AS/NZS ISO 31000:2009

Why ISO 31000

- A globally accepted framework and language for recognising and managing risk.
- While much risk management is common sense it is important to look at risk in a systematic way.
- Risk management is often done poorly (mechanistically) so becomes an overhead rather than adding value.
- Risk management should be a source of opportunities for improving the way resources are used to achieve objectives.

Key terms ISO 31000/Guide 73

- Risk - is the effect of uncertainty on objectives
- Risk Management - is the coordinated activities to direct and control an organisation with regard to risk.
- Risk management framework set of components that provide the organisational arrangements for designing, implementing monitoring and reviewing and continually improving RM in the organisation.
- Control- is a measure that is modifying risk
- Risk Treatment - is the process of developing, selecting and implementing controls

RM is systematic approach to:

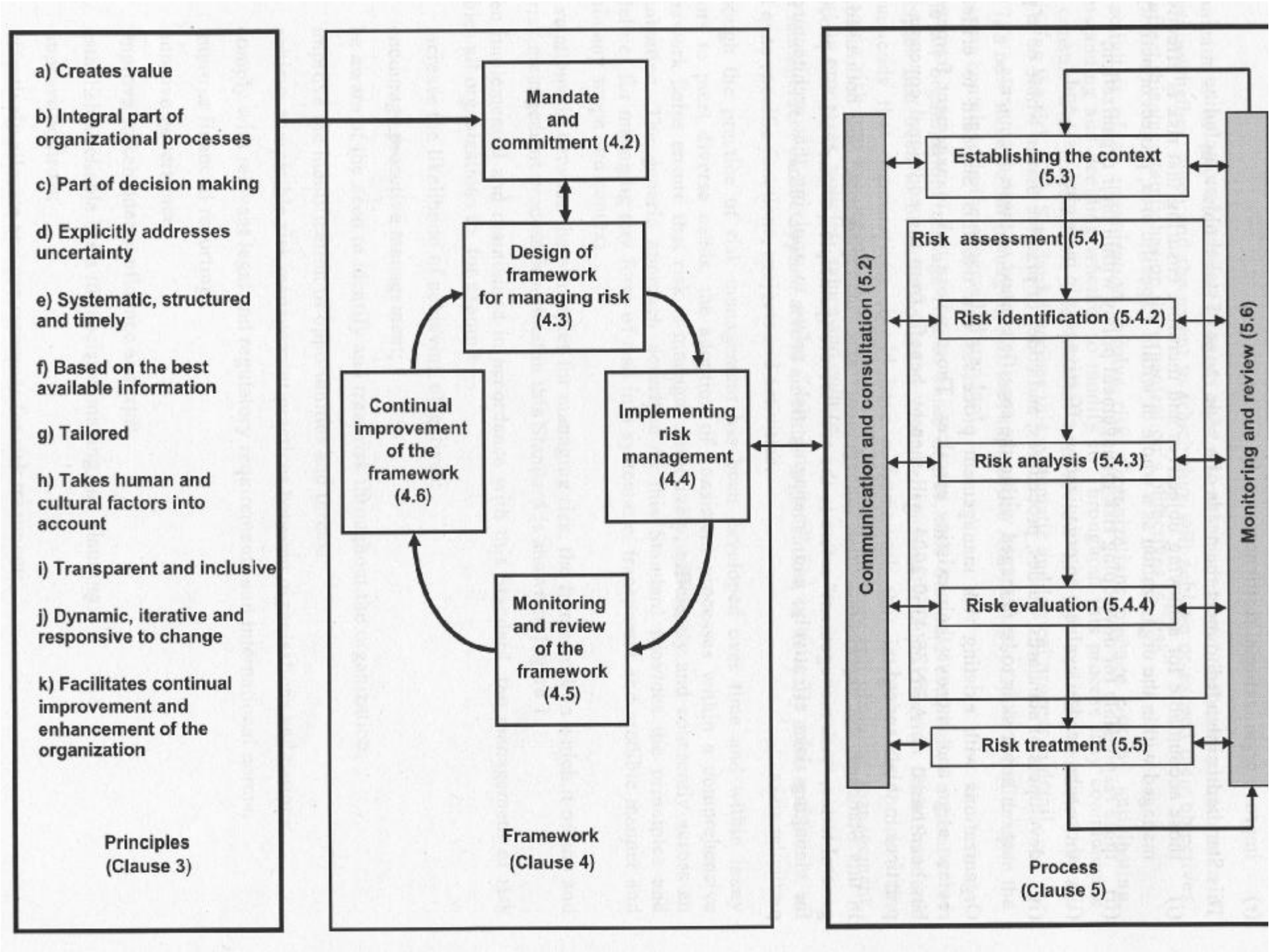
- Risk is implicit in all decision making and activities
- Understanding the organisations risks and controls through risk assessment.
- Guide the level and type of risk that the organisation is willing to accept.
- Treating or dealing with risks cost-effectively to reduce exposure or exploit benefits and rewards
- Instilling the ‘three whats’ thinking in an organisation:
  - What can happen?
  - What can cause it to happen?
  - What can I do to affect it happening?

Core elements of ISO 31000

The three core elements of ISO 31000 are:

- Principles for managing risk.
- Framework for managing risk.
- Process for managing risk.

The principles and attributes of enhanced risk management should be referred to regularly to guide an organisation in developing and implementing risk management.


a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization
Principles (Clause 3)
Mandate and commitment (4.2)
Design of framework for managing risk (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 and 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 and review (5.6)
Process (Clause 5)

Risk management framework

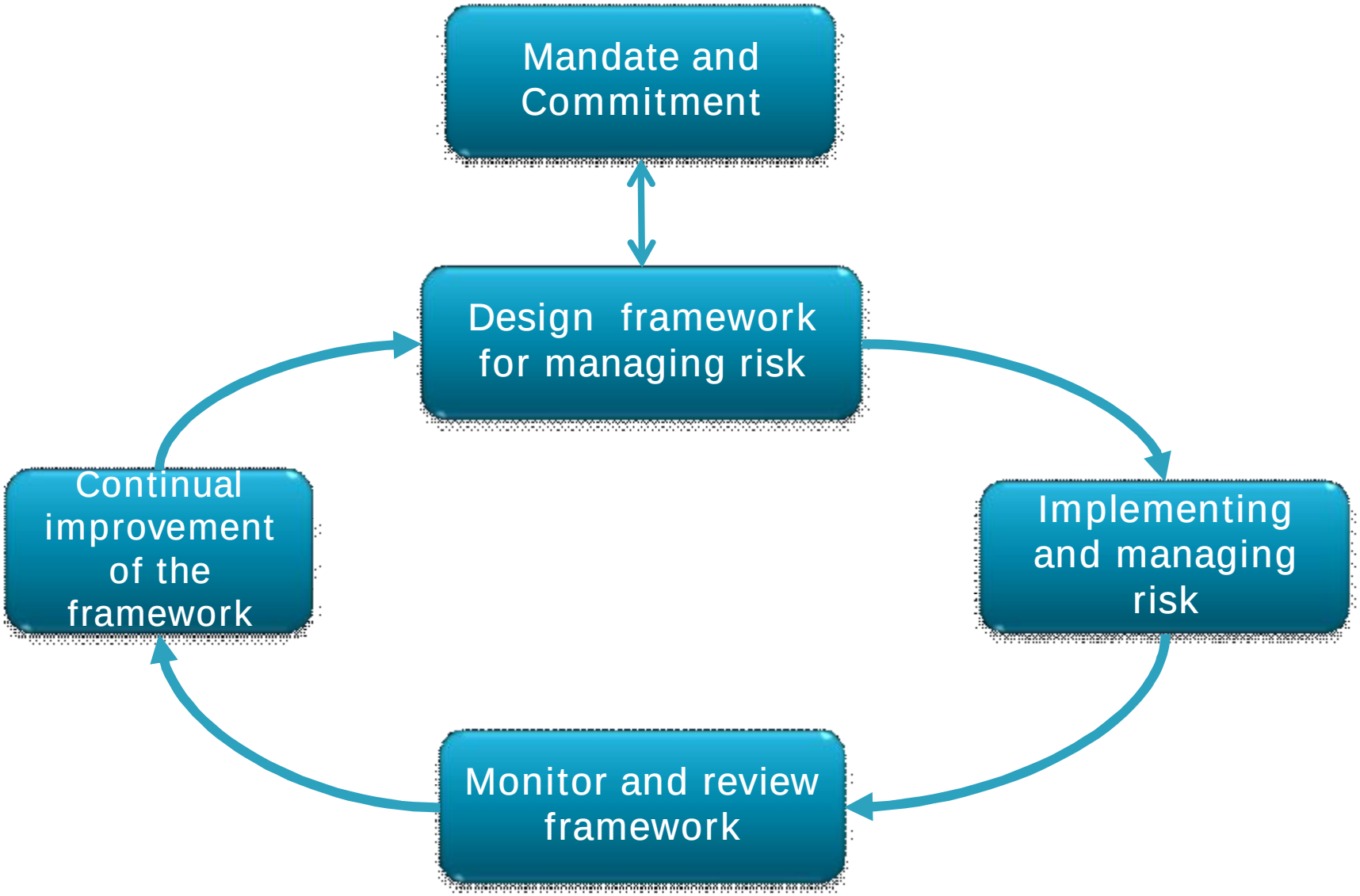
The risk management framework consists of:

- The policies
- Arrangements
- Structures to implement
- Sustain the risk management process

It needs to reflect

- Community and business processes,
- Structures
- Risk profile
- Risk appetite

Risk management framework

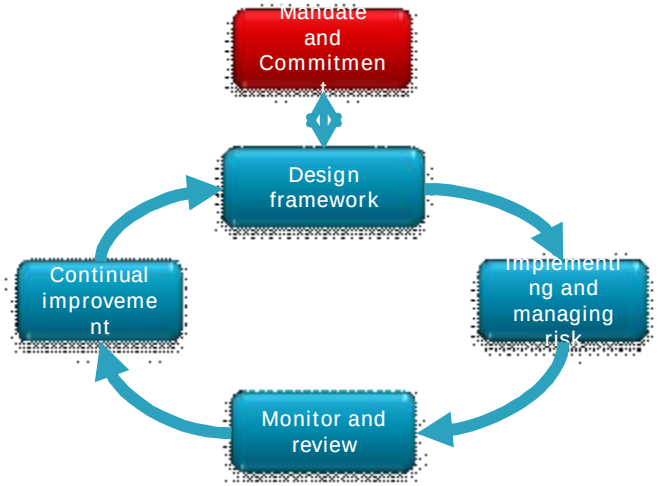


Mandate and Commitment

Effective risk management requires strong and sustained support from the executive and the board.

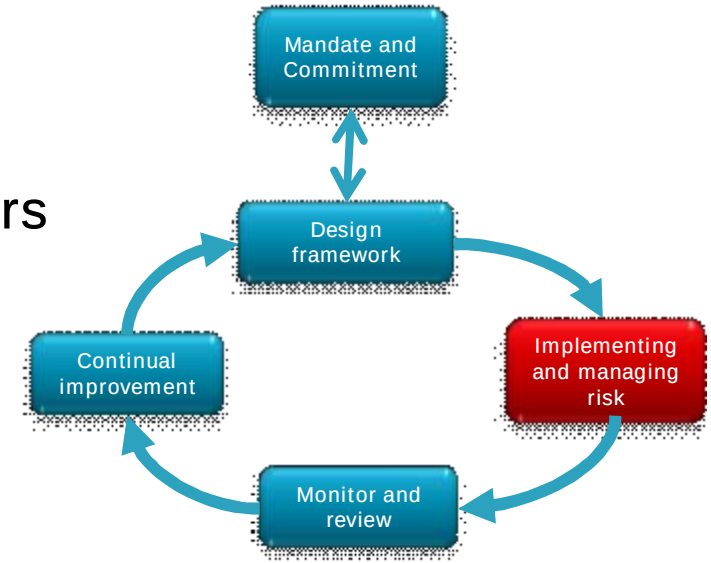
A common failing in risk management is that it becomes just another compliance exercise to produce reports to CEO and Board.

Typically risk management looses momentum when the risk register is generated. Reporting becomes an end in itself and distracts from actually treating the risk.



Implementing framework for managing risk

- Define timing and strategy
- Apply risk management policy and processes
- Comply with legal and regulatory requirements
- Ensure decision and objective setting in the organisation includes risk management
- Education training and information
- Communicate and consult with stakeholders about the framework

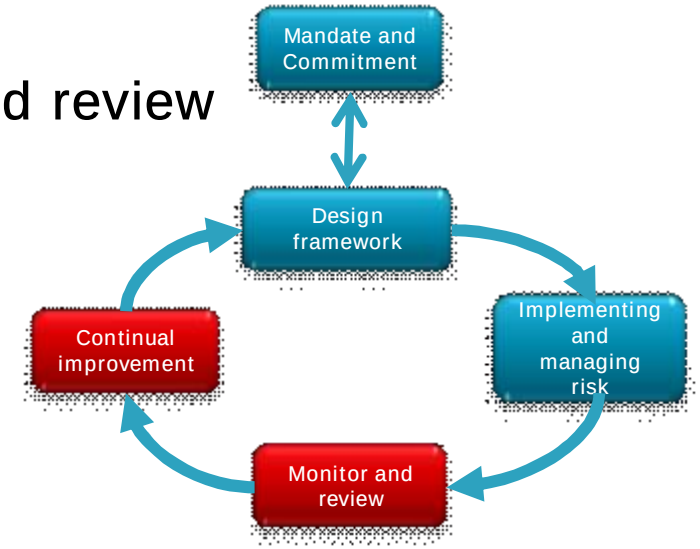


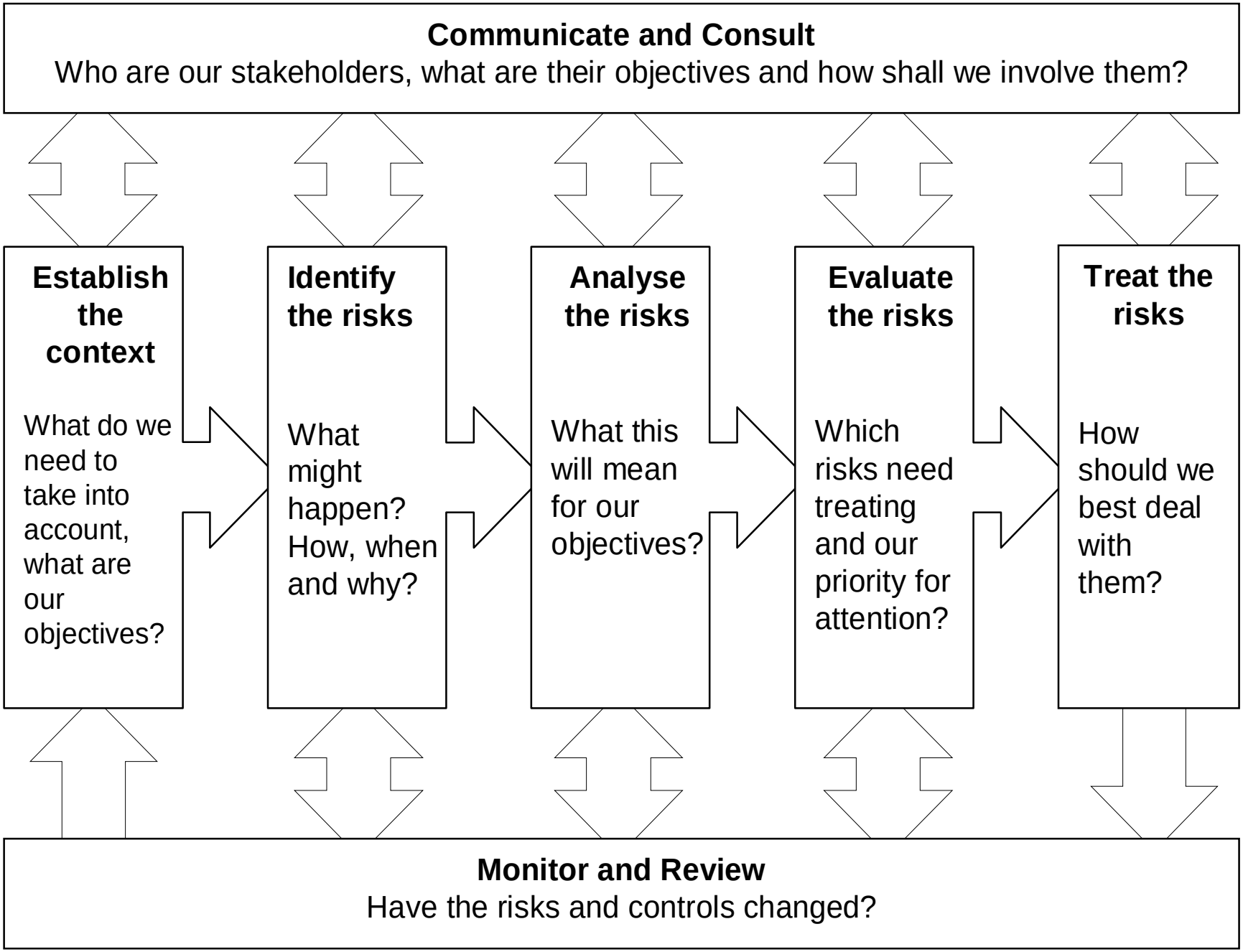
Monitor and review of the framework

To ensure risk management is effective the organisation should:

- Measure and report on RM performance & progress against RM plan
- Review RM framework to see if it is still appropriate and effective
- Establish internal and external reporting

Continual improvement based on monitor and review




Communicate and Consult
Who are our stakeholders, what are their objectives and how shall we involve them?
Establish the context
What do we need to take into account, what are our objectives?
Identify the risks
What might happen? How, when and why?
Analyse the risks
What this will mean for our objectives?
Evaluate the risks
Which risks need treating and our priority for attention?
Treat the risks
How should we best deal with them?
Monitor and Review
Have the risks and controls changed?