Crowe

Social Purpose and Non Profit Organisations

Fraud Risk Assessment

August 2022

Audit / Tax / Advisory

Smart decisions. Lasting value.

Fraud and the responsibilities of Governing Bodies

Why is tackling fraud important to Boards

The Australian Charities and Not-for-profits Commission (ACNC) has highlighted that fraud is a serious problem that Boards can't afford to ignore, with surveys revealing that up to 15% of not-for-profit organisations suffered a fraud event in the previous two years. Fraud poses a serious risk to valuable funds, as well as sensitive data, and can damage the good reputation of social purpose organisations, affecting public trust and confidence in the sector.

Boards are the custodians of their social purpose organisations and have a duty to manage their organisation's resources responsibly. They have legal duties and responsibilities to safeguard their organisation and to ensure that its funds and assets are protected, properly used and applied, and accounted for. The public needs to be sure that money donated to social purpose organisations is used properly and goes to the causes for which it is intended.

In this document references have been made to ACNC guidance. Although this is issued specifically for charities, it also identifies good practice which can be applied for all social purpose organisations.

What is fraud?

Fraud is a complex, flexible and continuously evolving phenomenon. The criminal law in respect of fraud primarily relates to offences set out in the Criminal Code Act 1995 (the Act) and various State and Territory legislation.

There are three ways to commit fraud:

- By false representation,
- By failing to disclose information, and;
- By abusing a position of trust.

In order to commit an offence, there must be:

- An element of dishonesty (as defined by the standards of ordinary reasonable people) on the part of the fraudster, and
- Evidence of their intent to make a gain or cause a loss. Gain or loss is limited to money and other property (including real, personal, or intangible property).

False accounting is covered in the Act under offences relating to the provision of false or misleading documents (Part 7.5 Section 137.2).

ACNC guiding principles

In its guide to tackling fraud in the charity sector the ACNC have set out six guiding principles:

1. **Be clear about ethical values your charity prioritises.** It is important for board and committee members and managers to 'set the tone at the top' on fraud and criminal behaviour. This includes ensuring that fraud, and the approach to responding to fraud, is understood within your charity.
2. **Be open about the possibility of fraud.** Discuss what fraud is, what it might look like in your charity, and reaffirm you take the threat of fraud seriously.
3. **Identify the types of fraud you may be susceptible to.** Consider the risks relevant to your charity, such as those related to the types of activities it undertakes, the roles and responsibilities of staff/volunteers, and the banking procedures and fundraising methods it uses.
4. **Understand your charity's 'red flags' for fraud.** It is important your charity understands any specific warning signs that may indicate fraud.
5. **Develop sound written policies and procedures.** Sound written policies provide accountability and fraud prevention.
6. **Report suspected fraud.** If you suspect a crime has been committed in your charity, then you should report your concerns to the police as soon as possible. This helps ensure your charity, and the sector, is protected from fraud.

What is a fraud risk assessment?

A fraud risk assessment is an objective review of the fraud risks facing a social purpose organisation to ensure they are fully identified and understood. This includes ensuring:

- Fit for purpose counter fraud controls are in place to prevent and deter fraud and minimise opportunity, and;
- Action plans are in place to deliver an effective and proportionate response when suspected fraud occurs including the recovery of losses and lessons are learnt.

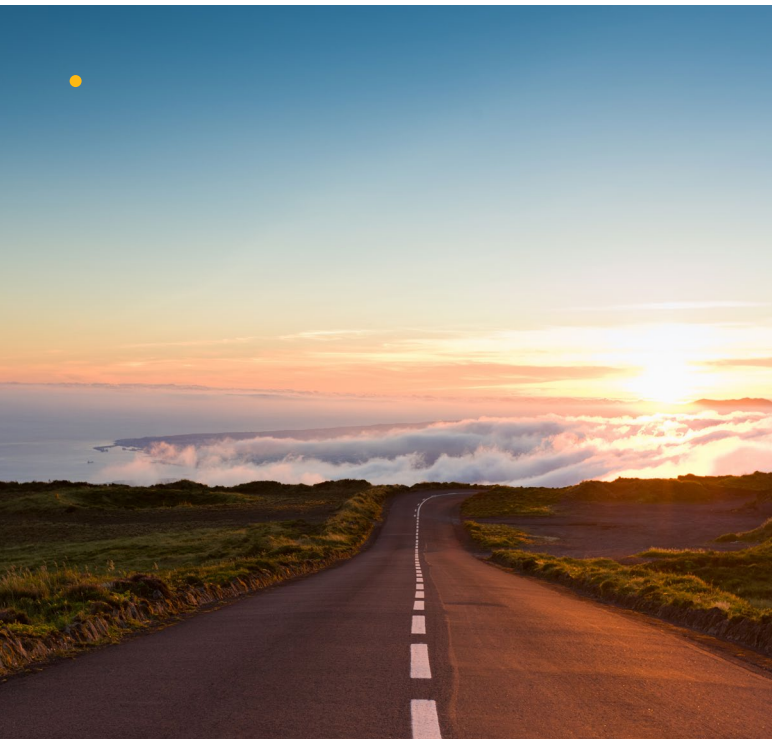
Good practice suggests that to be most effective the risk assessment should be undertaken at an organisational and operational level:

- **Organisational –** to assess the key policy, awareness raising and behavioural (including leadership commitment) requirements that need to be in place to build organisational resilience to counter fraud.
- **Operational –** a detailed analysis of the fraud risk and counter fraud control framework at the operational level – by function (activity) or individual business unit (including programmes and projects).

A one size fits all assessment of fraud risk and response rarely works.

Consider, a school and a charity operating internationally with the same level of controls, for example internal audit. The risk and impact of fraud at the school may be inherently lower simply because of its operating environment. So, a more nuanced approach is needed – one that considers the operating environment and the type and scale of fraud risk exposure. Some measures are focused only on expenditure but some of the largest frauds in the non-profit sector have been frauds of income diversion (discussed at Annex 3). This means that whilst many of the prevention, detection and response policies, systems and procedures may be similar they need to take in to account the different factors.

Any fraud risk assessment should not be a standalone exercise but rather an ongoing process that is refreshed on a regular basis. Carrying out the fraud risk assessment may reveal instances of actual or suspected fraud. Should this happen next steps will be determined on circumstances, the existing control framework (including any response plan(s)), and in consultation with the key members of the organisation's management team.



The Board's risk appetite and fraud

It is important that, as part of setting their overall risk appetite, the Board considers fraud within their tolerance for the risks associated with the management of the organisation's (and group's) funds. The development and continued assurance of a robust counter fraud control framework should then contribute to the organisation matching the risk appetite and tolerance agreed by the Board.

Organisational resilience

Organisational resilience is the ability of an organisation to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper.

In order to build organisational resilience in relation to fraud, defined as the measure of how well an organisation is protected against fraud, there are a number of key questions on the organisation's culture, policies and procedures which the Board should consider.

It is essential that Board members understand and meet their responsibilities to create organisational resilience to protect the funds and assets of the organisation from fraud. As part of their counter fraud strategy the Board should establish a counter fraud, bribery and corruption policy that is regularly reviewed together with a response plan for dealing with potential instances of fraud, bribery, and corruption.

Annex 1 sets out key questions for Boards to ask as a starting point in considering Fraud risk.

Annex 2 then sets out a more detailed Organisational Counter Fraud Checklist which lists key questions for Boards on areas of organisational resilience to assist the Board members to assess the adequacy and, where necessary, the development of their current organisational counter fraud policy and response plan.

Operational resilience

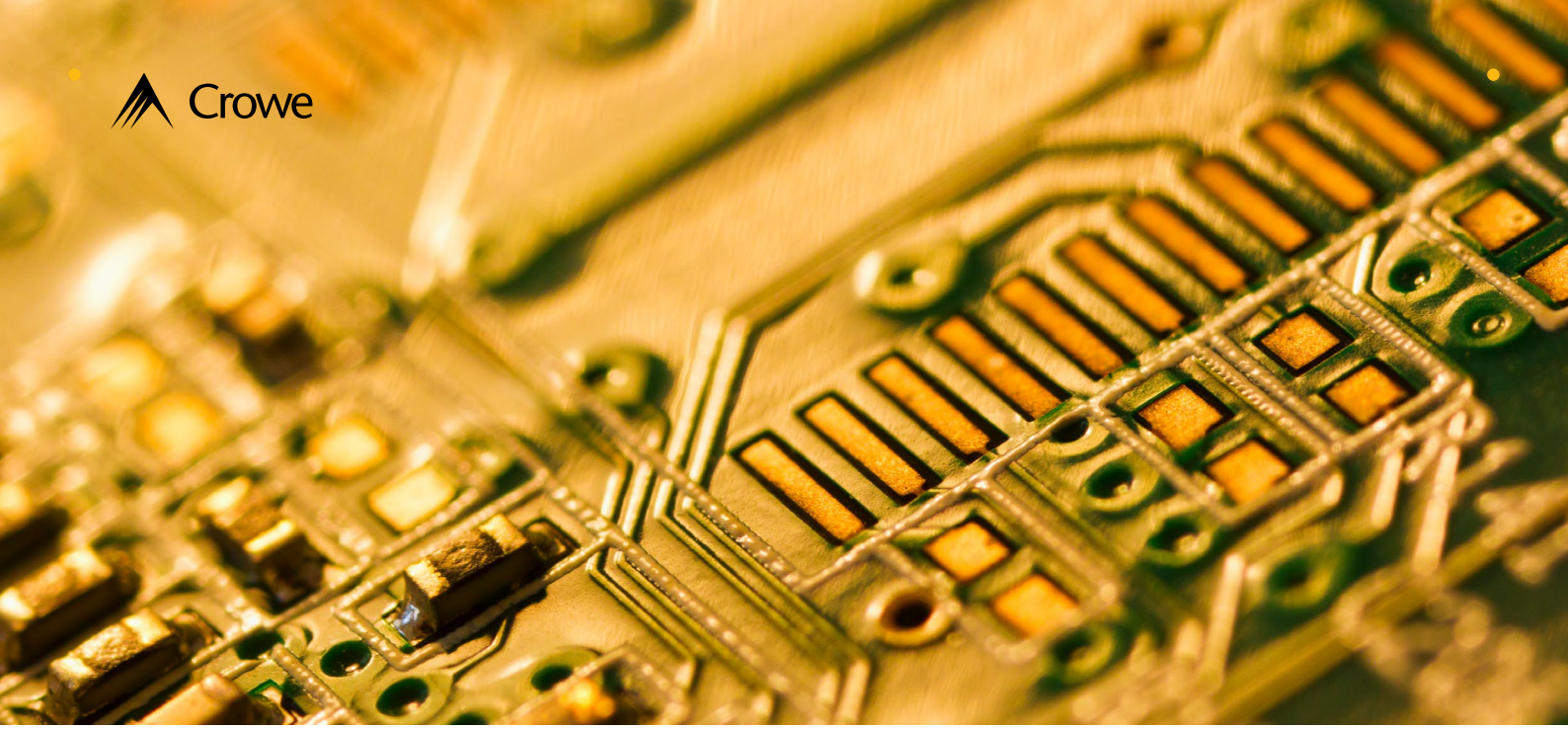
Operational resilience requires the organisation to have in place cost effective controls to deter and prevent fraud and error and the risk assessment must seek to identify all the potential fraud risks.

This will require an open and honest discussion of the type and nature of the fraud risks the organisation faces. This is best carried out at the operational level by those responsible for the delivery of key business processes where fraud may occur.

A fraud risk assessment at the detailed operational level consists of a structured approach to:

- Identifying as far as possible all the potential fraud risks facing a particular function or business unit;
- Completing an assessment of the potential risks to determine the likelihood of the risk and its impact if it were to occur;
- Matching the risks identified to the current control framework to deter or prevent fraud occurring;
- Assessing the adequacy of required actions to alert, stop, investigate and recover losses, and ensure lessons are learnt should suspected fraud occur;
- Assessing any weaknesses or gaps in the control framework and what actions are required to resolve them, together with a plan to achieve this, and;
- Setting key accountabilities and responsibilities.

Annex 3 is a checklist of potential fraud risks by function and activity and is intended to aid Board members to identify the types of operational fraud risks which may be relevant to the organisation. Identifying these fraud risks will assist the Board to address any identified gaps or weaknesses in the control framework to improve the organisation's capability and resilience to counter fraud.



Cyber security

It is well recognised that fraud has moved online and that no current fraud risk assessment can ignore the risks from cyber security. The Australian Cyber Security Centre (ACSC) is the Commonwealth Government agency responsible for promoting and advising on how to protect your charity online. ACSC together with other agencies has several publications on the topic, a summary of which can be found on the **Australian Securities & Investments Commission (ASIC) website.**

Crowe UK, in collaboration with Prof. Mark Button and Dr. Victoria Wang at the Institute of Criminal Justice Studies at University of Portsmouth have developed an online Cyber Vulnerability assessment that is free to access and provides a downloadable PDF report that assesses your organisation's:

- Attractiveness to cyber criminals;
- Potential damage in event of a cyber breach, and;
- Strength/weakness of cyber security and resilience.

Access can be found here.

Annex 4 lists a set of questions from the Australian Securities & Investments Commission publication "Key questions for an organisations Board of Directors" to assist with their existing strategic-level risk discussions on cyber security and specifically how to ensure the right safeguards and cultures are in place.

Contents

Annex 1

Key fraud questions for Boards

The following are key questions for Boards to ask as a starting point in considering fraud risk best practice.

Do we as a Board?	Comments
Understand our key fraud risks and how these change over time?	
Have a clear and proportionate anti-fraud strategy, balancing preventative, detective and deterrent activities?	
Actively promote the raising of concerns by staff, volunteers and/or third parties?	
Promote an anti-fraud culture and set the tone for the organisation?	
Understand the fraud risks within our supply chain?	
Understand the fraud risks within our third partner delivery organisations?	
Understand how we would identify if a significant fraud was happening based on data available to us?	

Do we as a Board?	Comments
Have a clear Fraud Response Plan, setting out responsibilities, membership and decision-making bodies and investigation processes?	
Identified that the right skills to respond to fraud and cyber fraud incidents are available within our organisation or how they can be scaled up as part of our response?	
Have an anti-fraud policy and code of ethics which is communicated and understood across staff, volunteers and third parties?	

All of the above questions need to be considered in the context of the structure and activities of the organisation and the fraud risks which it faces to enable the Board to ensure that the appropriate mitigating controls and action plans are put in place.

Annex 2

Organisational counter fraud checklist

Social Purpose Organisations should have as part of their counter fraud, bribery and corruption strategy:

- A counter fraud, bribery and corruption policy that is regularly reviewed; and
- A response plan for dealing with potential instances of fraud, bribery and corruption.

The following questions will assist Boards to assess the adequacy and, where necessary, the development of their current organisational counter fraud policy and response plan and to understand and meet their responsibilities to protect the funds and assets of the organisation from fraud.

Does the Board's organisational counter fraud policy set out:	Yes	No	Comments
The purpose of the policy in setting out the organisation's stance on, and its approach to preventing, detecting, reporting and investigating fraud, bribery and corruption?	☐	☐	
The scope of the policy, to whom it applies and the implications of non-compliance?	☐	☐	

Does the Board's organisational counter fraud policy set out:	Yes	No	Comments
A tone from the top that sends a clear message to staff and stakeholders on the standards of expected behaviour, and specifically that fraudulent behaviour is unacceptable, will not be tolerated and that the organisation is committed to reduce instances of fraud to an absolute minimum?			
How fraud and corruption is defined in the organisation with reference to current legislation and, where relevant, ACNC and other regulatory guidance?			
The organisation's approach to its fraud risk assessment?			
The key Board and management responsibilities in relation to the counter fraud policy within the organisation?			
How the organisation will continue to improve its counter fraud policy based on any lessons learnt?			

Counter Fraud Response Plan

Does the Board's organisational counter fraud response plan include:	Yes	No	Comments
Details of the organisation's whistleblowing policy, including how and where staff, partners and other stakeholders can report potential instances of fraud and corruption?	☐	☐	
How the organisation would respond to identified instances of fraud, bribery or corruption?	☐	☐	
The roles and responsibilities of staff, teams and functional operating groups in responding to instances of fraud, bribery or corruption?	☐	☐	
How any information on potential fraud, bribery or corruption should be reported, both within the organisation and to other relevant bodies (including law enforcement agencies)?	☐	☐	
How the organisation monitors the progress of any investigation, and makes decisions on them?	☐	☐	

Does the Board's organisational counter fraud response plan include:	Yes	No	Comments
The procedure for reporting identified loss from fraud, bribery or corruption both internally and externally and any associated recoveries?			
The allocation of responsibility for an annual fraud action plan that summarises and is used to monitor key actions to improve capability, activity and fraud resilience?			
Agreed activities to seek to detect fraud in high-risk areas where little or nothing is known of the potential risk of fraud, bribery or corruption activity?			
How staff will access training appropriate to their role to promote and understanding and awareness of the organisation's fraud risks and their responsibilities?			
The organisation's policies and procedures to identify potential conflicts of interest, including gifts and hospitality, and the requirements for staff to declare and record offers of gifts and hospitality (whether accepted or declined)?			

Annex 3

Operational counter fraud risk assessment

There is evidence that during times of economic instability there is an increased risk of operational fraud. This may be because resource constraints can reduce internal controls and oversight and because individuals facing hardship may be more likely to consider fraudulent practices. The following provides further information on the four key areas of operational fraud that social purpose organisations should consider.

Extraction fraud

This is where either assets in possession of the organisation are misappropriated or unauthorised liabilities are created for the organisation. Such frauds can involve the organisation's own staff, intermediaries, or partner organisations. Extraction frauds can be carried out by various means such as false invoices, overcharging, or making unauthorised grant and other payments, and with the developments in technology will also encompass cyber fraud.

Essentially such frauds take advantage of weaknesses in controls over assets and liabilities and potentially in IT controls. Important areas will be controls within the purchases, creditors, and payments cycles.

The cycles can be evaluated by considering questions such as how is access to the organisation's systems controlled, who authorises incurring liabilities, who records liabilities, who processes payments, who records payments and what checks and approvals are made? The close monitoring of management accounts and ledger entries, the implementation of adequate IT protocols and controls together with strict budgetary controls are generally seen as necessary for deterring and detecting frauds of this type.

Diversion fraud

This is where income or other assets due to the organisation are diverted before they are within the control and accounting records of the organisation. Social purpose organisations can have additional risks of this type where they are in receipt of grants and other voluntary income because, for example, unlike sales income, control by the organisation may not be possible until after the transaction has been initiated by the third party.

It may therefore be important for organisations to consider their different income streams and when and how they are received to ensure that any opportunities for diversion of income are minimised. For example, income received directly into the organisation's bank account will be a lower risk than income being received through third-party intermediaries.

Backhanders and inducements

There is the risk that individuals who can authorise expenditure or influence the selection of suppliers can receive inducements to select one supplier in preference to another. This risk can usually be mitigated by having robust supplier selection and tendering procedures.

For organisations operating overseas there can be a risk that payments authorised and released from Australia could be diverted, probably into the underground economy, as a result of inducements paid in the destination country. Social purpose organisations should be aware of the requirements and extent of the Act as this extends their liability to actions beyond the shores of Australia, to cover the actions of their intermediaries and agents. There is increasing cross-border cooperation between regulators/ investigatory agencies to investigate and enforce anti-bribery laws.

Financial reporting fraud

Financial reporting fraud involves the intentional overstatement or understatement of income, expenditure, assets or liabilities in the organisation's financial statements. This type of fraud can be used to conceal other frauds such as the misappropriation or diversion of assets, but may also occur where individuals are motivated by internal or external organisational pressures to hit performance targets with associated indirect benefits, for example avoiding the loss of a bonus payment or sometimes just to meet or exceed expected performance.

Boards should be aware that fraudulent financial reporting by management is often not easy to detect both because it can be difficult to separate overly optimistic reporting from deliberate misstatements and because financial reporting explanations provided to the Board may be from those in a position to carry out financial reporting fraud. Additionally, for many social purpose organisations there is no direct linkage between the cost of output and other financial measures, such as gross profit margin, which can be monitored to help manage the risks of material frauds including financial reporting fraud.

It is therefore important that Boards are aware of and consider the financial reporting fraud risks within areas such as income recognition and asset and liability misstatement as part of their Operational counter fraud risk assessment.

Risks to consider

A lack of controls or emphasis on ethical behaviour can promote a culture within an organisation where employees rationalise fraudulent behaviour and/or fraudulent financial reporting.

The table below, sets out some examples of operational risks by function which the Board may need to consider within their risk assessment.

Function / Activity	Potential Fraud Risks
Income: Fundraising	External parties: • Undertaking bogus collections for the organisation and keeping funds raised • Taking part in a fundraising event for the organisation and keeping sponsorship raised • Set up a bogus website purporting to be the organisation to collect and keep donations • Circulate bogus email(s) purporting to be the organisation to collect and keep donations Internal parties: • Staff members or volunteers divert fundraising receipts before being recorded within the organisation's records • Falsifying fundraising records to mask fraud elsewhere
Income: Grants	Internal parties: • Making grant applications to obtain funds outside of the organisation's systems and records • Falsifying grant monitoring documents for continued funding

Function / Activity	Potential Fraud Risks
Income: Shops	External parties: • Shoplifting • Price tag switching • Theft of cash • Theft through unauthorised access to staff-only areas and the stock room Internal parties: • Theft of inventory (including donated items) by staff or volunteers • Theft of cash (directly or through claimed expenses) • Identifying items as rag/scrap when they are not • Incorrect or incomplete transaction recording
Income: Legacies	The executor (lay or professional): • Fails to notify the organisation of their entitlement • Underpays the organisation by stealing / omitting assets or falsifying liabilities in the estate records • Sells assets cheaply to a friend or associate • Levies excessive fees A relative or carer: • Steals or conceals estate assets • Forges a will or codicil (a supplement to a will) • Conceals the existence of a will Internal parties: • Falsified legacy administration records (the will, estate accounts, etc) to facilitate - Diversion of legacy income - Income being paid to a bogus co-beneficiary

Function / Activity	Potential Fraud Risks
Expenditure: Grants	• An applicant organisation is created for the sole purpose of stealing funding (there was never any intention of delivering a project) • The organisation named in the grant application is unaware that an application has been made • Documents supplied to help the funder monitor the use of the grant (often invoices and bank statements) are fake or doctored
Expenditure: Procurement and Contract Management	• Under-provision of goods and services charged to the organisation • Over-charging for goods and services • Misrepresentation in tenders • Contract fixing through undeclared conflicts / personal relationships with suppliers • Sale of critical bid information, contract details or other sensitive information
IT / Digital Services	Technology enabled fraud: • Phishing • Hacking • Ransomware • Social engineering (using impersonation e.g. by phone/email) • Theft or abuse of proprietary or confidential information by our people (e.g. leavers)

Function / Activity	Potential Fraud Risks
Human Resources: Payroll expenditure	Payroll: • Fictitious (or ghost) employees on the payroll • Falsifying work hours to achieve fraudulent wage / overtime payments • Improper changes in salary levels • Abuse of holiday leave or time-off entitlements (including sickness absence to cover 'moonlighting') • Making false compensation claims • Theft of employee contributions to benefit plans Staff expenses: • Submitting inflated or false expense claims • Adding private expenses to legitimate expense claims • Applying for multiple reimbursements of the same expenses
Human Resources: Recruitment	External candidates: • Falsified employment requirements (e.g. qualifications and references) • Falsified external references and checks Internal parties: • Failure to declare potential conflicts of interest / personal relationships • Undeclared relationships with third party recruitment agencies

Function / Activity	Potential Fraud Risks
Finance: receipts and payments	Cash and cheque processing: • Skimming of cash (understating receivables) • Stealing incoming cash or cheques through an account set up to look like a bona fide payee • Theft of cheques • Depositing a cheque into a third-party account without authority • Counterfeiting / tampering with cheques • Issuing a cheque knowing that there are insufficient funds in the account to cover it • Wire transfer fraud (fraudulent transfers into bank accounts) Other income / payments: • Improper use of entity credit cards • Creating false payment instruction with forged signatures and submitting it for processing • False email payment request together with hard copy printout with forged approval signature • Pay and return schemes (where an employee creates an overpayment to a supplier and pockets the subsequent refund) • Using fictitious suppliers for false billing

Function / Activity	Potential Fraud Risks
Finance: Other transactions	Inventory and fixed assets: • Theft of inventory • False write off and other debts to inventory • False sales of inventory • Theft of fixed assets, including computers and other IT related assets • Unauthorised private use of the organisation's property/equipment Supplier transactions: • Mandate fraud - changing a direct debit, standing order or bank transfer mandate by purporting to be a supplier or organisation to which the organisation makes regular payments • Falsifying documents to obtain authorisation for payment • Forging signatures on payment authorisations • Submitting for payment false invoices from fictitious or actual suppliers • Improper changes to supplier payment terms or other supplier details • Intercepting payments to suppliers • Authorising orders to a particular supplier in return for a back-hander payment • Unrecorded sales or receivables

Function / Activity	Potential Fraud Risks
Finance: Management Accounts and Financial Statements	Improper revenue recognition: • Statements not prepared in line with accounting policies • Holding the books open after the end of an accounting period • Backdating agreements • Improper classification of revenues Misstatement of assets, liabilities and/or expenses: • Fictitious fixed assets, investments, bank accounts • Manipulation of fixed asset valuations • Understating loans and payables • Misstatement of prepayments and accruals • Off balance sheet items • Delaying the recording of expenses to the next accounting period Other accounting misstatements: • Concealment of losses (teeming and lading or other) • Fictitious general ledger accounts • Journal entry fraud • Improper or inadequate disclosures • Misrepresentation, non-clearance or improper clearance of suspense accounts
Other	Corruption • Conflicts / personal interest • Collusions • Favouritism • Employee setting up to supply goods and services to the organisation • Bribery • Extortion • Blackmail • Kickbacks (employee sells entity owned property at less than market value in return for a kickback)

Annex 4

Cyber security: a strategic risk management issue

Today's organisations collect, process and retain more information than they have ever done. For not-for-profits, this information can be:

- Internal, which is their own operations, employees or their 'business', or;
- External, such as from beneficiaries, donors, or even customers, if they run any trading activities.

The impact of this digital retention of information means that organisations have become more dependent on information systems and more vulnerable to attack by sophisticated cybercriminals or even their own employees.

Over the 2020–21 financial year, the Australian Cyber Security Centre (ACSC) reported receiving over 67,500 cybercrime reports, which equates to one report every 8 minutes - an increase of nearly 13 per cent from the previous financial year. A higher proportion of cyber security incidents in the 2020-21 financial year was categorised by the ACSC as 'substantial' in impact, with no sector of the Australian economy being immune from the impacts of cybercrime and other malicious cyber activity.

Making organisations cyber-resilient is therefore now regarded as a key strategic risk management issue which should be monitored by Chief Executives and Boards.

The following are some of the factors that organisations should consider.

Prioritise which information asset should be protected – so for example for an organisation with large donor base this could be the donor information.

- Consider differentiating protection based on the prioritisation – so for example, more rigorous passwords or encryptions;
- Integrate security into technology projects from the outset;
- Use defences such as firewalls to uncover attacks – consider penetration testing;
- Test the organisations response to breaches –make sure there is a strategy in place known by the communication team for managing the messages when a breach occurs;
- Raise your employees and users understanding and awareness of the importance of protecting the not-for-profit's information. Often organisations are made vulnerable to attacks because employees and volunteers do not observe the basic information security measures – for example by emailing sensitive files to a large group, using memory sticks with bugs or clicking on unsecure links. Help the organisation understand the risks;
- Cybersecurity should become a board agenda item and be integrated into functions such as HR or donor management or fundraising.

ACSC leads the Australian Government's efforts to improve cyber security and monitor cyber threats across the globe to enable it to alert Australians early on what action to take. ACSC provide advice and information about how to protect your business online. When there is a cyber security incident, ACSC provide advice to individuals, businesses and critical infrastructure operators.

ACSC has a number of publications including "Strategies to Mitigate Cyber Security Incidents" which is designed to help organisations mitigate cyber security incidents caused by various cyber threats.

In addition to **ACSC** the **ASIC** have a suite of resources aimed at an organisations management of cyber risk.

As per the ASIC website, the ASIC resources include a list of **"Key questions for an organisation's Board of directors".** These are listed below, how does your organisation compare?

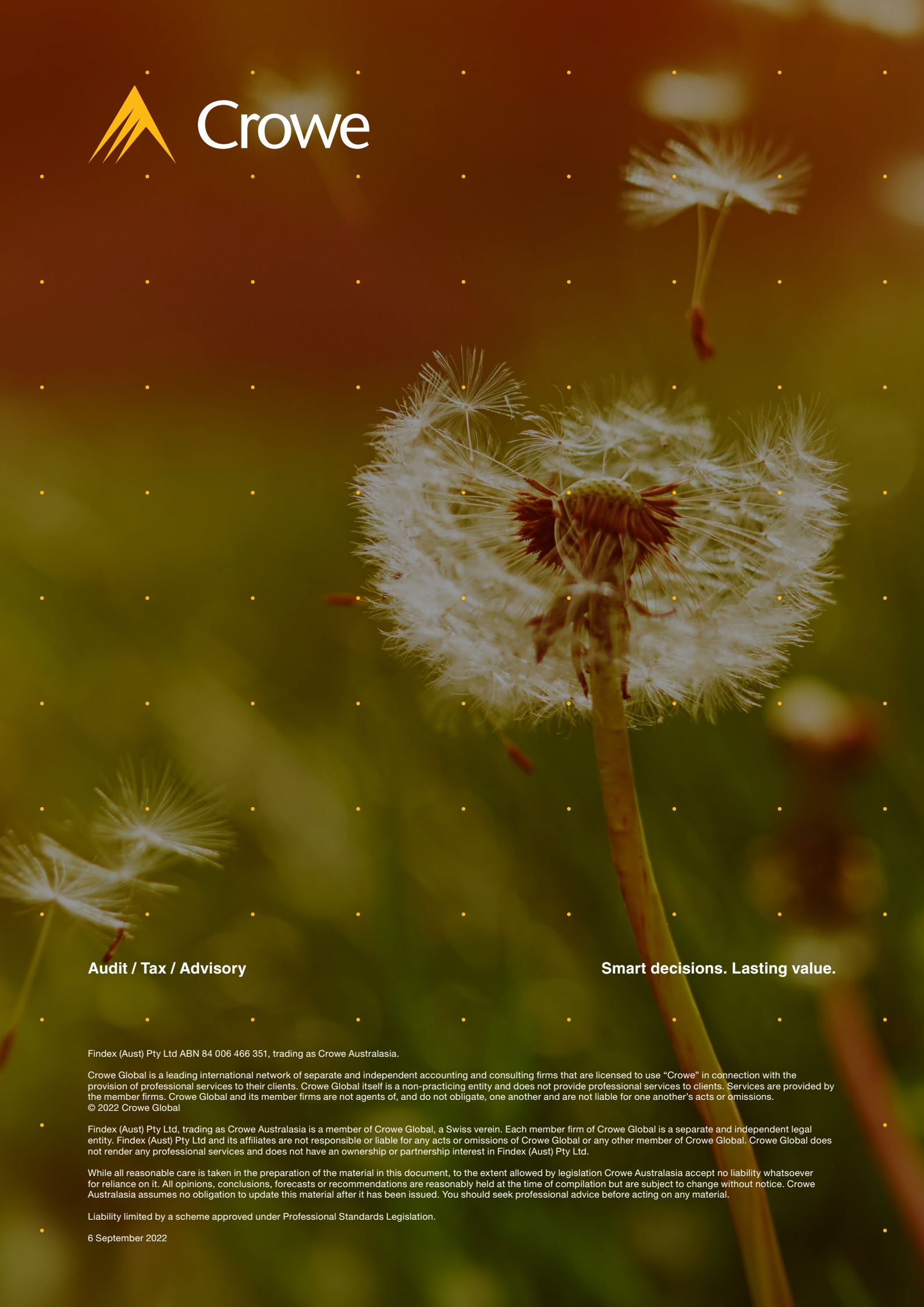
Key questions for an organisation's Board of directors	Comments
Are cyber risks an integral part of the organisation's risk management framework? The board should ensure that cyber risk is an element of the broader risk framework and that exposures are recognised, assessed for impacts based on clearly defined metrics such as response time, cost and legal or compliance implications, and planned for to attract investment commensurate to a risk-based assessment.	
How often is the cyber resilience program reviewed at the board level? Given the rate of change in the cyber risk landscape, and the speed at which a business can be severely compromised (potentially within hours or days); the board should consider whether periodic reviews (that are more frequent than for other risks forming part of the risk management framework) should be adopted.	
What risk is posed by cyber threats to the organisation's business? Different businesses will be exposed to different cyber risks and different potential consequences. It is important for the board to reflect on risks relevant to the particular business of the organisation. Without understanding the nature of the risk and its consequences it is difficult for a board to set a suitable risk tolerance and to ensure that cyber risks are adequately dealt with by the organisation's risk management framework.	

Key questions for an organisation's Board of directors	Comments
Does the board need further expertise to understand the risk? Although boards may not require general technology expertise, for many companies it may be advisable to have one or more directors who have a strategic understanding of technology and its associated risks, or who have a background in cybersecurity. In some circumstances, the board should consider the use of external cyber experts to review and challenge the information presented by senior management.	
How can cyber risk be monitored and what escalation triggers should be adopted? Trying to identify a cyber risk may pose particular challenges. Organisations at the forefront of good practice are using intelligence-driven solutions to deal with this challenge. For some organisations malicious cyber activities may be devastating to the organisation's business operations, therefore, it is important to consider what might lead to the provision of more detailed information on the risk to senior management and the board.	

Key questions for an organisation's Board of directors	Comments
What is the people strategy around cybersecurity? Despite significant advances in cybersecurity technology; products, lack of staff awareness of safe cyber practices, social engineering and negligent behaviours remain a major source of cyber issues. Boards should satisfy themselves that there is sufficient investment in staff awareness training given its prominence as a source of risk—and because a collective effort against cyber threats will better serve an organisation.	
What is in place to protect critical information assets? The board should be satisfied that critical information assets of the organisation are appropriately secure. There should be transparency surrounding the location of all critical assets (including third-party partners and service providers), how they are protected and how protection is being assured.	
What needs to occur in the event of a breach? Boards should ask themselves: If and when a problem arises, what processes are in place for communicating effectively, internally and externally, and managing the situation?	

Key questions for an organisation's Board of directors	Comments
Has there been a sufficient level of scenario planning and testing to ensure that response plans are valid and up to date, including with third-party suppliers and dependants? Boards may need to ensure that security and customer trust are central considerations as companies strive to deliver innovative products and services through technology. • **Application control** to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers. • **Patch applications** (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computers with 'extreme risk' security vulnerabilities within 48 hours. Use the latest version of applications. • **Configure Microsoft Office macro settings** to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate. • **User application hardening.** Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.	

Key questions for an organisation's Board of directors	Comments
• **Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing. • **Patch operating systems.** Patch/mitigate computers (including network devices) with 'extreme risk' security vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions • **Multi-factor authentication** including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository • **Regular backups** of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.	



Audit / Tax / Advisory

Smart decisions. Lasting value.

6 September 2022