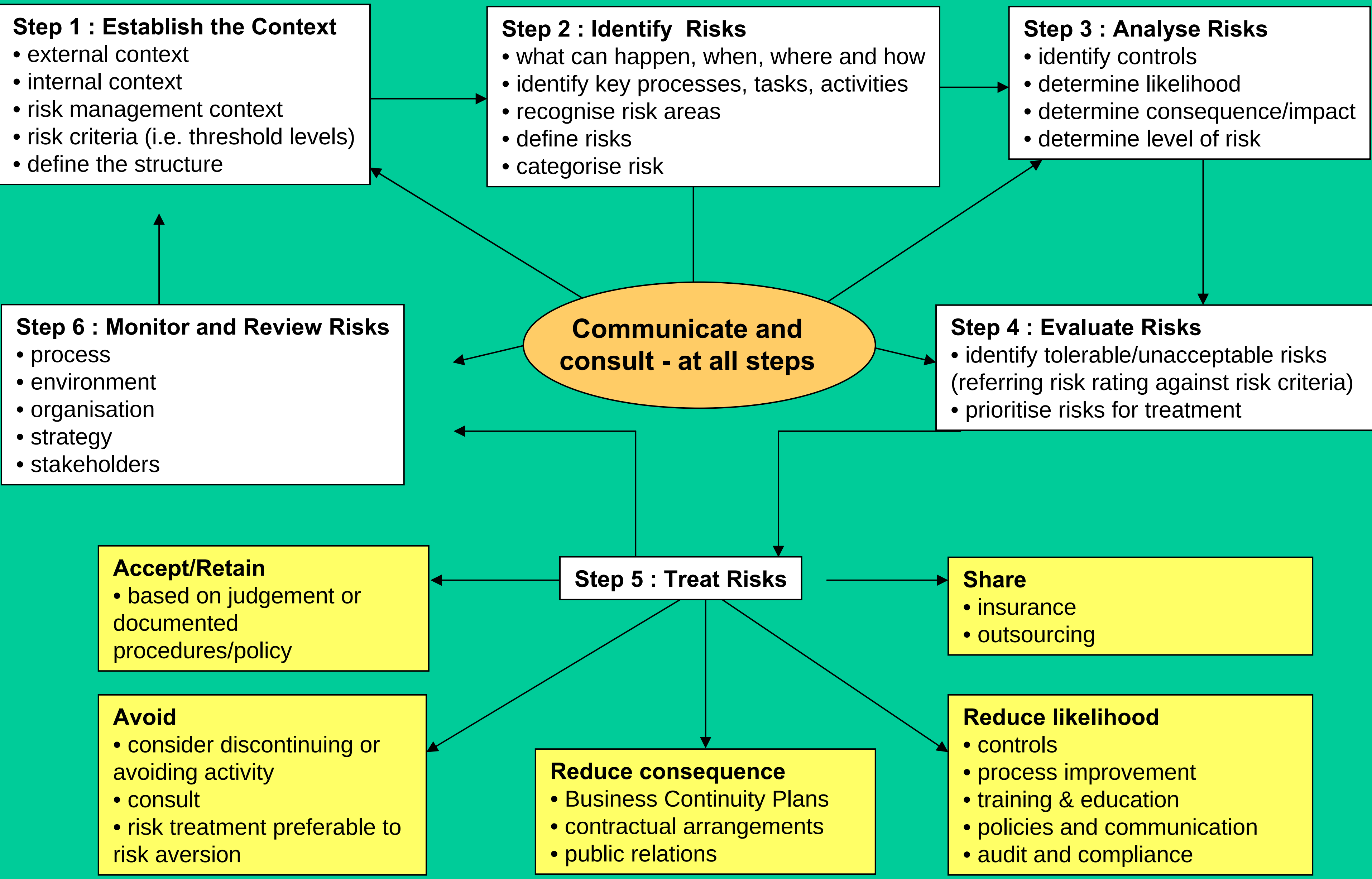
AS/NZS/ISO 31000:2009 Risk management process in detail

Communicate & Consult

- **Communicating risk successfully is neither a public relations nor a crisis communications exercise. Its aim is not to avoid all conflict or to diffuse all concerns.**

- **Risk communication seeks to improve performance based on informed, mutual decisions with respect to … risk.**

Jean Mulligan, Elaine McCoy and Angela Griffiths,
Principles of Communicating Risks,
The Macleod Institute for Environmental Analysis,
University of Calgary, Calgary, Alberta 1998



Step 1 : Establish the Context
- external context
- internal context
- risk management context
- risk criteria (i.e. threshold levels)
- define the structure

Step 2 : Identify Risks
- what can happen, when, where and how
- identify key processes, tasks, activities
- recognise risk areas
- define risks
- categorise risk

Step 3 : Analyse Risks
- identify controls
- determine likelihood
- determine consequence/impact
- determine level of risk

Communicate and consult - at all steps

Step 4 : Evaluate Risks
- identify tolerable/unacceptable risks (referring risk rating against risk criteria)
- prioritise risks for treatment

Step 5 : Treat Risks

Accept/Retain
- based on judgement or documented procedures/policy

Share
- insurance
- outsourcing

Avoid
- consider discontinuing or avoiding activity
- consult
- risk treatment preferable to risk aversion

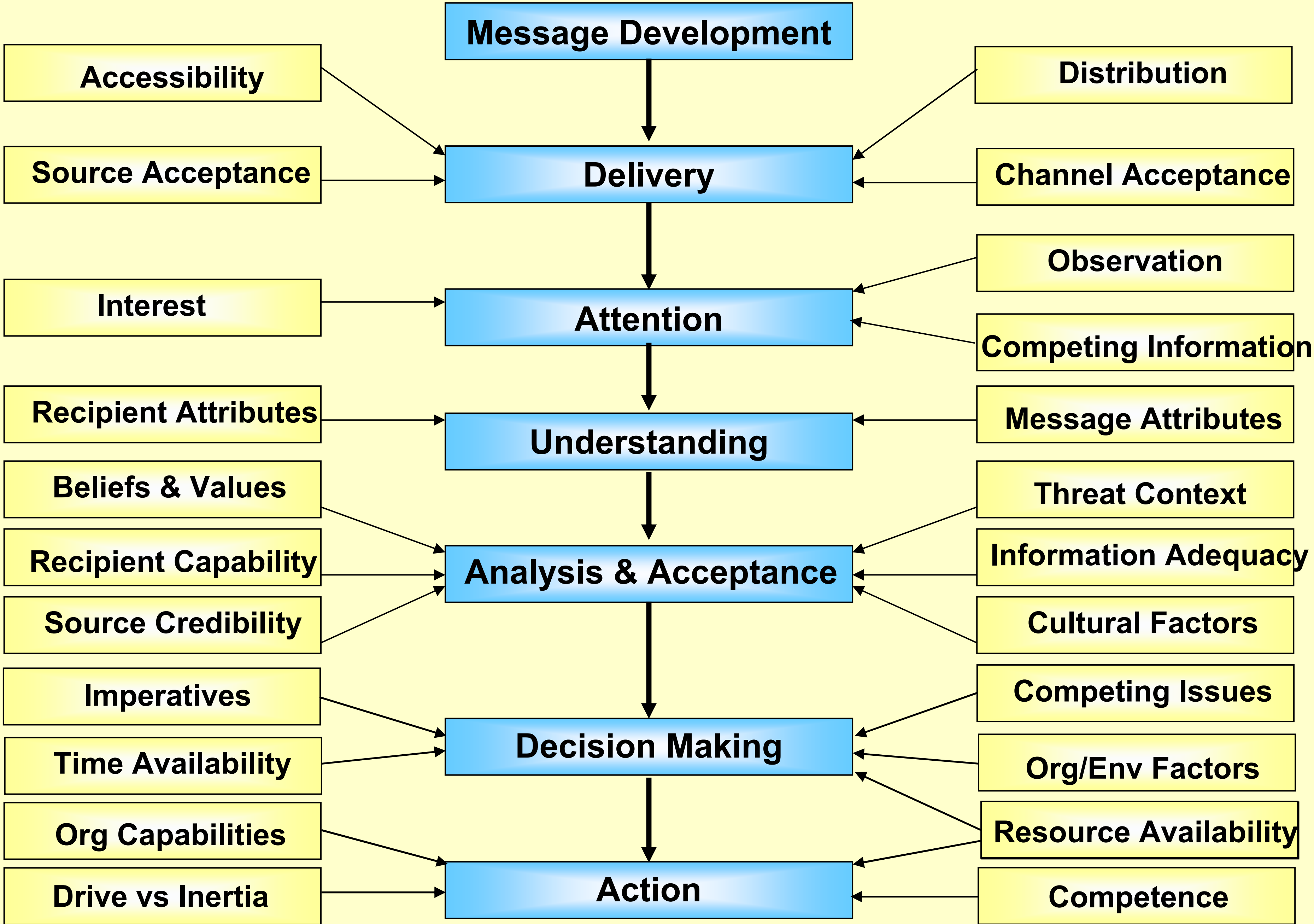
Reduce consequence
- Business Continuity Plans
- contractual arrangements
- public relations

Reduce likelihood
- controls
- process improvement
- training & education
- policies and communication
- audit and compliance

Step 6 : Monitor and Review Risks
- process
- environment
- organisation
- strategy
- stakeholders

Communication & Consultation in the risk management process

Getting the message across



Message Development

Accessibility

Source Acceptance

Delivery

Distribution

Channel Acceptance

Interest

Attention

Observation

Competing Information

Recipient Attributes

Understanding

Message Attributes

Beliefs & Values

Recipient Capability

Source Credibility

Analysis & Acceptance

Threat Context

Information Adequacy

Cultural Factors

Imperatives

Time Availability

Decision Making

Competing Issues

Org/Env Factors

Resource Availability

Org Capabilities

Drive vs Inertia

Action

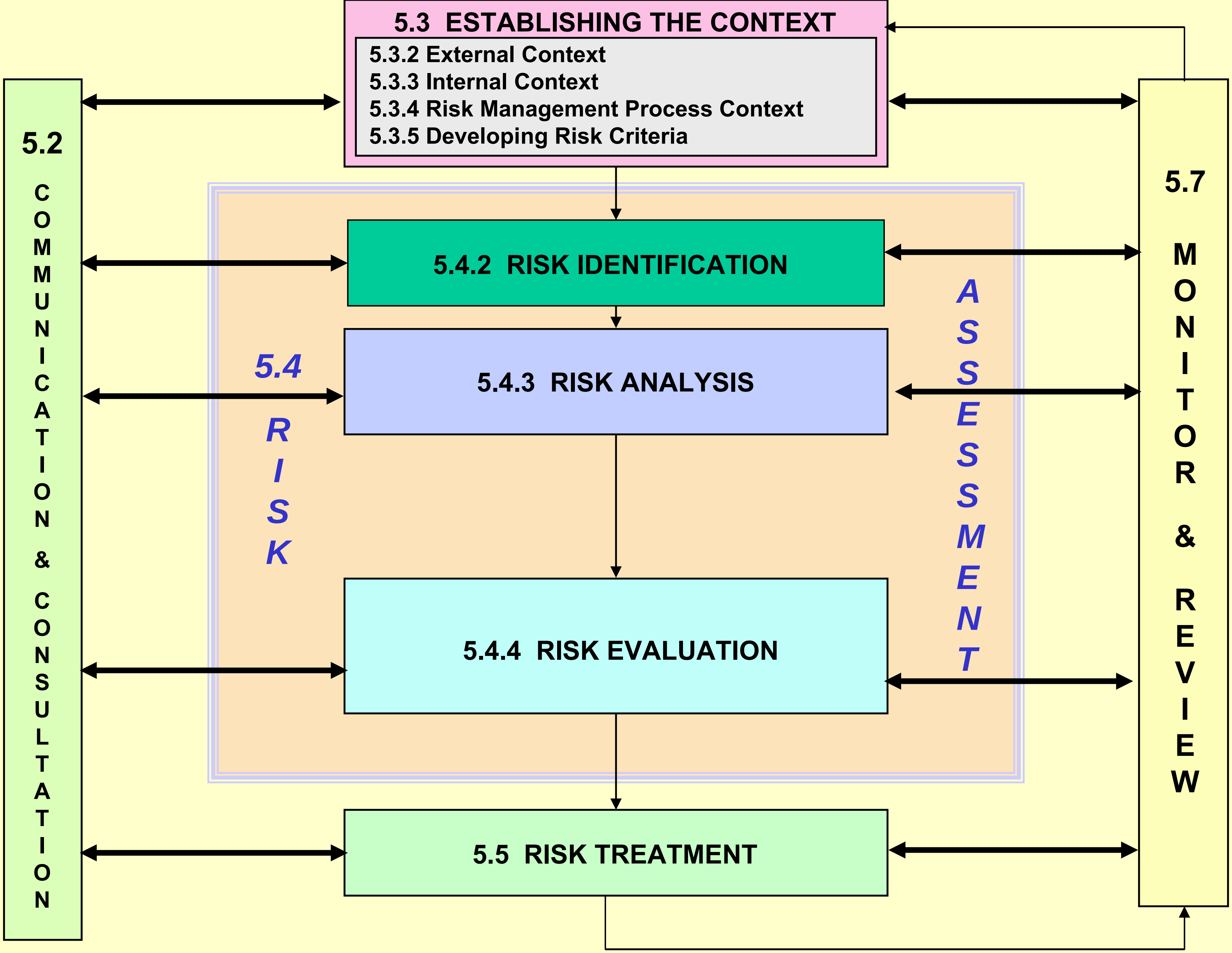
Competence

DISCUSSION

How does your agency currently communicate with external and internal stakeholders?

Does your current approach inform stakeholders and contribute to informed decision making?

If not, what do you need to do to ensure the effective communication of risk in your agency?



5.3 ESTABLISHING THE CONTEXT

5.3.2 External Context
5.3.3 Internal Context
5.3.4 Risk Management Process Context
5.3.5 Developing Risk Criteria

5.2 COMMUNICATION & CONSULTATION

5.4 RISK ASSESSMENT

5.4.2 RISK IDENTIFICATION

5.4.3 RISK ANALYSIS

5.4.4 RISK EVALUATION

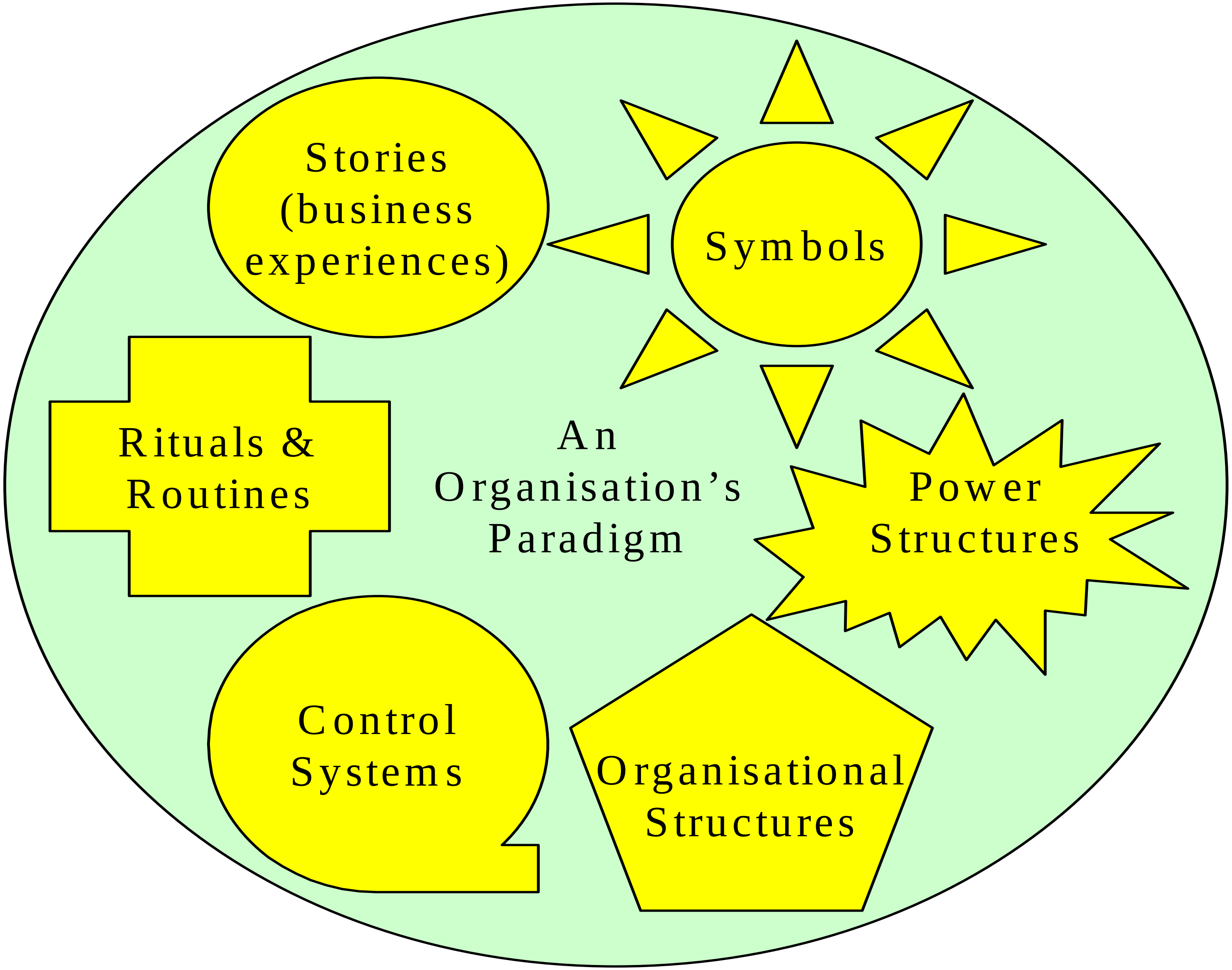
5.5 RISK TREATMENT

5.7 MONITOR & REVIEW

AS / NZS / ISO 31000:2009 Risk management process in detail

Establish the Context

- Objectives and environment
- Relevant Legislation
- Stakeholder identification & analysis
- Government Policy
- Corporate Policy
- Management Structures
- Community Expectations
- Criteria
- Consequence criteria

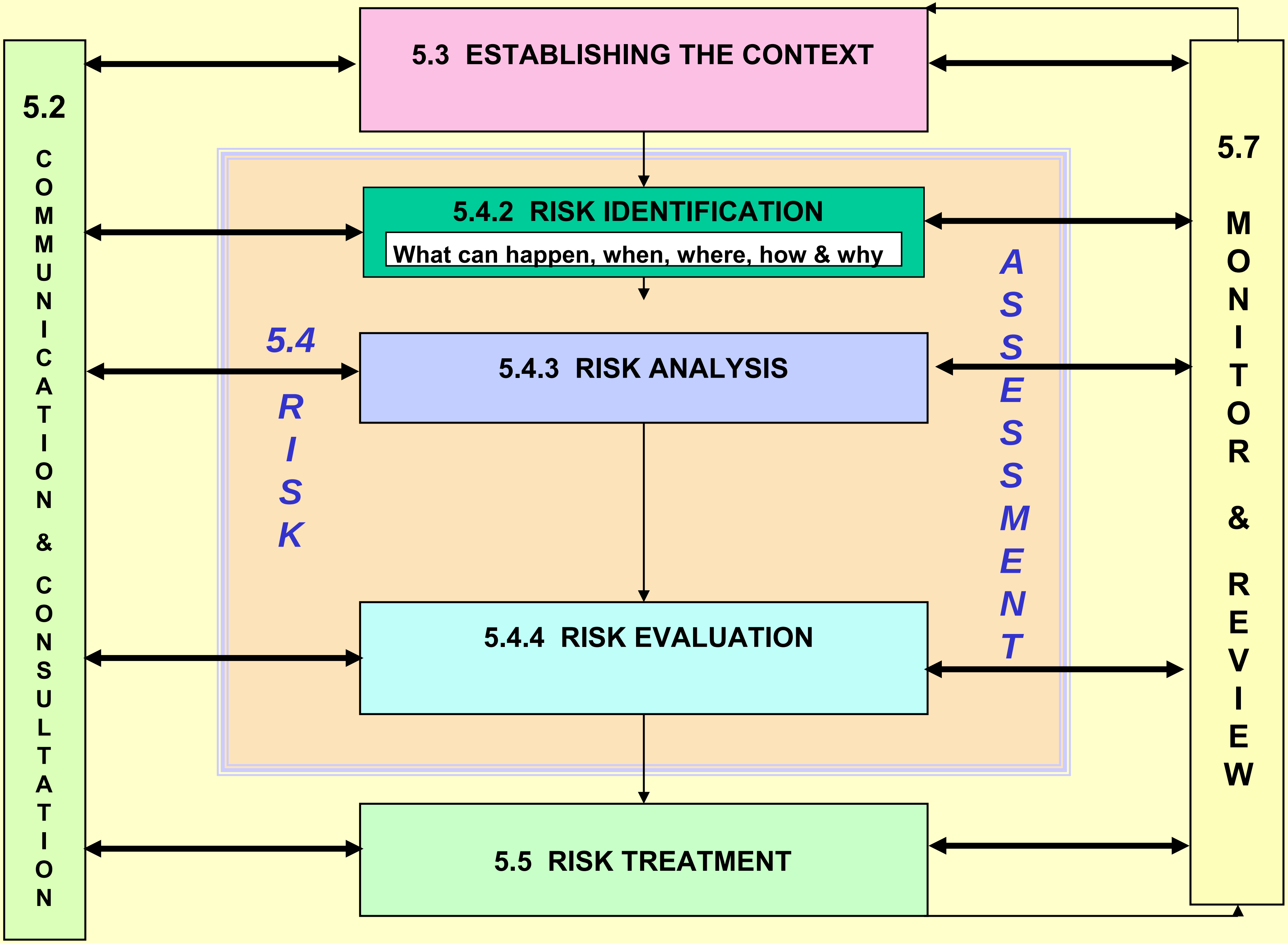

Stories (business experiences)
Symbols
Rituals & Routines
An Organisation's Paradigm
Power Structures
Control Systems
Organisational Structures

Adapted from Johnson & Scholes, 1993, p.61

DISCUSSION

Establishing the context for managing risk is often difficult.

What does your agency do to assist staff to adopt a consistent approach to identifying the context for managing risk?



5.2 COMMUNICATION & CONSULTATION

5.3 ESTABLISHING THE CONTEXT

5.4 RISK ASSESSMENT

5.4.2 RISK IDENTIFICATION

What can happen, when, where, how & why

5.4.3 RISK ANALYSIS

5.4.4 RISK EVALUATION

5.5 RISK TREATMENT

5.7 MONITOR & REVIEW

AS / NZS / ISO 31000:2009 Risk management process in detail

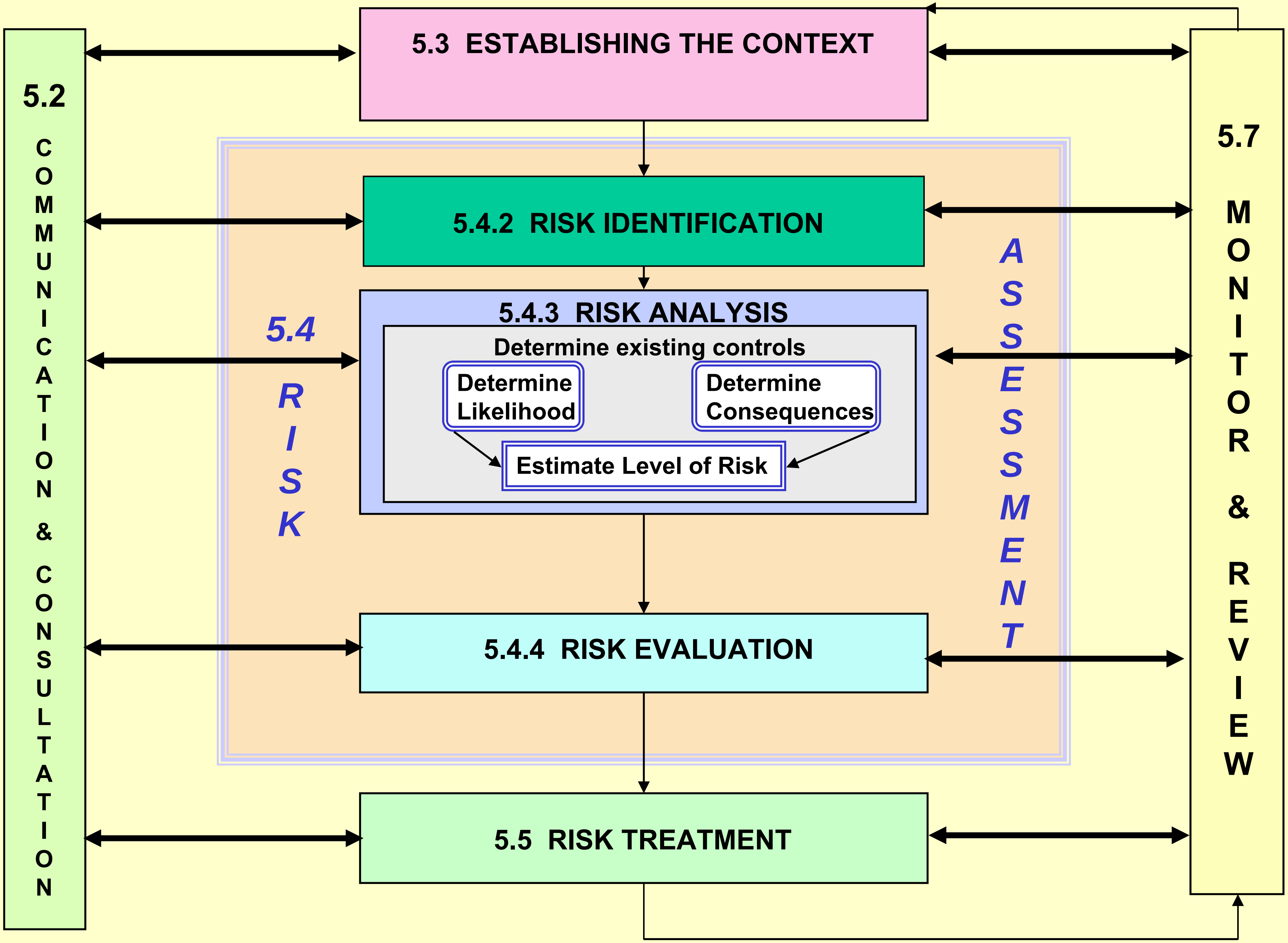
Identification of sources of risk

- Personnel/human behaviour.
- Management activities and controls.
- Economic circumstances.
- Natural and unnatural events.
- Political circumstances.
- Technology/technical issues.
- Commercial and legal relationships.
- Public/professional/product liability.
- The activity itself.

Components of a risk

A risk is associated with:

- **A *source* of risk or hazard.**
- **An *event* or *incident* – something that occurs such that the source of risk has the impact concerned.**
- **A *consequence, outcome* or *impact* on a range of stakeholders and assets.**
- **A *cause* (what and why) (usually a string of direct and underlying causes) for the presence of the hazard or the event occurring.**
- ***Controls* and their level of effectiveness.**
- ***When* could the risk occur and *where* could it occur.**



AS/NZS/ISO 31000:2009 Risk management process in detail

Risk Analysis

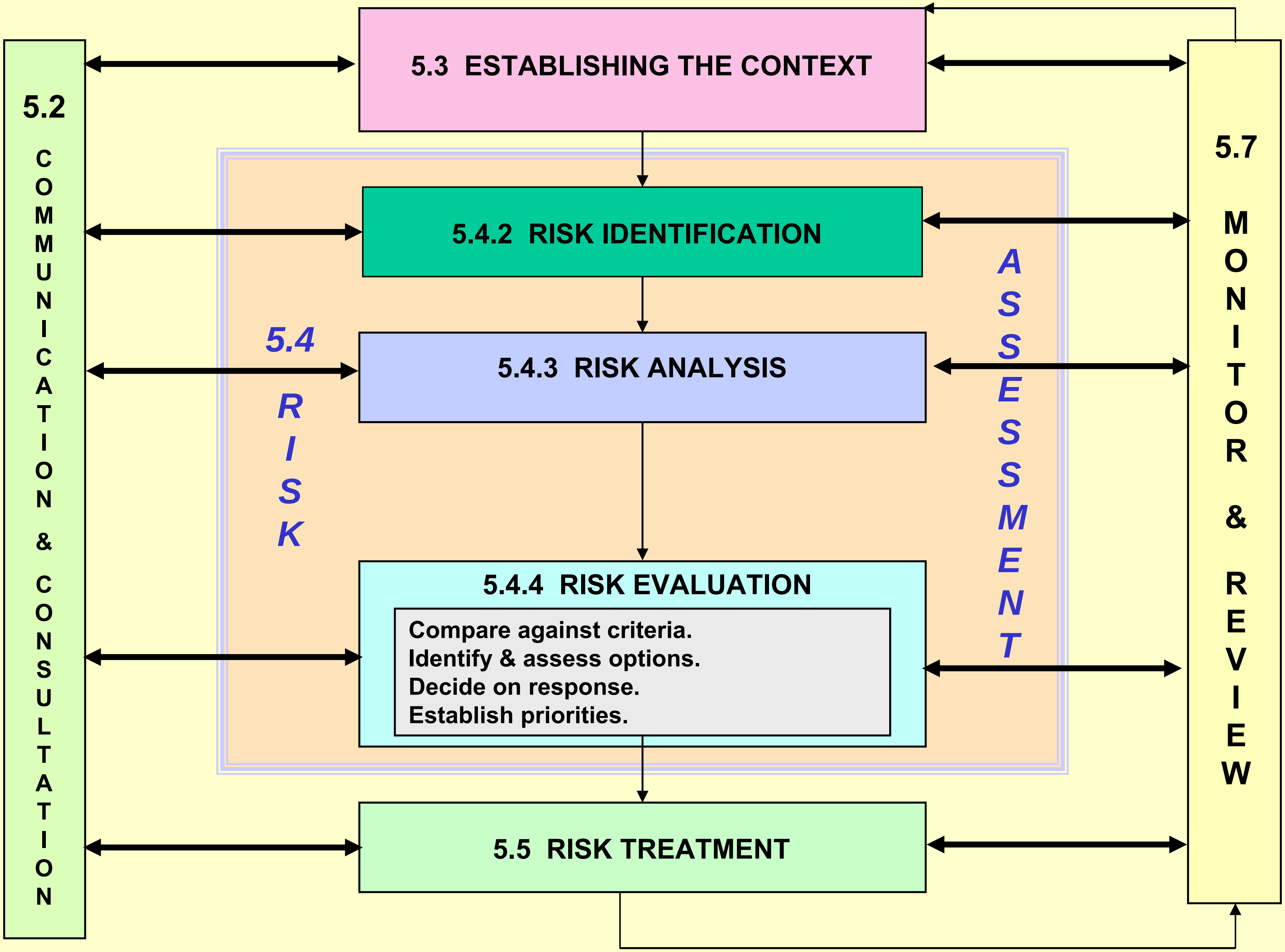
Where possible, confidence limits placed on estimates and the best available information sources are used.

Purpose:

- Separate minor risks from major.
- Provide data to assist in evaluation.

Preliminary analysis:

- Excluded risks where possible should be listed.

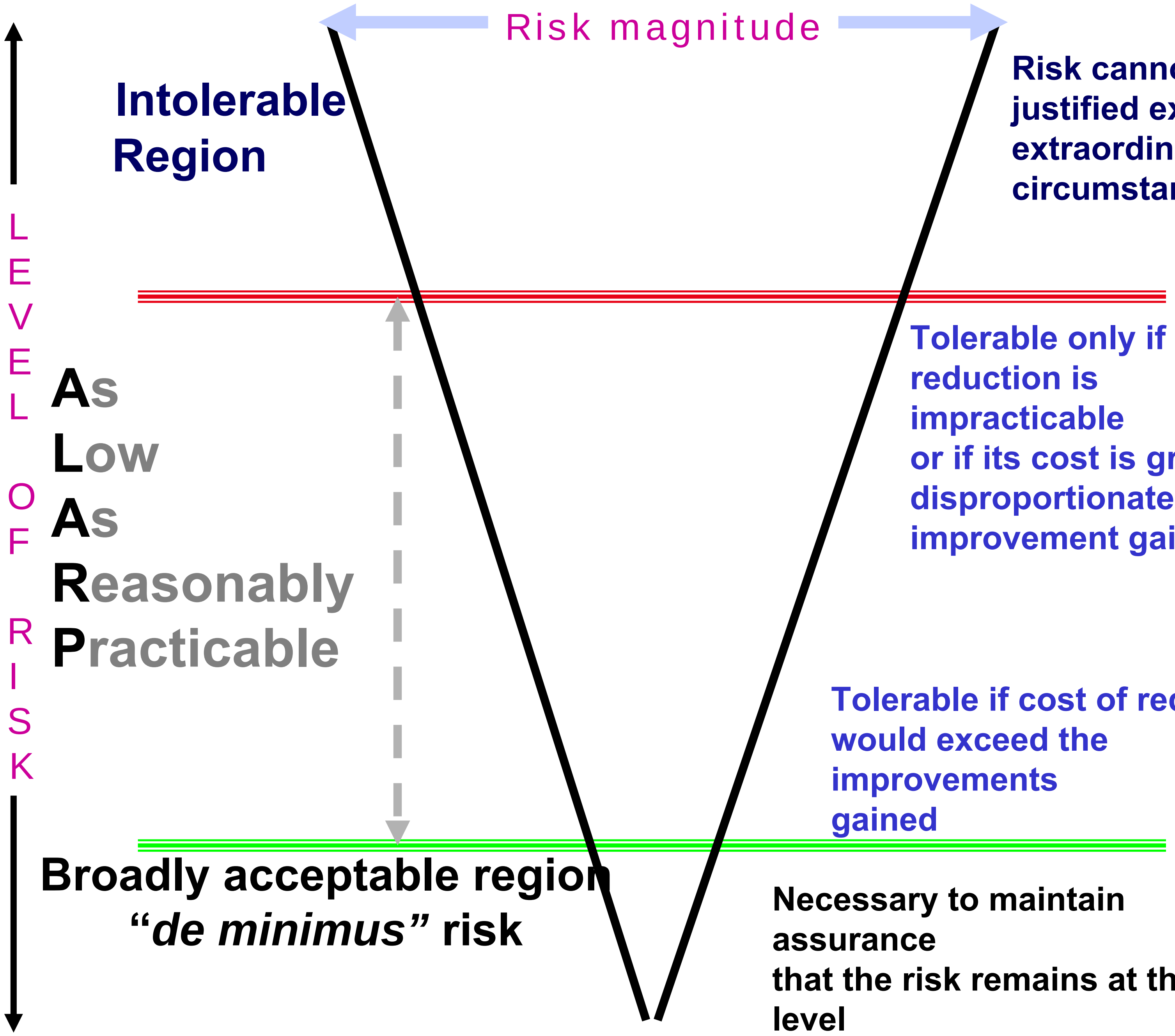


AS / NZS / ISO 31000:2009 Risk management process in detail

Risk Evaluation

Consider:

- Objectives of projects and opportunities
- Tolerability of risks to others
- Whether a risk needs treatment
- Deciding whether risk can be tolerated
- Whether an activity should be undertaken
- Priorities for treatment
- Comparing levels of risk found in analysis with previously established criteria.



Intolerable Region

Risk cannot be justified except in extraordinary circumstances

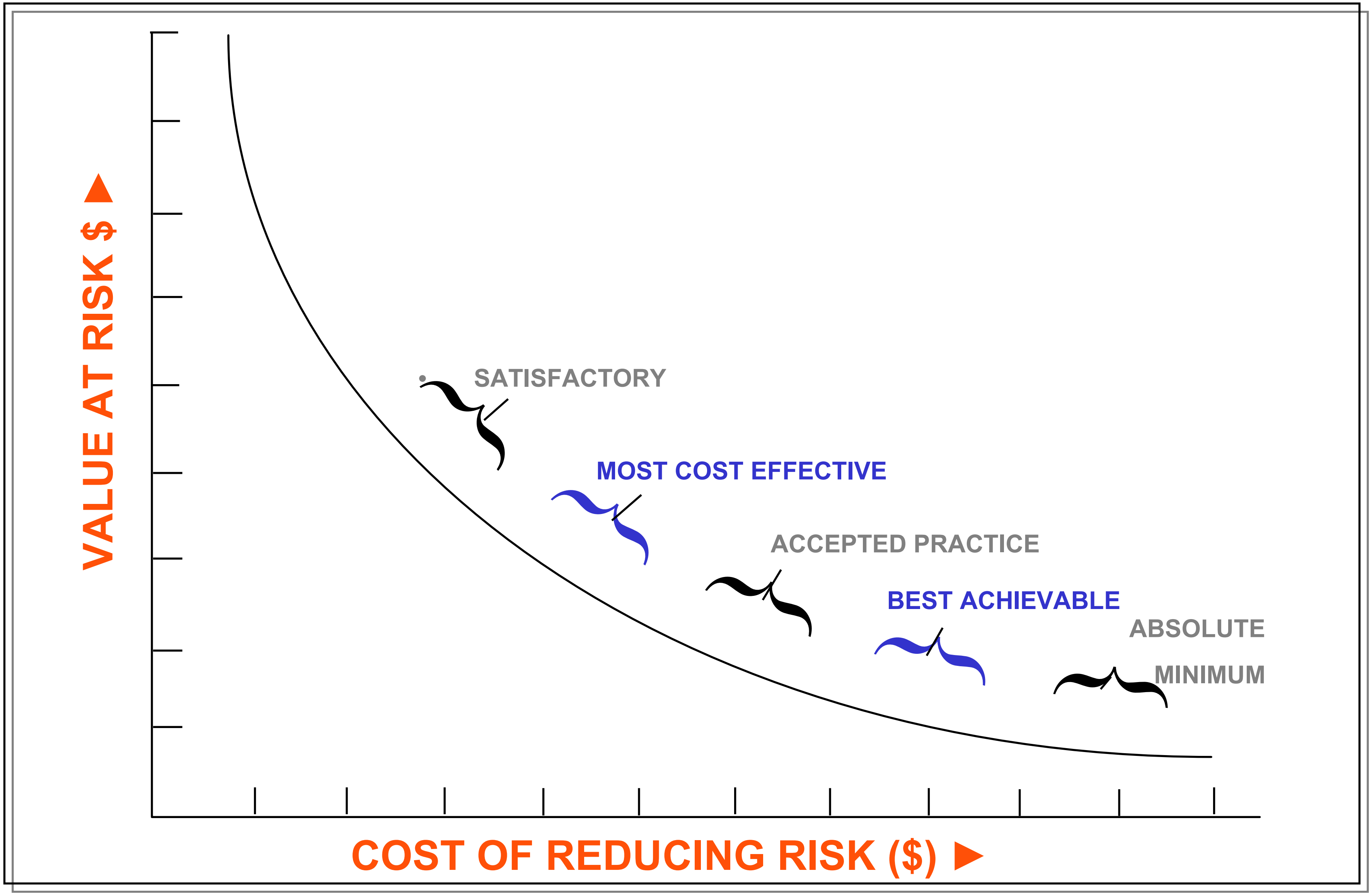
As
Low
As
Reasonably
Practicable

Tolerable only if risk reduction is impracticable
or if its cost is greatly disproportionate to the improvement gained

Tolerable if cost of reduction would exceed the improvements gained

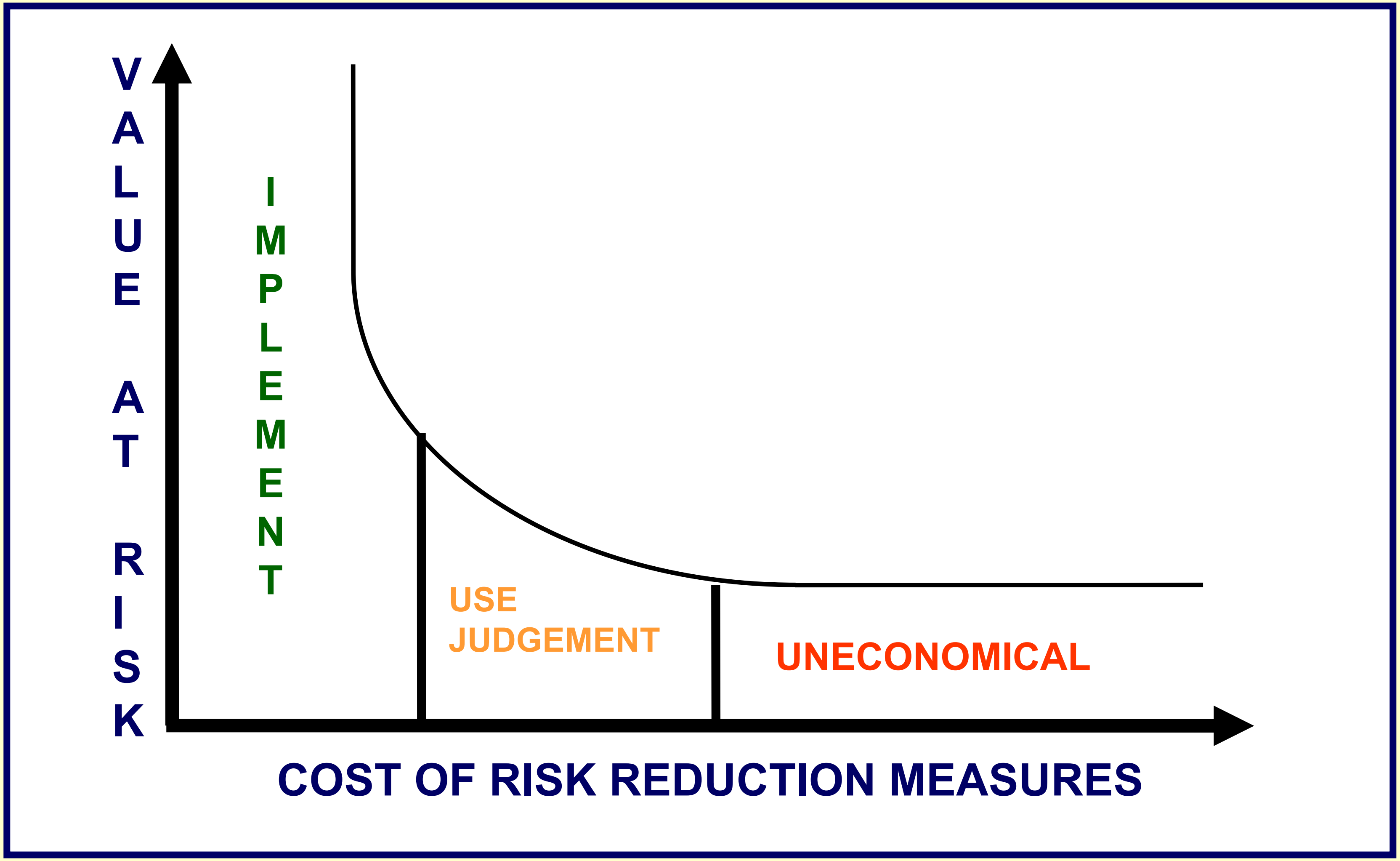
Broadly acceptable region
“*de minimus*” risk

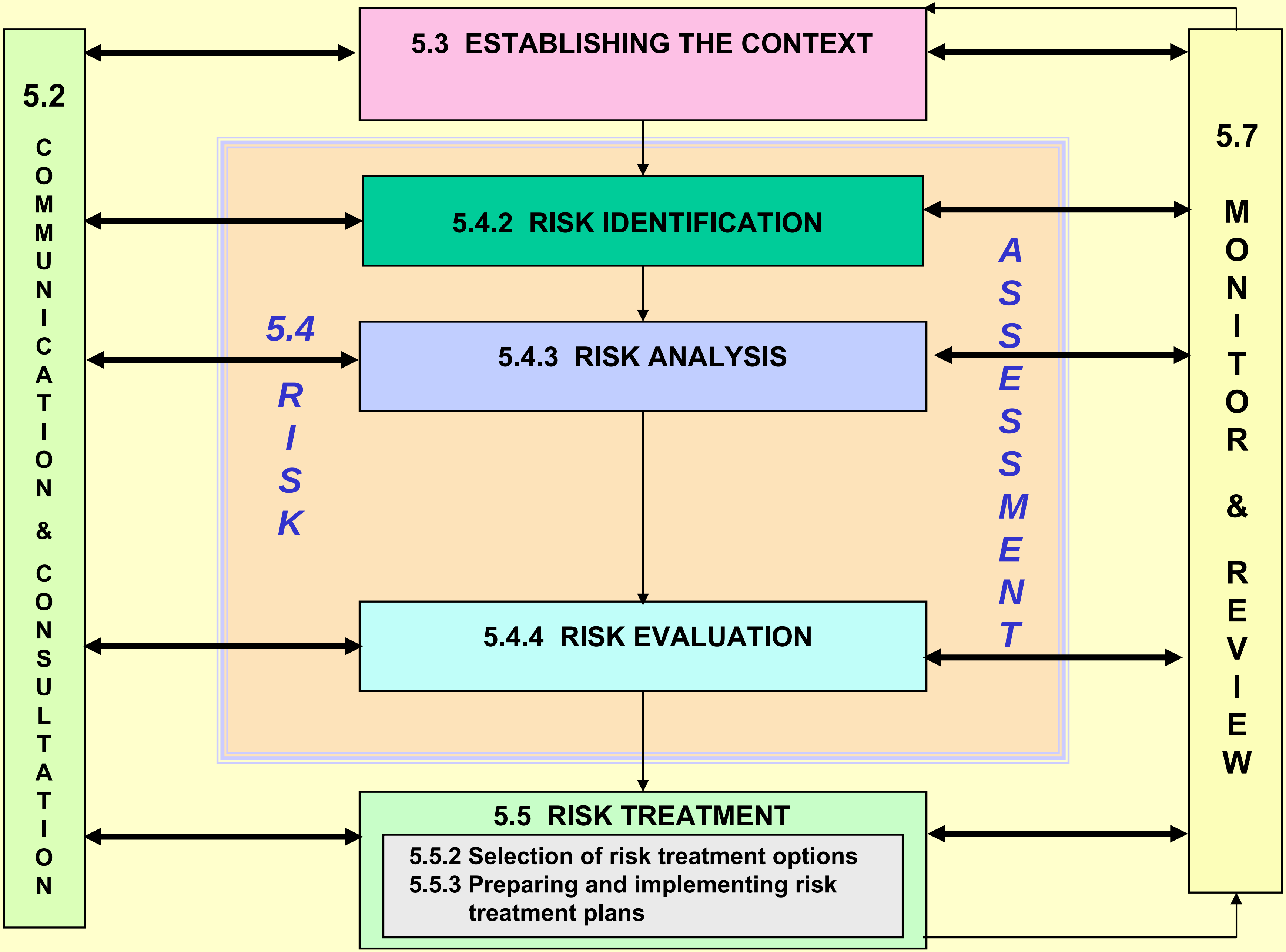
Necessary to maintain assurance
that the risk remains at this level



THE TRADE-OFF BETWEEN LEVEL OF RISK AND
COST OF REDUCING RISK B.F.Hough 1985

Cost of risk reduction measures





5.2 COMMUNICATION & CONSULTATION

5.3 ESTABLISHING THE CONTEXT

5.4 RISK ASSESSMENT

5.4.2 RISK IDENTIFICATION

5.4.3 RISK ANALYSIS

5.4.4 RISK EVALUATION

5.5 RISK TREATMENT

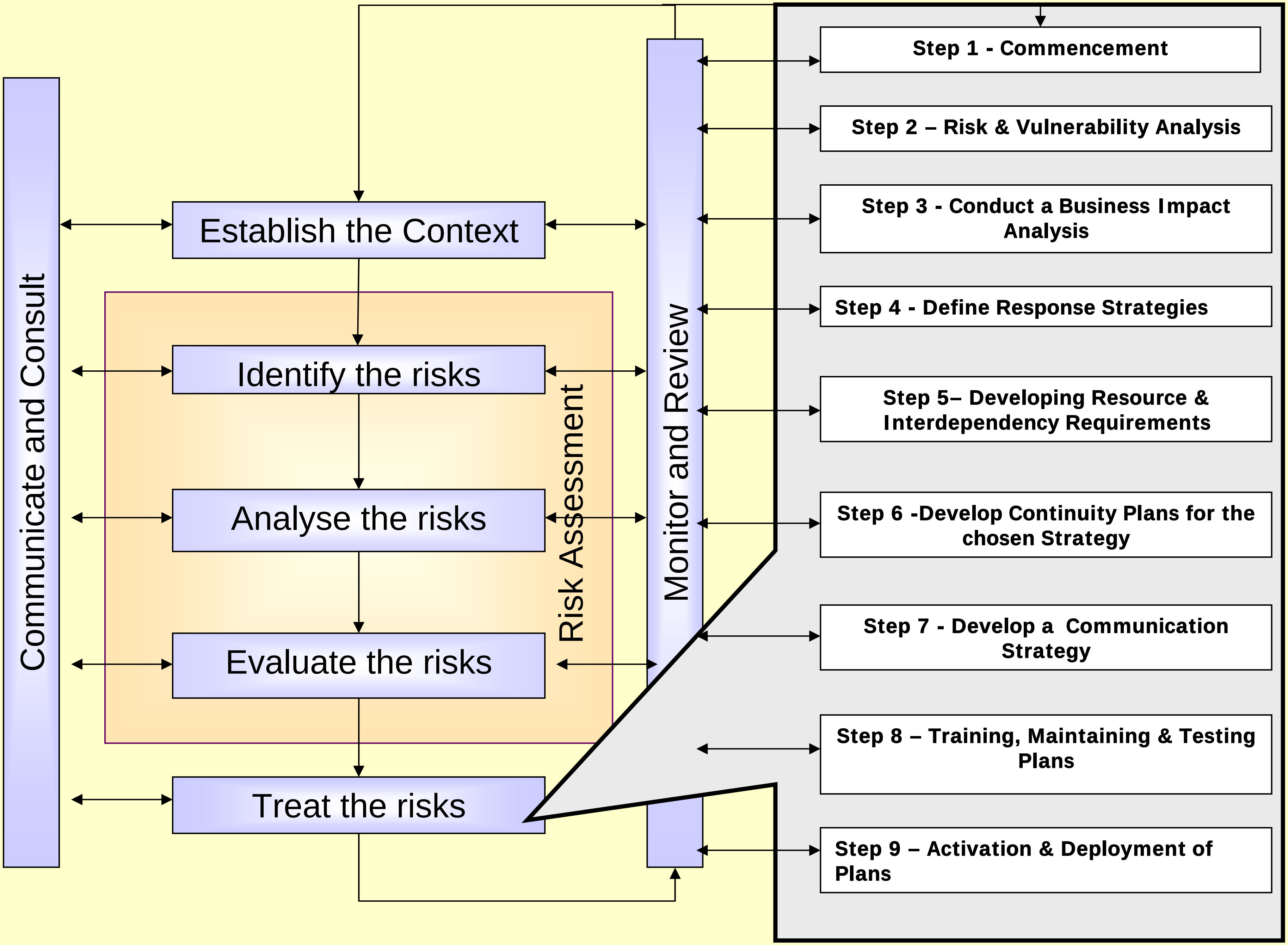
5.5.2 Selection of risk treatment options
5.5.3 Preparing and implementing risk treatment plans

5.7 MONITOR & REVIEW

AS / NZS / ISO 31000:2009 Risk management process in detail

Risk Treatment

- Reduce
  - Likelihood
  - Consequence
- Contingency planning
- Sharing in full or part (this creates a new risk)
- Avoid (but not because of aversion)
- Retain residual



Communicate and Consult

Establish the Context

Risk Assessment

Identify the risks

Analyse the risks

Evaluate the risks

Treat the risks

Monitor and Review

Step 1 - Commencement

Step 2 – Risk & Vulnerability Analysis

Step 3 - Conduct a Business Impact Analysis

Step 4 - Define Response Strategies

Step 5– Developing Resource & Interdependency Requirements

Step 6 -Develop Continuity Plans for the chosen Strategy

Step 7 - Develop a Communication Strategy

Step 8 – Training, Maintaining & Testing Plans

Step 9 – Activation & Deployment of Plans

HB 221:2004 BUSINESS CONTINUITY MANAGEMENT

Contingency Planning

Business Continuity Management:

- Emergency evacuation plans
- Off site data & information storage
- Business contingency plans
- Business relocation plans
- Business resumption plans
- Review, reassess and revise plans

Treatment Options

Consider:

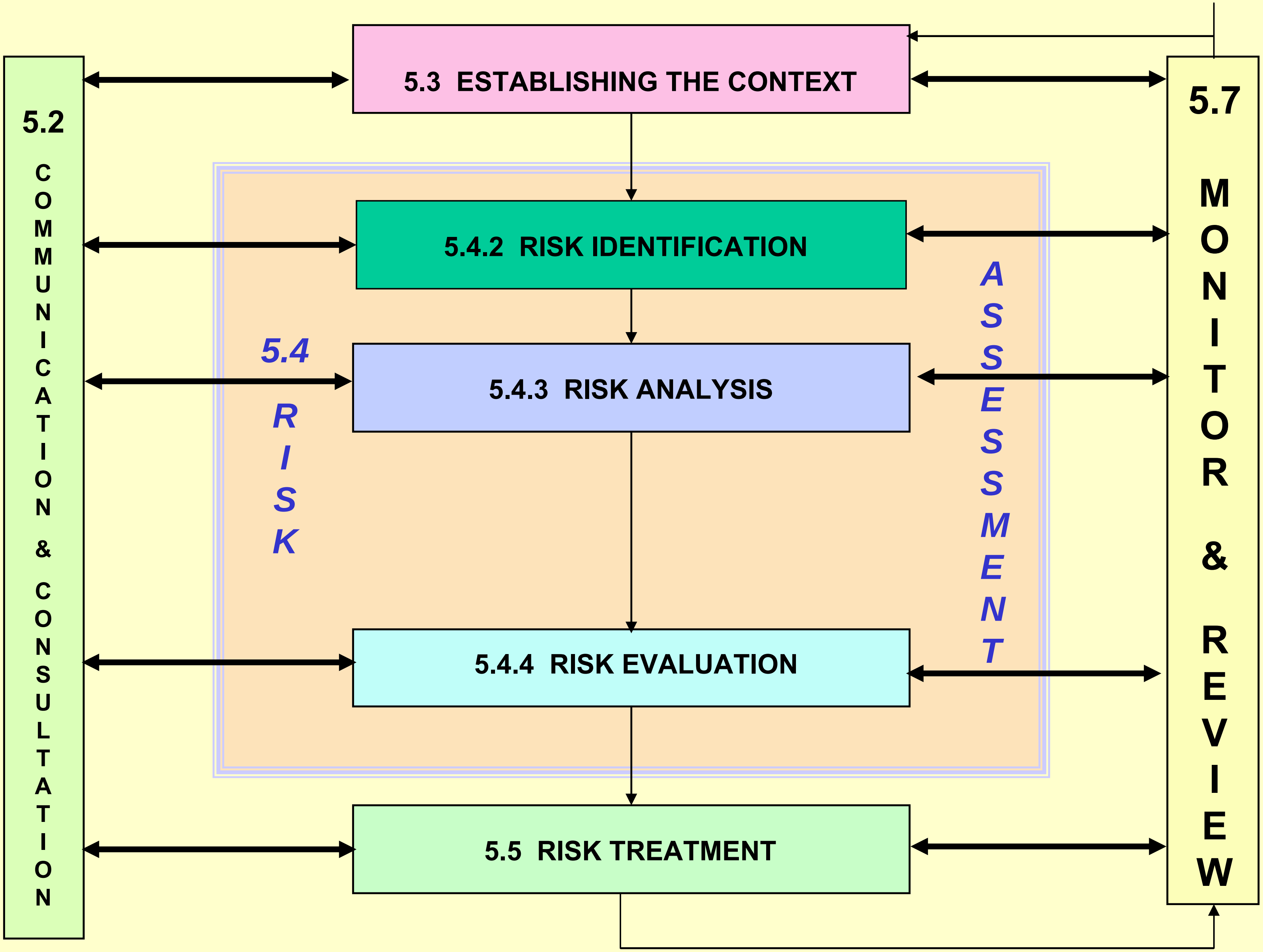
- Opportunities created by risk
- Cost of implementation vs. benefits
- Extent of risk reduction vs. benefits
- Criteria of tolerability
- Rare but severe risks
- Risk perception and communication

In general, costs of managing risk commensurate with benefits and adverse impacts as low as reasonably achievable.

Treatment Plans

Document how options implemented:

- Responsibilities
- Schedules
- Expected outcomes
- Budgeting
- Performance measures
- Review processes



AS / NZS / ISO 31000:2009 Risk management process in detail

DISCUSSION

Does your current risk management framework document how your treatment options will be implemented?

Is there a consistent approach in your agency to ensure that the cost of managing risk is considered?

Improving The Management of Risk

Monitor and Review

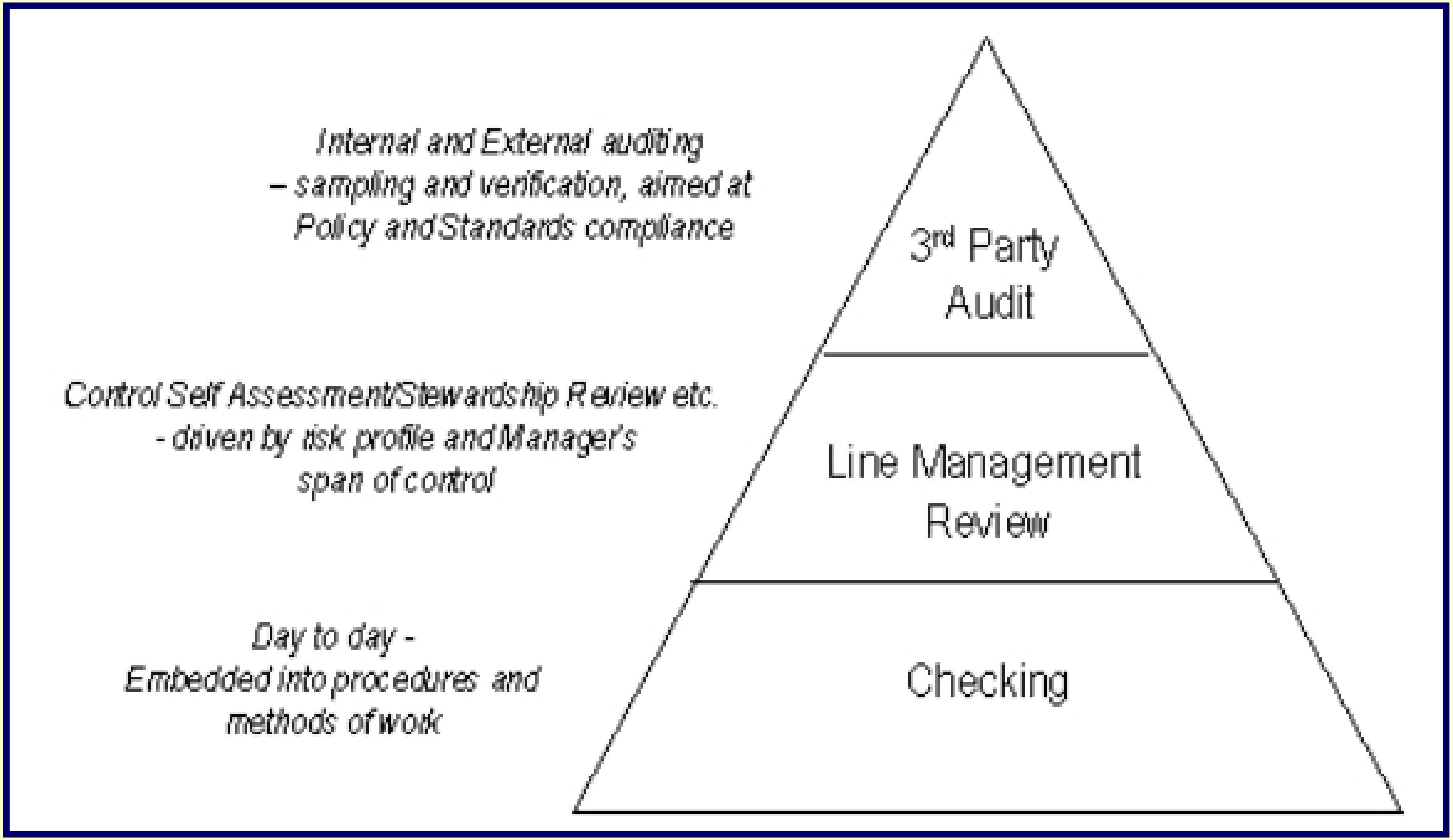
- **RM is a journey not a destination.**
- **What may be of minor significance today may be the disaster of tomorrow.**
- **Review is an integral part of the risk management process.**

AS/NZS/ISO 31000:2009
Extending The Process

The role of assurance activity, not just as a risk control, but as part of ‘Monitor and Review’ should be developed. This should go further than just audit.

Other interested stakeholders can also benefit from the risk process, such as quality assurance, security, safety & environment management. The process is all about facilitating linkages between different stakeholders across the organisation

AS/NZS/ISO 31000:2009
Role Of Assurance Activity



Internal and External auditing – sampling and verification, aimed at Policy and Standards compliance

3rd Party Audit

Control Self Assessment/Stewardship Review etc. - driven by risk profile and Manager's span of control

Line Management Review

Day to day - Embedded into procedures and methods of work

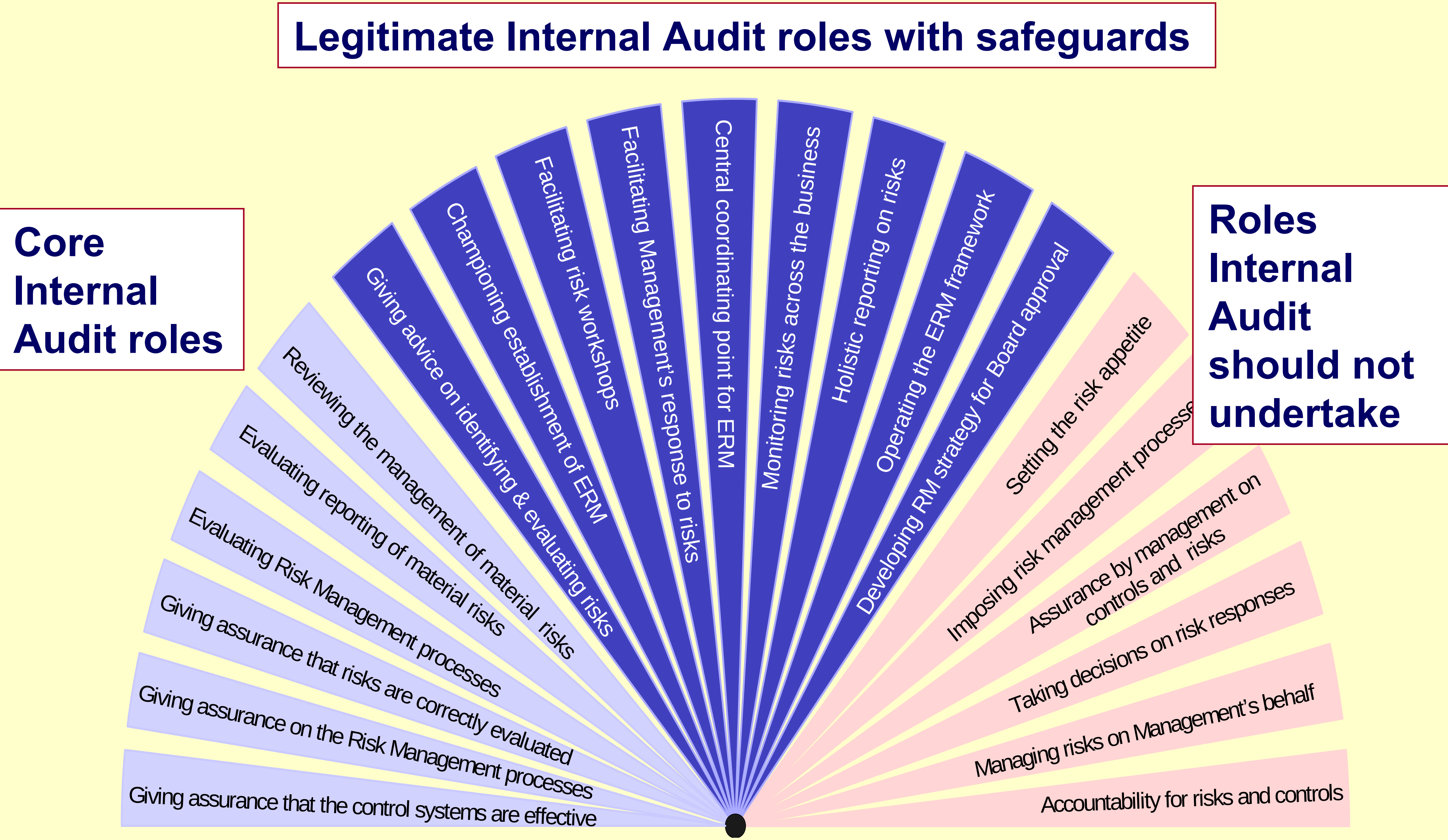
Checking

Internal Audits’ Role in ERM – priority should be given to…

- High exposure risks, that is, where the consequence of the event could be high
- High current residual risks, where there is evidence of low control effectiveness
- The potential for failure of controls, especially where this would result in high, or frequent, consequences
- Activities where change could give rise to significant risk
- Parts of the organisation that are consciously exposed to high levels of risk
- Technological advances that may offer more effective or lower cost alternatives to current risk treatment

HB 158—2006 Delivering assurance based on AS/NZS 4360:2004 Risk Management

Internal Audits’ Role in ERM – *who does what?*



Legitimate Internal Audit roles with safeguards

Core Internal Audit roles

- Giving assurance that the control systems are effective
- Giving assurance on the Risk Management processes
- Giving assurance that risks are correctly evaluated
- Evaluating Risk Management processes
- Evaluating reporting of material risks
- Reviewing the management of material risks

- Giving advice on identifying & evaluating risks
- Championing establishment of ERM
- Facilitating risk workshops
- Facilitating Management's response to risks
- Central coordinating point for ERM
- Monitoring risks across the business
- Holistic reporting on risks
- Operating the ERM framework
- Developing RM strategy for Board approval

Roles Internal Audit should not undertake

- Setting the risk appetite
- Imposing risk management processe
- Assurance by management on controls and risks
- Taking decisions on risk responses
- Managing risks on Management’s behalf
- Accountability for risks and controls

HB 158—2006 Delivering assurance based on AS/NZS 4360:2004 Risk Management

DISCUSSION

- What are the internal reporting and recording processes that your agency has in place?

- What is the role that internal audit undertakes in reviewing and monitoring your agency’s risk management framework and programs?

Reporting

- Reporting is incidental to good RM, not the sole focus of it!
- If you only focus on reporting, you will not motivate the required culture change
- Advanced Governance Codes (e.g. LSX and ASX) require two sets of reports:
  - The maturity and performance of the RM framework
  - The risk profile and how/why it has changed

Recording the Risk Management Process

- Demonstrates process conducted properly.
- Provides a record of risks.
- Provides decision makers with plan for approval and implementation.
- Provides accountability tool.
- Facilitates monitoring and review.
- Provides an audit trail.
- Enables sharing and communication of information.

And Finally!!

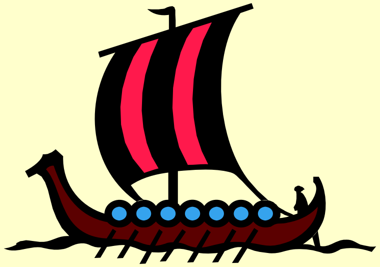
- AS/NZS/ISO 31000:2009 is the natural successor to the AS/NZS 4360 Standard
- Hopefully it will also dislodge COSO
- It encourages ‘ERM’, but also provides for silo/project risk management
- Following AS/NZS/ISO 31000:2009 will provide a low cost, high chance of success approach to ERM
- AS/NZS/ISO 31000:2009 will add value and reduce risk in risk management

Managing risk is about creating value out of uncertainty

The greatest risk of all

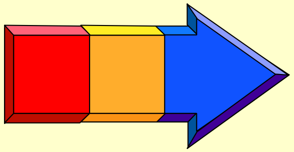
is to take no risk at all!

The Journey Continues



A journey ....

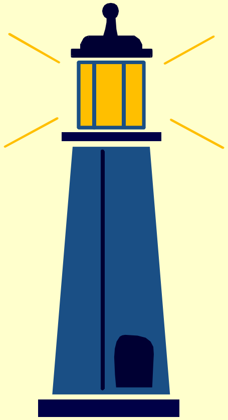
A race



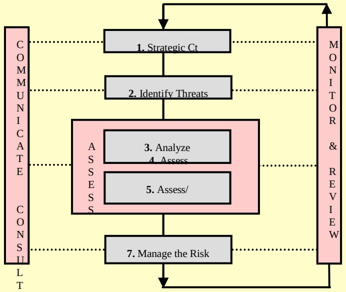
In pursuit of performance

Building Value

AS/NZS/ISO 31000:2009 provides generic guidance on how to embed risk management, and introduces the concept of "positive" risk to help you on the way.

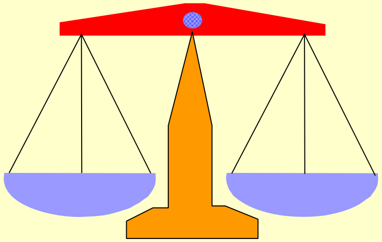


Structure Direction



Processes

Culture Communication



Opportunities Risks