1. Introduction

Economic sanctions are implemented by governments and supranational bodies, including the United Nations, European Union, United States, and United Kingdom against individuals, entities, and countries. They are used to influence behaviour or achieve a foreign policy goal, such as countering criminal activity, human rights abuses, and terrorism. Sanctions typically impose restrictions on the provision of services or making funds available to, or require freezing assets of, individuals and organisations (known in the UK and EU as "Designated Persons"). They may bar trade with a country or an individual, or place restrictions on trade with specific sectors (e.g. nuclear technology with Iran) and goods or vessels.

2. Why are economic sanctions so important for an FI to manage?

Sanctions are imposed for significant political and trade reasons and are backed up by criminal penalties that are usually rigorously enforced. It is therefore important for FIs to know the potential impact of sanctions on them.

Breaching economic sanctions would have a significant adverse effect on the reputation of an FI and can lead to large fines or operating licenses being revoked. For example, in 2015, BNP Paribas was fined a record US$8.9 Billion for violating sanctions against Sudan, Cuba and Iran, deliberately stripping information from payment messages to avoid being detected by the US system ("payment stripping"). It was also prevented from clearing certain transactions in US$ for one year.

3. Best practice management for FIs: Risk-based Approach

FIs should ensure they establish risk-based and proportionate policies, processes and resources to identify, assess and manage sanctions risks in line international best practice including implementing customer and payment sanctions screening systems, as required, and according to risks assessed e.g. customer typologies, locations of operations/transaction activity and services or products offered. Outlined below is best practice guidance:

- Sanctions risk assessment & policy

Senior management should prepare a formal Sanctions policy or Standard Operating Procedure (SOP) which includes, *inter alia*, the following:

- A clear statement that the FI is committed to complying with relevant sanctions regulations (stating regulations and penalties for breaching);
- Outline responsibility for the policy and nomination of a responsible senior person;
- A requirement that employees promptly report and escalate any sanctions hits of a sanctions person or team experienced and equipped to assess whether the hit is a "true" or "false" hit;
- Written details of mandatory procedures of the sanctions screening system (customers/payments) and compliance procedures, including escalation and assessment of sanctions hits, reporting requirements (including to the regulator) and procedures for freezing accounts, obtaining licences and exiting customers/restricting activity where sanctions breaches are confirmed;
- Provision of regular training to employees;
- A clear statement that any breach will be considered an act of gross misconduct;
- Regular reporting requirements on effectiveness of implementation of the policy (to Board / senior management and regulators;
- Record keeping provisions

In order to design an effective sanctions policy and determine sanctions screening requirements, FIs should first assess the sanctions risks to which it is exposed and then (if required) create a sanctions compliance & screening programme proportionate to the size, geographical scope and activities of the firm. Considerations include:

FIs operations and shareholding/investors

- Location of the FIs operations/offices (including subsidiaries) – in or close to sanctioned countries;

- Risk of sanctioned individuals being employed by the company (permanent/contract);
- Risk of investors/shareholders being subject to international sanctions, especially international investors;
- Heightened sanctions risk from FI products & services e.g. international trade finance and correspondent banking;
- Currencies utilised e.g. if FI transacting in US$ then parties to customer payments must be screened against US OFAC sanctions watchlists.

Customers

- Location of customer business (international/domestic), transaction flows (countries/volume), shareholding/beneficial ownership;
- Types of customers and the business they engage in to assess potential for business dealings with sanctioned countries e.g. international customers/suppliers (e.g. shipping); dealing in high-risk products e.g. military equipment, oil & gas;
- Size of customer contracts and distribution channels.

Third Parties

- Risk of third parties to the FI (suppliers, consultants, introducers, intermediaries) being subject to international sanctions.

Based on the above, a policy or process should be developed setting out sanctions screening requirements with a nominated experienced senior compliance officer responsible for maintenance of the policy, liaison with the regulator, reporting and training.

It must not be assumed that because a potential FI has no apparent links to the US that the requirements of US sanctions regimes can be ignored. They are very wide

ranging and have extra-territorial reach. For example, the act of settling a transaction in dollars, or via a US bank, or a non-US bank with an office in America, may impose the FI to US sanctions.

- Sanctions screening

  Wolfsberg Guidance on sanctions screening defines sanctions screening as "a control used in the detection, prevention and disruption of financial crime and, in particular, sanctions risk. It is the comparison of one string of text against another to detect similarities which would suggest a possible sanctions match." Data derived from the FI's operations, like customer and transactional records, are compared to lists of names of sanctioned entities or locations. FIs can source lists directly from regulators, which are publicly available, or may use third party lists. Publicly available sanctions lists include: the United Nations Security Council (UNSC) sanctions lists, national lists (for instance, the United Kingdom's Consolidated List of Financial Sanctions Targets and the United States' Office of Foreign Assets Control (OFAC) Sanction Lists) and the European Union's Consolidated Financial Sanctions List. These lists are continuously updated, often daily, by the relevant regulatory body responsible for sanctions compliance, for example the Office For Sanctions Implementation (UK) and OFAC (US).

  FIs should use screening to detect and prevent sanctions breaches, making it a vital part of the FIs financial crime controls. Screening can help identify sanctioned persons and organisations, in addition to illegal activity to which FIs are exposed.

  Generally, FIs use two main screening controls: transaction screening and customer screening. Transaction screening identifies transactions that involve targeted persons or entities (this is usually real time (e.g. wire transfers) to ensure funds are not released until the sanctions screening of the transaction has been performed. Customer screening identifies targeted individuals or entities at the on-boarding stage and throughout the business relationship (e.g. monitor the FIs customer database daily, weekly, monthly against relevant sanctions lists – frequency dependent on the risk assessment). Concurrently, these are part of the internal controls that FIs can use to identify sanctions targets.

  In order to design an effective sanctions screening programme, FIs should first determine the sanction risks to which it is exposed (see above) and then create a

sanction screening programme proportionate to the size, geographical scope and activities of the firm.

In addition, essential aspects of a sanctions screening programme include:

- Establishing procedures that define what must be screened and how frequently, how alerts should be escalated and the procedure for dealing with incomplete or unreliable alerts and escalation of true hits for further analysis and if required reporting to the relevant regulatory authority. The procedures must also set out actions the FI needs to take in the event of identifying a connection with a designated individual or entity.
- Appointing responsible persons with relevant skills and experience.
- Undertaking a risk assessment in order to determine what and when to screen as well as which sanctions lists to screen against.
- Establishing a clear governance structure and decision-making process.
- Understanding strengths and limitations of screening controls. It is important for FIs to document the configuration of their screening systems to demonstrate that these systems are appropriate to manage the FI's specific sanction risks and any limitations.
- Regular and documented testing of the screening system.

Screening can be undertaken manually or via automated systems. Most larger FIs use sophisticated third-party sanctions screening systems like Dow Jones, Lexis Nexis and Refinitiv WorldCheck that provide automated sanctions screening and algorithms to obtain a best 'true sanctions hit'. Useful guidance on how to design, implement and maintain an effective sanctions screening programme can be found in the Wolfsberg Guidance on Sanctions Screening , Financial Services Authority – Financial Services firms' approach to UK financial sanctions (2009) (LINK), FATF – Guidance for a Risk based approach – the Banking Sector