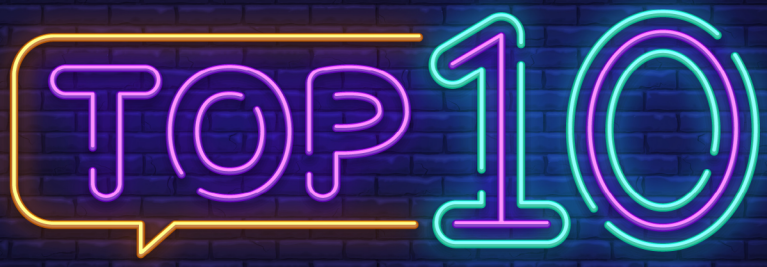
INSTITUTE OF COMMUNITY DIRECTORS AUSTRALIA
▸Knowledge ▸Connections ▸Credentials

ourcommunity.com.au
Where not-for-profits go for help



Ten questions a board member should ask about risk management

Being a board member of a not-for-profit (NFP) organisation involves being accountable for the governance, ethos and strategic oversight of the organisation. It requires you to ensure the organisation is working effectively to achieve its mission.

On one hand, the board must be aware of the risks to the organisation and ensure they are eliminated where possible, or reduced where they can't be eliminated. On the other hand, a board unwilling to take any risks at all may find the organisation dwindling over time, unable to keep up with its competitors because its lack of innovation is embedded in the culture.

Writing a risk appetite statement is a useful exercise to help bring the board and the executive into agreement, as it requires you to sift through what you are willing to take a risk on and what you are not. You can return to the document to help you make decisions, having already agreed that you are on the same wavelength regarding your willingness to take risks in the various areas of the organisation.

Your organisation should have a **risk management policy**.

These related policies will also be useful:

- **Cyber Security Policy**
- **Privacy Policy**
- **Financial Controls Policy**
- **Fraud Policy**
- **Workplace Health & Safety Policy**

A **risk management register** is a useful document to refer to at board meetings or for the Finance, Risk and Audit Committee to take accountability for. It will help you as a board member to ensure risks are documented, mitigated, managed and discussed.

Here are 10 critical risk areas that board members should ask about to fulfill their responsibilities:

1. Compliance

Are we complying with all applicable laws and regulations? This includes compliance with Australian Charities and Not-for-profits Commission (ACNC) requirements, Australian Taxation Office (ATO) laws, employment laws, and any sector-specific legislation such as health and safety standards.

2. Financial sustainability

How robust are our financial management systems (and what are they)? Are our financial resources managed efficiently? It's important to ask about sources of funding, financial health, budgeting, financial controls, and long-term financial planning.

3. Reputation and brand

What are the potential threats to our organisation's reputation? How do we manage public relations and stakeholder communications to reduce the reputational threats? Do we have processes documented and rehearsed for managing crises that could damage our reputation if they arise?

4. Strategic relevance

How effective is our strategy in responding to external environmental changes? Are our mission and ethos still relevant? Are we aware of how our environment is changing? Within what parameters can the executive and staff leaders make their own decisions about organisational changes designed to enable the organisation to keep up with the competition or lead the sector?

5. Governance structures

Are our governance structures appropriate and effective? Is there a clear delineation between board roles and management roles? Are governance practices up to date and are they reviewed regularly? Does our structure protect the organisation from possible threats; for example, an overthrow of the board or pressuring of the executive?

6. Operations

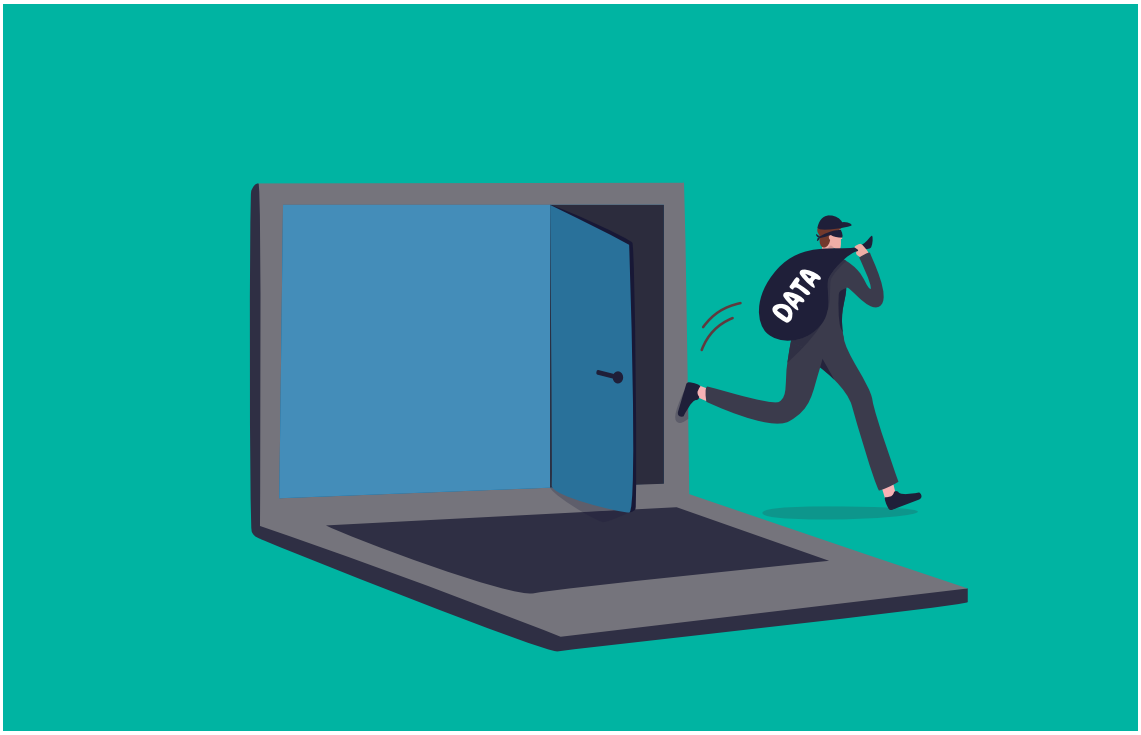
What operational risks could significantly affect our ability to operate effectively (e.g. failures of phone, internet or customer relationship management software systems, loss of staff or service delivery problems)? How are these risks being managed and how would you respond if these risks were to eventuate?

7. Human resources

How are we managing risks related to our staff and volunteers? These include recruitment, retention, training, performance management, compliance with workplace laws, and workplace health and safety.

8. Data security and privacy

How are we protecting the personal and sensitive information we hold? What processes and staff training do we have in place to prevent data breaches, and are these adequate? How do the board and organisational leaders stay on top of changes to relevant legislation?



9. Fundraising and donor engagement

How effective are our fundraising strategies and practices? How do we ascertain their effectiveness? How do we ensure compliance with the associated legal requirements and our own ethical standards?

10. Risk and culture

What is our organisational risk appetite? Are we too risk averse as an organisation, or too ready to take risks? Are we missing out on trying new things as a result of our fear of risks and failure? On the other hand, do we take appropriate risk management measures when making decisions?