

**ISO 31000:2009;  
ISO/IEC 31010  
& ISO Guide 73:2009  
International Standards for the  
Management of Risk**

**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 O BOX 226, NUNDAH Qld 4012, Australia  
E-mail: [kknight@bigpond.net.au](mailto: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.

# **risk owner**

**person or entity with the accountability and authority to manage a risk**

# **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.

# Yet to be defined

**Accountable** Liability for the outcomes of actions or decisions

**NOTE:** Includes failure to act or make decisions

**OR**

being obligated to answer for a decision

**OR**

obligation to answer for an action.

---

**Responsible** Obligation to carry out duties or decisions, or control over others as directed

**OR**

having the obligation to act

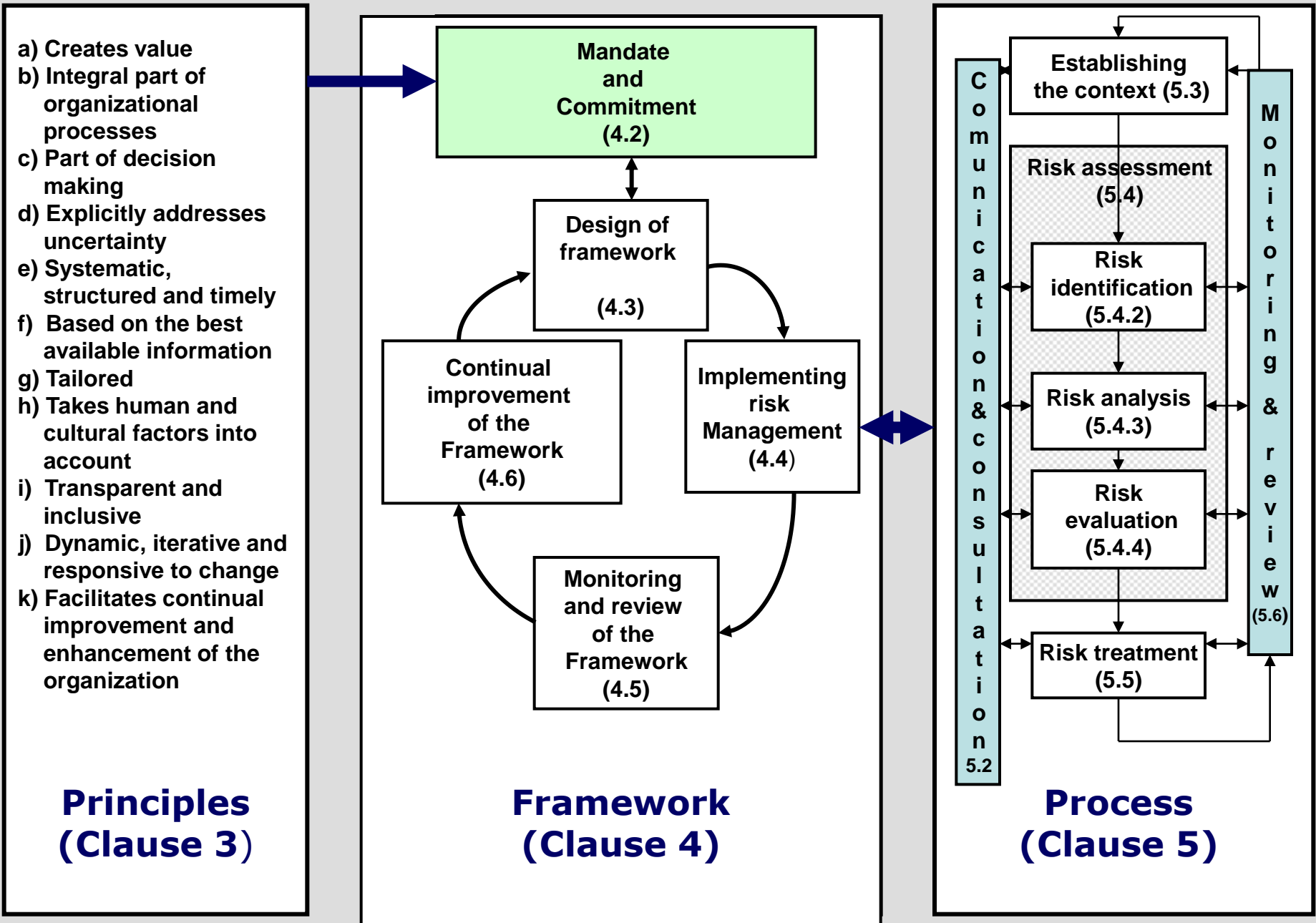
**OR**

obligation to carry out instructions.

# Corporate Governance

**The way in which an organisation is governed and controlled in order to achieve its objectives. The control environment makes an organisation reliable in achieving these objectives within a tolerable degree of risk.**

**It is the glue which holds the organisation together in pursuit of its objectives while risk management provides the resilience.**



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

# **Business Principles Approach**

**AS/NZS 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**



# **Risk management should create value**

- **RM contributes to the achievement of objectives.**
- **Protects value – minimise downside risk, protects people, systems and processes.**

# **Risk management should be an integral part of organizational processes**

- **RM is not a stand-alone activity from the management system of the organisation.**
- **RM is part of the process - not an 'additional' compliance task.**

# **Risk management should be part of decision making**

- **Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.**
- **Helps allocate scarce resources.**

# **Risk management explicitly addresses uncertainty**

- **Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.**
- **RM addresses uncertainty, no matter the level of uncertainty.**

# **Risk management should be systematic and structured**

- **A systematic, timely and structured approach to the management of risk contributes to efficiency and to consistent, comparable and reliable results.**
- **The more aligned – the more effective and efficient.**

# **Risk management should be based on the best available information**

- The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement.**
- Information costs money. Perfect information is not always possible.**
- Start with resources/expertise you have or gain easily.**
- Increase information as the level of risk increases.**

# **Risk management should be tailored**

- **Risk management is aligned with the organization's external and internal context and risk profile.**
- **Different risk appetites & different measurements.**
- **Context remains one of the most difficult areas.**

# **Risk management should take into account human factors**

**The management of risk recognizes the capabilities, perceptions and intentions of people that make every organisation different.**



# **Risk management should be transparent and inclusive**

- **Appropriate and timely involvement of stakeholders at all levels of the organization, ensures that the management of risk remains relevant and up-to-date.**
- **The management of risk must be clearly set out in job profiles/employment contracts and annual appraisals.**

# **Risk management should be dynamic, iterative and responsive to change**

- **External and internal events happen, context and knowledge change, monitoring and review take place, new risks emerge, some change, and others disappear.**
- **Must keep RM relevant and accurate so as to support decisions and strategies.**
- **Regular reviews of risk register and framework.**
- **Internal audit programme informed by corporate risk register.**

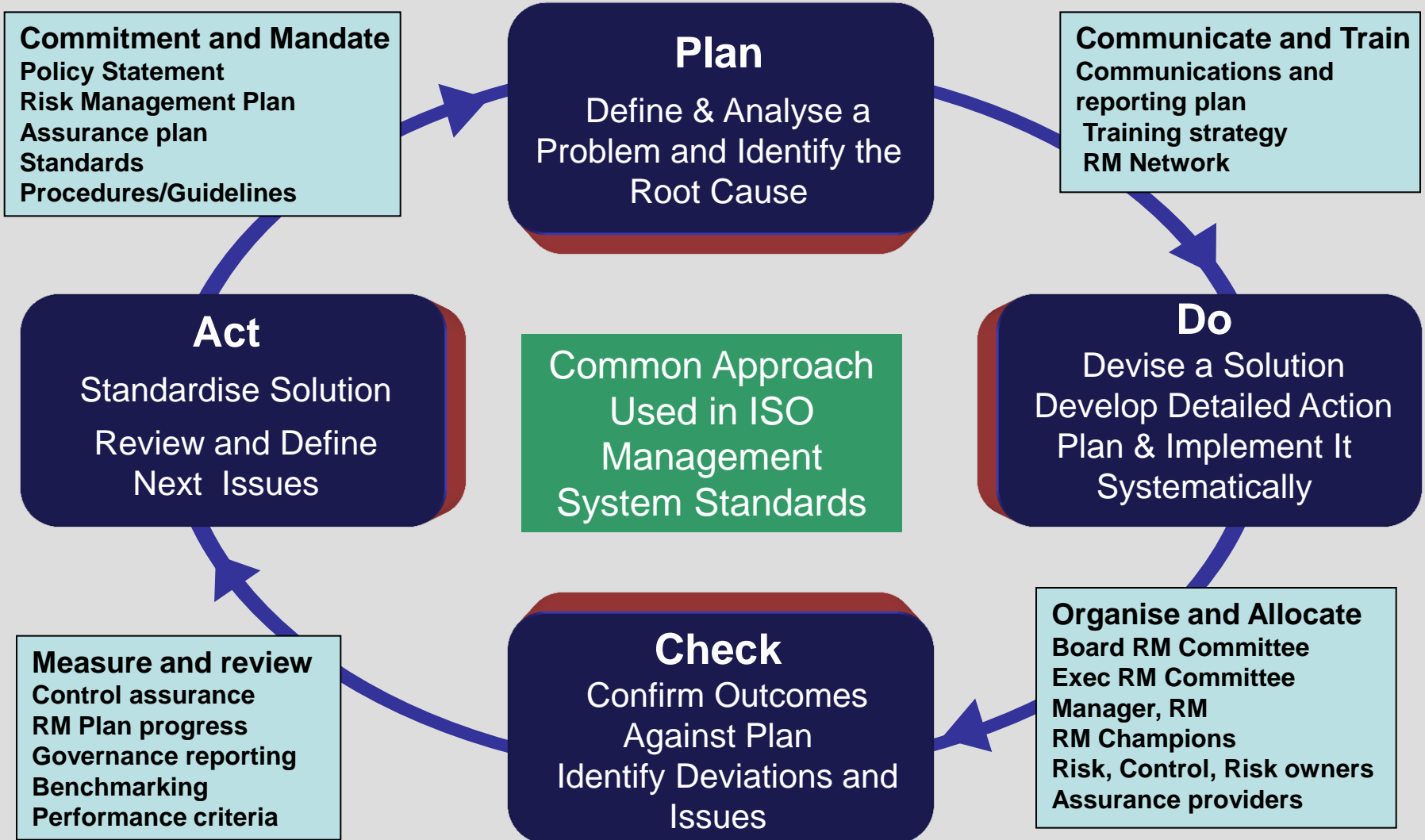
# **Risk management should be capable of continual improvement and enhancement**

- Organizations should develop and implement strategies to improve the maturity of their management of risk alongside all other aspects of their management system.**
- RM maturity and improvement strategies should be included in the RM Plan.**

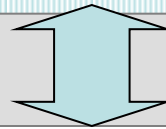
# **AS/NZS ISO 31000:2009 Risk management framework (Clause 4)**

- 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 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

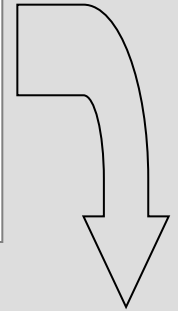
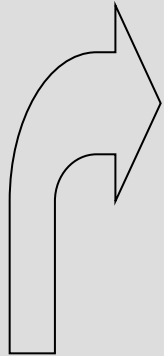


## Mandate and commitment (4.2)



### 4.3 Design of framework

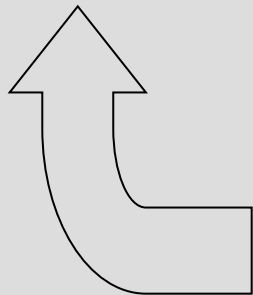
- 4.3.1 Understanding the organization and its context
- 4.3.2 Establishing risk management policy
- 4.3.3 Accountability
- 4.3.4 Integration into organizational processes
- 4.3.5 Resources
- 4.3.6 Establishing internal communication and reporting mechanisms
- 4.3.7 Establishing external communication and reporting mechanisms



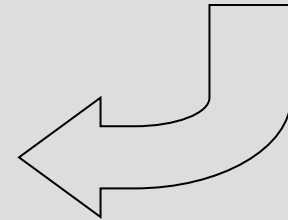
### 4.6 Continual improvement of the framework

### 4.4 Implementing risk management

- 4.4.1 Implementing the framework for managing risk
- 4.4.2 Implementing the risk management process



### 4.5 Monitoring and review of the framework



# **Understanding the organisation and its context**

- **External Context**

- **Consider:**

- **Trends**
    - **Key drivers**
    - **Perceptions/values of key stakeholders**
    - **PESTLE: (Political, Economic, Social, Technological, Legal, Environmental factors)**

# **Understanding the organisation and its context**

- **Internal Context**
  - **Governance Structures**
  - **Objectives, strategies and policies**
  - **Knowledge, skills and resources**
  - **Organisational culture**
  - **Contractual relationships**



# **Risk Management Policy**

- **Must be simple, achievable, understandable and auditable with the clear mandate and commitment of top management**
- **aligned to the organisation's culture with the risk makers and the risk takers the risk owners.**
- **Document components**
  - **Rationale and policy links**
  - **Accountability and responsibility**
  - **Management of conflicts of interest**
  - **Measurement of RM performance**
  - **Reporting processes**
  - **Policy review process/cycle**

# **Accountability**

- **All accountable risk owners are clearly identified and provided with authority & resources to manage risk**
- **Board accountability for framework implementation**
- **Accountability of risk owners at all levels of the organisation clearly identified**
- **Performance measurement processes in place**
- **Reporting and escalation processes clearly established**

# **Integration into organisational processes**

- **The management of risk should be part of routine organisational processes**
  - Policy development
  - Business/strategic planning
  - Change management
  - Decision-making processes
- **Risk Management Plan**
  - Organisation-wide
  - Linked to or integrated in to other plans: strategic plans, implementation plans, operational plans etc

# Resources

- **expenditure on the management of risk is an investment**
  - **Good RM will make an organisation more effective, but it requires dedicated resources**
- **Resources include:**
  - **People: skills, experience and competence**
  - **Time and funds: to execute the process**
  - **Defined processes, methods and tools**
  - **Information systems**
  - **Awareness, education and training programs**

# **Establishing internal & external communication and reporting mechanisms**

- **Internal**
  - Ongoing awareness, education and training
  - Framework performance reporting and outcome reviews
  - Information management
  - Stakeholder engagement
- **External**
  - Stakeholder engagement
  - Regulatory reporting requirements
  - Use reporting to build confidence
  - Business continuity (management of disruption related risk) communication

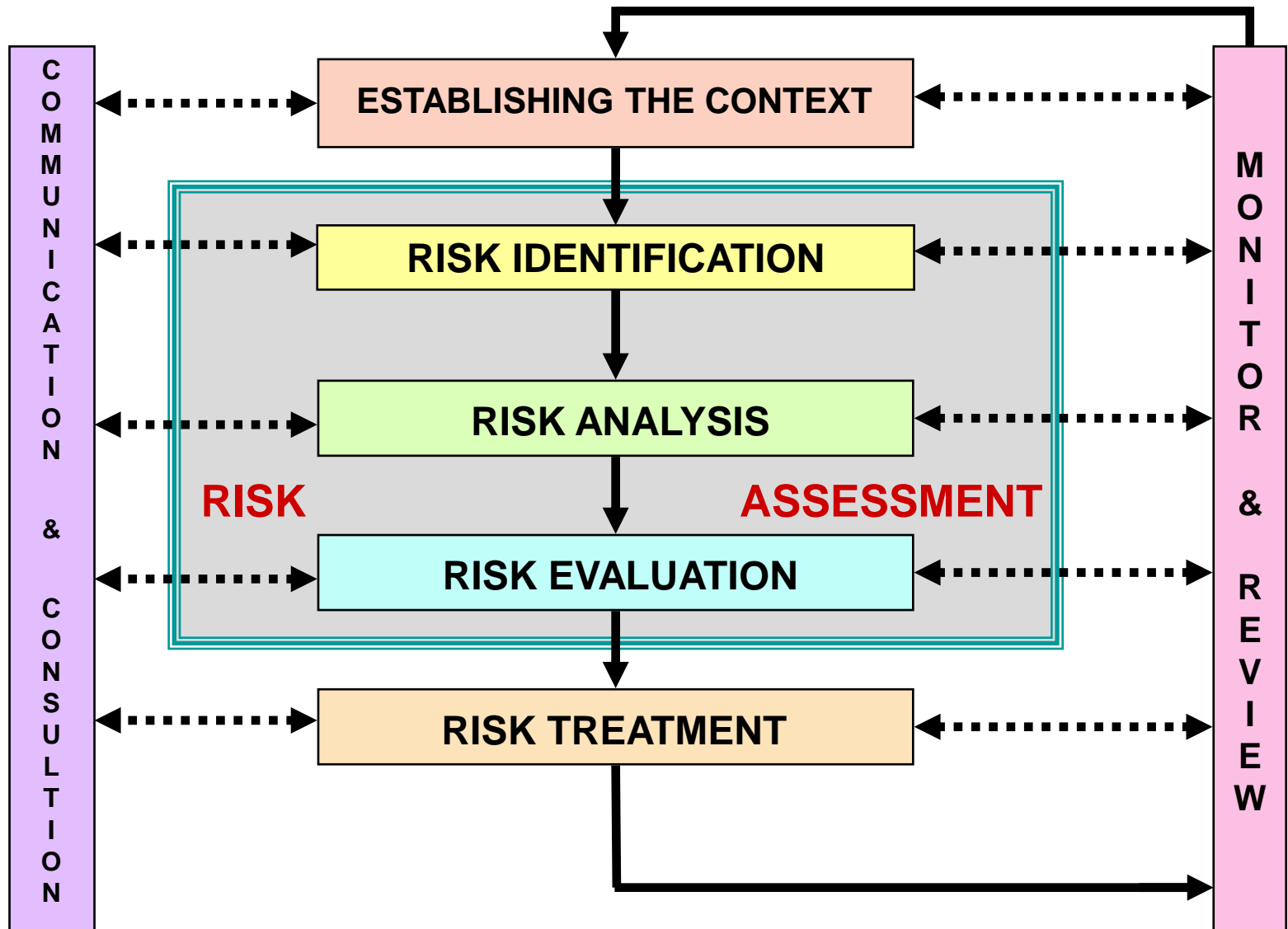
# Implementing risk management

- **Implementing the framework**
  - **Ensure**
    - **Appropriate timing**
    - **Alignment with organisational strategy and processes**
    - **Compliance with regulation**
  - **Apply to organisational processes**
  - **Train and educate staff**
  - **Communicate and consult**
- **Implementing the risk management process**
  - **Define the process for the organisation**
  - **Implement at all levels (appropriate processes)**
  - **Establish a monitoring process**

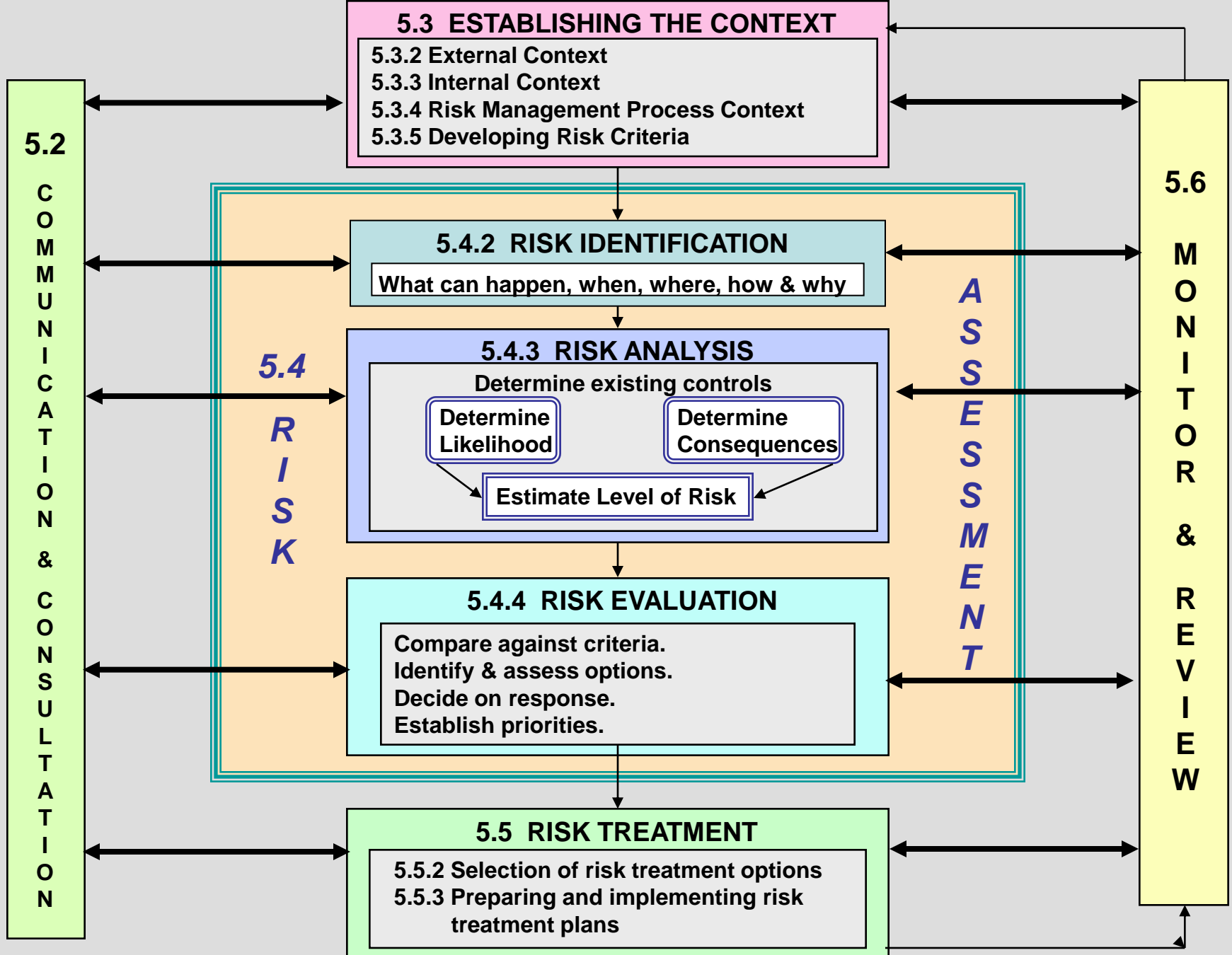
# **AS/NZS ISO 31000:2009 Risk management process (Clause 5)**

- 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.**

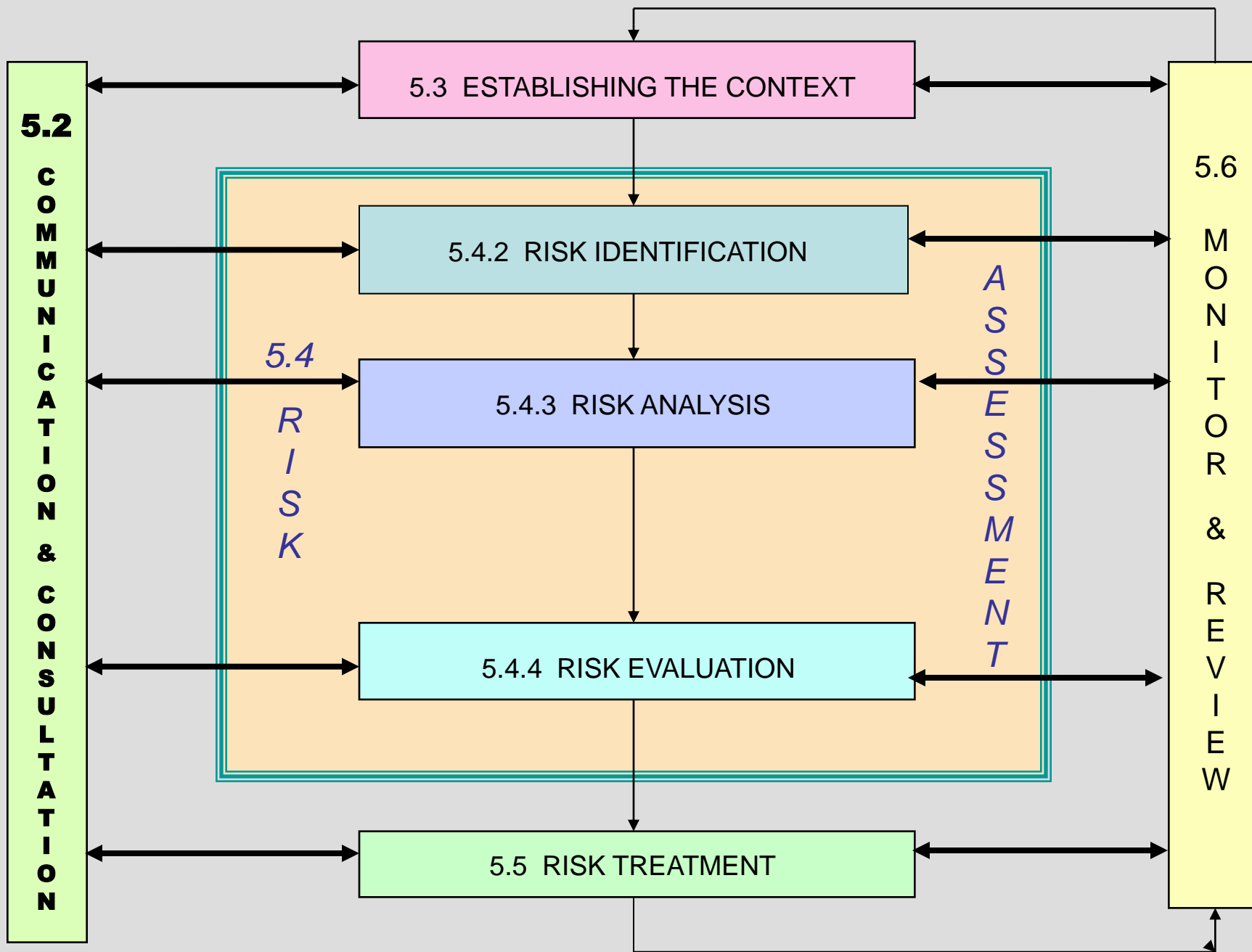
# AS/NZS ISO 31000:2009 Process Overview







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



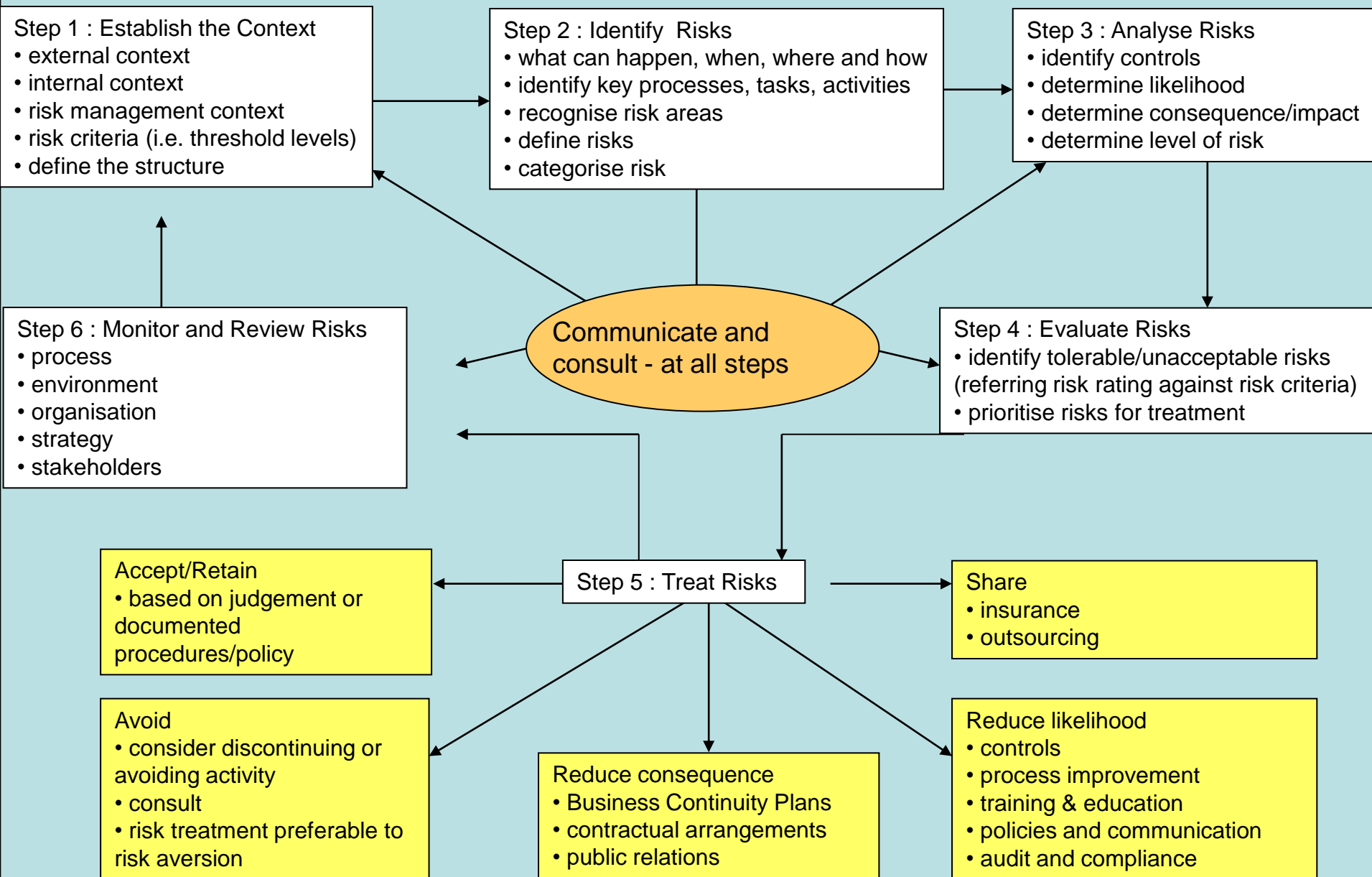
**AS/NZS ISO 31000:2009 Risk management process in detail**

# Communicate & Consult

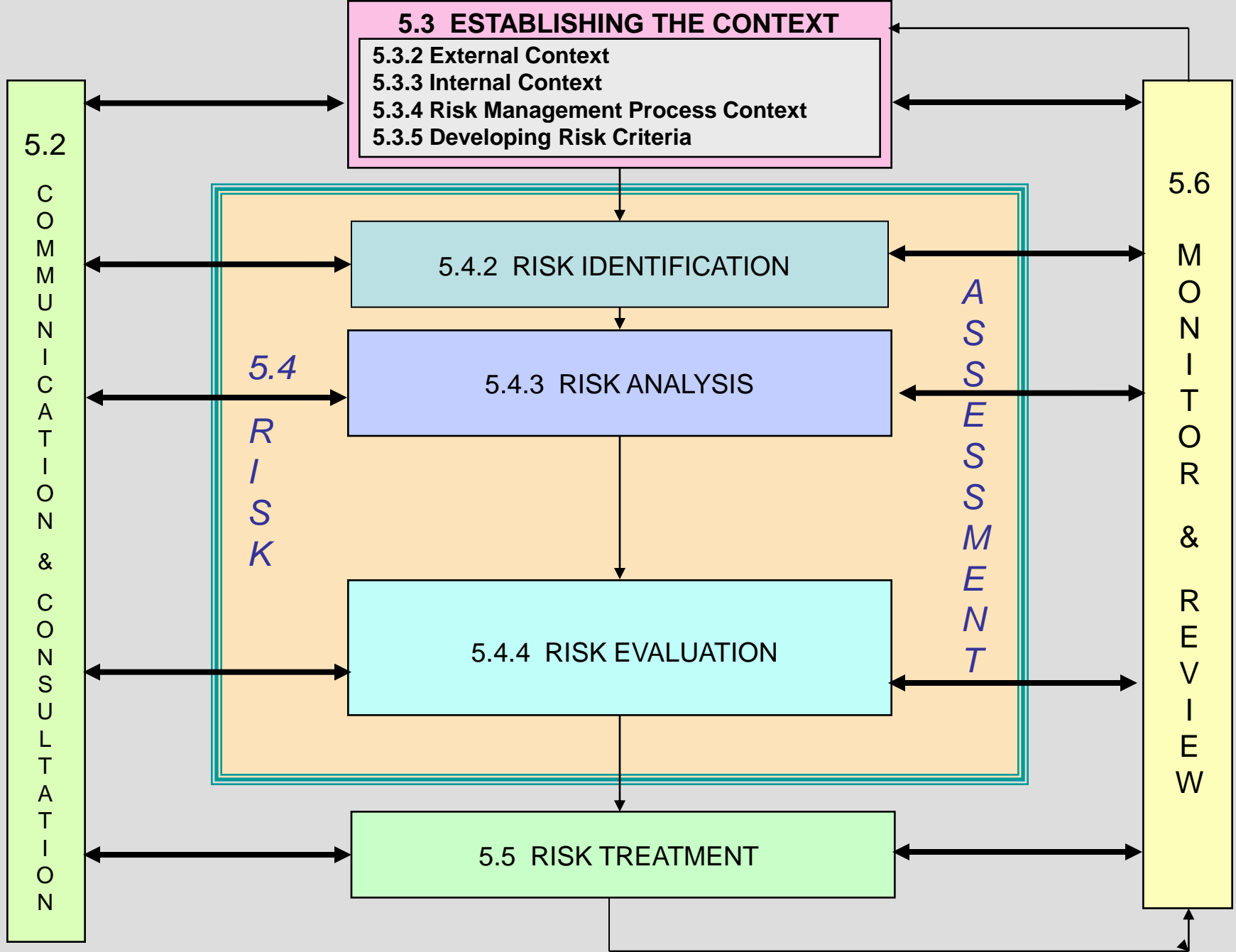
**Communicating risk successfully is neither a public relations nor a crisis communications exercise.**

**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.***

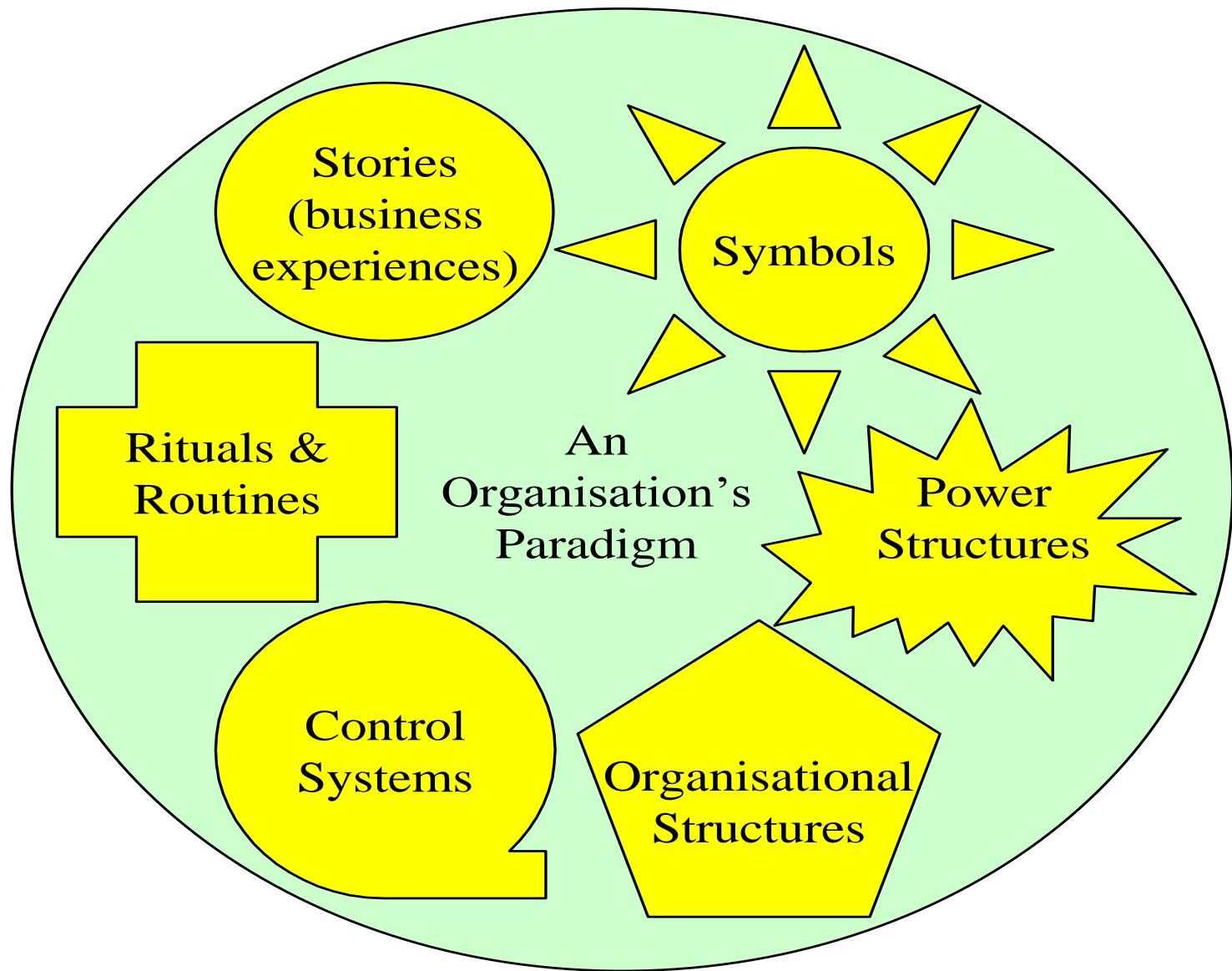


## Communication & Consultation in the risk management process

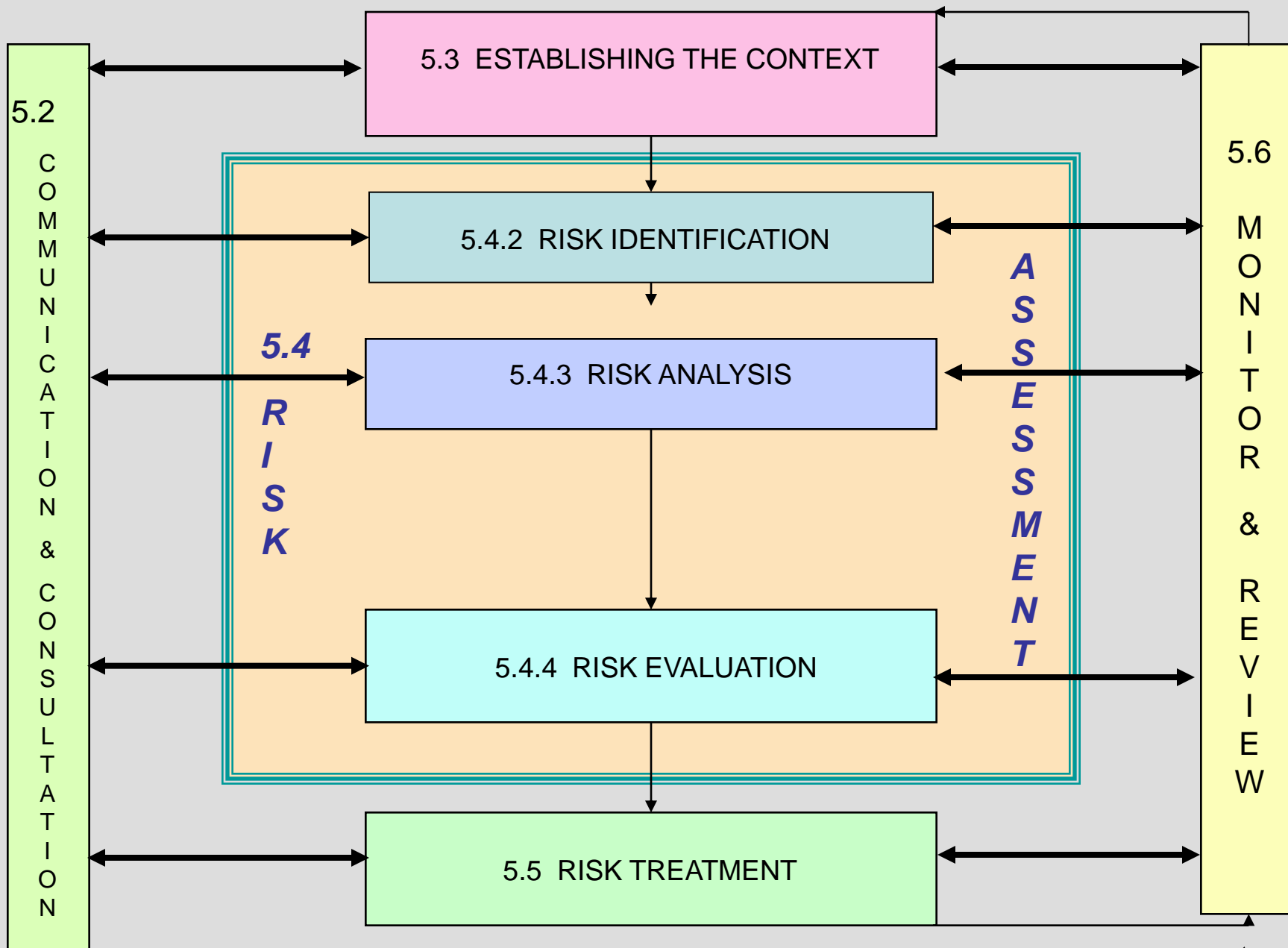


# Establish the Context

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



Adapted from Johnson & Scholes, 1993, p.61



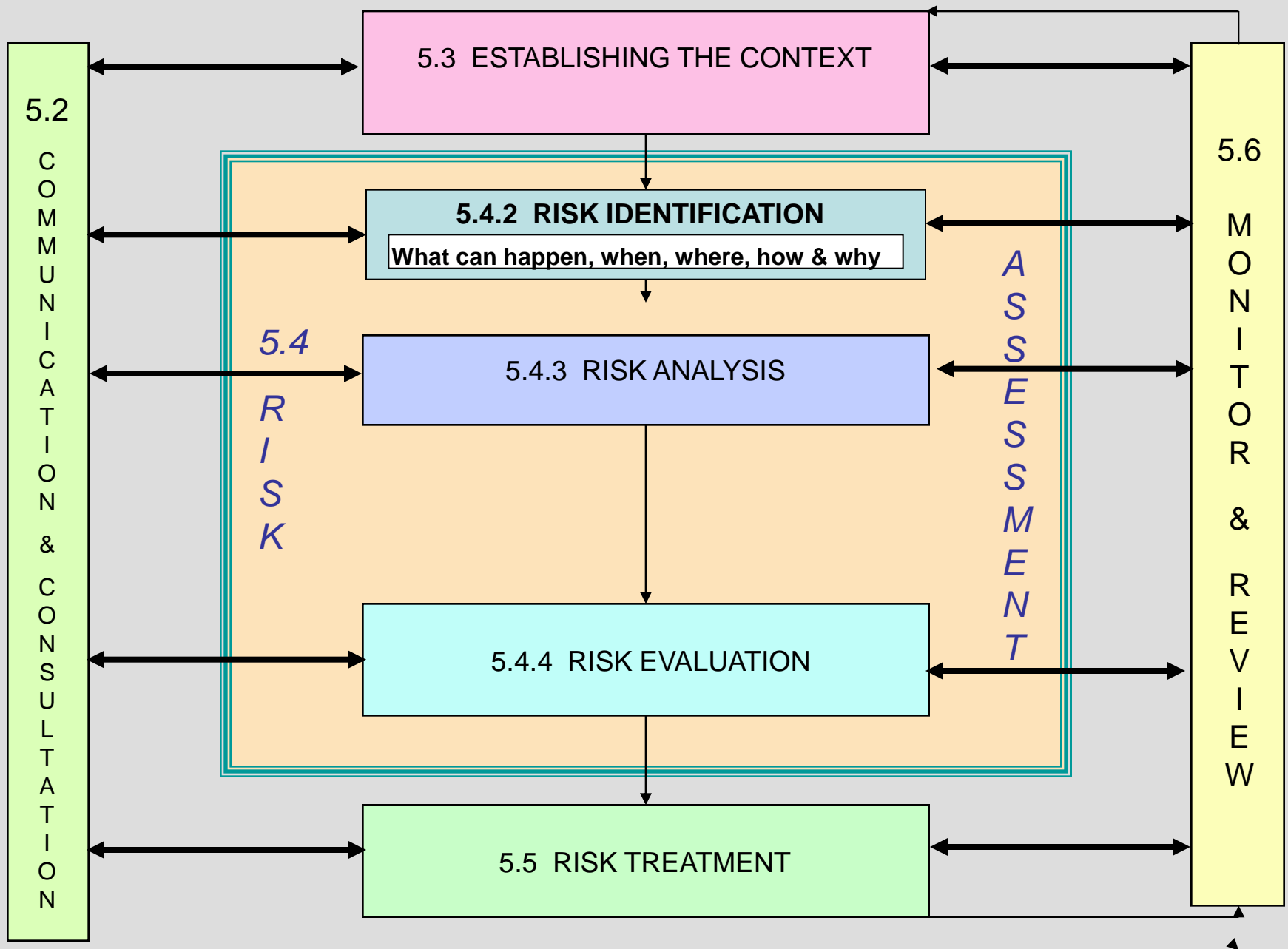


# **ISO/IEC 31010:2009**

## **Risk Management - Risk Assessment Techniques**

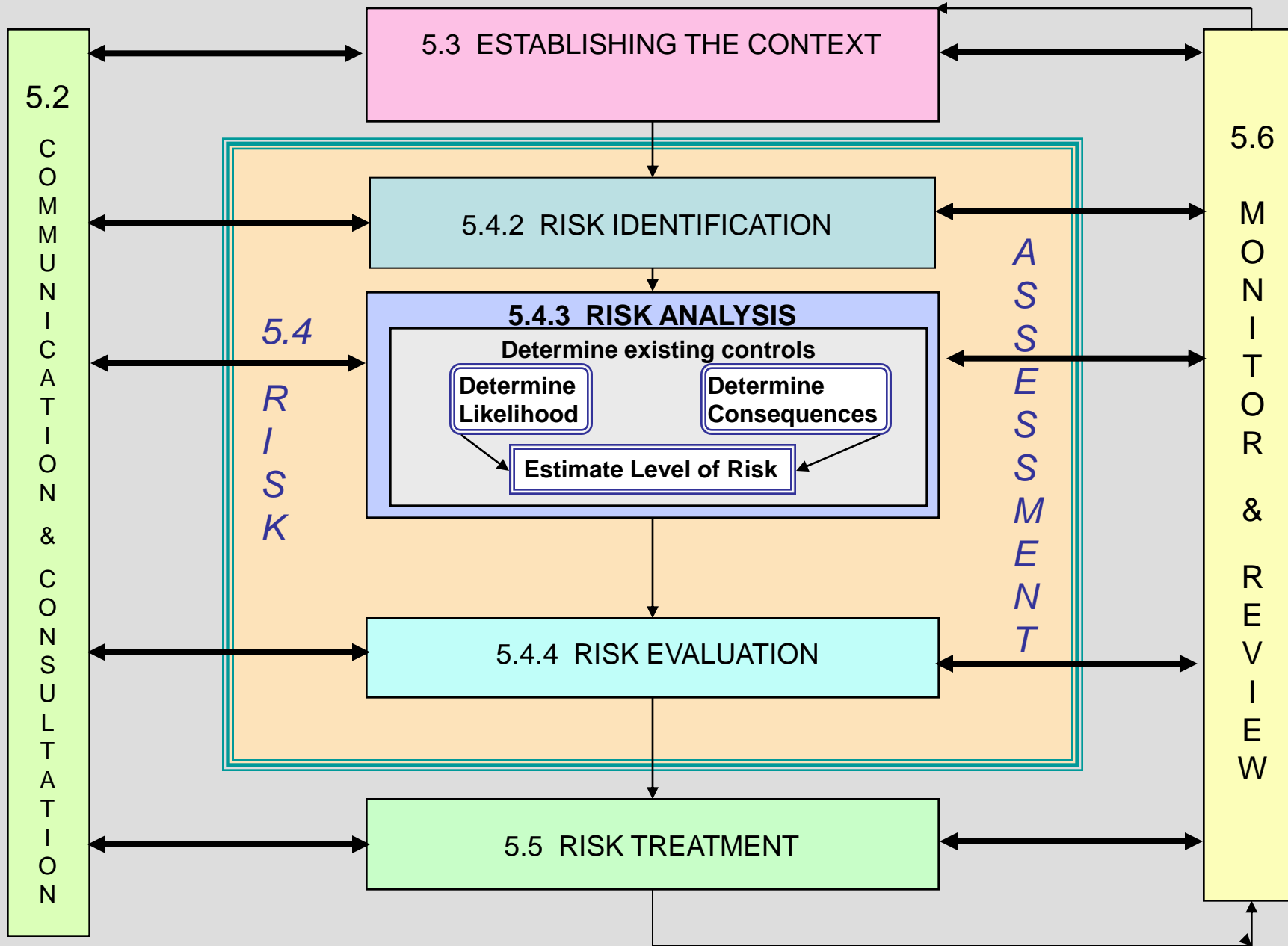
**In particular, those carrying out risk assessments should be clear about**

- 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.**



# 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.**



# **Risk Analysis**

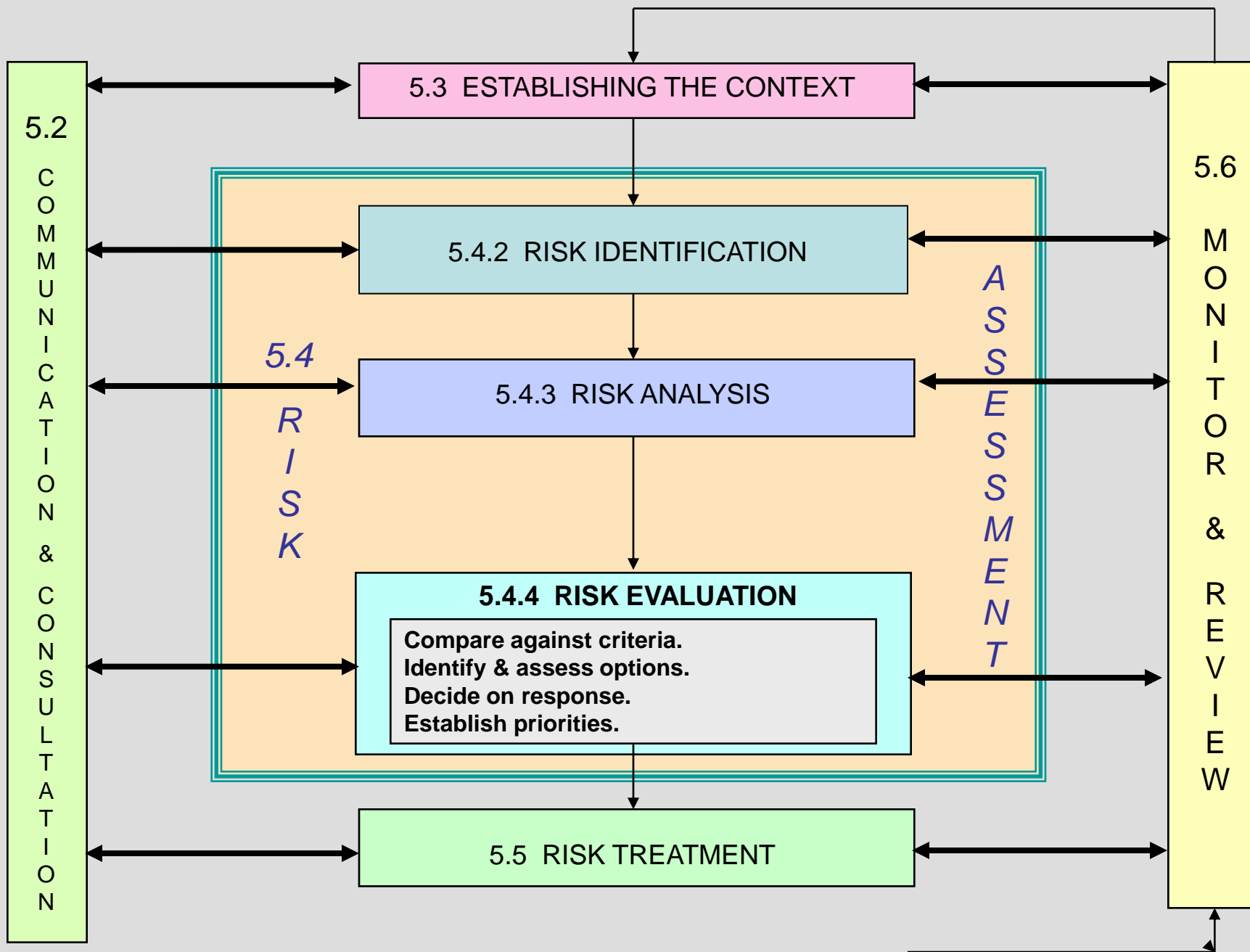
**Where possible confidence limits placed on estimates and the best available information sources are used.**

## **Purpose:**

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

## **Preliminary analysis:**

- ◆ **Excluded Risks where possible should be listed.**



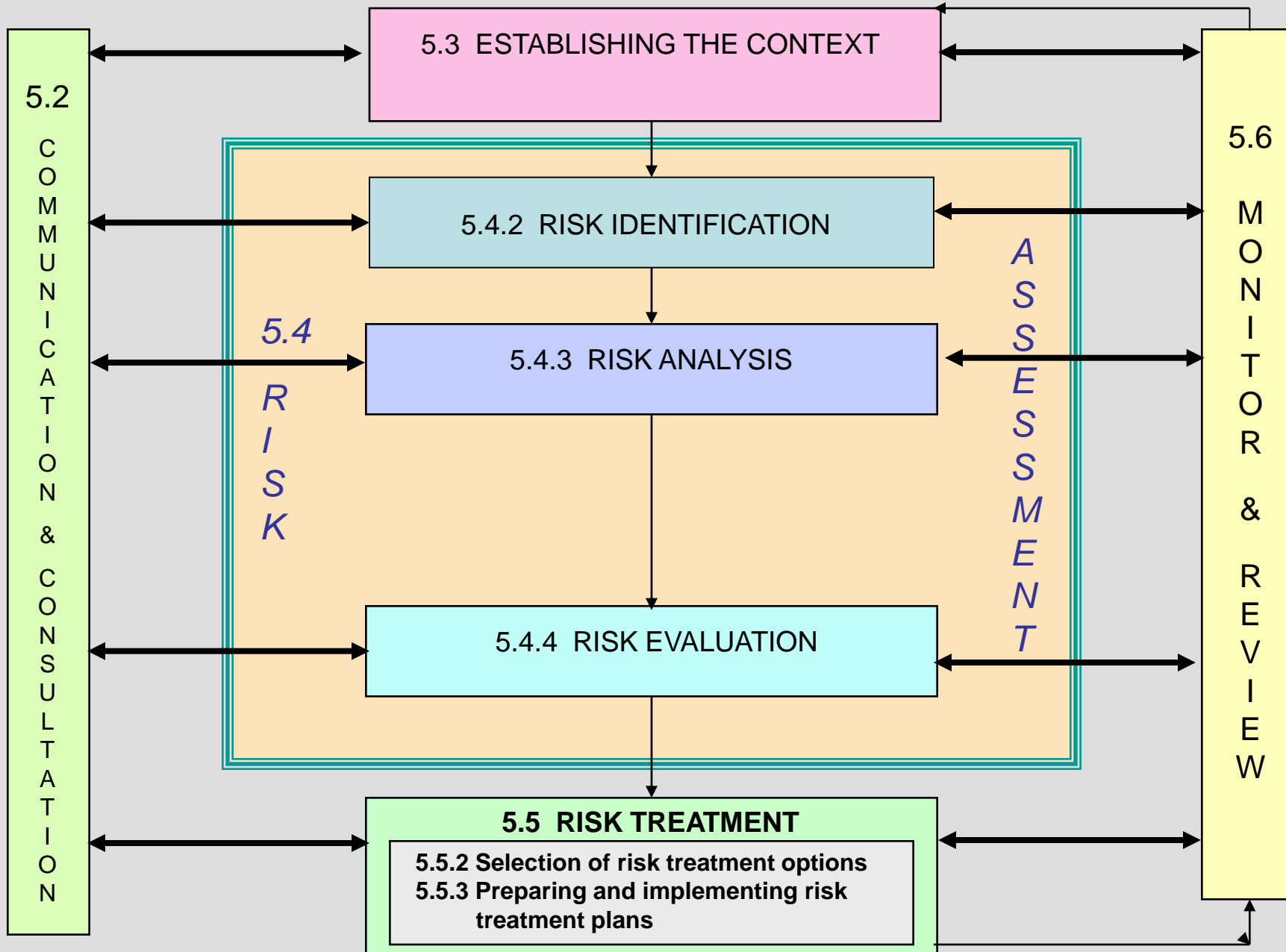
**ISO 31000:2009 Risk management process in detail**

# 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

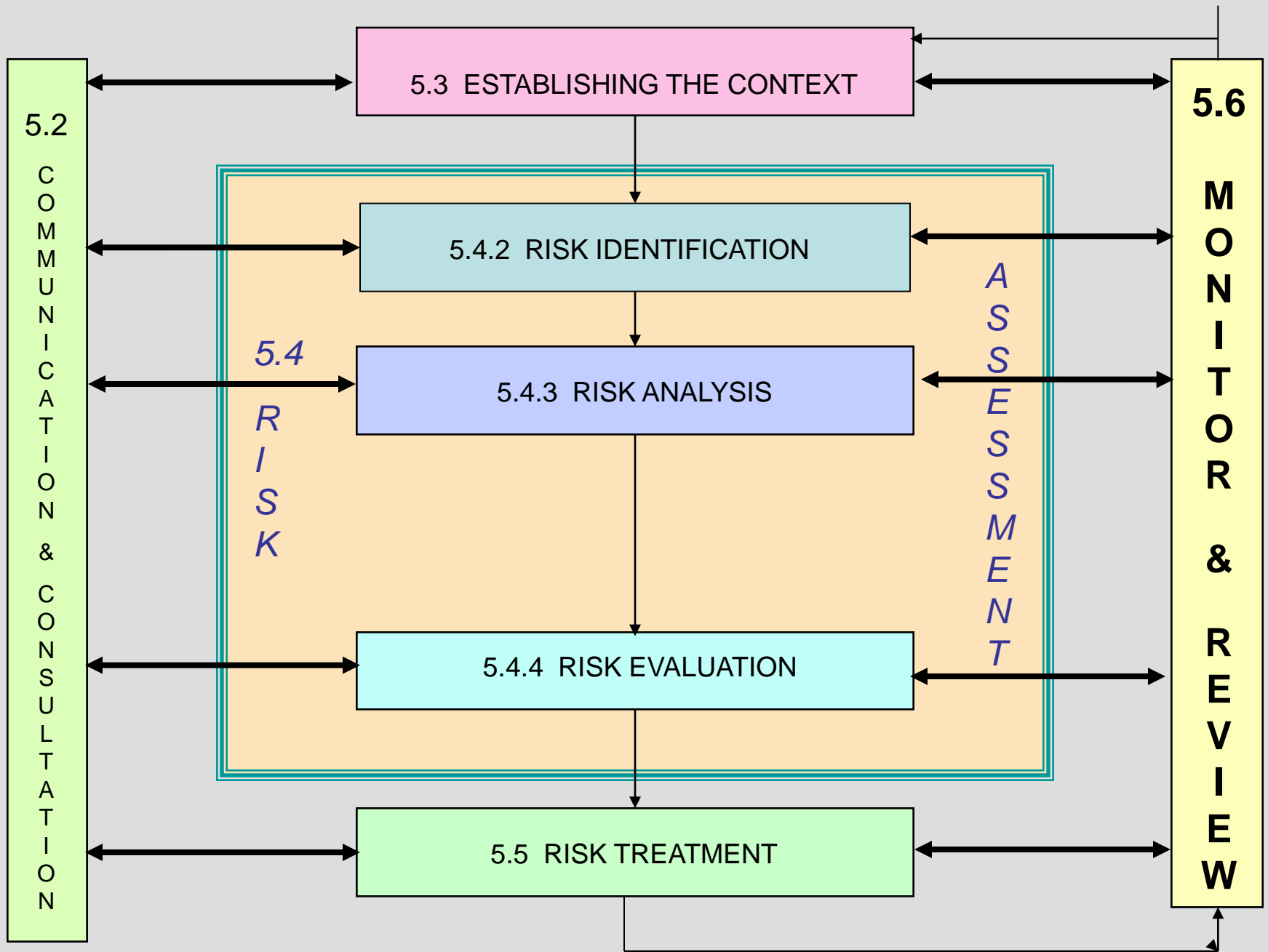
**Comparing levels of risk found in analysis with previously established criteria.**





# Risk Treatment

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



# Monitor and Review

- ◆ **What may be of minor significance today may be the disaster of tomorrow.**
- ◆ **Review is an integral part of the risk management process.**

# RISK MANAGEMENT

A Journey – Not a Destination



# **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

## Annex A

(Informative)

### Attributes of enhanced 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.

# **AS/NZS ISO 31000:2009**

## **Annex A**

(Informative)

### **Attributes of enhanced 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.***



# AS/NZS ISO 31000:2009

## Annex A

(Informative)

### **Attributes of enhanced 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.*



# **AS/NZS ISO 31000:2009**

## **– Reducing the Risk in Risk Management**

- **Avoids organisations re-inventing the wheel**
- **Allows all to benefit from proven best practice**
- **Provides a universal benchmark**
- **Reduces barriers to trade**
- **Advises 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**
- **Risk management = making optimal decisions in the face of uncertainty**

# And Finally!!

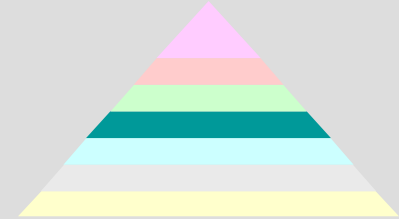
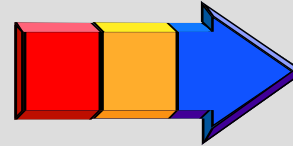
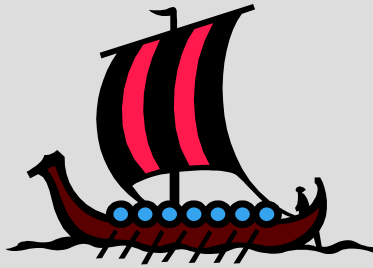
- **AS/NZS ISO 31000:2009 is the natural successor to AS/NZS 4360:2004**
- **It will fit 'ERM' requirements, but will also allow silo/project risk management**
- **Following AS/NZS ISO 31000:2009 will provide a low cost, high chance of success approach to ERM**
- **AS/NZS ISO 31000:2009 will add value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

**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

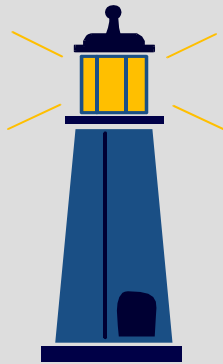


**A journey ..... A race**

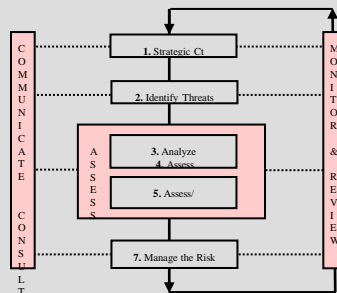
**In pursuit of performance Building Value**

**AS/NZS 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.**



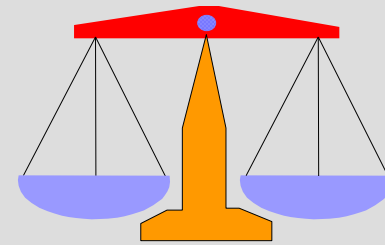
**Structure Direction**



**Processes**



**Culture Communication**



**Opportunities Risks**