Avoiding the risks of financial crime in the charity sector

BARCLAYS

Avoiding the risks of financial crime – 2019 Update

Welcome to our revised guide intended to provide some assistance to international charities on how to manage their financial crime risk. This document is a revision to that launched in 2017, following 2 years of learning from supporting our valued clients.

Introduction

The charity sector, including international charities, is very important to Barclays and we are proud to have retained our leading position in the Charity Financials Banking Spotlight Report 2018 for top 5,000 charities.

The banking sector still faces pressure to ensure it is not being used as a conduit of criminal proceeds and being abused to remit funds to terrorist groups, and rightly so. The sector continues to face fines; at the time of writing an international UK bank has just been fined over £100m for financial crime breaches. This motivates all banks to manage their financial crime risk.

Barclays, as ever, supports international charities who can demonstrate that they are appropriately managing their risk. In 2017 we launched our Enhanced Due Diligence process for international charities to better understand and manage our risk, and have supported a number of clients who we felt fell short of the standard achieved by their peers to improve. We continue to look to support those clients who appropriately manage their risk to make their permissible high risk payments, such as for humanitarian aid, including to sanctioned countries where payment channels permit.

The sector specialism in our charity specialist Relationship Directors improves our understanding of the sector, in the unique risks and opportunities it provides, further enabling the bank to be supportive of higher risk activity.

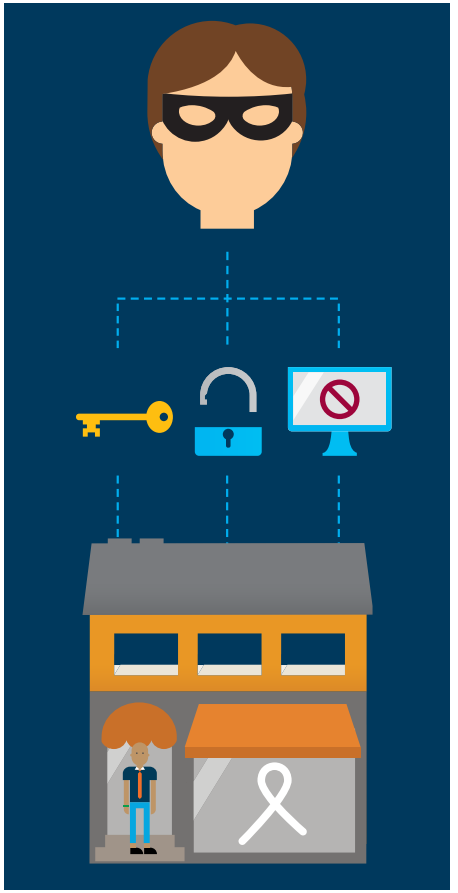
Collaboration is incredibly important to ensure better delivery of charity programming in future. As such, Barclays is an active participant in the Home Office organised "Tri-Sector Working Group", a consultation by Government involving the Charity Sector and Finance Sector to improve future legislation, guidance and support initiatives around training and best practise sharing. We also continue to support by speaking at sector conferences such as the 2019 BOND conference.

We look forward to further collaboration and learning between our clients and industry specialist in 2019 and beyond.

Roland Pearce
Relationship Director

Nazreen Visram
Head of Charities

Will Dodsworth
Group Head of Financial Crime Policy



Charities operating internationally have real financial crime and reputational risks.

Regardless of a charity's best intentions, even inadvertent involvement in financial crime can result in severe legal repercussions, irreparable reputational damage, regulatory fines, loss of donor funding and disruption to the charity's financial services. All of this will impact a charity's ability to fulfil 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 high-risk countries.

The 2018 safeguarding scandal caused significant reputational damage to the charity sector. The damage from funding terrorism for example, could be just as great, if not greater. Failure to protect the charity from the risk of financial crime could result in potential criminal prosecution and civil penalties including fines and imprisonment for the charity and individuals involved.

Charities need to be alert to these financial crime risks and put appropriate governance policies, procedures and staff training in place to identify and mitigate potential risk.

We have detailed some of the key issues a charity needs to consider in the following pages.

Banks' obligations

There is an increasing trend towards public/private partnerships in the fight against financial crime and the detrimental effect it has on the international community. The finance industry, charities, governments and regulators are working together to prevent the banking system from being used for financial crime.

Banks are subject to enhanced regulatory obligations due to the potential for abuse of financial institutions by criminals, such as to launder and move proceeds of crime, and fund terrorism.

Banks are obliged to carry out due diligence measures to gather information about their clients, including charities, such as;

- Where they operate
- Who they deal with
- Who controls them
- Their source of funds

Charities operating internationally, including in high risk or sanctioned countries, may also be asked to undertake enhanced due diligence. This may include requests to review governance policies, procedures and training materials used to manage financial crime risks.

Charities should be aware of the regulatory framework and international guidance covering anti-money laundering (AML), anti-bribery and corruption (ABC), counter-terrorist financing (CTF), sanctions and export controls. All of these result in the know your customer (KYC) requirements with which banks in the UK must comply to prevent criminals and terrorists accessing financial services.

Banks will expect their customers, including charities, to have due diligence processes to ensure both the bank and customer meet their regulatory obligations, in turn preventing financial crime.

Charity obligations – setting the right policy and tools

Charities have obligations as a result of their registration with the charity commission, and legal requirements as companies such as under the Companies Act 2006 and various financial crime acts and legislation. The financial crime legislation includes but is not limited to

- Bribery and corruption (Bribery Act 2010)
- Money laundering (Charities Act 2011 and charities should be aware of the obligations of their banks under the Money Laundering Regulations 2017)
- Terrorism (Terrorism Act 2000 and Proceeds of Crime Act 2002), and
- Sanctions (various including UK, EU, UN, USA sanctions regulations).

Charities therefore need to have a comprehensive financial crime policy or suite of policies to cover the legislation applicable to them and the operating risks that they face.

The role of a policy is to set an organisation-wide, pre-determined course of action and risk limits. It is a guide to the accepted organisational strategies, objectives and operating standards.

The policy should be a meaningful document which is central to the way a charity operates; it should fundamentally guide the operations of the organisation. This link is

through procedure (or operating frameworks) which provide the organisation with clear and easily understood plans of action to implement the policy. Procedure allocates responsibility and provides clear decision making processes and courses of action. Procedure operationally reflects the policy.

While the policy reflects a charity's risk appetite, objectives and operating standards, and procedures guide how a policy is implemented and allocates responsibility, employees need to be trained to ensure they fully understand what they need to do in order to be compliant.

A risk-based approach can be used in setting the detail of the policy, detail of the procedure and who undertakes what training. For example, charity staff who operate on the ground in sanctioned countries and conflict zones should be significantly more aware of the terrorist financing risk than perhaps domestic UK staff, with enhanced training provided to mitigate the risk and keep these staff safe.

Policies should be owned by trustees. They remain responsible due to their role as the company directors, even if they delegate the operational duties of keeping them up to date to members of the senior management team. The policies need to be reviewed periodically to ensure they reflect legislation and the operating environment at the time. A feedback mechanism is also necessary, whereby breaches of policy / procedures or "near misses" are reviewed and considered, determining updates to the policy or procedures as appropriate.

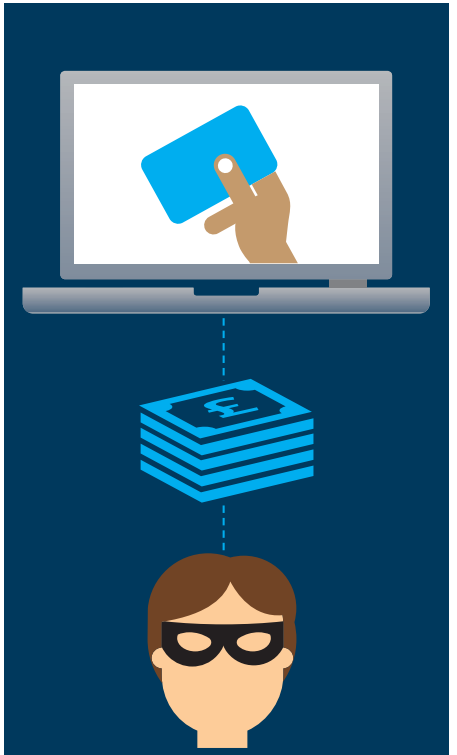
The risks of operating in sanctioned countries, conflict zones and high-risk countries are very real. Near misses and breaches, whilst undesirable, should be reported so that they can be understood and managed. It is therefore important to foster a transparent and open culture where staff feel that all matters can be reported.

Due diligence is 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 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, employees, volunteers, affiliated organisations / member organisations, partners and suppliers. 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. Charities also need to be comfortable that their partners operating with their funds, on their behalf, even if they are members of the same family or federation, are doing so to the charity's standards and in compliance with their regulatory obligations.

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.



Charities should know the people and organisations they work with and look out for unusual circumstances.

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).

Money laundering

It is important to be aware of your money laundering risks when conducting charitable activities. Charities should conduct a risk assessment to identify where they operate in high-risk areas and focus their risk mitigation processes on those jurisdictions. Due diligence also needs to be conducted on partners and employees on the ground in jurisdictions in which they operate in order to prevent funds from being diverted for terrorist or other criminal purposes. This should be done on a risk-based approach which might mean that the amount of due diligence applied varies depending on several factors such as type or nature of activity, third party partners involved, and the jurisdiction in which you operate.

Receiving large donations from anonymous donors is a red flag, and you should have processes in place to mitigate this risk. Be sure to find out and document how the funds were raised, and why the donation is to be made anonymously. Consider the level and type of due diligence required on different private donation amounts, and where the funds originated. Conditions attached to these donations may also be a red flag - is the donor asking you to spend the money in a particular area? You should understand why the donor made the request, and consider whether additional processes need to be put in place to prevent potential money laundering.

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.

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, suppliers 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 and North Korea. Charities should understand what activity is prohibited and be cautious that neighbouring 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 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.

To illustrate the importance of ensuring your charity's financial crime controls are effective, in April 2018, Norwegian People's Aid (NPA) were fined $2.025 million by the Department of Justice (DOJ) of the USA after programmes they provided, funded by USAid, breached US sanctions laws. NPA were found to have:

- Provided an educational training programme aimed at encouraging effective youth participation in the political process, which senior officials of designated terrorist organisations attended
- Funded training for mine clearance operations in Iran which materially benefitted the oil development in Iran

The DOJ determined that NPA's internal policies were insufficient to identify these financial crime concerns, and did not provide effective oversight and management of the programmes. NPA were further required to undertake a review of their financial crime policy, and are required to be audited by external auditors annually.

Terrorist financing

Charities need to have controls in place to ensure that they are not being used to launder money for terrorist purposes, or being used to fund terrorism. For example, where a charity uses a third party in a high-risk jurisdiction to build infrastructure such as a school, the third party may embezzle money to fund a terrorist group, and

In April 2018 the Norwegian Peoples Aid (NPA) were fined $2.025m by the USA Department of Justice for Sanctions Breaches.

attempt to conceal this from the charity. Controls such as due diligence processes, audit trails for money paid and audits for building works are needed to ensure the funds are used for their intended purpose. Charities are prohibited from facilitating any activity for UK Home Office Proscribed Terror Groups, which are banned by UK law. Charities have a duty to disclose any known or suspected terrorist activity to the National Crime Agency (NCA). Under the Terrorism Act 2000 failure to disclose a known or suspected offence is a criminal offence.

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 your bank and advisors first.

Work in partnership with your bank

Both the charity and its financial partners are subject to financial crime legislation but the banking sector has been increasingly in the spotlight as governments attempt to fight financial crime and its funding of global terrorism.

With banks facing numerous fines for breaches or insufficient financial crime controls reaching billions, banks have been increasing their due diligence requirements on their customers or "de-risking" by reducing their appetite to support activity perceived to be high-risk.

For charities operating in high-risk and/or sanctioned countries, we recommend that you are fully transparent and communicate early with your bank:

- Keep your bank up to date on how you are managing and mitigating risk, such as updates to your financial crime policies, improvements to procedures such as your due diligence processes or staff training
- Involve your bank early in any new plans to operate in a high risk or sanctioned country. Let your bank know where you are considering operating, what you are considering doing and how you will manage the risk
- Large charities may benefit from having a Manager at their bank who is a specialist in the charity sector. This will depend on the bank but is nearly always the case at Barclays for large charities. A sector specialist Manager helps provide a greater level of understanding of some of the unique exemptions from some sanctions for "humanitarian aid" activity, and therefore have greater willingness to support. Smaller charities should work closely with their manager and help them understand how risk is being appropriately managed and therefore should be acceptable to the bank.
- If you have a breach, notify your bank as soon as possible.

Case study: Relief Against Poverty

To illustrate the risks of financial crime, Barclays' has developed an 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, a prince of the 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 under UK/EU/USA sanctions legislation 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 and anti-bribery and corruption 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 to Syria is currently 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 (both in the UK and USA), gain appropriate approvals from sanctions authorities (if required and available), 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 intends to send payment to the UAE company for the panels in UK Pounds Sterling. The UAE company will then export the panels.

Red flags and actions required

In this instance, the charity should confirm there has been no breach of UAE and UK 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 trans-shipped 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 for Iran

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 to ensure there are no designated individuals under sanctions legislation or linkages with other financial crime.

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 and likely risk of funds being diverted to known and sanctioned terrorist groups. It would be challenging to realistically mitigate the risk of diversion in such an area.

Questions to consider in evaluating your Financial Crime risk

1. Do you have a financial crime policy and is it robust enough? Do you consider all of the following in addition to fraud risk:
   - AML
   - Terrorist financing
   - Economic Sanctions
   - Anti-bribery and Corruption
   - Export Controls
2. What training and guidance do you provide your staff / volunteers / partners to ensure they understand your policy to ensure compliance, with particular focus on those based in high risk jurisdictions?
3. How do you consider the varying risk of the different countries / jurisdictions in which you operate?
4. How do you look to understand the financial crime risk associated with your activity?
5. If you operate through partners, what due diligence do you undertake on them to ensure they are operating to your standards? What on-going monitoring do you have in place?
6. What are your funding sources and what due diligence do you undertake on those sources of funds? Does your due diligence consider:
   - Country of Origination and associated risk
   - Government funding
   - Anonymous donations – how do you get comfortable with the source of funds?
   - The reason and risk associated with conditions attached to funding?
7. What day-to-day monitoring / oversight / controls do you have in place over your activity?

Useful information

ABC – Anti-bribery and Corruption

UK.Gov - Anti-bribery policy
https://www.gov.uk/anti-bribery-policy

Bribery Act 2010 guidance (UK Legislation)
https://www.gov.uk/government/publications /bribery-act-2010-guidance

UK anti-corruption strategy 2017 to 2022
https://www.gov.uk/government/publications /uk-anti-corruption-strategy-2017-to-2022

Foreign Corrupt Practices Act - (US Department of Justice)
https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act

AML – Anti money laundering

Charities Commission compliance toolkit
https://www.gov.uk/government/collections/protecting-charities-from-harm-compliance-toolkit

The Crown Prosecution Service Proceeds Of Crime Act 2002 Part 7 - Money Laundering Offences
https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences

Charities Commission

Charities Commission compliance toolkit
https://www.gov.uk/government/collections/protecting-charities-from-harm-compliance-toolkit

Export Controls

Department for International Trade
https://www.gov.uk/government/organisatio ns/department-for-international-trade

Export Control Joint Unit
https://www.gov.uk/government/organisatio ns/export-control-organisation

Overview of U.S. Export Control System
https://www.state.gov/strategictrade/overview/

Sanctions

European Sanctions blog
https://europeansanctions.com/

European Sanctions Map and Guidance
https://www.sanctionsmap.eu/#/main

Sanctions, embargoes and restrictions
https://www.gov.uk/guidance/sanctions-embargoes-and-restrictions

Office of Financial Sanctions Implementation (OFSI) HM Treasury
https://www.gov.uk/government/organisatio ns/office-of-financial-sanctions-implementation

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

Terrorist Financing

Charities Commission compliance toolkit
https://www.gov.uk/government/collections/protecting-charities-from-harm-compliance-toolkit

The Crown Prosecution Service Terrorism
https://www.cps.gov.uk/terrorism

Terrorism Act 2000
http://www.legislation.gov.uk/ukpga/2000/11

Terrorism Act 2000 Part III Terrorist Property
https://www.legislation.gov.uk/ukpga/2000/11/part/III

Current list of designated persons, terrorism and terrorist financing
https://www.gov.uk/government/publications /current-list-of-designated-persons-terrorism-and-terrorist-financing

U.S Department of the Treasury
https://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/default.aspx

Financial Action Task Force (FATF) Terrorist Financing PDF
http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf

barclayscorporate.com

@BarclaysCorp

Barclays Corporate Banking