# Social Purpose and Non Profit Organisations

## Fraud Risk Assessment

April 2021

Audit / Tax / Advisory / Risk

Smart decisions. Lasting value.

# Fraud and the responsibilities of Governing Bodies

## Why is tackling fraud important to Boards

The Charity Commission has highlighted that fraud is a serious problem that Boards can't afford to ignore, with a cost to the social purpose organisation sector of hundreds of millions, potentially billions, of pounds each year. 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 as a whole.

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 under charity and other law 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 Charity Commission 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 Fraud Act 2006. Under the act 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).

As well as the Fraud Act, a number of other relevant offences are found elsewhere in statute, in particular false accounting contrary to s.17 of the Theft Act 1968. This covers the falsification, alteration or otherwise dishonest manipulation of any accounting document.

### Charity Commission guiding principles

In their guide to tackling fraud in the charity sector the Charity Commission have set out eight guiding principles:

1. **Fraud will always happen** – simply being a charity is no defence. Even the best-prepared organisations cannot prevent all fraud. Charities are no less likely to be targeted than organisations in the private or public sector. Fraudsters do not give a free pass to charitable activities.
2. **Fraud threats change constantly.** Fraud evolves continually, and faster, thanks to digital technology. Charities need to be alert, agile and able to adapt their defences quickly and appropriately.
3. **Prevention is (far) better than cure.** Financial loss and reputational damage can be reduced by effective prevention. It is far more cost-effective to prevent fraud than to investigate it and remedy the damage done.
4. **Trust is exploited by fraudsters.** Charities rely on trust and goodwill, which fraudsters try to exploit. A strong counter-fraud culture should be developed to encourage the robust use of fraud prevention controls and a willingness to challenge unsusal activities and behaviour.
5. **Discovering fraud is a good thing.** The first step in fighting fraud is to find it. This requires charities to talk openly and honestly about fraud. When charities do not do this the only people who benefit are the fraudsters themselves.

6. **Report every individual fraud.** The timely reporting of fraud to police, regulators and other agencies is fundamental to strengthening the resilience of individual charities and the sector as a whole.
7. **Anti-fraud responses should be proportionate to the charity's size, activities and fraud risks.** The vital first step in fighting fraud is to implement robust financial controls and get everyone in the charity to sign up to them.
8. **Fighting fraud is a job for everyone.** Everybody involved – trustees, managers, employees, volunteers, beneficiaries – has a part to play in fighting fraud. Trustees in particular should manage fraud risks actively to satisfy themselves that the necessary counter-fraud arrangements are in place and working properly.

### 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 a number of levels within the organisation:

- 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 if 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 seen as 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

The Charity Commission's first guiding principle as explained above recognises that fraud will always happen.

It is therefore 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.

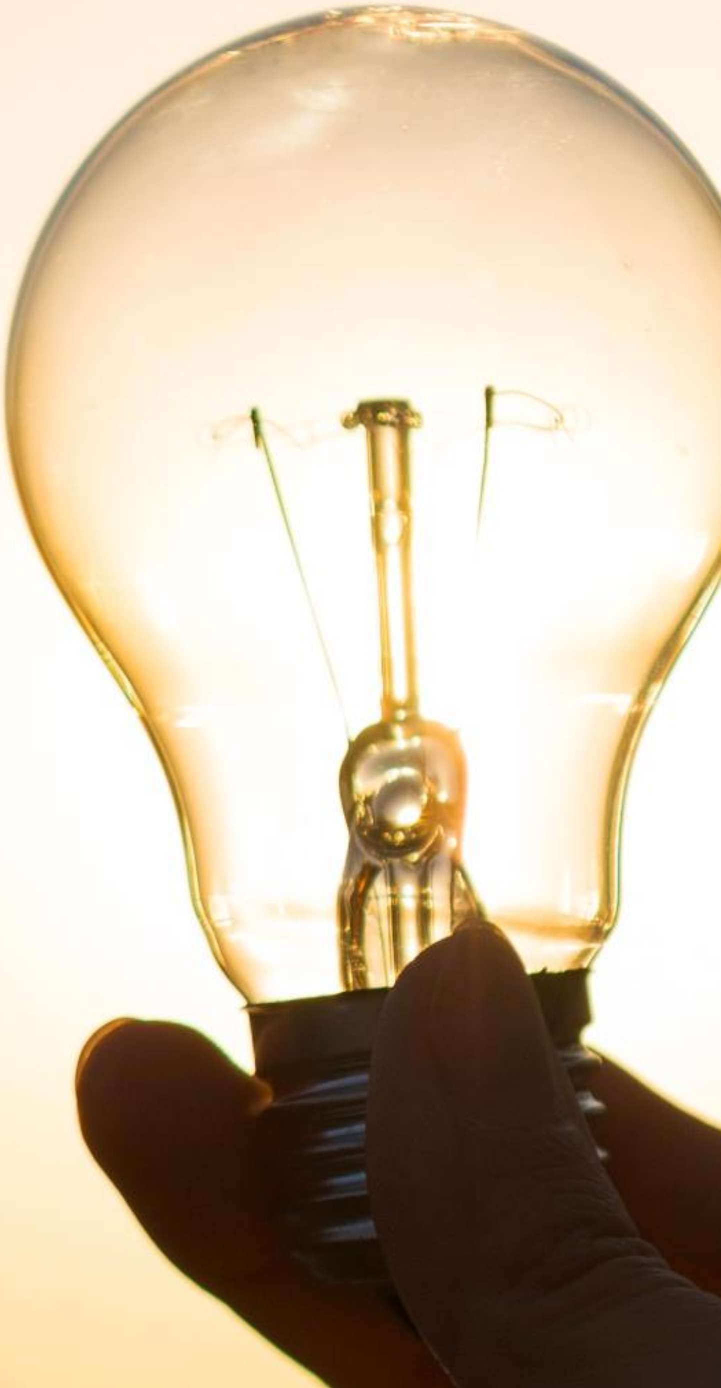
**Annex 3 is a checklist of potential fraud risks by function and activity and is intended to aid Board members to identify the types of operational fraud risks which may be relevant to the organisation. Identifying these fraud risks will assist the Board to address any identified gaps or weaknesses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

### Cyber security

It is well recognised that fraud is and has moved online and that that no fraud risk assessment can today ignore the risks from cyber security. The National Cyber Security Centre (NCSC) was launched in October 2016 to provide a single point of contact for SMEs, larger organisations, government agencies, the general public and departments. NCSC now has a number of publications including a Cyber Security Toolkit for Boards which is available on their website https://www.ncsc.gov.uk/collection/board-toolkit.

**Annex 4 lists a set of questions from the NCSC publication “10 Steps to Cyber Security” to assist Boards 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 |
|---|---|
| 1. Understand our key fraud risks and how these change over time? | |
| 2. Have a clear and proportionate anti-fraud strategy, balancing preventative, detective and deterrent activities? | |
| 3. Actively promote the raising of concerns by staff, volunteers and/or third parties? | |
| 4. Promote an anti-fraud culture and set the tone for the organisation? | |
| 5. Understand the fraud risks within our supply chain? | |
| 6. Understand the fraud risks within our third partner delivery organisations? | |
| 7. Understand how we would identify if a significant fraud was happening based on data available to us? | |
| 8. Have a clear Fraud Response Plan, setting out responsibilities, membership and decision-making bodies and investigation processes? | |
| 9. 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? | |
| 10. 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? | | |
| • 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, charity commission 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 takes decisions on them? | | |
| • 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 an 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 also 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, unlike for example 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 by through third-party intermediaries.

## Backhanders and inducements

There is the risk that individuals who are able to 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 the UK 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 UK Bribery Act 2010 as this extends their liability to actions beyond the shores of the UK to cover the actions of their intermediaries and agents. Organisations are required to put in place proportionate measures to prevent backhanders and inducements from being paid, either by their workers, agents or intermediaries or to their workers, agents or intermediaries.

## 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, which has drawn from amongst others material from the Charity Commission, the Fraud Advisory Panel and the National Cyber Security Centre, 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:<br>• Undertaking bogus collections for the organisation and keeping funds raised<br>• Taking part in a fundraising event for the organisation and keeping sponsorship raised<br>• Set up a bogus website purporting to be the organisation to collect and keep donations<br>• Circulate bogus email(s) purporting to be the organisation to collect and keep donations<br>Internal parties:<br>• Staff members or volunteers divert fundraising receipts before being recorded within the organisation’s records<br>• Falsifying fundraising records to mask fraud elsewhere |
| **Income: Grants** | Internal parties:<br>• Making grant applications to obtain funds outside of the organisation’s systems and records<br>• Falsifying grant monitoring documents for continued funding |

| Function / Activity | Potential Fraud Risks |
|---|---|
| **Income: Shops** | External parties:<br>• Shoplifting<br>• Price tag switching<br>• Theft of cash<br>• Theft through unauthorised access to staff-only areas and the stock room<br>Internal parties:<br>• Theft of inventory (including donated items) by staff or volunteers<br>• Theft of cash (directly or through claimed expenses)<br>• Identifying items as rag/scrap when they are not<br>• Incorrect or incomplete transaction recording |
| **Income: Legacies** | The executor (lay or professional):<br>• Fails to notify the organisation of their entitlement<br>• Underpays the organisation by stealing / omitting assets or falsifying liabilities in the estate records<br>• Sells assets cheaply to a friend or associate<br>• Levies excessive fees<br>A relative or carer:<br>• Steals or conceals estate assets<br>• Forges a will or codicil (a supplement to a will)<br>• Conceals the existence of a will<br>Internal parties:<br>• Falsified legacy administration records (the will, estate accounts, etc) to facilitate<br>○ Diversion of legacy income<br>○ Income being paid to a bogus co-beneficiary |
| **Expenditure: Grants** | • An applicant organisation is created for the sole purpose of stealing funding (there was never any intention of delivering a project)<br>• The organisation named in the grant application is unaware that an application has been made<br>• Documents supplied to help the funder monitor the use of the grant (often invoices and bank statements) are fake or doctored |

| Function / Activity | Potential Fraud Risks |
|---|---|
| **Expenditure:**<br>**Procurement and Contract Management** | • Under-provision of goods and services charged to the organisation<br>• Over-charging for goods and services<br>• Misrepresentation in tenders<br>• Contract fixing through undeclared conflicts / personal relationships with suppliers<br>• Sale of critical bid information, contract details or other sensitive information |
| **IT / Digital Services** | Technology enabled fraud:<br>• Phishing<br>• Hacking<br>• Ransomware<br>• Social engineering (using impersonation (e.g. by phone/email)<br>• Theft or abuse of proprietary or confidential information by our people (e.g. leavers) |
| **Human Resources:**<br>**Payroll expenditure** | Payroll:<br>• Fictitious (or ghost) employees on the payroll<br>• Falsifying work hours to achieve fraudulent wage / overtime payments<br>• Improper changes in salary levels<br>• Abuse of holiday leave or time-off entitlements (including sickness absence to cover ‘moonlighting’)<br>• Making false compensation claims<br>• Theft of employee contributions to benefit plans<br>Staff expenses:<br>• Submitting inflated or false expense claims<br>• Adding private expenses to legitimate expense claims<br>• Applying for multiple reimbursements of the same expenses |

| Function / Activity | Potential Fraud Risks |
|---|---|
| **Human Resources: Recruitment** | External candidates:<br>• Falsified employment requirements (e.g. qualifications and references)<br>• Falsified external references and checks<br>Internal parties:<br>• Failure to declare potential conflicts of interest / personal relationships<br>• Undeclared relationships with third party recruitment agencies |
| **Finance: Receipts and payments** | Cash and cheque processing:<br>• Skimming of cash (understating receivables)<br>• Stealing incoming cash or cheques through an account set up to look like a bona fide payee<br>• Theft of cheques<br>• Depositing a cheque into a third-party account without authority<br>• Counterfeiting / tampering with cheques<br>• Issuing a cheque knowing that there are insufficient funds in the account to cover it<br>• Wire transfer fraud (fraudulent transfers into bank accounts)<br>Other income / payments:<br>• Improper use of entity credit cards<br>• Creating false payment instruction with forged signatures and submitting it for processing<br>• False email payment request together with hard copy printout with forged approval signature<br>• Pay and return schemes (where an employee creates an overpayment to a supplier and pockets the subsequent refund)<br>• Using fictitious suppliers for false billing |

| Function / Activity | Potential Fraud Risks |
|---|---|
| **Finance: Other transactions** | Inventory and fixed assets:<br>• Theft of inventory<br>• False write off and other debts to inventory<br>• False sales of inventory<br>• Theft of fixed assets, including computers and other IT related assets<br>• Unauthorised private use of the organisation’s property/equipment<br>Supplier transactions:<br>• 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<br>• Falsifying documents to obtain authorisation for payment<br>• Forging signatures on payment authorisations<br>• Submitting for payment false invoices from fictitious or actual suppliers<br>• Improper changes to supplier payment terms or other supplier details<br>• Intercepting payments to suppliers<br>• Authorising orders to a particular supplier in return for a back-hander payment<br>• Unrecorded sales or receivables |

| Function / Activity | Potential Fraud Risks |
|---|---|
| **Finance:**<br>**Management Accounts and Financial Statements** | Improper revenue recognition:<br>• Statements not prepared in line with accounting policies<br>• Holding the books open after the end of an accounting period<br>• Backdating agreements<br>• Improper classification of revenues<br>Misstatement of assets, liabilities and/or expenses:<br>• Fictitious fixed assets, investments, bank accounts<br>• Manipulation of fixed asset valuations<br>• Understating loans and payables<br>• Misstatement of prepayments and accruals<br>• Off balance sheet items<br>• Delaying the recording of expenses to the next accounting period<br>Other accounting misstatements:<br>• Concealment of losses (teeming and lading or other)<br>• Fictitious general ledger accounts<br>• Journal entry fraud<br>• Improper or inadequate disclosures<br>• Misrepresentation, non-clearance or improper clearance of suspense accounts |
| **Other** | Corruption:<br>• Conflicts / personal interests<br>• Collusion<br>• Favouritism<br>• Employee setting up to supply goods and services to the organisation<br>• Bribery<br>• Extortion<br>• Blackmail<br>• 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 so can be about their own operations or employees or their ‘business’ or collected from external sources 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.

The results of numerous surveys and research show that organisations are still not adequately protected against cyber-attacks. Nearly two-thirds of companies across sectors and regions responding to a joint research carried out by McKinsey and the World Economic Forum described the risk of cyber-attack as a “significant issue that could have major strategic implications.”

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 – so 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 or 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.

The National Cyber Security Centre (NCSC) was set up to help protect critical services from cyber-attacks, manage major incidents and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organisations. Its stated aim is “Helping to make the UK the safest place to live and work online”.

NCSC have developed a product “Cyber Essentials” which helps you to guard your organisation against cyber attack and allows organisations to advertise that they meet a government endorsed standard of cyber hygiene. Cyber Essentials Certification has become a requirement for any organisations bidding for central government contracts which involve handling sensitive and personal information or the provision of certain technical products.

NCSC also has a number of publications including “10 Steps to Cyber Security” which is designed to help organisations protect themselves in cyberspace. It breaks down the task of defending your networks, systems and information into its essential components, providing advice on how to achieve the best possible security in each of these areas and emphasising that protecting your information is a board-level responsibility which has benefits at strategic, financial and operational levels.

The NCSC “10 Steps” publication includes a set of questions to assist Boards with their existing strategic-level risk discussions and specifically how to ensure the right safeguards and cultures are in place. These questions, with a slight change in focus, are equally applicable to social purpose organisations.

| Key questions for Senior Management and Boards | Comments |
|---|---|
| **Protection of key information assets is critical.**<br>• How confident are we that our organisation's most important information is being properly managed and is safe from cyber threats?<br>• Are we clear that the Board and Senior Management are likely to be key targets?<br>• Do we have a full and accurate picture of:<br>○ the impact on our organisation's reputation or existence if sensitive internal, supporter or beneficiary information held by the organisation were to be lost or stolen?<br>○ the impact on the organisations activities if its online activities were disrupted for a short or sustained period? | |
| **Exploring who might compromise our information and why is critical.**<br>• Do we receive regular intelligence from the Chief Information Officer / Head of Security on who may be targeting our organisation, their methods and their motivations?<br>• Do we encourage our technical staff to enter into information sharing exchanges with other organisations in our sector and/or across the economy in order to benchmark, learn from others and help identify emerging threats? | |
| **Pro-active management of the cyber risk at Board level is critical.**<br>• The cyber security risk impacts reputation, culture, staff, information, process control, brand, technology, pricing and finance. Are we confident that:<br>○ We have identified our key information assets and thoroughly assessed their vulnerability to attack?<br>○ Responsibility for the cyber risk has been allocated appropriately? Is it on the risk register?<br>○ We have a written information security policy in place, which is championed by us and supported through regular staff training? Are we confident the entire workforce understands and follows it? | |

## Start the conversation

**Naziar Hashemi**

National Head of Social Purpose
and Non Profit Organisations

+44 (0)20 7842 7229

naziar.hashemi@crowe.co.uk

**Pesh Framjee**

Global Head of Social Purpose
and Non Profit Organisations

+44 (0)20 7842 7228

pesh.framjee@crowe.co.uk

## About us

Crowe UK is a national audit, tax, advisory and risk firm with global reach and local expertise. We are an independent member of Crowe Global, the eighth largest accounting network in the world. With exceptional knowledge of the business environment, our professionals share one commitment, to deliver excellence.

We are trusted by thousands of clients for our specialist advice, our ability to make smart decisions and our readiness to provide lasting value. Our broad technical expertise and deep market knowledge means we are well placed to offer insight and pragmatic advice to all the organisations and individuals with whom we work. Close working relationships are at the heart of our effective service delivery.

@CroweUK

www.crowe.co.uk

Crowe U.K. LLP is a member of Crowe Global, a Swiss verein. Each member firm of Crowe Global is a separate and independent legal entity. Crowe U.K. LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Global or any other member of Crowe Global. Crowe Global does not render any professional services and does not have an ownership or partnership interest in Crowe U.K. LLP.

This material is for informational purposes only and should not be construed as financial or legal advice. You are encouraged to seek guidance specific to your circumstances from qualified advisors in your jurisdiction. Crowe U.K. LLP is registered to carry on audit work in the UK by the Institute of Chartered Accountants in England and Wales and is authorised and regulated by the Financial Conduct Authority.