Social Purpose and Non Profit Organisations

Fraud Risk Assessment

July 2023

Audit / Tax / Advisory / Risk

Smart decisions. Lasting value.

Fraud and the responsibilities of Governing Bodies

Why is tackling fraud important to Boards

The Regulator of Social Housing has highlighted that fraud is a serious problem that Boards can't afford to ignore, with a cost to the social purpose 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 the 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 given to social purpose organisations is used properly and goes to the causes for which it is intended.

For social housing providers, fraud can generally be split between tenancy and corporate fraud. Tenancy fraud occurs when a tenant breaches certain terms of their agreement or misleads a registered provider to secure a tenancy. This can manifest itself in a variety of ways including application, right to buy, key selling, subletting and succession fraud. This is a significant issue for the sector, with recent research[1] indicating that some 150,000 social homes are involved in tenancy fraud. This document addresses the risks posed by corporate fraud, as these have a direct quantifiable financial loss to housing providers.

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.

Regulator of Social Housing reporting requirements in respect of fraud

The Regulator sets out the reporting requirements on fraud in its publication "Regulating the Standards". Registered providers that own a thousand social housing units or more must provide an annual report on fraud losses, the requirements set out in the Governance and Viability Standard:

- Adherence to all relevant law
- Safeguarding taxpayers' interests and the reputation of the sector
- Having an effective risk management and internal controls assurance framework; and
- Protecting social housing assets

[1] Inside Housing - News - Nearly 150,000 social homes involved in tenancy fraud, report warns

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 non-profit 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.
2. **Fraud threats change constantly.** Fraud evolves continually, and faster, thanks to digital technology. Non-profits 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.** Non profits 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 unusal activities and behaviour.
5. **Discovering fraud is a good thing.** The first step in fighting fraud is to find it. This requires non-profits to talk openly and honestly about fraud. When organisations 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 the sector as a whole.
7. **Anti-fraud responses should be proportionate to the entity's size, activities and fraud risks.** The vital first step in fighting fraud is to implement robust financial controls and get everyone in the organisation 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. Board Members 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 that:

- 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. Both the fraud risks themselves and their impact will differ between housing providers due to size, scale, local/national operations, and the inclusion of any non-social housing activities or developments. A more nuanced approach is needed to consider both the operating environment and the type and scale of fraud risk exposure. Whilst many of the prevention, detection and response policies as well as systems and procedures may be similar, they need to take these different factors into account.

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, or areas of control weakness for further review. Should an actual fraud be identified the 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 first guiding principle as explained above recognises that fraud will always happen.

It is important that the Board considers fraud within their tolerance for the risks associated with the management of the organisation's assets when setting their overall risk appetite. 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.

Sector Risk Profile – Fraud Risks;

Each year the Social Housing Regulator sets out its assessment for housing providers as arising in the areas of procurement, mandate fraud, supplier fraud, finance function fraud, and cyber security.

The sector risk profile also reinforces Boards' responsibilities in respect of fraud. Anti-money laundering legislation requires Boards to ensure that;

- There is a robust system of control procedures in place;
- Anti-fraud policies should be subject to regular review and well communicated, with employees receiving regular training;
- There are processes in place to enable the detection and countering of instances of tenancy and other fraud in their stock; and
- There is a culture in place which demonstrates a rigorous attitude to combatting fraud.

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, there are a number of key questions that 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.

International Standard on Auditing 240

In 2021 The Financial Reporting Council updated their International Standard on Auditing (ISA) 240 The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements. Auditors are required to discuss the risks of fraud in the entity, including those specific to the entity's business sector with the Board. They must document the understanding of how "those charged with governance" exercise oversight of management processes for identifying and responding to the risks of fraud and the internal controls that management has established to mitigate these risks. This includes assessing how those charged with management:

- View the risks of fraud in the entity, both misappropriation of assets and fraud relating to financial reporting;
- The general risks of fraud in the social housing sector, and how the organisation mitigates these risks;
- The monitoring and review processes for identifying and responding to the risks of fraud in the entity;
- Understand the controls management have put in place to mitigate those risks;
- Have knowledge of any actual or suspected frauds during the year; and
- Have had any allegations regarding potential frauds made to them during the year.

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.

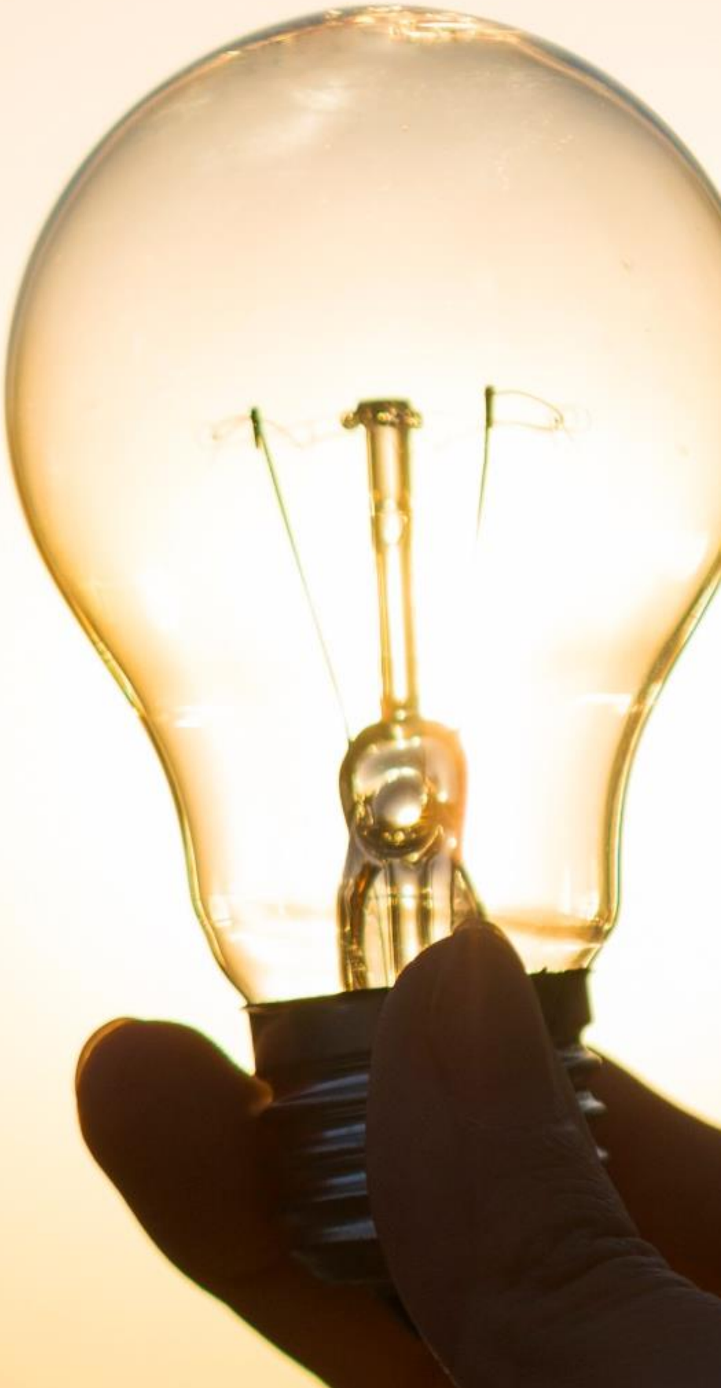
Annex 4 is a methodology and scoring matrix for assessing inherent fraud risk

Cyber security

It is well recognised that fraud 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 5 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 reducing 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 and Regulator of Social Housing 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 including and requiring reporting to regulators?		
• 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 four key areas of operational fraud that social purpose organisations should consider.

Procurement fraud

Procurement fraud is one of the most significant areas of potential fraud for social housing providers given the typical size of spend in this area. The procurement lifecycle is vulnerable to the risks of fraud and corruption at any stage in the process, including procurements that involve a formal tendering process and those that do not. There are risks both in high-value OJEU tendering processes and also in the use of a purchasing card or petty cash. The risks can stem from internal staff, external parties or collusion between the two.

Emphasis has often been placed on the risks of fraud and corruption in the central section of the process, from the invitation of tender to the award of the contract. There are however significant risks in the pre-tendering phase and in the implementation and contract management phase of the process.

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 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. One Provider incurred a loss of ~£1m when fraudsters mimicked the domain and email details of known contacts that were providing services to the group, which allowed them to recreate an email thread this misled those that were copied into the email that it was a genuine follow up to an existing conversation, and led to supplier bank details being fraudulently changed.

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.

Employee/Contractor fraud

There is a wide range of different types of potential fraud risk in this area, including theft of cash, equipment and data by either staff, contractors or suppliers, submission of false claims for travel expenses that have not been incurred or overtime not worked, using organisations credit cards for personal use as well as the creation of invoices for non-existent suppliers.

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. Whilst bonuses are still relatively uncommon in the sector, there can be pressure to manipulate the reported results to manage loan covenants.

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 Sector Risk Profile, 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
Expenditure: procurement fraud	Internal • Bid tailoring schemes • Collusion • Bribery and kickbacks External • Bid rigging • Bid suppression • Bid rotation • Phantom bids
Expenditure: supplier payments	Internal • Changing supplier account details (fraud or through deception) • Falsifying documents to obtain authorisation for payment • Duplicate or false invoices • Submitting for payment false invoices from fictitious or actual suppliers External • Mandate fraud • Improper requests to change supplier bank account details

Function / Activity	Potential Fraud Risks
Finance: receipts and payments	Internal • Bank mandates not up-to-date • Only one person on bank mandates • Inadequate control over manual cheques (for example physical security) • Inadequate control over BACS payments (for example supplier payment details not checked/authorised by a 2nd person) • Wire transfer fraud • Improper use of credit cards External • Inadequate control over changes to supplier detail requests from external parties
Income: rent and service charges	Internal • Creating dummy tenant accounts • Zero/low rent charges • Teeming and lading from tenant accounts • Improper allocation of receipts • Unauthorised w/off's External • Tenancy fraud
Income: non-rental income	Internal • Complex areas of revenue accounting, either through complexity, uncertainty or subjectivity. Area's to consider include income from joint ventures, profit sharing agreements and complex contractual agreements such as where there is overage or waterfall agreements

Function / Activity	Potential Fraud Risks
Payroll	Internal • Falsifying timesheets • Sick Leave • Ghost employees • Misclassification (payscales) External • Construction Industry Scheme abuse

Annex 4 Assessing Inherent Fraud Risk

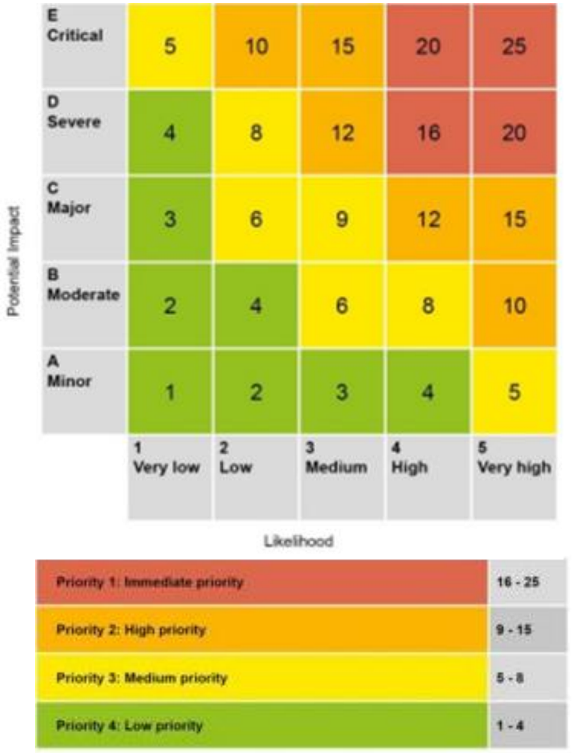
Once potential fraud risks have been identified it is useful to make an assessment of the inherent risk that the risk poses, based on an assessment of the likelihood and impact of the risk occurring in the absence of a control framework. This process is similar to that required to be conducted by auditors under International Standard on Auditing 315 “Identifying and Assessing the Risks of Material Misstatement” which became effective for accounting periods beginning on or after 15 December 2021. This Standard introduces the concept of a “spectrum of inherent risk” based on a number of factors including complexity, subjectivity, change, uncertainty or susceptibility to misstatement due to management bias or other fraud risk factor.

Risks should be assessed and scored against the likelihood of their occurrence and the impact if they do occur (in the same way as that for a normal risk map) and scoring definitions which are meaningful for the risks need to be articulated. When assessing likelihood it is acknowledged that fraud risks are often limited to a single occurrence. Using a scoring system that is based on assessing both occurrence and frequency will result in a quantification of the risk. The output is a heatmap which demonstrates what the assessed key fraud risks to the organisation are, clearly identifying those which should be focussed on. This heatmap can then be assessed against the organisation’s risk appetite in each area and produce actions to mitigate them to acceptable levels.

Scoring Matrix for Fraud Risk;

Likelihood of Occurrence	**Likelihood** of Frequency	**Impact** - Duration of Fraud	**Impact** - Materiality
1 Unlikely	1 Only likely to be a occasional occurrence	1 Fraud should be prevented or detected immediately	1 Unlikely to result in a material loss / reputational risk
2 A possibility it will happen	2 A few instances likely to occur	2 Fraud should be prevented or detected quickly	2 Material loss / reputational risk likely to be avoided
3 Likely to happen	3 A number of instances likely to occur	3 Fraud could go undetected for a period of time	3 Could result in some material loss / reputational risk
4 Quite certain to happen	4 Likely to be a lot of instances	4 Fraud could go undetected for a long duration	4 Could bring high material loss / reputational risk
5 Certain to happen	5 Likely to be multiple instances	5 Fraud could remain undetected	5 Could result in significant material loss / reputational risk

Heatmap for assessing fraud risk



Potential Impact

E Critical	5	10	15	20	25
D Severe	4	8	12	16	20
C Major	3	6	9	12	15
B Moderate	2	4	6	8	10
A Minor	1	2	3	4	5
	1 Very low	2 Low	3 Medium	4 High	5 Very high

Likelihood

Priority 1: Immediate priority	16 - 25
Priority 2: High priority	9 - 15
Priority 3: Medium priority	5 - 8
Priority 4: Low priority	1 - 4

Annex 5 Cyber security: a strategic risk management issue

Cyber security (incorporating data security) is increasingly seen as a key risk for the social housing sector. The Sector Risk Profile 2022 highlights the instances where cyber security threats have resulted in significant interruptions to data, systems and services, and states that "***we expect boards to actively manage this risk***". The heightened risk in this area is reflected in data security and cyber-related risk being included in the top 5 principal risks faced by the top 100 providers in their financial statements for the first time in 2022.

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 assets should be protected. – providers hold sensitive tenant data including bank account details and protected characteristics of tenants
- 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 organisation's 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 subject to the same level of scrutiny as other significant risks.

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. • How confident are we that our organisation’s most important information is being properly managed and is safe from cyber threats? • Are we clear that the Board and Senior Management are likely to be key targets? • Do we have a full and accurate picture of: ○ 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? ○ 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. • 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? • 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?	
Proactive management of the cyber risk at Board level is critical. • The cyber security risk impacts reputation, culture, staff, information, process control, brand, technology, pricing and finance. Are we confident that: ○ We have identified our key information assets and thoroughly assessed their vulnerability to attack? ○ Responsibility for the cyber risk has been allocated appropriately? Is it on the risk register? ○ 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

Head of Social Purpose and Non Profits

+44 (0)20 7842 7229

naziar.hashemi@crowe.co.uk

Richard Evans

Head of Social Purpose and Non Profits Risk and Assurance

+44 (0)20 7842 7221

richard.evans@crowe.co.uk

Julia Poulter

Head of Social Housing

+44 (0)20 7842 5216

julia.poulter@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 limited liability partnership registered in England and Wales with registered number OC307043. The registered office is at 2nd Floor, 55 Ludgate Hill, London EC4M 7JW. A list of the LLP's members is available at the registered office. Crowe U.K. LLP is registered to carry on audit work in the UK by the Institute of Chartered Accountants in England and Wales. All insolvency practitioners in the firm are licensed in the UK by the Insolvency Practitioners Association. 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.

This material is for informational purposes only and should not be construed as financial or legal advice. Please seek guidance specific to your organisation from qualified advisors in your jurisdiction.