Policy & Resources Committee

Committee *for* Home Affairs

GUIDANCE ON COMBATTING PROLIFERATION AND PROLIFERATION FINANCING

DECEMBER 2022

TABLE OF CONTENTS

INTRODUCTION

The Bailiwick of Guernsey ("the Bailiwick") has a longstanding legal framework in place to address proliferation of weapons of mass destruction and financing of the proliferation of weapons of mass destruction[1]. "Proliferation" in this context refers to the proliferation of nuclear, chemical and biological weapons, also known as weapons of mass destruction or WMD.[2] As a result, businesses in the Bailiwick have been required for many years to take all necessary steps to ensure that they comply with measures to combat proliferation and proliferation financing.[3]

The international community, through the issue by the UN of sanctions (and periodic and routine assessment of compliance by jurisdictions with aspects of those sanctions by the FATF and other bodies), has expressed particular concern about the WMD programmes of Iran and the Democratic People's Republic of Korea (commonly referred to as the DPRK, or North Korea) and the financing of those programmes.

This is the main context for the issue of this guidance paper, which is issued by the Policy & Resources Committee and the Committee *for* Home Affairs of the States of Guernsey. It has been prepared with input from the Bailiwick of Guernsey Sanctions Committee.[4]

This guidance paper builds on previous guidance and outreach, and aims to:

- raise awareness of proliferation and proliferation financing;
- outline the legal obligations in the Bailiwick concerning proliferation and proliferation financing; and
- provide practical guidance on good practices to identify, assess, manage and reduce the risks of proliferation and proliferation financing, and to emphasise that such practices involve more than screening databases against lists of individuals and entities subject to international sanctions.

This guidance paper takes the form of frequently asked questions (FAQs). It is divided into two sections:

[1]The Bailiwick has had measures in place to implement all UN sanctions regimes dealing with proliferation and proliferation financing (and other issues) since their inception. As a result of Brexit, with effect from the end of 2020 the Bailiwick implements UN regimes by giving domestic effect to UK regulations that implement the UN regimes. This replaced the previous practice of implementing UN regimes by giving domestic effect to EU regulations that implemented the relevant UN regimes.

[2] Section 1 and the Glossary contain a more detailed definition of proliferation.

[3] They have been assisted in this by targeted outreach from the authorities, including presentations by Dr Jonathan Brewer in December 2016 and December 2018. Details of these presentations and other information on proliferation and proliferation financing are available on the States of Guernsey website.

[4] The Bailiwick of Guernsey Sanctions Committee is a multi-agency (non-political) committee that is responsible for coordinating sanction activities within the Bailiwick, ensuring that information on sanctions is distributed publicly and providing advice on matters relating to sanctions.

- Section 1: Understanding proliferation and proliferation financing. This section provides an overview of proliferation and proliferation financing, explains the risks of these activities, and identifies the legal obligations in force in the Bailiwick. The legal obligations are summarised in more detail in Annex B to this guidance paper.

- Section 2: Guidance on good practices to identify, assess, manage and reduce the risks of proliferation and proliferation financing.

It contains three Annexes:

- Annex A: Possible indicators of proliferation and proliferation financing. This annex includes a table of possible indicators that may help businesses in identifying, assessing and managing risks relating to proliferation and proliferation financing. Please note that the presence of one or more of the possible indicators set out in Annex A does not necessarily mean that proliferation or proliferation financing activities are taking place. Instead, it might imply an increased risk of such activities, which may call for further investigation and/or steps to be taken to manage or mitigate these risks.

- Annex B: A summary of the legal obligations in the Bailiwick that concern proliferation and proliferation financing.

- Annex C: Glossary. Some words used in this guidance paper have a particular meaning in the context of proliferation and proliferation financing. As a result, the Glossary provides a range of definitions.

This guidance paper does not have the force of law and should be read alongside the relevant legal provisions identified in Annex B. It does not take the form of (or replace the need for) legal advice.

Section 1: Understanding proliferation and proliferation financing

Question 1: What is proliferation?

Proliferation involves:

- the illegal manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, supply, stockpiling or use of entire manufactured systems of weapons of mass destruction; or

- the illegal manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, supply stockpiling or use of components for use in WMD; or

- the acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of means of delivery of manufactured systems of WMD; or

- the supply or sale of components for the means of delivery of weapons of mass destruction; or supply or sale of related materials/goods or services (such as technologies, software, dual-use goods or expertise) for the construction of manufactured systems of weapons of mass destruction, their components or the means of delivery of weapons.[5]

A WMD programme involves a wide range of activities within the umbrella of activities described above, including the construction and maintenance of infrastructure for the production of WMD and the procurement of goods and services, such as materials and machinery for the production and delivery of WMD. For ease of reference these activities are described in this guidance paper as proliferation activities or the procurement process. Numerous components and services can be needed as part of the procurement process.

Those involved in proliferation activities are referred to in this guidance paper as proliferators; it should be appreciated that proliferators can use agents to facilitate procurement processes. Proliferation may be undertaken by anyone, including States and non-State actors. Examples of persons that may participate in activities relating to proliferation include:

- States seeking to develop and/or enhance their own WMD capabilities;

- individuals or entities seeking to profit from the development and sale of WMD. An example of this is provided in Figure 1 below; and

- terrorist groups that may seek to develop and/or acquire WMD for use in acts of terrorism.

[5] This definition is derived from a working definition of proliferation financing developed by the FATF, which is set out in Question 2 below.

Figure 1 - Proliferation by individuals/entities: the AQ Khan Network

The activities of the AQ Khan network are a widely reported example of proliferation by non-State actors. AQ Khan, a former nuclear scientist from Pakistan, is said to have operated a clandestine network that obtained and sold sensitive nuclear goods and technologies to North Korea, Iran and Libya. He relied on a network of front companies throughout the world to complete these trades and routed financial payments through complex structures in order to conceal the parties to the transaction.

SOURCE: RUSI, COUNTERING PROLIFERATION FINANCE: AN INTRODUCTORY GUIDE FOR FINANCIAL INSTITUTIONS (2017)

Question 2: What is proliferation financing?

Proliferation does not exist in isolation. Proliferation activities and procurement processes require financing and, therefore, financial transactions. A working definition of proliferation financing, developed by the FATF, is as follows:

> *"Proliferation financing" refers to:*
>
> *the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.*

Three elements are frequently a feature of financing a WMD programme:[6]

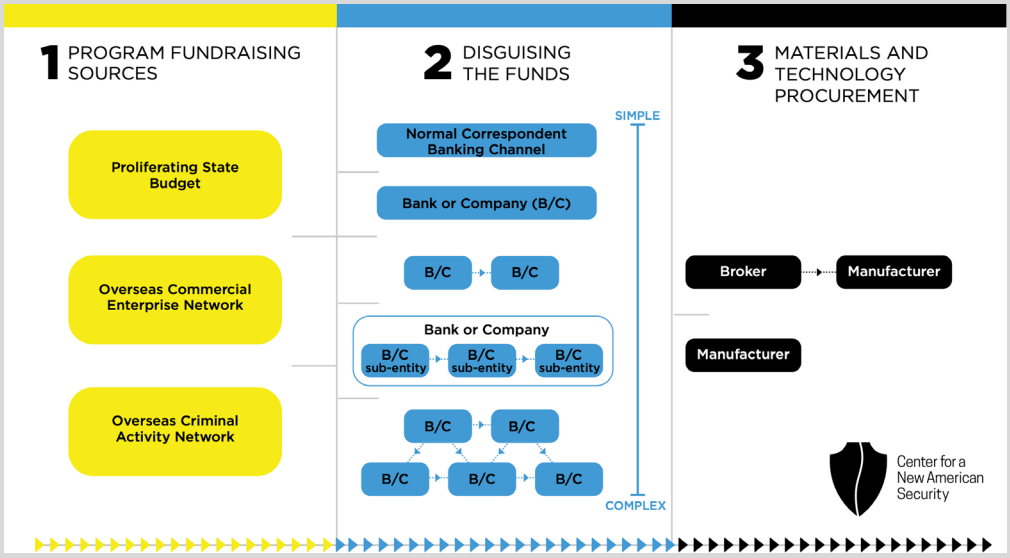
- Programme fundraising: a proliferator raises funds to finance a WMD programme.
- Disguising the funds: a proliferator transfers these funds into the international financial system for e.g. trade purposes.
- Procurement of materials and technology: a proliferator or its agents uses those funds to pay for goods and services.

[6] Dr Jonathan Brewer, *The Financing of Nuclear and Other Weapons of Mass Destruction,* available online.

Those elements are summarised in the diagram in Figure 2.

Figure 2 – Three financial elements of a WMD programme

This diagram provides an overview of three key financial elements of a WMD programme and identifies some of the people or entities that might be involved.



SOURCE: DR JONATHAN BREWER, THE FINANCING OF NUCLEAR AND OTHER WEAPONS OF MASS DESTRUCTION PROLIFERATION (CENTER FOR A NEW AMERICAN SECURITY, 2018)

Proliferation financing can involve:

- Payment for goods and services that might be used, directly or indirectly, for proliferation.
- All forms of financial services provided in support of any part of the proliferation process. By way of illustration, this might include:
  - facilitating or making payments for the provision of proliferation-sensitive goods and services by providing front companies or by acting as agents;
  - providing trade finance or insurance services or any payment for the transport of proliferation-sensitive goods and services.

Preventing proliferation financing is an important part of combatting proliferation. It is essential to disrupt the financial flows available to and used by proliferators and to obstruct the procurement of the illicit material/goods and services needed for the development of WMD and their means of delivery.

Question 3: Why is it important to be aware of the risks of proliferation and proliferation financing?

As explained in the introduction, the main context for the issue of this guidance paper is concern by the UN and others about the WMD programmes of Iran and North Korea, which has led to the enactment of international measures to address this. It is also important to be aware of the risks of proliferation and proliferation financing for the following reasons (among others):

- Policy: the proliferation of WMD and their means of delivery is a serious threat to global peace and security. If appropriate safeguards are not established, maintained and enforced for proliferation-sensitive goods and services, they may become accessible to individuals and entities seeking to profit from their acquisition and sale, and ultimately be used in WMD programmes. Proliferation-sensitive goods and services can also find their way into the hands of those willing to employ WMD in acts of terrorism.

- Legal: persons subject to Bailiwick law must comply with a number of legal obligations relating to proliferation and proliferation financing. These are summarised in response to Question 7 and explained further in Annex B to this guidance paper.

- Regulatory: where persons are subject to a regulatory regime applicable in the Bailiwick (for example, if they are involved in a "specified business" pursuant to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999) they could face regulatory investigation and penalties, including loss of their licence to operate in the Bailiwick.

- Sanctions: involvement in proliferation or proliferation financing can lead to persons or entities breaching legal provisions concerning financial sanctions and/or being included on sanctions lists drawn up by the UN, UK and others (including the EU and the USA).

- Reputation: involvement in proliferation or proliferation financing, even if inadvertent, can cause serious reputational damage. It may result in being denied access to banking or other services due to activities being perceived as high risk or illicit.

Question 4: What are the challenges in identifying activity linked to proliferation and proliferation financing?

It can be very difficult to distinguish proliferation and proliferation financing activities from ordinary trade and commerce and the financing of such trade and commerce, as those involved in proliferation and proliferation financing can go to great efforts to seek to disguise their activities. The difficulties in identifying proliferation and proliferation financing activities include the following factors.

Proliferators may purchase individual components for use in proliferation rather than fully assembled WMD systems.

It may be clear from the nature of some components that they are likely to be intended for use in WMD (e.g. highly enriched uranium or biological toxins). Other components may have legitimate uses, which makes it difficult to ascertain whether they will be used in proliferation. These are known as dual-use goods. Examples of dual-use goods include:

- chemicals such as chlorine, which is used in a range of household cleaning products and has industrial uses such as the sanitation of water. Chlorine can also be used to produce chlorine gas, which can be used in chemical weapons;

- materials such as aluminium alloys and steel, which are used in the manufacture of a range of products and can be used in the development of missiles;

- electronics such as GPS systems, gyroscopes and accelerometers, which can be used in missile systems;

- components such as valves and vacuum pumps, which have a range of potential uses, including in the oil and gas industry, but may also be used in a WMD programme.

Proliferators may seek to disguise their activities through the use of agents acting on their behalf either for ideological purposes or for profit motives, or a combination of the two, and by intermediary vehicles such as the use of front companies or other companies or other legal persons. Intermediary vehicles may be used to add complexity, opacity and/or cross-border activity to a WMD programme so as to disguise the existence of the programme and the end-use or end-user of proliferation-sensitive goods and services. Clearly, it is not in the interests of proliferators to identify the end-use or end-user(s) for such goods and services. The use of agents and/or intermediary vehicles are not in themselves an indication of proliferation or proliferation financing; businesses mostly use agents and companies for legitimate purposes.

Use of a front company is a common example of use of an intermediary vehicle in proliferation programmes. This is a company established for a seemingly legitimate purpose but which serves as a means to conduct illicit operations on behalf of another person or entity. Front companies may be shell companies/corporations with a fictitious business or may combine their illicit activities with normal commercial and industrial operations which are used as a cover or front.

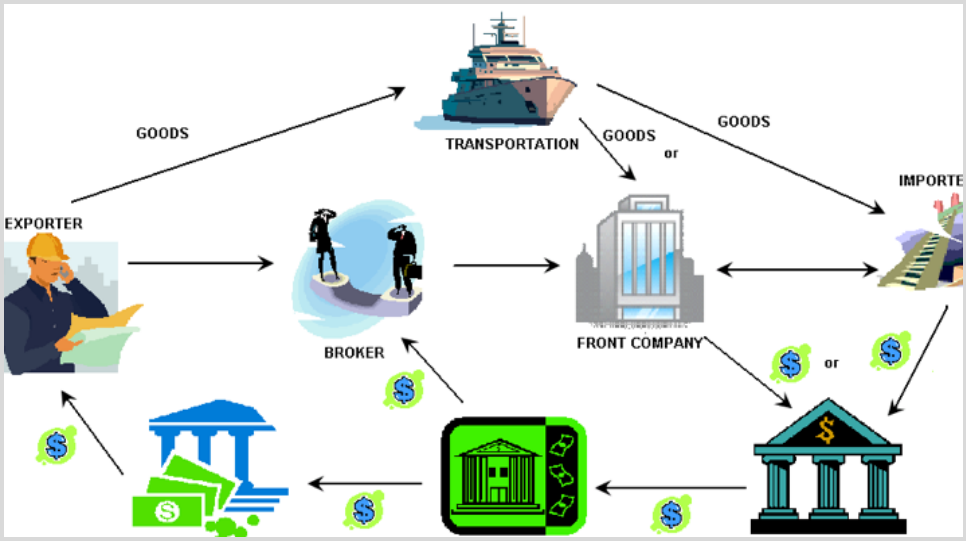
Front companies may be used to conduct a range of activities relating to proliferation, such as arranging shipping services and/or (re-)routing goods acquired by a proliferator or its agents. Front companies can also be used to conduct financial transactions in order to conceal the movement of funds related to proliferation. An example of the use of front companies in proliferation networks is contained in Figure 3.

Proliferators may seek to use the services of other businesses or professionals to assist with forming front companies (such as company formation agents, trust and company service providers ("TCSPs") or firms providing legal services) or for numerous other purposes to add complexity, opacity or cross-border activity or to provide the appearance of legitimacy and substance.

Figure 3 – Use of front companies in proliferation networks

The diagram below is an example of the use of a front company to procure goods on behalf of an importer. In this example, a front company is used to provide payment for the goods and/or receive the goods on behalf of the importer. This would conceal the importer's identity from the exporter.

The diagram also includes examples of other persons that may be involved (wittingly or unwittingly) in proliferation networks. For example, a broker could be used to act on behalf of the front company in connection with the payment of goods and/or their delivery, and financial services businesses (including those involved in operating money remittance businesses or exchange houses) may be used to transfer funds.



SOURCE: FATF, PROLIFERATION FINANCING REPORT (2008)

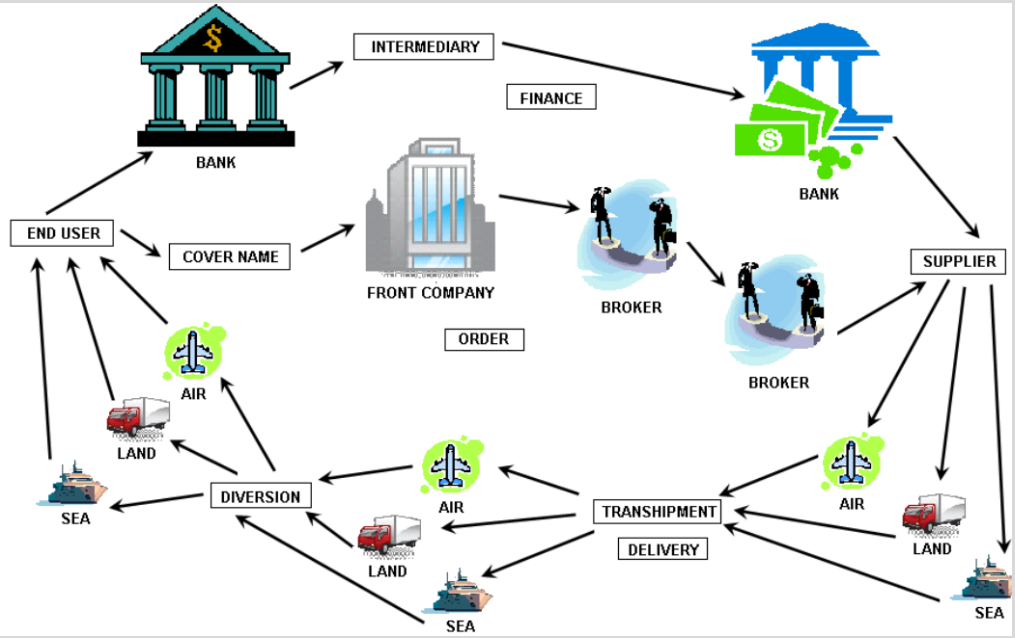
This is a basic overview of a proliferation network. The procurement of goods and services for proliferation, and the movement of funds in support of proliferation financing, often involve more complex transaction structures. This may include front companies, agents, intermediary vehicles and other parties in a number of jurisdictions to conceal the movement of the goods, including the end-user, and their financing.

Proliferators may exploit weaknesses in global trade controls: proliferators may operate in countries with weak export controls or in free trade areas, where their procurements and shipments might escape scrutiny or be subject to limited scrutiny.[7] They may seek to disguise the origin, destination and/or end-user of proliferation-sensitive goods and services by diverting them through transhipment hubs or free trade areas. Figure 4 provides an example of the use of transhipment hubs.

[7] The FATF maintains lists of "high risk" and other monitored jurisdictions, which are identified as having deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation. These lists are available on the FATF's website. The Peddling Peril Index is a biennial project that evaluates the effectiveness of national strategic trade controls in 200 countries, territories, and entities, produced by the Institute for Science and International Security.

Figure 4 – Use of transhipment hubs in proliferation networks

This diagram illustrates the use of transhipment or diversion hubs to conceal the movement of goods and services. In this example, goods are routed through two hubs (labelled "transhipment" and "diversion" in the diagram) before being delivered to the end-user. The supplier may not be aware of the intended end-user of the goods, since it may only be involved in the shipment of the goods to the transhipment point.



This example also demonstrates that a range of actors in the global supply chain may become involved in activities relating to proliferation and proliferation financing, particularly since the global network that supports the transport of goods and services relies on a range of industries.

SOURCE: FATF, PROLIFERATION FINANCING REPORT (2008)

Proliferators seek to disguise their funds using international proliferation networks. Methods used to achieve this include:

- the use of front companies or other companies or other intermediary vehicles operating in different jurisdictions. For example, a Panel of Experts established by the UN Security Council has identified that North Korea uses front companies to facilitate payments for goods and equipment (including proliferation-sensitive goods and services) procured overseas;

- the use of correspondent banking services. A Panel of Experts established by the UN Security Council has identified that some banks in North Korea use correspondent banking accounts in order to facilitate financial transactions on behalf of a DPRK counterpart and provide an access point to the wider financial system;

- keeping assets in more than one jurisdiction to conceal their ownership or jurisdictions which specialise in regional or international asset administration;

- arranging for the manufacture, supply or transport of illegitimate goods and services by blending them with legitimate goods and services (which may or may not include proliferation-sensitive goods and services) and financing of a blend of legitimate and illegitimate goods and services;

- using multiple jurisdictions in relation to purchase, transport and financing arrangements and any one financial institution, firm of advisers or other business may be used for only one part of, or in a very limited role in, a project or a wider proliferation programme. It serves the purpose of proliferators to obscure the entirety of a chain of transactions in proliferation-sensitive goods and services and their financing. This could involve relabelling of goods and changes of relevant documentation or elements of relevant documentation such as reference to the contents of a consignment or the amount or value of a consignment;

- use of agents. Agents (knowingly or unknowingly) may act on behalf of proliferators and, amongst other roles, add complexity, opacity and cross-border elements to proliferation programmes;

- use of cash to trade in proliferation-sensitive goods or services in order to avoid detection;

- use of digital assets in order to avoid detection;

- use of false end-users: it is not in the interests of proliferators to make obvious the end-user(s) of illicit materials/goods.

The activities undertaken by proliferation networks to obscure the delivery of WMD components to the real end-users can be complex and multi-jurisdictional in nature, using a variety of means to seek to escape detection, although it should not be assumed that proliferation projects within programmes or that aspects of projects will always be complex or that the examples mentioned above will be utilised or are the only examples used in proliferation programmes.

A number of financial transactions relating to proliferation, such as the payment of intermediaries or suppliers, may be undertaken using the international financial system. Use of the formal financial system is typical of proliferation programmes, together with use of companies. For example, proliferators may seek to purchase proliferation-sensitive goods and services from reputable suppliers and to pay for them using the international banking system to make these activities appear less suspicious. The international financial system can be abused by proliferators to carry out transactions and business dealings, and financial institutions, and their legal or other advisers, can unwittingly become facilitators of proliferation financing. By way of illustration, the following factors are relevant to varying degrees in Guernsey:

- trade finance might be used to fund the international transport and supply of proliferation-sensitive goods; or

- a bank account might be used to facilitate the activities of a manufacturing business relevant to dual-use goods, an import/export business, a logistics or transport business, or a business engaged in the oil or gas industry (where the use of equipment which can withstand hostile environments is common place) directly involved with proliferation-sensitive goods; or a bank account might be used to facilitate the activities of a business providing a service to a company or other business involved with proliferation-sensitive goods, and this service might be part of the proliferation programme; or

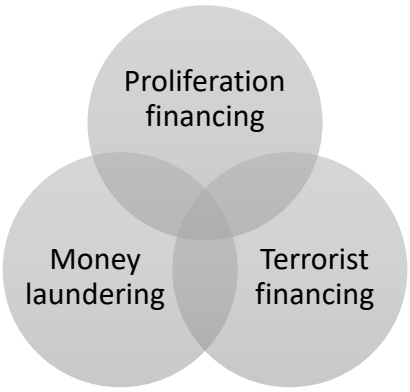
- a TCSP and its services might be involved in the formation, administration or management of a business involved with proliferation-sensitive goods (or the TCSP might be providing a different activity), a company providing a service to such a business or the holding company of such a business/company; or

- legal or accountancy advice might be obtained on the structuring of a finance package or structuring of legal persons or transactions relevant to proliferation-sensitive goods or services.

It is important to be aware of these challenges and factors when implementing measures to prevent or detect proliferation and proliferation financing. Businesses also need to ensure that they are familiar with the techniques that may be used to evade sanctions measures relating to proliferation and proliferation financing. Further guidance on this and other issues is provided in Section 2, and in the sources of information under Question 13. Linked with this, the annual validation requirements for the Guernsey Registry in relation to Guernsey legal persons have recently been revised, and these requirements include information on the activities of legal persons relevant to the above factors.

Question 5: What is the difference between proliferation financing, money laundering and terrorist financing?

Money laundering, terrorist financing and proliferation financing have a number of similar characteristics and differences. An understanding of these is important in order to develop strategies to identify and combat proliferation and proliferation financing, as distinct from other illicit activities.



Money laundering involves concealing the proceeds of criminal conduct to disguise their illegal origin. This may entail changing their form or moving them to a place where they are less likely to attract attention.

Money laundering has a number of features in common with proliferation financing, since the methods used to conceal funds, such as the use of front companies and other intermediaries, may be similar. The proceeds of criminal conduct might be used to finance proliferation.

Proliferation financing differs from money laundering in important respects:

- Different funds trail: the movement of funds in money laundering is circular. This is because the purpose of this activity is to disguise the source of the funds, while ultimately returning them to the person or entity generating them either directly or by enabling them be used by the person or entity. The funds trail in proliferation financing is linear in that funds are used to purchase goods and services for use in a WMD programme. Funds do not need to be returned to the State financing a WMD programme.

- Different sources of funds: although proliferation financing and money laundering may involve the use of proceeds of criminal activity, proliferation may also involve the use of legitimately sourced funds or it may be financed directly by a State as part of a state WMD programme.

- Different detection/investigation focus: the focus of money laundering investigations is predominantly on the source of funds, and whether funds have been generated from criminal conduct. An investigation into suspected proliferation financing will consider both the source of funds, and the use of funds for illicit purposes that might have come from legitimate sources.

Terrorist financing is the provision, collection, receipt, possession or use of money or other property for the purposes of terrorism. It also includes (money) laundering of terrorist property.

Money laundering, terrorist financing and proliferation financing can overlap as regards, for example, the methods used to conceal funds and the use of the proceeds of criminal conduct. Terrorist organisations may also operate their own WMD programmes (or be involved in the purchase or supply of WMD), and funding provided for this purpose would also constitute proliferation financing.

Terrorist financing differs from proliferation financing in that it is more often financed through illegal activities, and may involve greater use of informal finance networks or cash couriers in its transactions.

Question 6: Who should be concerned to identify potential proliferation or proliferation financing activities?

As can be seen from the examples given in response to question 4, activities relating to proliferation and proliferation financing may involve a range of different businesses in the global manufacturing and supply chain and a range of different types of financial or other transaction/activity which might finance proliferation or otherwise facilitate proliferation. All businesses operating in the Bailiwick should therefore be aware of the risks of proliferation and proliferation financing, particularly given the need to comply with the legal obligations summarised in Annex B.

The following organisations may be particularly vulnerable to the risks of proliferation and proliferation financing, and should pay particular attention to identifying and combatting these activities:

- Financial services businesses - banks; proliferators and their agents typically use formal financial channels such as banks and may use their services to hold or transfer funds or assets, settle trade and pay for services. Banks might also engage in one or more of the activities mentioned below.

- Financial services businesses involved in or providing advice in relation to the formation, structuring, administration or management of legal persons, such as companies; proliferation and proliferation financing networks often make use of front companies, to conceal their activities. These businesses include TCSPs and businesses that also provide legal services. Even the most limited of services to a company involved in proliferation or proliferation financing might create a potential vulnerability for the TCSP as it would create a link between Guernsey, the TCSP and the potential consequences of proliferation. The formation, structuring, administration and management of trusts and other legal arrangements cannot be excluded but their role in proliferation and proliferation financing appears to be extremely rare.

- Other financial services businesses such as firms providing trade finance, investment or insurance products; a number of proliferation and proliferation financing activities use these products. The challenges and factors described above, combined with the international and varied nature of

Guernsey's customer base highlight the importance of financial institutions more generally being alert to the possibility of use of them by proliferators and their agents. For example, financial institutions might also be used to park assets in Guernsey or to lend funds which facilitate the transport of dual use goods.

- Businesses involved in the manufacture of dual-use goods, such as the manufacture of centrifuges or gyroscopes or pumps able to withstand hostile environments for the oil and gas industry (see question 4), or businesses offering services to those businesses.

- Businesses involved in importing and exporting goods and services (including transport and logistics); since their activities may involve the import/export of items, including dual-use goods, which could be used in proliferation.

- Businesses, including brokers, involved in import and export logistics and transport; since their services may be used to transport items used in proliferation.

Question 7: What legal measures are in force in the Bailiwick regarding proliferation and proliferation financing?

The Bailiwick's legal framework contains a number of measures to combat proliferation and proliferation financing. They fall into the following categories:

- the Bailiwick implements UN and UK sanctions regimes which target (among others) countries, entities and individuals suspected of involvement in proliferation and proliferation financing;

- anti-weapons or anti-proliferation offences which make it unlawful to engage in certain activities relating to proliferation and/or proliferation financing;

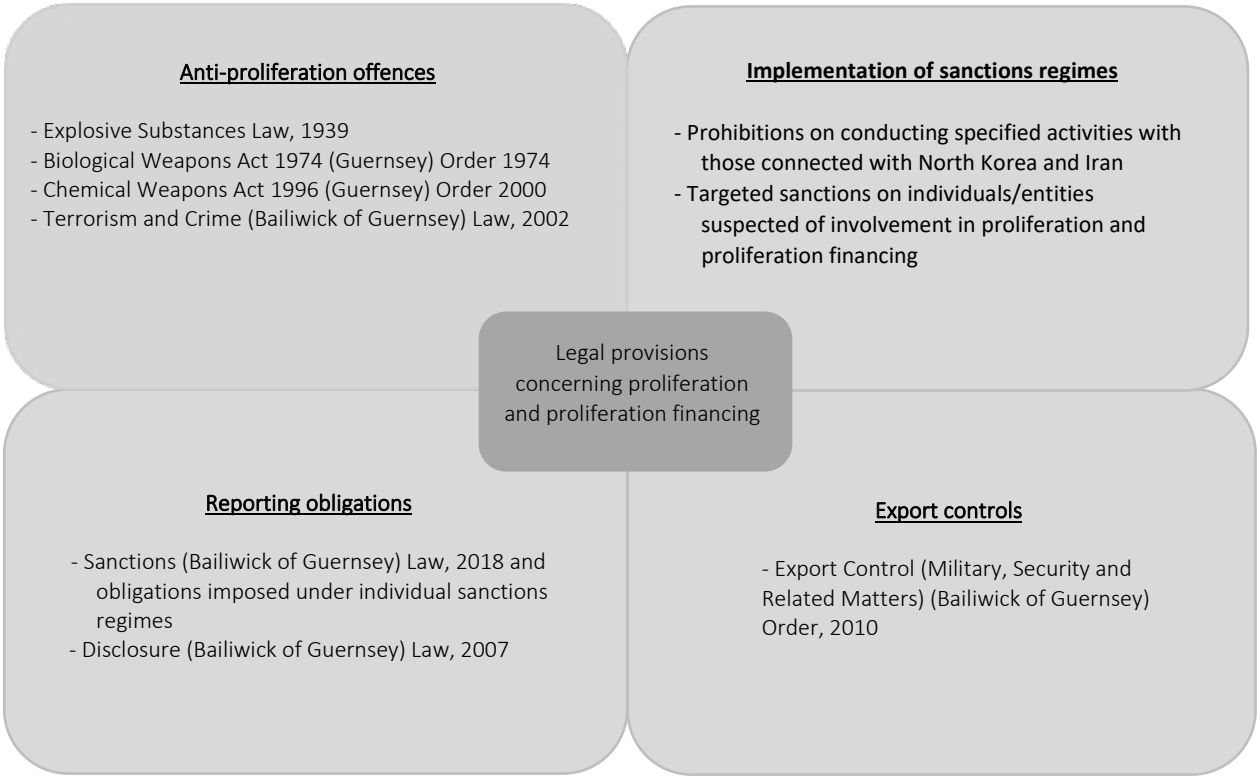
- reporting obligations which require persons to report suspicions or knowledge of proliferation and proliferation financing and related activity; and

- export controls which seek to control and prevent the acquisition and transfer of goods, services, technology and expertise that might be used by proliferators.

The legal framework applicable in the Bailiwick broadly mirrors the equivalent legislation in the United Kingdom. In most cases, Bailiwick law directly incorporates a legal provision in force in the UK by providing that it has effect in the Bailiwick. However, the Bailiwick legal regime is separate from, and operates independently of, the UK regime.

An overview of the legal framework in force in the Bailiwick is contained in this diagram:

Annex B to this guidance paper provides a summary of these legal provisions.



Section 2: Guidance on Good practices to identify, manage and reduce the risks of proliferation and proliferation financing

Question 8: What steps can be taken to identify, assess, manage and reduce the risks of proliferation and proliferation financing?

UN and UK sanctions include a freeze on all assets owned, held or controlled, directly or indirectly, by a listed person or entity, and they also prohibit any person or entity from making funds or other assets, economic resources or certain financial services available, directly or indirectly, to or for the benefit of listed persons and entities, or to or for the benefit of persons or entities that are solely or jointly owned or controlled, directly or indirectly, by listed persons or entities. These measures apply to any kind of assets, funds or economic resources (including any type of property or interest derived from those assets, funds or economic resources) and it is immaterial whether the assets funds or economic resources are wholly or jointly owned, held or controlled. In addition to the restrictions applicable to listed persons, the UN and UK sanctions impose trade restrictions affecting the supply of a wide range of goods and technology to or from countries that are considered to present a risk of proliferation and proliferation financing. Importantly, in some cases these restrictions apply to named parties in a particular country, who may not be listed persons and entities for the purposes of targeted financial sanctions.

The Bailiwick has implemented UN and UK sanctions regimes, some of which relate to an individual, entity or country's involvement in proliferation or proliferation financing. Therefore, effective implementation of sanctions is an important part of combatting proliferation and proliferation financing. This is discussed further in Question 12, and details of the potentially relevant obligations are provided in Annex B.

In order to address the risks of proliferation and proliferation financing fully, these risks need to be considered separately to other risks and risk identification, assessment and reduction frameworks tailored accordingly.

As part of their controls for AML and CFT and for sanctions compliance in general, many businesses have screening systems for relationships, transactions and counterparties in order to identify whether or not the firm is exposed to the risk of transferring assets in some way (in the context of this guidance paper) to persons or entities listed by the UN or UK as presenting a proliferation or proliferation financing risk. Typically, a screening system includes matching relevant data of a business (such as lists of customers and their beneficial owners or recipients of transfers) against lists in IT software provided by a third party specialist in gathering public information about persons and entities, such as lists of persons and entities subject to sanctions frameworks, from around the world. It is important to stress that, while screening systems are important for demonstrating compliance with sanctions frameworks, they are not sufficient by themselves to ensure compliance with any sanctions regime no matter how sophisticated the screening system might be. Listed persons or entities in relation to proliferation financing will not wish to make their involvement in a relationship or transaction or as an end-user obvious; as indicated above, proliferators and their agents will wish to disguise the financing of proliferation and other proliferation activity. Screening, not only of customer relationships but also of transactions and counterparties which might be vulnerable to proliferation or proliferation financing, can only be one mechanism for sanctions compliance within a more comprehensive system.

The steps which can be taken to identify, manage and reduce the risks of proliferation and proliferation financing will differ according to the type of business and the risk profile of the business.

By virtue of the UN and FATF requirements, globally, businesses subject to AML and CFT obligations have a high profile and importance in combatting proliferation and proliferation financing even if the risk in practice to individual businesses or sectors in some jurisdictions might be very low. For those businesses in the Bailiwick subject to AML and CFT obligations and supervised for compliance with those obligations by the Guernsey Financial Services Commission or the Alderney Gambling Control Commission, adoption of the same requirements for proliferation and proliferation financing as those for AML and CFT under Schedule 3 to the Proceeds of Crime Law and the Guernsey Financial Services Commission's Handbook on Countering Financial Crime and Terrorist Financing and in the Alderney eGambling Ordinance and the Alderney eGambling Regulations would have merit in demonstrably addressing the risks of proliferation and proliferation financing and in linking the policies, procedures and controls to address those risks with well-established systems for AML and CFT. Indeed, complementing AML and CFT policies, procedures and controls by adding specific policies, procedures and controls to them in relation to combatting proliferation and proliferation financing would be the best way of ensuring and demonstrating sanctions compliance, not least because global expectations are much more likely to increase rather than to stay the same or diminish. The six measures articulated below largely reflect AML and CFT principles.

Six measures are recommended that will assist in identifying, managing and reducing the risks of proliferation and proliferation financing:

1. Carry out and document a suitable business risk assessment, which is specific to the individual business, in order to identify the extent to which there is exposure, and the type of exposure, to risks of proliferation and proliferation financing. This is discussed further in response to Questions 9 and 10 below, and a list of possible indicators of proliferation and proliferation financing activities is provided in Annex A.

   Detailed guidance on assessing and mitigating the risk of proliferation financing has been issued by the FATF and is available here: *Guidance on Proliferation Financing Risk Assessment and Mitigation (fatf-gafi.org)*.

   Businesses should ensure that they are familiar with the FATF guidance. They should also note that it is possible that the risks of proliferation and proliferation might have a "long tail" in that exposure might still exist even where a transaction has been completed or where a contractual or customer relationship is no longer active. To that end, businesses subject to AML and CFT obligations should consider whether, for any person or entity listed under the UN's sanctions frameworks in relation to Iran and North Korea, their screening and other systems might in any way have failed to lead to the freezing of assets the same day as the listing was issued by the UN. Information on listings and the date of listing can be found on the UN website.

   Where legal persons (e.g. companies) and/or legal arrangements (e.g. trusts) are administered or managed by a Guernsey business, consideration should be given to how procedures and controls might be affected not only by the administered/managed entity but also by any exposure to risk through entities in the control and ownership chain above or below the locally administered/managed entity, whether this be the risk of involvement in a sanctions breach, the risk of reputational damage, or both. The revised annual validation requirements of the

Guernsey Registry might assist businesses with assessing whether other entities in the ownership chain are at risk of being involved in proliferation or proliferation financing, as information on the activities of subsidiaries of legal persons must be provided to the Registry by TCSPs which are resident agents. A licence, authorisation or consent issued by a foreign government in relation to proliferation or proliferation financing might also be relevant.

However, it should be stressed that even if there is reason to believe that entities in the chain present a risk of proliferation or proliferation financing, this will not necessarily mean that the locally administered/managed entity (and therefore the TCSP) is at risk of involvement in a sanctions breach. The key issue for these purposes is not the formalities of the relationship with those other entities but instead is whether the locally administered/managed entity or the TCSP is able to exercise any actual control over them, whether direct or indirect. This could be control over assets linked to those entities (e.g. by involvement in the movement of assets along the chain) or control over their activities (e.g. by authorising a particular transaction that another entity in the chain wishes to carry out). Where the locally administered/managed entity or the TCSP has direct or indirect control of this kind, the TCSP should take whatever further measures are reasonable in the circumstances to assess the risk of proliferation or proliferation financing resulting from its links with the other entities in the chain. Where neither the locally administered/managed entity nor the TCSP has any control over the assets or activities of other entities in the chain, there is unlikely to be any risk of breaching sanctions. Therefore, in those circumstances TCSPs will not ordinarily be required to take any further risk assessment measures, but they may wish to do so in order to identify any reputational risks that might arise from being linked to the other entities in the chain. This is advised as a matter of good practice.

Business risk assessments should be regularly reviewed and updated.

2. Implement or adapt policies and procedures to reflect the risks posed by proliferation or proliferation financing.

   Appropriate changes should be made to policies and procedures specifically to address the Bailiwick's legal requirements in relation to, and the risks of, proliferation and proliferation financing. This should include:

   - Introducing a compliance policy concerning proliferation and proliferation financing requirements or adapting existing compliance policies to take account of these requirements.

   - Specifically referring to proliferation and proliferation financing sanctions in procedures manuals. Globally, it is common for procedures manuals to refer to terrorist financing sanctions but not to proliferation financing sanctions. This absence must have a bearing on the global effectiveness of measures to identify possible links to proliferation or proliferation financing. Reference in manuals should include at least a summary of the legal requirements and reference to controls – including the other five measures described in this part of the guidance paper - and the steps to be taken if there is an issue such as a match with a person or entity who is listed.

3. Establish basic controls with a specific focus on proliferation and proliferation financing:

- The current reporting requirements relating to proliferation and proliferation financing, sanctions, and to AML or CFT where there may be a link to proliferation and proliferation financing. Details of these requirements are set out in Annex B. All of these reporting requirements need to be embedded in the controls.

- Identification and assessment of risks in respect of each relevant relationship customer and counterparty relationship (and potentially employees). This would mean risk profiling individual relationships for proliferation and proliferation financing risk and calibrating any further actions such as CDD based on that risk. It is envisaged that, where relationships have not yet been risk profiled for proliferation and proliferation financing risk, such relationships will be risk profiled for proliferation and proliferation financing risk at the same time the relationship is subject to ongoing monitoring for AML or CFT purposes (and, for the avoidance of doubt, where there has been a trigger leading to enhanced attention by the business).

  Relationships include customers and counterparties (e.g. manufacturers, suppliers, consultants or agents) whose activities might involve a risk of involvement in proliferation and/or proliferation financing. With regard to counterparties, consideration might be given to the inclusion of clauses relating to compliance with legal provisions on proliferation and proliferation financing into contracts.

  The process would include ensuring that the extent to which any customer, country/jurisdiction, transaction, product/service, distribution channel and counterparty risk in relation to transhipment hubs linked to countries subject to proliferation and proliferation financing sanctions (see figure 4) affects the risk profile of a particular customer relationship or other contractual relationship.

- Customer due diligence (CDD). This should include e.g. consideration of factors that might indicate an increased risk of activities relating to proliferation and/or proliferation financing when assessing whether to take on a customer relationship, whether to undertake or provide advice in relation to a transaction, and undertaking ongoing monitoring of individual customer relationships for AML and CFT purposes. These factors are discussed further in Question 10.

- Understanding beneficial ownership of relationships and the source of wealth and funding of relationships and transactions.

- Beneficial ownership is not simply about the amount of a shareholding but also about control. This concept is well-established within the Bailiwick's AML and CFT requirements and was also introduced in relation to Guernsey and Alderney legal persons in 2017 as, since that year, beneficial ownership information on such legal persons has had to be filed with the Guernsey and Alderney Registries. The same precepts of control included in guidance issued under the AML and CFT framework and by the Registries are applicable when considering beneficial ownership in the context of sanctions compliance. This is particularly pertinent for proliferation and proliferation financing in light of the importance to proliferators and their agents of disguising their objectives and control networks within proliferation and proliferation financing activity.

- Understanding the source of wealth of relationships and the funding of transactions is also important as this might indicate potential links to a proliferation network. There has been a notable number of cases internationally where earlier and better attention to inconsistencies or unusual factors in funding would have led to earlier discovery of proliferation financing.

- Ongoing monitoring of relationships based on the risk. This would include embedding indicators and red flags, which, if they were to occur, would trigger further scrutiny by the business.

4. Undertake enhanced due diligence and enhanced monitoring activities for high-risk customer relationships, contracts and/or transactions that are relevant to addressing proliferation and proliferation financing risks. Where a customer or other business relationship, contract and/or transaction presents a high risk of potential involvement in proliferation or proliferation financing, enhanced due diligence and monitoring should be undertaken with a view to identifying whether illicit activities are or have been taking place. Individual transactions within a customer relationship might have an elevated risk of proliferation or proliferation financing and will warrant specific attention. This is addressed further in Question 11.

5. Staff training. Businesses should ensure awareness among their staff of the risks relating to proliferation and proliferation financing activities that might be encountered in their operations. They should ensure that staff have sufficient and up-to-date training, information and resources to:

   - enhance their understanding of proliferation and proliferation financing, including the techniques used to evade detection and indicators.

   - increase their awareness of the relevant legal obligations in the Bailiwick, including the need to screen for any activities that might constitute a breach of the relevant sanctions regimes.

   - ensure they are able to effectively implement risk management or risk mitigation procedures.

   - know where to seek further information or guidance where this is required.

6. Corporate governance. The board of directors or equivalent body should regularly and specifically consider compliance with the legal requirements relating to proliferation and proliferation financing as part of a focus on sanctions compliance, together with to what extent the business's policies, procedures and controls have been met. As indicated above, businesses have long been subject to legal requirements in relation to proliferation and proliferation financing (which are outlined in Annex B) and their management should in any case have been monitoring compliance with those requirements. By way of illustration, annual consideration might normally be sufficient (although there might be circumstances which would warrant more urgent consideration).

The concepts and requirements expressed above will be familiar to financial services businesses and other businesses meeting Guernsey's AML and CFT requirements, including requirements relating to UN and UK sanctions on terrorist financing. It is increasingly recognised globally that proliferation and proliferation financing sanctions are more likely to be met in the round if businesses have identified and assessed the risks relevant to them. By extension, while businesses might have comprehensive controls in relation to identifying and verifying beneficial ownership of legal persons and legal arrangements and sophisticated monitoring systems, a focus on combatting proliferation and proliferation financing as a distinct focus, as a complement to a focus on AML and CFT, can only be of benefit.

More generally, while this guidance paper advocates a separate focus on addressing proliferation and proliferation financing risk as a complement to the existing separate focus on each of AML and CFT policies, procedures and controls, AML and CFT and sanctions compliance in general can usefully work together as a complementary and unifying whole. Measures established to address money laundering (and predicate criminality such as corruption and tax evasion) and terrorist financing, and the risks of proliferation and proliferation financing, have many similar features in common, but an appreciation of the individual risks and indicators for each, and tailoring of measures accordingly, enhances responses to those risks.

Question 9: How might a business conduct a risk assessment relating to proliferation and proliferation financing?

The purpose of a business risk assessment is not to eliminate risk altogether. It enables businesses to understand the risks they face and ensure they have appropriate and proportionate policies, procedures and controls in place to manage these risks.

The guidance provided below is general to business risk assessments for all proliferation and proliferation financing risks that a business might encounter in its activities. It should be read in conjunction with the FATF Guidance on Proliferation Risk Assessment and Mitigation referred to under Question 9.

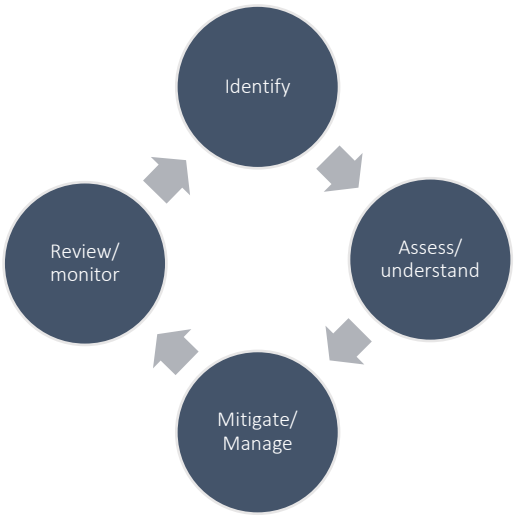
In order to understand the risks of proliferation financing it is important also to understand the risks of proliferation and any financing relating to those risks.

There should be a specific, documented business risk assessment process for proliferation and proliferation financing. If a business already conducts risk assessments in areas such as money laundering and terrorist financing, the risks of proliferation and proliferation financing can be incorporated into or added to that framework – provided that the risks of proliferation and proliferation financing are considered separately from other risks. It is a matter of preference for the individual business as to whether the proliferation and proliferation financing risk assessment document is a separate document or forms a (separate) part of a document which also covers money laundering, sanctions and/or terrorist financing. Risk assessments should be regularly reviewed and updated, in particular to take account of any new or emerging practices and obligations involving proliferation and/or proliferation financing.

The structure for a proliferation and proliferation financing risk assessment might be based on the requirements and guidance provided in relation to AML and CFT business risk assessments contained in Schedule 3 to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 and in the Guernsey Financial Services Commission's Handbook on Countering Financial Crime

and Terrorist Financing (and in Schedule 4 to the Alderney eGambling Ordinance and Chapter 4 of the Guidance for eGambling Businesses on Countering Financial Crime and Terrorist Financing). The key principles are outlined below.

A business risk assessment involves the following steps:



- Identifying the threats posed to the business and those areas of activity with the greatest vulnerability.
- Assessing the likelihood of those threats occurring and their potential impact.
- Mitigating the likelihood of occurrence of identified threats and the potential for damage to be caused, through the application of appropriate and effective policies, procedures and controls.
- Managing the risks arising from the threats that the business has been unable to mitigate.
- Reviewing and monitoring those risks to identify whether there have been any changes to the threats posed to the business which necessitate changes to its policies, procedures and controls.

Any business risk assessment should consider risks that might arise in relation to all relevant customer relationships and counterparties. The business risk assessment should also involve a consideration of whether breaches of the relevant legal requirements in Annex B might have already occurred, and any steps that might be taken in relation to this conduct (such as whether a reporting obligation applies and what should be done to avoid breaches occurring in the future).

The scope of a business risk assessment should be appropriate to the nature, size and complexity of the business. For example, a firm operating on an international scale, or with an international client base, may assess a wider range of risks than a smaller domestically-focused institution. Firms engaged in the types of activities outlined in Question 6 above, which may be particularly vulnerable to proliferation and proliferation financing activities, may assess a wider range of risks compared with firms whose activities have limited potential exposure to proliferation and proliferation financing.

If a business considers that it is exposed in practice to a risk of proliferation and/or proliferation financing, as with the requirements in place for the AML and CFT frameworks, it may also be appropriate to establish a separate risk assessment process (i.e. risk profiling) that applies prior to establishing a customer relationship, or carrying out a transaction, which focuses on the specific risks posed by that relationship and/or transaction and allows any mitigation steps to be taken accordingly. With regard to existing customer relationships, for firms subject to the Proceeds of Crime legislation, such risk profiling might take place at the same time as a customer relationship is subject to monitoring under the AML and CFT frameworks.

Question 10: What types of risks might be relevant to a proliferation and proliferation financing risk assessment?

The risks that might be identified and assessed in a risk assessment concerning proliferation and proliferation financing fall into four main categories, relating to:

- customers, including their beneficial owners;
- counterparties, including their beneficial owners;
- countries and geographic areas involved in customer relationships and/or transactions;
- products, services, transactions and delivery channels.

Businesses that are experienced in the identification and assessment of money laundering and terrorist financing risk will be familiar with these categories, albeit that counterparty risk has been added as a distinct category given its particular relevance to proliferation and proliferation financing risk. There is no exhaustive list of the risks within each category that a business should consider as part of a proliferation and proliferation financing risk assessment. As explained in response to Question 9, the scope of a business risk assessment should be appropriate to the nature, size and complexity of the business. It should also be appropriate and proportionate to the proliferation and proliferation financing risks associated with the business's activities.

Each business should decide which risks will be included in their risk assessment based on their circumstances. These risks should also be assessed alongside factors that indicate a decreased risk of proliferation and proliferation financing activities, such as the duration of a particular customer or counterparty's relationship and the overall transparency and understanding of that relationship. In identifying and assessing these risks, it may be helpful to have regard to possible indicators of proliferation and proliferation financing activities. A number of organisations, including the FATF, have identified potential indicators. Annex A provides a list of these indicators, which are summarised under the categories of risks identified above.

It is important to be aware that the presence of one or more of the possible indicators set out in Annex A does not necessarily mean that proliferation or proliferation financing activities are taking place. It might imply an increased risk of such activities, which may call for further investigation, focus and/or steps to be taken to manage or mitigate these risks.

Question 11: What types of enhanced due diligence and/or monitoring measures could be used in relation to proliferation and proliferation financing risks?

A large number of businesses operating in the Bailiwick already have a customer due diligence process within their organisation. As mentioned in response to Question 8 above, this should be adapted or supplemented to include factors that may indicate a risk of proliferation and proliferation financing activities.

Where a risk assessment relating to a particular customer or other business relationship or transaction indicates a higher risk of proliferation and/or proliferation financing, a business should consider using enhanced due diligence and/or monitoring measures to mitigate the particular risks identified.

This process will be familiar to persons that are subject to the Bailiwick's AML and CFT regime. Schedule 3 to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 requires the use of enhanced due diligence and monitoring measures where a customer relationship or occasional transaction is considered as being at high risk of money laundering or terrorist financing. Further guidance on enhanced due diligence and monitoring measures in this context is provided in Chapter 8 of the Guernsey Financial Services Commission's Handbook on Countering Financial Crime and Terrorist Financing and in Chapter 8 of the Guidance for eGambling Businesses on Countering Financial Crime and Terrorist Financing. Some of the suggested enhanced due diligence measures contained in these documents could also be applied in the context of proliferation and proliferation financing. Nevertheless, it remains important to focus separately on proliferation and proliferation financing risk and to tailor measures taken accordingly. There is more emphasis on counterparty risk than is normally expressed in literature globally to address money laundering and terrorist financing.

Bearing in mind that those involved in proliferation and proliferation financing may seek to disguise their activities, and that many typologies (or case studies) for proliferation or proliferation financing note the existence of something unusual occurring within a relationship or transaction (or linked series of transactions), enhanced due diligence and/or monitoring activities, particularly in relation to transactions and the source of wealth for transactions, are key. Enhanced due diligence and monitoring that might be undertaken on relationships or transactions posing a high risk of proliferation or proliferation financing include:

- Enhanced checks on, or requesting further verification of, the identity or ownership of customers and/or counterparties, including their beneficial ownership. This could be supplemented by consulting publicly available reports through the media and the internet.

- Consulting open source databases, such as company and beneficial ownership registries, to gain more information on shareholders, directors and beneficial owners of customers and/or counterparties in order to understand whether any of them might be of particular concern for proliferation or proliferation financing.

- Requesting further explanation of and/or documentary evidence on the source of funds and/or wealth for particular transactions.

- Consulting other publicly accessible sources such as shipping and aircraft registries, chambers of commerce, third party experts, publications or the media so as to understand better the context for the movement of goods and equipment and/or the supply chains involved in a particular relationship or transaction, in order to establish whether the relationship or transaction is consistent with these contexts.

- Requesting further explanation of and/or documentary evidence regarding high risk customers, relationships or transactions in order to understand better the purpose or intended nature of the customer relationship or individual transaction. For example, where the transaction involves the transfer of proliferation-sensitive goods or services, a shipment of dual-use goods or the shipment of goods or equipment to a transhipment hub, further documentation (such as export control information and certifications) could be requested in order to verify the intended end-use or end-user.

- Taking measures to establish, understand and independently verify particular transactions, whether for the import/export/shipping of goods or related financial transactions, for example by checking the known history of relevant vessels and/or tracking the physical movement of goods/equipment or vessels.

- Requesting further information and/or documentary evidence regarding the routing of goods (including as to their final destination) and their financing, and considering whether to take further steps where the routing or the jurisdiction of end-use or the end-user is a jurisdiction engaged in proliferation or a jurisdiction which has close trading links to one or more jurisdictions engaged in proliferation.[8]

- Conducting further supply chain analysis, for example by requesting further explanation of and/or documentary evidence about the nature, end-use or end-user of goods, particularly where the transaction relates to dual-use goods or other proliferation-sensitive goods and/or services.

- Requesting further export control information, such as copies of export control or other licences or authorisations issued by export control authorities, and/or end-user certification, so as to ascertain the nature of the goods, whether they have been properly authorised, and whether there has been any change to the volume or value of goods as they are transported between jurisdictions.

- Enhanced monitoring of customers that are engaged in transactions that appear outside the usual profile for or practices of those customers.

Question 12: What steps should be taken to comply with relevant sanctions obligations in force in the Bailiwick?

The Bailiwick implements UN and UK sanctions regimes, some of which relate to an individual, entity or country's involvement in proliferation or proliferation financing. Effective compliance with these sanctions is an important part of combatting proliferation and proliferation financing.

Any person falling within the jurisdiction of Bailiwick law should be aware of the obligations and prohibitions in the legislation implementing sanctions regimes and should put all necessary policies, procedures and controls in place to ensure that they comply with these measures. Details of the potentially relevant obligations are provided in Annex B.

Businesses should screen transactions, counterparties and other business relationships to identify whether there are any sanctions concerns. In particular, they should:

- Check that they are not engaging in activities prohibited by sanctions regimes.

- Ensure that they treat all accounts, funds and economic resources belonging to, owned, held or controlled (directly or indirectly) by a designated person, entity or body as frozen, without the consent of the licensing authority. For the vast majority of sanctions regimes this is the States of Guernsey Policy & Resources Committee.

[8] Further information on countries of proliferation concern is provided in Annex A.

- Refrain from making any funds or economic resources available directly or indirectly to any designated person without the consent of the licensing authority.

Effective implementation of sanctions requires more than checking whether there are business relationships with those persons appearing on sanctions lists:

- Certain sanctions regimes, such as that relating to North Korea, contain prohibitions on conducting certain activities with individuals or entities based in, or acting on behalf of a particular country.

- It is also necessary to screen for prohibited activities and those whose object or effect is to circumvent sanctions prohibitions.

Where an entity suspects conduct that may raise sanctions concerns, it should take legal advice and ensure it is complying with the rules in force relating to that sanctions regime, including reporting obligations. Failure to comply with sanctions can have serious repercussions. This could involve prosecution for criminal offences and/or financial penalties, and may also involve personal penalties. This is explained further in Annex B. Where a business might consider that a person not listed by the UK or UN should be listed in relation to proliferation financing, representation should be made to the Policy & Resources Committee with full justification.

The guidance provided in Section 2 will assist businesses in complying with the relevant sanctions regimes. However, separate and additional measures are likely to be necessary in order to reflect the particular obligations and prohibitions in sanctions legislation. The following resources may be helpful:

- The website for the States of Guernsey, which contains guidance on sanctions, including a Frequently Asked Questions guide on the Bailiwick sanctions regimes produced by the Policy & Resources Committee.

- The Guernsey Financial Services Commission's guidance on sanctions screening in Chapter 12 of its Handbook on Countering Financial Crime and Terrorist Financing. The Handbook is predominantly directed at those persons subject to the Bailiwick's AML and CFT measures, but the guidance on sanctions screening in Chapter 12 is likely to be of assistance to all businesses.

- The Alderney Gambling Control Commission's guidance on sanctions screening in Chapter 10 of its Guidance for eGambling Businesses on Countering Financial Crime and Terrorist Financing.

- HM Treasury's website contains guidance and FAQ documents on financial sanctions.

Persons that are subject to Bailiwick law should adopt a range of measures in order to achieve three aims identified in the diagram below.

Question 13: What other sources of guidance are available on proliferation and proliferation financing?

A list of sources providing further information on proliferation and proliferation financing (including case studies) are set out below.

DOCUMENTS PRODUCED BY THE FATF AND THE UN

- FATF - Typologies Report on Proliferation Financing (2008)
- FATF - Combatting Proliferation Financing: A status report on policy development and consultation (2010)
- FATF - Guidance on Counter Proliferation Financing – The implementation of financial provisions of United Nations Security Council Resolutions to counter the proliferation of weapons of mass destruction (2018)
- FATF- Guidance on Proliferation Financing Risk Assessment and Mitigation (2021)
- United Nations – Panel of Experts Reports concerning DPRK sanctions

DOCUMENTS PRODUCED BY AUTHORITIES IN OTHER JURISDICTIONS

- Bahamas – Guidance note on proliferation and proliferation financing (2018)
- Cayman Islands Financial Reporting Authority – Identifying Proliferation Financing (2020)
- Cayman Islands Department of Commerce and Investment – Guidance Notes: Counter Proliferation Financing (2020)
- Cayman Islands Monetary Authority – Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands (2020)
- Gibraltar Financial Intelligence Unit – Counter Proliferation Financing: Guidance Notes (2020)
- Isle of Man – Financial Sanctions Relating to Proliferation - Guidance (2020)
- Isle of Man – Proliferation and Proliferation Financing Risks (2018)
- Monetary Authority of Singapore – Sound Practices to Counter Proliferation Financing (2018)

DOCUMENTS PRODUCED BY INDEPENDENT BODIES

- David Albright et al – Illicit Trade Networks – Connecting the Dots, Volume 1 (Institute for Science and International Security) (2020)
- Dr Jonathan Brewer – The Financing of WMD Proliferation: Conducting Risk Assessments (2018)
- Dr Jonathan Brewer – The Financing of Nuclear and other Weapons of Mass Destruction Proliferation (2018)
- Dr Jonathan Brewer – Study of Typologies of Financing of WMD Proliferation: Final Report (2017)
- Emir Dall and Tom Keatinge – Securing the Supply Chain: Implementing North Korea Sanctions Beyond Banking (2019)
- Eda Erol, Leonard Spector – Countering North Korean Procurement Networks Through Financial Measures: The Role of Southeast Asia (2017)
- Togzhan Kassenova – Challenges with Implementing Proliferation Financing Controls: How Export Controls Can Help (2018)
- Lloyd's of London – Market Bulletin: Countering North Korean and other Sanctions Evasion Tactics (2019)
- RUSI – Countering Proliferation Finance: An Introductory Guide for Financial Institutions (2018)

- RUSI – “Project Sandstone” publications on North Korean illicit shipping networks.
- Stockholm International Peace Research Institute - Proliferation Red Flags and the Transport Sector (2016)
- The Wolfsberg Group – Guidance on Sanctions Screening (2019)

Annex A: Possible Indicators of proliferation AND proliferation financing

The table below sets out some of the possible indicators of proliferation or proliferation financing activity. The list is principally based upon indicators identified by the FATF, and is supplemented with further indicators and notes from other sources.

The indicators in the table are grouped into three categories:

- Indicators relating to countries or geographic areas (referred to as **Geographic Indicators**).

- Indicators relating to customers and counterparties involved in a transaction and/or business relationship (referred to as **Customer/Counterparty Indicators**).

- Indicators relating to products, services, transactions and delivery channels (referred to as **Transaction Indicators**).

These indicators are intended to help businesses in identifying, assessing and managing possible risks relating to proliferation and proliferation financing. They could be used in the following way(s):

- They could be incorporated into any risk assessment process for proliferation and proliferation financing, discussed in response to Question 10 above.

- They could form part of a screening process for proliferation and proliferation financing activities (including any breaches of applicable sanctions legislation).

These indicators are not intended to be an exhaustive list, and are not prescribed as a checklist. It is for businesses to decide which indicators will be included in their risk assessment and/or screening process based on their circumstances. They should also be assessed alongside other factors that indicate a decreased risk of proliferation and proliferation financing activities, such as the duration and quality of a particular customer or counterparty's relationship and the transparency of that relationship.

Of course, the presence of one or more of the indicators set out in the table below does not mean that proliferation or proliferation financing activities are taking place. It might help decide whether there is an increased risk of such activities, which may call for further investigation and/or steps to be taken to manage or mitigate these risks.

Indicator[9]	Further notes[10]
Geographic Indicators	
Transaction involves a country of proliferation concern.	North Korea and Iran are the principal countries of proliferation concern. Other countries and actors may also seek components for WMD and related delivery systems (for example Syria). North Korea is subject to sanctions for its proliferation activities, and there are some other proliferation-related sanctions programmes. Further information on the Bailiwick's implementation of sanctions is provided in Annex B, and a full list of the sanctions regimes currently in force in the Bailiwick can be found on the States of Guernsey website. However, most do not relate to proliferation or proliferation financing. Where a business relationship or transaction involves a country of proliferation concern, it is important to be aware of, and/or take further steps to understand, the underlying activities that are involved in that relationship or transaction. For example, a company incorporated or administered locally may be involved in providing corporate services (such as sourcing staff) that involve countries of proliferation concern. It is important to take steps to understand the nature of the underlying activities involved in that relationship and/or transaction.
Transaction involves country of diversion concern.	Diversion or "hub" jurisdictions (including free trade zones and free port areas) can be used to conceal the intended end-use or end-user of goods.

[9] Adapted from the list contained in the FATF's *Guidance on Counter Proliferation Financing: the implementation of financial provisions of United Nations Security Council Resolutions to Counter the proliferation of weapons of mass destruction* at page 32 (available online). The indicators have also been supplemented by material contained in other sources, which are listed in Question 13, and in particular the Project Alpha Final Report (available online) and the Stockholm International Peace Research Institute's good practice guide entitled *Proliferation Red Flags and the Transport Sector* (available online).

[10] This material in this column is based, in particular, on that set out in Annex 2 of RUSI's *Countering Proliferation Finance: An Introductory Guide for Financial Institutions* (available online) and the sources cited therein.

	This could include neighbouring countries to a country of proliferation concern. For example, certain Southeast Asian jurisdictions (and parts of those jurisdictions) are known to host North Korean corporate networks. As with the previous indicator, where a business relationship or transaction involves a country of diversion concern, it is important to be aware of, and/or take further steps to understand, the underlying activities that are involved in that relationship or transaction and the source of wealth leading to that transaction.
Transaction involves a country that presents a proliferation financing risk, or has strategic deficiencies in the fight against money laundering, terrorist financing and/or the financing of proliferation.	The FATF maintains lists of "high risk" and other monitored jurisdictions, which FATF identifies as having deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation. This list is available on the FATF's website.
Transaction involves a jurisdiction with weak export control laws or weak enforcement of export control laws.	The Peddling Peril Index evaluates the effectiveness of national strategic trade controls in 200 countries, territories, and entities produced by the Institute for Science and International Security.
Transaction involves a financial institution with known deficiencies in AML and CFT controls or located in a country with weak export control laws or weak enforcement of export control laws.	For example, it is said that North Korea has used correspondent accounts held with Chinese banks in order to facilitate international financial transfers that are of proliferation concern.
Transaction involves shipment of goods inconsistent with normal geographic trade patterns.	This may involve the shipment of goods through several jurisdictions for no apparent commercial reason (i.e. such a transaction does not make economic sense) or to/from a country that does not normally import/export the goods involved.
Transaction involves shipment of goods that are not normally associated with the country to which it is being shipped. This may also include the quantity of goods shipped being inconsistent with normal trade patterns.	An example is a shipment of semiconductor manufacturing equipment to a country that has no, or a limited, electronics industry.

Customer/counterparty Indicators	
The customer or a person or entity in the customer relationship might be engaged in activity which has vulnerability to abuse for proliferation.	Examples, which are not exhaustive, might include logistics businesses or businesses engaged in aspects of the oil and gas industry.
Customer activity does not match business profile or end-user information does not match end-user's business profile.	This may involve transactions that are beyond the capacity or substance of a customer, and/or out of line with their business strategy or historical pattern of trade activity. For example, this could include a customer or counterparty declared to be a commercial business, whose transactions suggest they are acting as a money-remittance business, or the involvement of a small trading, brokering or intermediary company carrying out transactions inconsistent with their normal business. This will require an understanding of the nature of a customer or counterparty's business and the clients and jurisdictions with whom they usually trade. In particular, financial institutions should have an awareness of which of its clients trade in sensitive goods and technology and be aware of deviations in normal trading patterns of those clients.
The customer or counterparty or its address is similar to one of the parties found on publicly available lists of persons designated for proliferation-related reasons.	This includes consulting international sanctions lists related to proliferation activities. Businesses, particularly financial institutions, may also consider maintaining a list of entities and persons not designated, but who are known to have connections to proliferation activities.
Customer has previously had dealings with individuals or entities that are now designated persons for proliferation and/or proliferation financing reasons.	This could include customers who have entered into a joint venture or a cooperation agreement with designated persons.
Order for goods placed by firms/individuals from countries other than the country of the stated end-user.	
Customer provides vague/incomplete information, and is resistant to providing additional information when queried.	Possible indicators include a customer acting excessively/aggressively, or who is reluctant to

	provide clear answers to routine financial, commercial technical or other questions.
Transaction Indicators	
Delivery of proliferation-sensitive or military goods and/or services, particularly to the higher-risk jurisdictions identified above.	This includes transactions involving items controlled under proliferation-related export control regimes or national control regimes. Links to further information on the Bailiwick's export control regime is provided in Annex B .
Delivery of products and/or services that are subject to proliferation-related UN or UK sanctions.	For example, the North Korea sanctions regimes include a number of activities subject to sanctions ranging from correspondent banking relationships through to leasing or chartering vessels or the provision of crewing services. Further information on the Bailiwick's implementation of UN and UK sanctions is provided in Annex B, and a full list of the sanctions regimes currently in force in the Bailiwick can be found on the States of Guernsey website. Most are unrelated to proliferation.
Transaction demonstrates links between customers or counterparties, or between the representatives of companies exchanging goods (e.g. same owner or management).	For example, the customers or counterparties to transactions might be linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated). They might also provide only a registered agent's address or have other address inconsistencies (for example, conducting business out of a residential address). In addition to transactions involving connected parties, individuals or entities may ask questions if there are transacting parties who share addresses or any other identifying information with entities involved in proliferation activities.
Transaction involves possible front companies or shell companies.	This might include: (i) companies that do not have a high level of capitalisation; (ii) companies that lack an online or physical presence; (iii) dormant companies that suddenly become active; or (iv) abrupt or unexplained changes in directorship, beneficial owners or authorised signatories.

Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.	Payment instructions are illogical, contain last minute changes or there is an unusual complexity or unconventional use of financial products. This could also include a situation whereby a customer provides the total required funds in advance of transaction in one large sum, if this is not typically characteristic of the industry in question.
Wire transfer/payment from or due to parties not identified on the original letter of credit or other information.	The transaction may involve an unusual intermediary or number of intermediaries. This may include requesting payment to be made to a beneficiary's account held in another country other than the beneficiary's stated location.
Circuitous route of shipment and/or circuitous route of financial transaction.	Transaction structure and/or shipment route appears unnecessarily complex or unusual and designed to obscure the true nature of the transaction. This could include offshore shipments, e.g. the transaction happens in Country A, for a shipment between Country B or C.
Evidence that documents or other representations (e.g. relating to shipping, customs or payment) are false or fraudulent.	For example, trade documentation appears illogical, altered or fraudulent (including unusual codes, markings or stamps). Certain documentation may be absent that would be expected given the nature of the transaction.
Based on the documentation obtained in the transaction, the declared value of the shipment was obviously undervalued vis-à-vis the shipment cost.	The shipment does not make economic sense. This would include payment of transport costs that may not correspond with the nature of the goods being shipped, e.g. a shipment with a declared value of $50 being shipped as 'priority air express' at a cost of $350. While it may be difficult to determine whether a specific good is under or over-valued, care should be exercised where the transaction seems to make little financial sense, either for the seller or the buyer.
Inconsistencies between information contained in trade documents and financial flows (such as names, addresses, destinations).	This can entail: (i) discrepancies between the descriptions of the goods on trade documentation and the actual goods; (ii)

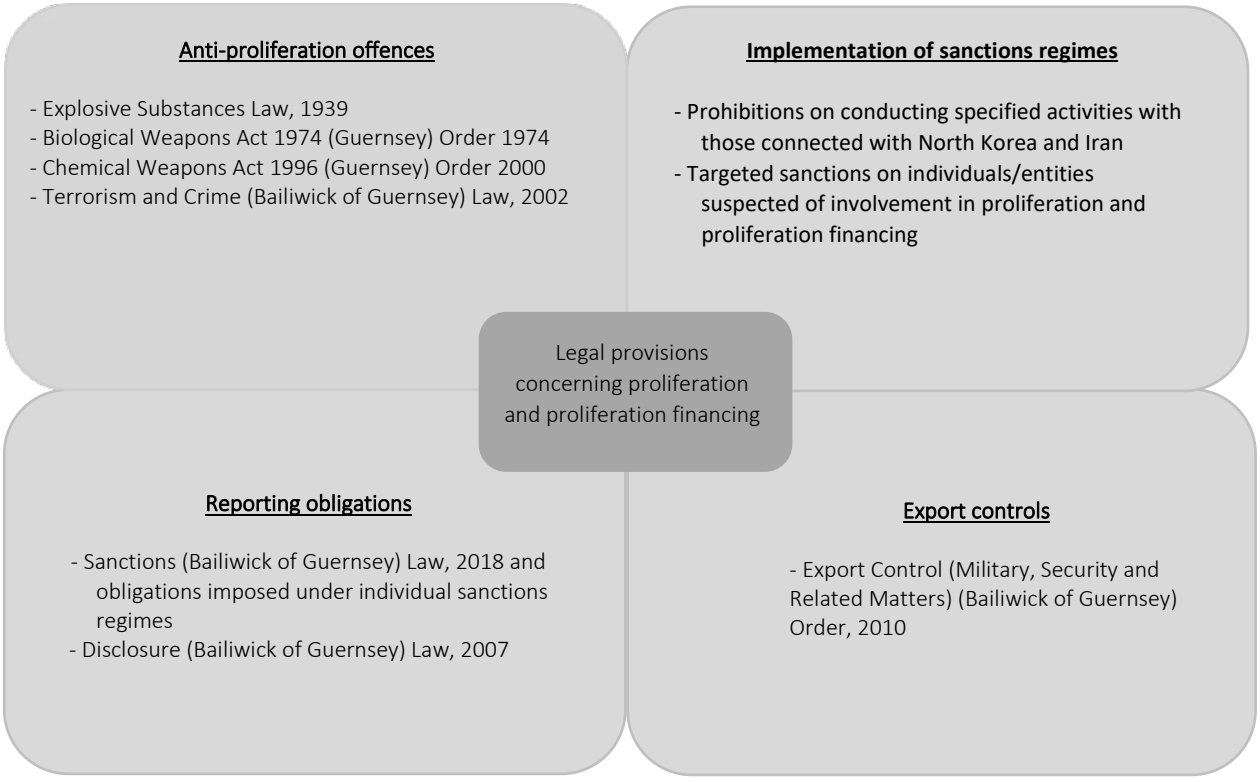
	discrepancies between the invoicing and shipping documents; (iii) involvement of unexplained third parties; (iv) changes in shipment locations; and/or (v) changes in the quality of goods shipped.
End-user not identified, e.g. a bank, hotel or freight forwarding company listed as consignee or final destination.	
Description of goods on trade or financial documentation is non-specific or misleading.	Examples are: “spare parts”, “samples”, “machine tools” or “electrical goods”.
Use of cash or precious metals (e.g. gold) in transactions for industrial items.	
Transactions between companies on the basis of “ledger” arrangements that obviate the need for international financial transactions.	
Payment of freight costs by a third party	In particular, where payment is made by a third party that does not appear to have a relationship with the sender/exporter or receiver/importer, or a third party that is located in a country other than that of the sender/exporter or receiver importer.
Use of personal accounts to purchase industrial items.	

Annex B: Legal obligations relevant to proliferation and proliferation financing

This Annex provides a summary of the legal obligations in the Bailiwick of Guernsey that are relevant to proliferation and proliferation financing, namely:

- The criminal offences in Bailiwick law, which make it unlawful to engage in certain activities relating to proliferation and/or proliferation financing.
- The United Nations and UK sanctions regimes implemented in the Bailiwick which are relevant to proliferation and proliferation financing.
- Reporting obligations that require persons to report suspicions or knowledge of proliferation and proliferation financing and related activities in the Bailiwick.
- The Bailiwick's export control regime, which seeks to control and prevent the acquisition and transfer of goods, services, technology and expertise that might be used by proliferators.
- International obligations relating to proliferation and proliferation financing.

The relevant legal framework in force in the Bailiwick is summarised in the diagram below.



This Annex does not seek to provide legal advice or guidance on the interpretation or application of any of these legal provisions. It is not a replacement for seeking legal advice.

Bailiwick offences relating to proliferation and proliferation financing

PROLIFERATION OFFENCES

There are criminal offences in Bailiwick law relating to the development, production, acquisition, stockpiling, retention or transfer of biological, chemical and nuclear weapons. These are contained in:

- The Biological Weapons Act 1974 (Guernsey) Order 1974, which applies the provisions of the Biological Weapons Act 1974 to the Bailiwick.

- The Chemical Weapons Act 1996 (Guernsey) Order 2000, which applies the provisions of the Chemical Weapons Act 1996 to the Bailiwick.

- The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002. Sections 63 – 65 contain offences relating to nuclear weapons.

These offences apply both to acts committed within the jurisdiction of the Bailiwick, and to acts committed outside the Bailiwick by individuals or bodies incorporated or established under the law of any part of the Bailiwick.

Furthermore, activities relating to proliferation may fall within the definition of terrorism set out in the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 and such activities may constitute one or more offences under that Law.

In addition, section 66 of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 provides that a person who "aids, abets, counsels or procures, or incites, a person who is not a Bailiwick person to do a relevant act outside the Bailiwick is guilty of an offence." A "relevant act" is an act that, if done by a Bailiwick person, would contravene:

- Section 1 of the Biological Weapons Act 1974.

- Section 2 of the Chemical Weapons Act 1996.

- Section 63 of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002.

Persons operating in the Bailiwick should also have regard to sections 2 and 3 of the Explosive Substances Law, 1939, which creates the following offences which could encompass activities relating to proliferation:

- Section 2 provides that an offence is committed where any person within the Bailiwick (or any British citizen within the Republic of Ireland) "unlawfully and maliciously causes by any explosive substance an explosion of a nature likely to endanger life or to cause serious injury to property… whether any injury to person or property has been actually caused or not".

- Section 3 provides that an offence is committed where any person within the Bailiwick, the UK, the other Crown Dependencies or the Overseas Territories, or any British citizen anywhere in the world, unlawfully and maliciously:

- Does any act with intent to cause, by an explosive substance, or conspires to cause by an explosive substance, an explosion in the Bailiwick or in the Republic of Ireland of a nature likely to endanger life or to cause serious injury to property; or

- Makes or has in their possession or under their control any explosive substance with intent to endanger life, or cause serious injury to property in the Bailiwick or in the Republic of Ireland, or to enable any other person to endanger life or cause serious injury to property in the Bailiwick or in the Republic of Ireland.

An offence is committed under section 3 irrespective of whether: (i) any explosion, in fact, occurs; and (ii) any injury to person or property has actually been caused.

The concept of an "explosive substance" includes: (i) any materials for making an explosive substance; (ii) any apparatus, machine, implement or materials used, or intended to be used, or adapted for causing, or aiding in causing, any explosion in or with any explosive substance; and (iii) any part of such apparatus, machine or implement.

Section 5 also creates an offence in respect of any person who "by the supply of or solicitation for money, the providing of premises, the supply of materials, or in any manner whatsoever, procures, counsels, aids, abets, or is accessory to, the commission of any crime under this Law".

PROLIFERATION FINANCING OFFENCES

Activities involving proliferation financing may constitute offences pursuant to:

- Section 66 of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002, which creates as number of ancillary offences (aiding and abetting etc) in respect of activity outside the Bailiwick relating to biological, chemical or nuclear weapons.

- Sections 8 – 11 of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 which contains a number of offences relating to the financing of terrorism. As noted above, the definition of terrorism could encompass activities relating to proliferation.

- Part II of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999, which creates a number of offences in connection with the acquisition, possession, use, transfer, concealment or retention of proceeds of criminal conduct, which could include proliferation and proliferation financing activities.

- The offence under section 5 of the Explosive Substances Law, 1939 referred to above.

The financial services and e-gambling regulators in the Bailiwick could also apply civil penalties to any action involving proliferation and proliferation financing on the part of businesses subject to their jurisdiction which comprises breaches of the applicable framework for AML and CFT.

Bailiwick reporting obligations relating to proliferation and proliferation financing

There are three sets of reporting obligations that are or might be relevant to proliferation and proliferation financing:

- Proliferation and proliferation financing suspicion reporting obligation: There is an obligation to report a suspicion of proliferation or proliferation financing to the Financial Intelligence Unit under the Disclosure (Bailiwick of Guernsey) Law, 2007. This should be done in the form and manner prescribed by the Disclosure (Bailiwick of Guernsey) Regulations, 2007.

- Sanctions reporting obligations: Under the Sanctions (Bailiwick of Guernsey) Law, 2018, there are reporting obligations in respect of sanctions regimes implemented in the Bailiwick that apply to financial services businesses and other parties subject to the AML and CFT framework. These obligations extend to knowledge or reasonable cause to suspect that a person is a sanctioned person or is linked to a sanctioned person, or has committed a sanctions breach. This includes sanctions relating to proliferation and proliferation financing. In some sanctions regimes, there are additional reporting obligations. For example, the obligations concerning the North Korea sanctions regime as implemented in the Bailiwick include a requirement for businesses to report to the Financial Intelligence Unit knowledge or reasonable cause for suspicion that a person is providing proliferation financing. Further guidance on those reporting obligations can be found on the States of Guernsey website.

- Money laundering and terrorist financing: As explained in response to Question 5, proliferation financing can involve elements of money laundering and terrorist financing. There is an obligation to report a suspicion of money laundering and/or terrorist financing to the Financial Intelligence Unit under the Disclosure (Bailiwick of Guernsey) Law, 2007 and the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002. If dealings with any person or entity give rise to knowledge or suspicion that another person is engaged in money laundering or terrorist financing, or reasonable grounds for such knowledge or suspicion, a disclosure should be made in the form and manner prescribed by the Disclosure (Bailiwick of Guernsey) Regulations, 2007 and the Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007.

Bailiwick implementation of UN and UK sanctions

There are three sanctions regimes in force in the Bailiwick that specifically concern proliferation and proliferation financing activities. These are the regimes imposed by the UN and UK that relate to the Democratic People's Republic of Korea (DPRK, also known as North Korea), Iran and to activities relating to Chemical Weapons. These regimes are summarised below.

DPRK / NORTH KOREA

The sanctions regime in relation to the DPRK is implemented in the Bailiwick by the Sanctions (Implementation of UK Regimes) (Bailiwick of Guernsey) Regulations, 2020.

These regulations implement the UK sanctions regime contained in Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019. The UK regulations implement the relevant provisions of the UN Security Council ("UNSC") Resolutions on the DPRK (and imposes obligations in the UK going beyond those UN Resolutions). A list of the relevant UNSC measures can be found here.

The UK regulations contain a wide range of sanctions, which include:

- Activity-based sanctions which prohibit conducting a number of activities with the DPRK and entities or individuals based in, or acting on behalf of, the DPRK. These activity-based sanctions are extensive, and cover a number of economic sectors. For example, there are restrictions and/or prohibitions on the purchase and/or supply of certain goods or services from the DPRK, ranging from sectors such as financial services through to transportation (including crewing) services. Given the wide scope of the activity-based sanctions in the DPRK sanctions regime, it is important for persons subject to Bailiwick law to check that they are not engaging in any prohibited activities relating to the DPRK.

- Targeted sanctions on individuals and entities designated under the UK regulations. The targeted sanctions consist of:

    - An asset freeze, which has the effect that all funds and economic resources belonging to or owned, held or controlled by any designated person shall be frozen, and no funds or economic resources shall be made available, directly or indirectly, to that person.

    - A travel ban, whereby a designated person is not permitted to enter or transit through the UK.

IRAN

The sanctions regime applicable to Iran concerning nuclear proliferation is implemented in the Bailiwick by the Sanctions (Implementation of UK Regimes) (Bailiwick of Guernsey) Regulations, 2020. There is a separate sanctions regime applicable to Iran in the field of human rights, which is not relevant to this guidance paper.

The regulations implement the UK sanctions regime contained in the Iran (Sanctions) (Nuclear) (EU Exit) Regulations 2019.The UK regulations implement the relevant provisions of the UNSC Resolutions on Iran (and imposes obligations going beyond those Resolutions). Details of the UN measures relating to Iran can be found here.

Most sanctions imposed on Iran concerning nuclear weapons proliferation were lifted following the Joint Comprehensive Plan of Action which came into effect on 18 October 2015. However, two types of sanctions remain in place:

- Trade restrictions on certain types of equipment, commodities and services; and

- Targeted sanctions (in the form of asset freezing and travel bans) against individuals and entities designated under the UK regulations.

CHEMICAL WEAPONS

The UK sanctions regime that relates to Chemical Weapons is implemented in the Bailiwick by the Sanctions (Implementation of UK Regimes) (Bailiwick of Guernsey) Regulations, 2020.

The regulations implement the UK sanctions regime in the Chemical Weapons (Sanctions) (EU Exit) Regulations 2019.

The Chemical Weapons sanctions regime imposes targeted sanctions, in the form of asset freezing and travel bans, on those individuals and entities designated under the UK regulations. The individuals and entities concerned are those persons designated by the UK as being responsible for, providing financial, technical or material support for, or are otherwise involved in, manufacturing or using chemical weapons, as well as those who assist and encourage such activities.

OFFENCES AND ENFORCEMENT

A person who infringes, or causes or permits any infringement of, any prohibition or requirement contained in the North Korea, Iran and Chemical Weapons sanctions regimes commits a criminal offence punishable with imprisonment and/or a fine, unless the activity in question is the subject of a licence from the States of Guernsey Policy & Resources Committee (or the Committee *for* Home Affairs in the case of trade sanctions).

These regimes also contain a prohibition on participating, knowingly or intentionally, in activities the object or effect of which is to circumvent sanctions.

Where a body corporate is guilty of an offence, and the offence is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, any director, manager, secretary or other similar officer of the body corporate, or any person purporting to act in any such capacity, that person as well as the body corporate is guilty of the offence and may be proceeded against and punished accordingly.

For further information on the enforcement of sanctions in the Bailiwick, including the possibility for individuals/entities subject to sanctions to apply for a licence to carry out an activity that would otherwise be prohibited, please consult the FAQ document produced by the Policy & Resources Committee.

OTHER SANCTIONS REGIMES AND FURTHER INFORMATION

In addition to the above, a number of other sanctions regimes imposed by the UN and UK are in force in the Bailiwick. Some targeted sanctions imposed under certain regimes (such as that applicable to Syria) may concern an individual or entity's activities relating to proliferation or proliferation financing.

Information on all sanctions regimes in force in the Bailiwick is on the official website for the States of Guernsey. All those subject to Bailiwick law should consult this site regularly, since sanctions regimes are updated and amended frequently. The website of the UK's office-of-financial-sanctions-implementation also has information and updates on all UN and UK sanctions regimes *Office of Financial Sanctions Implementation - GOV.UK (www.gov.uk)*

In addition, the States of Guernsey Policy & Resources Committee has produced a Frequently Asked Questions guide on the Bailiwick sanctions regimes.

Persons operating in the Bailiwick should also be aware of sanctions regimes in effect in other jurisdictions, since some of these regimes contain provisions that have some extra-territorial effect, so that they may apply to some of the parties involved in a Bailiwick transaction even if there is no nexus to that jurisdiction in the transaction.

In particular, individuals and entities in the Bailiwick should be aware of sanctions implemented by the EU and by the USA's Office of Foreign Assets Control (OFAC). Full details of the sanctions currently imposed by the EU can be found here; - www.europeansanctions.com. Full details of the sanctions currently imposed by the US can be found on OFAC's website which also contains a number of guidance documents and FAQs.

Some US sanctions (known as "secondary sanctions") apply to non-US persons even whether there is no US-nexus. This would encompass, for example, sanctions imposed on foreign financial institutions for facilitating significant transactions for or on behalf of any person that is subject to US sanctions under a relevant US regime. An example of secondary sanctions in the context of proliferation are those relating to Iran's nuclear proliferation activities. Details of these sanctions can be found on the dedicated section of the US Department of the Treasury's website relating to Iran.

The Bailiwick's export control regime

The Bailiwick's export control regime is contained in the Export Control (Military, Security and Related Matters) (Bailiwick of Guernsey) Order, 2010. Separate guidance issued by Guernsey Customs and Excise on export controls is at *Export Licence Controls - States of Guernsey (gov.gg)*. The guidance focuses primarily on applications for, and licensing of, the export of military goods, dual-use goods and goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment (collectively referred to as "strategic military and dual-use items"). It also highlights the controls on the exports of goods in relation to arms embargo, trade sanctions and other trade restrictions. This guidance is intended to assist exporters and their agents in understanding the requirements of the laws concerned with the export licensing of strategic military and dual-use items in the Bailiwick of Guernsey.

Other International obligations relating to proliferation and proliferation financing

Although they do not apply directly to individuals and entities, it should be noted that the Bailiwick complies with a number of international conventions and treaties. These include:

- International conventions or treaties that control or prohibit the proliferation of nuclear, chemical and biological weapons, such as:

    - Treaty on the Non-Proliferation of Nuclear Weapons, which seeks to prevent the spread of nuclear weapons and weapons technology, to promote cooperation in the peaceful uses of nuclear energy and weapons technology and to further the goal of achieving nuclear disarmament and general and complete disarmament.

    - Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction.

- Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction.

- UN Security Council Resolution 1540 (2004), which obliges States to take a range of actions to prevent and counter the proliferation of WMD, their means of delivery, and related materials. In particular, this Resolution:

  - Prohibits States from providing support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery.

  - Requires States to "adopt and enforce appropriate and effective laws which prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in them as an accomplice, assist or finance them".

  - Requires States to take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials.

- Other measures seeking to combat financial crime risks (including those posed by proliferation financing) such as the FATF Recommendations. A number of these recommendations have been given effect through the Bailiwick's implementation of sanctions and/or its AML and CFT regime.

Annex C: Glossary of terms used in this Guidance

Term	Definition
AML	Anti money laundering
CFT	Countering the financing of terrorism
Designated or listed person, entity or body	A person, entity or body that is subject to targeted sanctions pursuant to a sanctions regime.
Dual-use Goods	Goods that have legitimate commercial or industrial uses, and may also be used in WMD.
Financial Action Task Force (FATF)	The FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of WMD. FATF has developed a series of Recommendations that are recognised as the international standard for combatting money laundering, the financing of terrorism and the proliferation of WMD.
Front company	A company used to conceal the true end-use or end-user of traded goods and services, or the parties involved in a financial transaction.
Licence or Licensing	A licence is permission granted by the relevant licensing authority to undertake certain activities that would otherwise be prohibited by sanctions.
Means of delivery	Missiles, rockets and other unmanned systems capable of delivering nuclear, chemical, or biological weapons, that are specially designed for such use. This definition is taken from UN Security Council Resolution 1540 (2004).
Non-State Actor	Any individual or entity, not acting under the lawful authority of any State in conducting activities. This definition is taken from UN Security Council Resolution 1540 (2004).
Proliferation	Proliferation involves the illegal manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials. This definition is derived from a working definition of proliferation financing developed by the FATF, which is set out in full below.

Proliferation financing	The working definition of proliferation financing, developed by the FATF, is as follows: *"Proliferation financing" refers to:* *the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.*
Proliferation-sensitive goods and services	Encompasses a range of goods and services (including technology, software and expertise) that may be used in proliferation. This includes goods and services that have the purpose of being used in WMD, and those which may have another, legitimate, purpose (i.e. dual-use goods).
Proliferator	An individual or entity involved in activities relating to proliferation.
Related materials	Materials, equipment and technology covered by relevant multilateral treaties and arrangements, or included on national control lists, which could be used for the design, development, production or use of nuclear, chemical or biological weapons and their means of delivery. This definition is taken from UN Security Council Resolution 1540 (2004).