Connect › Support › Advance

The Institute of Internal Auditors Australia

Factsheet: Risk Management

Updated 2020

Risk management history

People apply risk management without thinking about it. In everyday situations, we make decisions which include assessment of risks, for example when we cross a busy road. These days the concept of risk management also applies to decision-making within organisations.

For many years, risk management was an informal process. Australia produced the world's first risk management standard – Australian Standard 4360: 'Risk management', accompanied by Handbook HB 436: 'Risk Management Guidelines'.

In 2009, the first international risk management standard was issued – ISO 31000:2009 'Risk management – Principles and Guidelines'. This was based upon the Australian 4360 standard. This was updated in February 2018 as ISO 31000:2018 'Risk management – Guidelines'.

Other guidance on risk management is available, most notably the COSO 'Enterprise Risk Management Integrated Framework'. It defines essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management.

What is risk management?

Risk is the effect of uncertainty on objectives, with:

- An effect being a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.
- Objectives having different aspects and categories, and can be applied at different levels, for example within an organisation.
- Risk is usually expressed in terms of:
  - Risk sources.
  - Their consequence (impact).
  - Their likelihood (probability).

Risk management comprises co-ordinated activities to direct and control an organisation with regard to risks. This requires co-ordinated and economical application of resources to:

- Minimise, monitor, and control unforeseen events.
- Maximise the realisation of opportunities.

Risk management definitions

Consequence	Outcome of an event affecting objectives – may also be called impact
ERM	Enterprise risk management
Inherent risk	Risk before controls are applied
Likelihood	Chance of something happening – may also be called probability
Impact	Outcome of an event affecting objectives – may also be called consequence
Probability	Chance of something happening – may also be called likelihood
Residual risk	Risk remaining after risk treatment
Risk	Effect of uncertainty on objectives – can be positive or negative
Risk appetite	The amount of risk an organisation is willing to take or accept in pursuit of its objectives
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk is acceptable, tolerable, or unacceptable
Risk identification	Process of finding, recognising and describing risks
Risk management	Co-ordinated activities to identify and control an organisation with regard to risk
Risk source	Element which alone or in combination has the potential to give rise to risk
Risk tolerance	Boundaries for risk taking, commonly expressed as a range of upper and lower limit. Exposures outside the upper risk limit are unacceptable and outside the risk appetite
Risk treatment	Process to modify risk
Risk universe	The full range of risks which could impact either positively or negatively on the ability of the organisation to achieve its objectives

Where is risk management applied?

Risk management applies at all organisation levels:

- Enterprise-wide (strategic).
- Business unit (operational).
- Project-specific (tactical).

Risk management should be performed at an enterprise-wide level which includes business unit risks. Risk management need not necessarily be done at the enterprise level before it

can apply elsewhere – while ERM is a good idea, its absence does not preclude application of localised risk management. Where projects may be initiated within an organisation, for example an ICT project, a separate risk assessment should be completed and risk management applied to the project.

Risk management principles

Integrated	Risk management is as an integral part of all organisational activities.
Structured and comprehensive	A structured and comprehensive approach to risk management contributes to consistent and comparable results.
Customised	The risk management framework and process are customised and proportionate to the organisation's external and internal context related to its objectives.
Inclusive	Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.
Dynamic	Risks can emerge, change or disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.
Best available information	Inputs to risk management are based on historical and current information, as well as on future expectations. Risk management takes into account limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.
Human and cultural factors	Human behaviour and culture significantly influences all aspects of risk management at each level and stage.
Continual improvement	Risk management is continually improved through learning and experience.

Risk management benefits

- Proactive rather than reactive management.
- More effective allocation and use of resources.
- Fewer surprises.
- Exploitation of opportunities.
- Improved planning, performance and effectiveness.
- Enhanced efficiency, effectiveness, economy and ethics.
- Improved stakeholder relations.
- Improved information for decision-making.
- Enhanced reputation.
- Better accountability, assurance and governance.
- Reduced insurance cost.

Risk appetite

Risk appetite can be defined as the amount of risk an organisation is willing to take or accept in pursuit of its objectives. The following table is an example of how it may be illustrated:

Extent of Risk Appetite	Risk Tolerance Level	Risk Management Approach
Acceptable Appetite (Acceptable) Will operate in this area after risks have been effectively mitigated	Moderate Tolerance	Confident
Low Appetite (Tolerable) May operate in this area where the value is assessed as worthwhile, but only after risks have been effectively mitigated	Limited Tolerance	Conservative
No Appetite (Unacceptable) Will not operate in this area	Zero Tolerance	Avoid

Risk Management process

Step 1 →	Communicate and consult
Step 2 →	Scope, context, criteria
Step 3 →	Risk assessment: • Risk identification • Risk analysis • Risk evaluation
Step 4 →	Risk treatment
Step 5 →	Monitoring and review
Step 6 →	Recording and reporting

Helpful references

- ISO 31000:2018 'Risk management – Guidelines'
- COSO Enterprise Risk Management Integrated Framework

The Institute of Internal Auditors Australia