Avoiding the risks of financial crime
Charities need to have robust risk management procedures in place to ensure they avoid involvement in financial crime.
Barclays Charities Risk Governance webinar explored some of the key issues that charities need to consider to manage financial crime risk which are summarised in this article.

Regardless of a charity’s best intentions, even inadvertent involvement in financial crime can result in severe legal repercussions, irreparable reputational damage, regulatory fines and disruption to the charity’s financial services. All of this will impact on a charity’s ability to fulfill its mission.

Financial crime includes a number of different risks, namely bribery and corruption, terrorist financing, money laundering, and sanctions/export controls. All charities should be alert to laws applicable to them and to regulated financial institutions such as banks designed to prevent financial crime, particularly if they work in sanctioned or otherwise high risk countries.

A recent report from Reuters revealed that 300 UK charities have been affected by a global crackdown on illegal funds in the past two years.

Charities need to be alert to these financial crime risks and put appropriate procedures in place to identify and mitigate potential 'red flags'.

Banks’ obligations

Charities need to be aware of the anti-money laundering (AML) laws and know your customer (KYC) requirements, with which banks in the UK must comply to prevent criminals and terrorists accessing financial services and to prevent breaches of sanctions and export control laws.

Banks are obliged to carry out customer due diligence measures to gather information about their customers, including their charity customers, where the charity operates, and who the charity deals with. Banks will expect their customers, including charities, to have due diligence processes to ensure both the bank and customer meet their regulatory obligations and to prevent financial crime.

1 http://uk.reuters.com/article/uk-banks-charities/three-hundred-uk-charities-hit-by-global-crackdown-on-illegal-funds-idUKKB1N1A0F3
Due diligence is the key

Just as a bank must perform due diligence on the people and businesses it comes into contact with, so should a charity. Due diligence is the key to mitigating financial crime, and a bank will expect a charity to have diligence procedures in place. Charities therefore need to have risk-based processes in place to ensure they know enough about donors, beneficiaries and partners. A risk-based approach means: the greater the risks, the more due diligence required.

For example, charities should know where donations come from and the reasons for any conditions attached. Charities should know the people and organisations they work with, and look out for unusual circumstances. Charities have been misused in the past by terrorists and other criminals to move money to associated groups. Charities operating in sanctioned or otherwise high-risk countries must ensure they comply with applicable sanctions and export control laws. If the charity is dealing with a "politically exposed person", there may be additional financial crime risks, particularly corruption.

Due diligence measures should be a part of the financial crime policy agreed by a charity’s Trustees. Senior management must understand the requirements of the policy and ensure that staff are adequately trained to implement it. All due diligence procedures and reasons for decisions should be recorded. The Charity Commission provides a useful compliance toolkit for monitoring and verifying the end use of charitable funds (see link in the useful information section at the end of this report).

Bribery and corruption

In most countries, it is a criminal offence to offer, promise, give, request, accept or agree to receive a bribe of any kind, in any form, either directly or indirectly. This usually applies to public officials and those working in the private sector.

Public officials include employees of state-owned and controlled entities, even when they operate in a commercial capacity – for example, sovereign wealth funds and state-owned hospitals.

In the UK, the key legislation is the Bribery Act 2010. In the US, the relevant law is the Foreign Corrupt Practices Act 1977. There may also be additional local laws depending on the jurisdiction in which a charity operates.
Bribery and corruption rules are not just aimed at cash payments, but cover things like gifts, travel, entertainment, training programmes, work experience, charitable contributions and sponsorships. Charities need to ensure they have procedures in place to prevent bribery and corruption when dealing with third parties that provide services on their behalf.

The UK Financial Conduct Authority (FCA) can impose heavy fines on an organisation for lack of sufficient anti-bribery and corruption controls. The FCA may take action for insufficient controls regardless of whether any bribery or corruption has actually taken place.

**Sanctions and Export Controls**

Economic sanctions restrict dealings with certain individuals or entities, apply restrictive measures against a whole country, and control exports of particular products. Sanctions are primarily introduced by the UK, EU, US or the United Nations Security Council, but can be introduced by any country, so international charities should be aware they may be subject to more than one set of rules. Banks with global operations are often subject to multiple jurisdictions’ sanctions laws and a charity should be aware of the information a bank might need to ensure sanctions compliance.

Organisations registered in an EU member state and their EU and non-EU branches must comply with EU sanctions. Those registered outside of the EU must comply with EU Sanctions in respect of any business conducted in the EU. EU Nationals, even if located outside of the EU, and individuals located in the EU (irrespective of that individual’s nationality) must also comply with EU Sanctions.

US companies and their non-US branches, US citizens and permanent residents ('green card' holders) wherever they are located, any person on US soil and non-US entities owned or controlled by US persons must comply with US Sanctions. In some cases, non-US persons can violate US Sanctions if they cause a US person to breach sanctions. Goods, software or technology that are of US origin or contain a certain degree of ‘controlled’ US content can also be restricted by US sanctions and export control laws.

One of the largest sanctions risks for Charities is inadvertently dealing directly or indirectly with a restricted person or entity. Indirect dealing includes when a third party is acting on behalf of the restricted person.

---

2 Export control laws also exist separate from sanctions regimes, for example to control export of military or "dual use" goods.
Restricted persons (also known in the EU as designated persons and in the US as specially designated nationals) include identified terrorists and criminals, so it is crucial to check names of donors, beneficiaries and partners against restricted persons lists maintained by the relevant government authority (see links at the end). Charities should not provide or make available services, funds or benefits to these restricted individuals and entities.

Certain countries are subject to broad sanctions on conducting activity in those countries, for example, Syria. Charities should understand what activity is prohibited and be cautious that neighboring countries could be used as a conduit to evade sanctions. Goods and other items, particularly technology, might be controlled products under sanctions and export control laws when sent to a particular country – even when just one component of a product is controlled.

Banks will also be concerned about “facilitation risk”, which would be a breach of sanctions law if the bank processes a payment on behalf of a charity that facilitates prohibited activity or benefits restricted persons.

Forewarned is forearmed

Due diligence should be top of a charity’s action list to help identify potential financial crime risks and avoid facilitating criminal or terrorist activity.

If you are in any doubt about a project involving a potentially risky area, get in contact with us first.
Case study: Relief Against Poverty

To illustrate the risks of financial crime, Barclays’ Charities Risk Governance webinar used the example of a fictitious charity called Relief Against Poverty (RAP) working in Afghanistan, Bangladesh, India, Pakistan and Syria. The charity was said to receive grant funding from numerous development agencies, private foundations and corporations, as well as individuals.

The following mock scenarios involving RAP highlight a number of potential financial crime risks, or “red flags”, and the actions that the charity would need to take to manage those risks.

Scenario 1: Working with local partners in Syria

In this scenario, RAP wants to open a health and educational centre in Aleppo, Syria, working with a local hospital and another local health-related charity as partners.

The local health-related charity has specifically requested funding in US dollars. In addition, the head of the local hospital is a director of a government health agency and, in exchange for hosting RAP’s project, requests that RAP donates 12 laptop computers to the hospital.

Funding for the project will be coming from a private donor foundation in the UK that RAP has not worked with before, while one of the foundation’s trustees, His Highness Prince Omar Abadi of the Emirati Al-Qasimi royal family, suggested the donor to RAP.

Red flags and actions required

A potential risk in this scenario is that the donor is connected to a politically exposed person, commonly referred to as a PEP. As part of the due diligence checks undertaken by the Charity, the donor’s PEP status should be identified. Although the involvement of a PEP does not prohibit a donation, the Charity should be aware there may be additional bribery, corruption and money laundering risks because the PEP is in a position of political influence. The Charity should undertake Due diligence to ensure that the PEP is not suspected of involvement with corruption.

A further red flag is that the head of the local hospital is a director of a government agency within Syria. There are a number of designated persons in the Government of Syria, and the Syrian Government itself is designated. Charities should ensure that the director is not designated and is not acting on behalf of the Government of Syria.

In relation to the suggested laptop donation the charity should have effective internal controls to approve and monitor donations, understand the position around the use of the laptops, and confirm the project complies with US and EU sanctions law. Questions to ask include:

- Are there any export control issues because of the laptop technology? This should be considered from a UK as well as US perspective
- What will the laptops be used for? If laptops are supplied and misused in Syria then the charity may face regulatory censure
- Is the activity dependent on the donation of the laptops? The charity should ensure that the donation does not amount to a bribe. The director is considered a PEP, so this is a particular red flag to focus on.

Sending funds in USD is most likely subject to US sanctions, even if the funds are sent from the UK, as most major banks will route USD through a US branch or correspondent bank. As such, the charity needs to understand its sanctions compliance, gain appropriate approvals from sanctions authorities (if required), and liaise with the charity’s bank for approval to send the funds.
**Scenario 2: Third-party suppliers and sub-contractors**

Before opening the health and educational centre, RAP needs to export solar panels to Syria in order to provide power to the centre. RAP has identified a company in the United Arab Emirates to supply the panels and this company suggests that RAP also employs a particular sub-contractor to ship the panels from the UAE to Syria.

RAP UK intends to send payment to the UAE company for the panels in UK pounds sterling. The UAE company will then export the panels, which are potentially restricted under export control regulations, to Syria.

**Red flags and actions required**

In this instance, the charity should confirm there has been no breach of export controls and whether a licence is necessary to go ahead with the transaction. This will mean finding out if the product in question is dual-use, if there is a certificate for the exact end use of the goods, the panels’ country of origin (or components within) and if they fall under any export control classification. The Export Control Organisation can provide assistance in relation to UK export controls.

There are further red flags raised by the involvement of the UAE company as a sub-contractor. Questions to ask include:

- Who are they sourcing the panels from? Does the charity have oversight of this to ensure that there are no designated persons involved?
- Why have they suggested a particular sub-contractor to ship the panels? Although this doesn’t mean the transaction is necessarily prohibited, the charity should undertake due diligence to ensure that the sub-contractor is not a designated person and that there is no adverse information against them. The charity should also consider if there is any evidence to suggest that there are bribes being paid to/from the sub-contractor in exchange for business.
- Does the charity know the shipping route? If the goods are transshipped via Iran, i.e. the goods will pass through Iran before being delivered to Syria, then the charity should alert their bank and consider sanctions compliance issues.

**Scenario 3: Private donation via money service bureau**

RAP now requires additional funds to complete the project and a private foundation in the US has offered to make a donation. RAP has not worked before with this foundation, which intends to donate to RAP in the UK in US dollars.

The charity will use a UK USD account to send the funds to Turkey, where it will use a money service bureau (MSB) to send the funds on to Aleppo. The MSB advises RAP that a generic reference should be included within the payment, with no mention of Syria or Aleppo.

Before RAP is able to open the health and educational centre, their local charity partner informs them that they are required under local law to apply for a government licence. The local charity says it knows a government official who will facilitate the application for a small fee.

**Red flags and actions required**

Here, although using an MSB is not prohibited, the charity should be cautious about the potential money laundering risks of using an MSB. It should confirm why it must use an MSB, whether the MSB is regulated, whether it is acting as a principal or an agent, and whether it carries out audits of its anti-money laundering (AML) and counter-terrorist financing (CTF) controls. Due diligence should be undertaken on the MSB, its owners and directors.

The charity is required to detail the purpose of the payment, which should reference Syria as the ultimate destination in the payment instructions. Excluding such information could be seen as an attempt to circumvent banks’ sanctions screening and therefore, a crime.
The charity should confirm the transaction complies with US and EU sanctions law and that due diligence checks have been made on the private foundation.

There is also a bribery and corruption risk relating to the fee payable to the government official. The charity should confirm this is legally permissible, check the local law and ensure any payment complies with routine action required to obtain licenses.

**Scenario 4: Anonymous donor with conditions attached**

RAP decides to set up another health and educational centre in an ISIL-controlled region in Syria. The charity is anonymously contacted by a potential UK donor, who wishes to donate £1 million to the centre – but only if RAP partners with a particular local charity.

**Red flags and actions required**

The charity should only accept the donation if it knows the source of funds and can verify the donor. The charity should demonstrate to its bank the reasons the donor would like to send the funds and the reasons for the donor’s anonymity because these are indicators of potential money laundering and terrorist financing.

The charity should also conduct due diligence on the proposed local charity and should not send any funds until the review has been completed.

The charity should confirm the transaction complies with US and EU sanctions law, that there has been adequate screening of parties involved and that there is no restricted person involved or risk of diversion to sanctioned groups.

In practice, ISIL is known to illicit heavy ‘taxes’ on entities and individuals within its controlled areas and therefore the Charity should be mindful of the very high risk of funds being diverted to a known and sanctioned terrorist groups. It would be challenging to realistically mitigate the risk of diversion in such an area.
Useful information

Financial crime
Charities Commission compliance toolkit

European Sanctions blog
https://europeansanctions.com/

OFSI
https://www.gov.uk/government/organisations/export-control-organisation

FCPA blog
http://www.fcpablog.com/

FATF Guidance
http://www.fatf-gafi.org/documents/guidance/?hf=10&b=0&s=desc(fatf_releasedate)

UK Gov AML guidance

OFAC FAQs
https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/ques_index.aspx

Export controls
UK
Export control organisation
https://www.gov.uk/government/organisations/export-control-organisation

Office of Financial Sanctions Implementation (OFSI) licences
https://www.gov.uk/guidance/licences-that-allow-activity-prohibited-by-financial-sanctions

US
Dept of State – export controls
https://www.state.gov/strategictrade/resources/c43182.htm

Dept of Commerce – Bureau of Industry and Security
https://www.bis.doc.gov/index.php/about-bis/resource-links

Sanctions
UK Sanctions List
https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

US Sanctions List
https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

FAQs on restrictive measures in Syria