Month 9

You've Looked at Your Internal Controls – how do They Stand up to Fraud?

SUDHIR SINGH
—
MHA MacIntyre Hudson

The Charity Commission has recently highlighted its concerns over the level of fraud and mis-management in the charity sector.

This article identifies other actions you can do to mitigate fraud risks.

Establishing a robust anti-fraud environment

Set out below are three steps you should follow:

1. Ensure your anti-fraud policies are reviewed regularly and are easily accessed by everyone in the organisation. This particularly applies to whistle-blowing policies which are still one of the most effective ways of fraud being identified.
2. Establish good systems and controls, document them in a formal manner such as through a financial procedures manual, and review them regularly. For example, through an annual review by your finance or audit committee.
3. Review the adequacy of key systems and controls in a structured way. For example, through examination by internal auditors or by asking external auditors to undertake some extended systems testing. Internal reviews are also effective, and using the Charity Commission's publication, CC8, as a checklist can be helpful, particularly for smaller charities.

Review the adequacy of key systems and controls in a structured way.

However, at times these approaches are not effective at identifying where the charity may be vulnerable to fraud. The problem often is that you find what you are looking for, which is a trait that fraudsters can exploit.

So I would recommend that you periodically seek to challenge the received wisdom, and ask yourselves, and others in your charity, some simple questions about the way things are done This will involve spending time considering the "what if" scenarios that could affect your organisation.

It is difficult to think "outside the box', so set out below are some real-life examples of frauds I have come across in the charity sector. The losses made by the charities concerned ranged between £10k and £3m, and the facts have been changed to protect the innocent, and not so innocent!

Some real-life examples of frauds in charities

Not taking notice of your auditor

Recommendations were made in an audit management letter to this charity concerning two areas – maintenance of their fixed asset register (to keep the FAR up to date and undertaking regular physical checks of the existence of assets) and procedures regarding dealing with conflicts of interest (to ensure that interests of both trustees and senior staff were identified formally and regularly).

The charity, however, failed to act on these recommendations as they were deemed to be low priorities.

The fraud was discovered by the finance team, and related to IT procurement, whereby assets purchased were not in fact received by the charity, and had been misappropriated by the Head of IT. The purchases had been made from a supplier that was his brother in law.

Risks of electronic banking

This charity had a strong procurement system, with every purchase invoice being approved by the Finance Director. However, the electronic banking system only required one individual to both initiate and authorize payments. The Head of Finance led the Finance Director astray by indicating erroneously that dual authorization was not possible, and perpetuated a fraud by making payments to himself, coding the costs to a variety of expense codes.

Not seeing the wood for the trees

This charity had a poor finance function – there was a high turnover of staff, information was always provided late, and management accounting was weak. But the trustees felt reassured that key controls were in place for purchasing and payroll. The difficulties were considered to be temporary and were attributed to just poor "housekeeping". This situation was exploited by a member of staff who made fraudulent expenses claims. Whilst this was one of the smallest losses in this set of examples, amounting to less than £10,000, there was a large amount of trustee and management time spent on investigations and disciplinary actions. And the charity was badly affected for several years due to the resultant culture of mis-trust that ensued.

Covering up the tracks

This is not one example, but several. All involve individuals having inappropriate access to accounting systems, particularly standing data. This included the ability to change bank account details of suppliers in the accounting system; setting up new suppliers, including with connected persons with insufficient approval; falsifying invoices, particularly changing bank details for otherwise valid payments; and creating ghost employees on the payroll. The common factor was the ability of the perpetrator to make subsequent amendments and changes to prevent detection of their actions.

Cash, cash, cash

This visitor attraction charity had three cash frauds in a single year. Entry fees were stolen at the gate, fraud took place at the tills of its catering outlet, and cash was stolen on transit to its shop. As we all know, the handling of cash always brings with it a greater risk, so particular care is always needed.

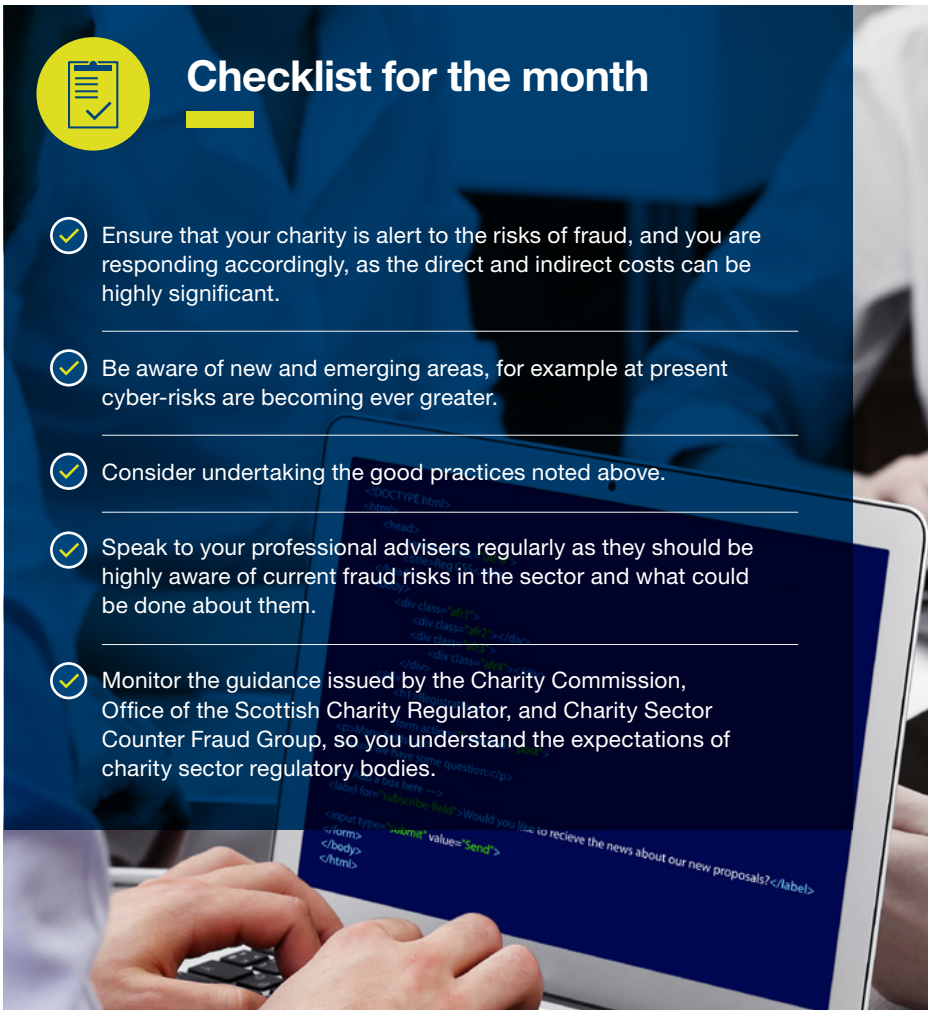
The trusted employee

The long-serving Head of Finance of this charity was very loyal and hard-working, and held an important position in their own church. However, she was always rather grumpy with both internal and external auditors, and when information was requested during audits it never appeared to be her priority. She stated that audits were a distraction from her job. It transpired that this lady had for many years been creating false invoices, and the lack of segregation of duties for all areas of purchase authorisation, meant the fraud was not identified for several years.

Fraudsters that don't benefit from their frauds

It is important to realize that not all frauds involve financial losses. In this charity the CEO had initiated a new fundraising initiative. After it had operated for a year, the results were good and the trustees were happy. The reality was the fundraising was a flop, and to cover up his tracks the CEO had been making disguised anonymous personal donations to the charity to avoid his embarrassment. The hidden identity of donors created this veneer of success.

Checklist for the month



- Ensure that your charity is alert to the risks of fraud, and you are responding accordingly, as the direct and indirect costs can be highly significant.
- Be aware of new and emerging areas, for example at present cyber-risks are becoming ever greater.
- Consider undertaking the good practices noted above.
- Speak to your professional advisers regularly as they should be highly aware of current fraud risks in the sector and what could be done about them.
- Monitor the guidance issued by the Charity Commission, Office of the Scottish Charity Regulator, and Charity Sector Counter Fraud Group, so you understand the expectations of charity sector regulatory bodies.

Where can I get more information?

The Charity Commission has supported the development of the Charities Sector Counter Fraud Group and created an online resource at

charitiesagainstfraud.org.uk/

This is an excellent portal for further information and guidance which also highlights the increasingly important work of the Cyber Fraud Resilience Group.

If you have any questions arising from this article or would like to speak to a member of our team about how we can help. Please get in touch with your local MHA member firm.