Why is risk management important?

Introduction

Effective risk management provides an early warning system for organisations in an uncertain environment. There are many benefits of effective risk management, including:

- The reduction of uncertainty
- Encouraging anticipation and resilience
- Supporting the development of a strong internal control environment.

This advice sets out general advice and guidance relating to risk management which is designed for any type or size of co-operative to consider. It is supported by more detailed guidance and templates. We provide links to these resources below.

Definitions

What is risk?

- Risk may be defined as the threat or possibility that an action or event will adversely, or beneficially, affect an organisation's ability to achieve its objectives.
- A risk can be something uncertain – it might happen, or it might not. A risk matters because, if it happens, it will have an effect on objectives and an organisation's ability to meet them.
- Risk arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or errors will be made.

What is risk management?

- The process which aims to help organisations understand, evaluate and take action on all their risks with a view to increasing the probability of their success and reducing the likelihood of failure.
- Risk management is the process of identifying risks to the organisation, assessing their relative likelihood and impact, implementing appropriate actions to mitigate the risk and providing assurance of this.
- Risk management gives comfort to members and other stakeholders that the business is being effectively managed.

What is assurance?

- Written, evidenced-based information
- Data, facts and figures as well as narrative, supporting text
- It is usually provided internally to the Board from officers, members etc.

- It can also be provided externally from auditors, consultants etc.
- It is not solely verbal. This is an important distinction – verbal information alone is re-assurance and must be supported by some form of evidence base.

This resource has been written by Angela Lomax from David Tolson Partnership, Chair of the Co-operative Governance Expert Reference Panel.

The link between risk and effective governance

For co-operative organisations, the Code of Governance (at Section 5, Principle C) states that

"The board is responsible for and should establish procedures to manage risk, oversee the internal control framework, and (with input from the executive leadership if applicable) identify the nature and extent of the principal risks the co-operative is willing to take in order to achieve its long-term strategic objectives and success in accordance with the ICA Values and Principles."

Risk management and corporate governance are closely related. Effective risk management supports the internal controls of an organisation and this ensures it can achieve its objectives. Good governance should ensure the long-term sustainability of an organisation where its activity is safeguarded, or value is generated through the 'exploitation' of opportunities.

For co-operative organisations, the Code of Governance (at Section 5, Provision 5) states that:

"The Board should, or the audit and risk committee could be delegated to, carry out a robust assessment of the co-operative's emerging and principal risks. The board should confirm in the annual report that it has done so and should include information detailing:

- *A description of the principal risks*
- *Confirmation of the procedures in place to identify emerging risks*
- *An explanation of how risks are being managed and/or mitigated."*

Effective risk management can also support strategy development, helping boards to develop strategies that are appropriate to the risk preferences of its members and wider stakeholders and the opportunities and threats that exist within its current operating environment.

So, good governance should effectively manage, not eliminate, risk. Organisations need to build both resilience and agility in all of their activities, enabling them to adequately respond to change in circumstances or to deal with the consequences of unforeseen events.

This resource has been written by Angela Lomax from David Tolson Partnership, Chair of the Co-operative Governance Expert Reference Panel.

How does risk management work?

Why undertake risk management?

Risk management is not always a “stopper” to activity, it can be an enabler, helping organisations to see challenges and opportunities. Good risk management provides a framework which improves the success and speed of decision-making, supporting pro-active actions which are more likely to be effective.

The process of developing a risk management framework improves the organisation’s ability to scan its horizon, ensuring more realistic business and project planning. It helps to identify the unknown unknowns, builds flexibility and adaptability and in doing so increased the resilience of the organisation. In turn, this can provide more certainty in achieving goals, growth, objectives and / or improved performance and control, with fewer costly surprises.

What are the warning signs that might prompt you to think that your organisation needs to think about risk management?

The organisation has:

- Never thought about new, emerging or changing risks (or risk at all) in relation to its activity and desired outcomes
- Areas of performance which are changing – either for better or for worse
- A plan to do something new, different, ambitious or expensive
- Aims, objectives, resources and timeframe overall, or a particular plan or activity that are not clearly understood or agreed by everyone
- Gaps in information or data
- Expectations, commitments or liabilities that are vague, over optimistic or under-valued
- Not considered contingencies or plan B actions for particular activity(s)
- Significant changes in the operating/trading environment

What does should risk management involve?

There are five key principles within a robust risk management framework:

1. Comprehensive – it must cover all aspects of the business and organisation
2. Continual – risk management is not a one-off exercise, the approach must be routinely maintained and regularly refreshed and updated
3. Integrated – effective risk management must be embedded and part of all operations and systems within an organisation
4. Suitable – there is no ‘one size fits all’ approach to risk but instead there are common principles, policies and practices that can be adapted to any activity
5. Proportionate – the approach must have a realistic sense of proportion – for the size and scope of the organisation and in the attitude towards benefits and risks

This resource has been written by Angela Lomax from David Tolson Partnership, Chair of the

Co-operative Governance Expert Reference Panel.

Risk and resilience

Resilience is *"the capacity to recover quickly from difficulties and changing circumstances"*. (Strength in Numbers Report, SIB, 2018)

There are five key areas for organisational resilience. The extent to which these apply to your organisation will depend on the size, complexity and operating context but each area is worth considering:

1. Governance: There must be sound board and team alignment and consistent clarity of mission and values.
2. Openness: To feedback, to partnerships, to experimentation, to learning.
3. Finance: Good information, reserves, strategies, diversification.
4. Networking: A comprehensive awareness of the external landscape, partnerships and other sources of support.
5. Adaptation: A commitment to the mission (relating to risk) and not a fixed model which must be aligned with an ability to flex as best fits to the organisation.

In the face of growing uncertainty, organisations may need to invest in resilience, resulting in an ability to:

- Respond quickly to mitigate the effects of unanticipated events supported by effective crisis management
- Recover quickly from the aftermath of an unanticipated event with sound business continuity management
- Review past unanticipated events to improve future resilience and learn

The respective roles of Board, Audit Committee (if one is in place) and staff:

The respective roles of Board, Audit Committee (if one is in place) and staff

The roles from the above diagram:

The Board

- Must lead on risk management; is ultimately responsible
- Should be identifying new risks, challenging existing risks
- Must understand where impact of each risk lies within the organisation
- Must seek assurance on effective risk management
- Should identify its risk appetite and then use it
- Must receive regular updates on risk register
- Risk should be a standard agenda item for each meeting
- Should monitor and review risk.

Audit Committee

- Independent adviser to the board
- Understands where to skim, question or dig deep
- Focuses on key risks
- Ensures risks are fully reflected in audit plan
- Undertakes or commissions additional detailed work on risk where necessary
- Commissions / uses external audit to test and validate risk management and controls
- Adds value to the Board’s work on risk (but ultimately Board is responsible)
- Has responsibility for the internal audit function.

Staff

- Identify new and emerging risks
- Review the strategic risk register and update quarterly
- Ensure strategic risk register is brought to Board regularly
- Provide assurance to the Board that risk is being managed
- Embed a culture of risk management throughout the staff, and make risk management a key aspect of the performance management framework.

This resource has been written by Angela Lomax from David Tolson Partnership, Chair of the Co-operative Governance Expert Reference Panel.

Linking risk to decision making and a risk register

All matters for decision which are considered by a Board should include a review of the potential risk implications and impacts. It is useful for Boards to be clear about what the risks are in the decision, where these risks feature in a risk register, what area of the strategic plan the risks link to and where the impact of the risks in the decision lies within the organisation.

Risk appetite can also be referenced. This should link where the decision lies in terms of the organisation's risk appetite in the given area.

See our section on risk appetite

Read more

The board should discuss the risks, understand their implication, consider trade-offs, and accept inherent risks prior to making a decision. Equally, an effective risk assessment can equally be used to decide not to do something.

A risk register sets out the approach used to manage and control events that could have a negative impact on the organisation. It will usually involve at a basic level, a table with three columns:

1. Risk identified
2. Risk assessment
3. Risk mitigation

Risk identified sets out any exposures to uncertainty and can be identified through dedicated planning sessions, planning for particular activity, external sources (learning from others, good practice guidance, audits, customer feedback etc.).

Risk assessment covers the likelihood (or probability) that a risk will occur and the impact it would have.

The risk register usually scores risks in terms of a likelihood and impact baseline score – where there are no controls in place and a target score – where the score would be expected to be with controls and mitigation in place. These are usually around a scale of 1 (very low risk of occurrence – extremely unlikely) up to 5 (very high risk of occurrence – almost certain).

Examples are set out below:

SCORE	LIKELIHOOD	CRITERIA
1	Negligible	• 0-5% extremely unlikely • Virtually impossible (i.e. one off event)
2	Low	• 6-20% low but not impossible • An event that is unlikely to occur more than once every few years or has not occurred historically
3	Medium	• 21-50% fairly likely to occur. • Possibly could occur but infrequently but not more than once every 12 months • Could occur more than once within the time period and may be difficult to control due to some external influences
4	High	• 51-80% more likely to occur than not • Likely could occur but on a sporadic basis • i.e. at least once a year • Potential of it occurring several times within the time period or has occurred recently
5	Severe	• 81-100% almost certainly will occur • Highly likely could occur on a regular basis i.e. several times a year

Example of how risk likelihood and impact baseline score is calculated

An impact score is calculated on a scale of 1(insignificant impact) to 5 (catastrophic impact).

SCORE	IMPACT	CRITERIA
1	Insignificant	No impact
2	Minor	Minor impact within one or more criteria
3	Moderate	Moderate impact within one or more criteria
4	Major	Major impact within one or more criteria
5	Catastrophic	Severe impact within one or more criteria

Example of how an impact score is calculated

Risk mitigation is defined as taking steps to reduce adverse effects. Examples include:

- Terminate (avoid/eliminate): A level of risk that should be avoided and if possible should be eliminated. Some risks will only be dealt with to acceptable levels by terminating the activity
- Treat (control/reduce): This refers to the level of cost-effective (corrective) controls put in place to manage the risk to an acceptable level. The majority of risks will be managed in this way
- Transfer (insurance / contract): Where the decision is taken to transfer the risk to a third party usually by means of insurance or contractual transfer such as paying a third party to take the risk
- Tolerate (accept/retain): The risk here is considered acceptable to the organisation or the ability to do anything about the risk is limited, or the cost of taking action may be disproportionate to the potential benefit gained. A tolerated risk should be monitored and re-evaluated in the future.

It is also important that risk management is ongoing and that the Board consider risk in every decision that it takes. There should be plans in place to review the risk register, risk appetite and the wider risk management framework to ensure that it is up-to-date and relevant as an organisation grows and changes.

This resource has been written by Angela Lomax from David Tolson Partnership, Chair of the Co-operative Governance Expert Reference Panel.

Risk appetite

What is risk appetite?

Risk appetite is the level of risk an organisation is prepared to accept in order to meet its strategic objectives, deliver its values and make its target returns.

Why is a risk appetite statement important?

By considering and defining the risk appetite, the organisation can arrive at an appropriate balance between uncontrolled activity and excessive caution. It provides guidance on the level of risk permitted and encourages consistency of approach across the organisation.

The risk appetite statement is then used to inform decision making by articulating the level of risk that the organisation is willing to take in different areas of its activity and operations in order to meet its objectives. It can be useful in selecting which projects or activity to undertake, as the organisation's desire to take on risk or mitigate risk in given areas is clearly stated.

Risk appetite changes from time to time, and the organisation may vary the amount of risk it is prepared to take dependent on time and circumstances (e.g. it may be prepared to accept a higher degree of risk if something is a strategic priority, or if there is an agreed and appropriate exit strategy). It may also be necessary to tolerate risks that fall outside of the appetite if they are beyond the organisation's control. As such, the risk appetite statement should be reviewed – at least annually.

What does a risk appetite statement look like?

A risk appetite statement is not complex and is usually set out in a table which lists each of the organisations objectives and then describes the amount of risk for each that the Board considers it appropriate to accept.

The risk appetite descriptors and definitions used are different for every organisation usually in line with the examples list set out below. What is important is that they are meaningful and consistently understood.

- Enthusiastic: Eager (perhaps willing to be innovative) about delivering activity or projects and in doing so, will accept any increased or substantial risk levels associated with this
- Open: Prepared to consider different options to delivery activity or projects and will take on increased risk if this results in positive outcomes
- Balanced: Will only take on modest levels of risk to achieve desired outcomes
- Cautious: Will take some low risks (or only take safe options) to achieve desired outcomes but these will be limited
- Averse: Prepared to take only very low levels of risk (or avoid all risk and uncertainty) to achieve desired outcomes

A simple example of a risk appetite statement is as follows:

[Organisation Name]: Risk Appetite Statement

Organisational objective	Risk Appetite	Summary Rationale	Last reviewed (date)
To maintain an excellent reputation	Cautious	• Generally low appetite for reputational risk • Consider that a strong reputation aligns with high standards of service and compliance with legal requirements	October 2021
To attract and retain skilled and motivated staff	Cautious	• We seek to use skills, knowledge and experience of staff flexibly and in ways that provide agile and responsive service to customers. • We offer and expect high degree of autonomy from staff and place high level of trust in them. • We actively manage change and are transparent in communications with staff.	September 2020

This resource has been written by Angela Lomax from David Tolson Partnership, Chair of the Co-operative Governance Expert Reference Panel.

https://www.uk.coop/resources/why-risk-management-important

Last updated: Wednesday, April 6, 2022 - 14:32