Auditing a UK/European Bank's Sanctions Compliance Programme

By Samar Pratt (CAMS)
February 2019

Contents

1. Background and introduction

1.1 The objective of this paper is primarily to help UK/European bank auditors understand what a sanctions and embargoes compliance programme is (collectively known as "sanctions compliance programme"), what risks it is designed to mitigate, and how to audit it end-to-end effectively. This paper therefore describes the risks and controls that make up an effective sanctions compliance programme and sets out how to test controls end-to-end, as well as how to leverage effective risk-based sampling to assure that controls are effectively mitigating a firm's higher sanctions risks.

1.2 A secondary objective is to explore what bank auditors should consider when assessing their institutions' compliance with sanctions regimes and the effect on their auditing approach to updated sanctions laws. An example is the updated EU Blocking Regulation and re-imposition of US secondary sanctions in relation to Iran following the US withdrawal from the Joint Comprehensive Plan of Action (JCPOA). This paper therefore also explores what UK and European bank auditors should consider as a result of this ever-changing sanctions regulatory landscape.

2. What is a sanctions compliance programme and what risks does it help to mitigate?

2.1 In order to understand what a bank's sanctions compliance programme is, and the risks it is designed to mitigate, auditors need to first understand what financial or economic sanctions are and how they relate to their institution. Economic or financial sanctions are strategic tools employed by governments around the world (such as the UK and the US governments) and multinational bodies (such as the European Union and the United Nations) to apply pressure on a sanctioned party, which may be specific countries, specific governments, companies, sectors, or individuals that threaten their interests (e.g. through proliferation of weapons of mass destruction) or violate international norms of behaviour (e.g. commit human rights violations, drug trafficking, or acts of terrorism). Economic sanctions come in many guises, including asset freezes, import/export trade embargoes, travel bans, and other restrictions. They can be comprehensive in nature (i.e. prohibiting all commercial activity with regard to an entire country), or targeted (i.e. blocking transactions with particular groups, companies, or individuals)[1].

2.2 Banks operating in the EU are prohibited from carrying out certain activities wherever they are in the world in relation to a sanctioned party under EU legislation. As the EU implements all UN Security Council resolutions, a country's compliance with EU regulations also ensures its

[1] Council on Foreign Relations. (17 August 2017). What Are Economic Sanctions? Retrieved from https://www.cfr.org/backgrounder/what-are-economic-sanctions

compliance with the UN sanctions regime. Many EU countries, such as the UK, France, Sweden, and Switzerland, have also implemented autonomous local sanctions regimes that must also be complied with by banks operating in those jurisdictions. Licensing exemptions and authorizations to sanctions are typically administered by local government agencies such as the Office for Sanctions Implementation (OFSI) and the Export Control Joint Unit in the UK, the General Directorate of the Treasury in France, the National Board of Trade in Sweden, and the Federal Council in Switzerland[2].

2.3 Banks operating in the US, processing US dollar-denominated payments or other transfers of value, or dealing in goods of US origin will also need to comply with US sanctions, administered by the Office of Foreign Asset Control (OFAC). The US does not allow US persons[3] or US businesses and their foreign branches from transacting with sanctioned targets on the OFAC Specially Designated National and Blocked Persons (SDN) list. Foreign branches of US-based businesses and non-US entities that handle US-origin goods must also comply (e.g. in the case of Cuban sanctions). This also includes financial institutions that make US dollar transactions, such as banks based in Europe[4].

2.4 Banks that breach any of these sanctions programmes—particularly US sanctions—face significant fines, criminal prosecution, or revocation of banking licenses. Readers will no doubt have heard of the considerable monetary penalties levied against European banks by US authorities over the last 10 years[5]. Banks may also be banned from entering into certain types of financial transactions (such as US dollar clearing in the case of BNP Paribas in 2014) that could have a devastating effect on any bank's business[6].

2.5 International legislative frameworks for financial sanctions do not dictate what banks must do to achieve compliance with their legal obligations. However, various regulators around the world have issued guidance to help banks establish an effective sanctions compliance programme, such as the Financial Conduct Authority in the UK[7] and the Federal Financial Institutions Examination Council[8]. These guide UK and European banks with a nexus to the US

---

2 Eversheds Sutherland. (2018). European Union Global Sanctions Guide. Retrieved from https://sanctionsguide.eversheds-sutherland.com/countries/the-european-union/#map-europe-title

3 Per OFAC FAQs, all U.S. persons must comply with OFAC regulations, "including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S. incorporated entities and their foreign branches. In the cases of certain programs, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S.-origin goods to comply."

4 Eversheds Sutherland. (2018). European Union Global Sanctions Guide. Retrieved from https://sanctionsguide.eversheds-sutherland.com/countries/the-european-union/#map-europe-title

5 Refinitiv.com. (2019). Fines for banks that breached US sanctions. Retrieved from https://www.refinitiv.com/en/resources/infographics/fines-banks-breached-us-sanctions

6 Reuters. (30 June 2014). U.S. imposes record fine on BNP in sanctions warning to banks. Retrieved from https://www.reuters.com/article/us-bnp-paribas-settlement/u-s-imposes-record-fine-on-bnp-in-sanctions-warning-to-banks-idUSKBN0F52HA20140701

7 Financial Conduct Authority. (January 2019). Financial Crime Guide: A firm's guide to countering financial crime risks. Retrieved from https://www.handbook.fca.org.uk/handbook/FCG/1/1.html

8 Federal Financial Institutions Examination Council. (2014). Bank Secrecy Act / Anti-Money Laundering Examination Manual. Retrieved from https://www.ffiec.gov/default.htm

to establish and maintain an effective and documented sanctions compliance programme, to help them comply with applicable sanctions regulations and prevent financial crime around the world.

2.6 A bank's sanctions compliance programme must be commensurate with its global sanctions risk profile (based on its relevant products, services, customers, jurisdictions, and distribution channels) and risk appetite. The programme should identify areas of higher risk through a documented risk assessment and require appropriate governance and oversight, metrics, and reporting for effective ongoing monitoring and management and internal controls, including sanctions screening, escalation and reporting of sanctions matches, independent testing, training, and adequate, skilled resources to manage sanctions risks.

3. A conflict in law has arisen caused by the updated EU Blocking Regulation and the re-imposition of US Iranian secondary sanctions following US withdrawal from the JCPOA—what auditors should know and need to consider

3.1 Auditors need to be aware of risks posed to their financial institutions due to a new conflict in sanctions laws as a result of recent actions taken by: 1) the US government in withdrawing from the Joint Comprehensive Plan of Action (JCPOA) on Iran and re-imposing secondary sanctions; and 2) the EU's response by updating its Blocking Regulation to include certain US Iranian sanctions.

3.2 "Extraterritorial" or "secondary sanctions" relating to Iran can be imposed by the US on non-US persons for conduct that occurs entirely outside US jurisdiction. Secondary sanctions put pressure on third parties (i.e. EU banks and corporates) to stop their activities with the persons or countries targeted by US sanctions. Secondary sanctions are enforced through US persons (i.e. US banks) which are prohibited from transacting with any third party designated under the secondary sanctions. Non-US persons could be hit with a range of punitive measures, including being added to the SDN list, restricted from obtaining financing provided by US financial institutions, and essentially denied access to US dollar clearing facilities, all outcomes that EU banks and corporates would want to avoid.

3.3 The original EU Blocking Regulation introduced in 1996 was in response to the extraterritorial reach of certain US sanctions in relation to Cuba. The Blocking Regulation prohibited EU persons from complying with such US sanctions. Following US withdrawal from the JCPOA, the EU has updated the Blocking Regulation to include several of the US extraterritorial sanctions in relation to Iran that were re-imposed by the US in August and November 2018. Understandably, the EU is seeking to protect Iran-related business interests of European companies and individuals from US secondary sanctions. So the consequence of the United States' re-imposition of secondary sanctions targeting Iran and the EU's subsequent updating of the Blocking Regulation is that the respective laws are now directly in conflict. As a

result, all companies operating in the EU now have the daunting job of determining which of the two laws to comply with, as complying with one may result in automatic non-compliance with the other, opening them up to considerable legal risk.

3.4 According to the UK trade association for the UK banking and financial services sector, UK Finance, the potential consequences of non-compliance with the Blocking Regulation vary significantly across the EU countries, ranging from small fines to criminal prosecution and unlimited fines. In addition, anyone suffering losses because of an EU person's compliance with US sanctions in breach of the regulation can claim damages against the EU person[9]. So, if your bank adheres to US secondary sanctions relating to Iran in violation of the Blocking Regulation, it could be sued by its customers for doing so, increasing the risk of civil litigation. UK Finance has also commented that although the old EU Blocking Regulation has been in place since 1996, it has rarely been enforced and "to date has not been considered … to offer any real protection against US secondary sanctions". Indeed, the US authorities have historically not seen the Blocking Regulation as being an adequate defence to non-compliance with secondary sanctions[10]. The question that begs to be answered is why the EU has even bothered to update the Blocking Regulation at all, given that it is unlikely to offer any real protection against US secondary sanctions. However, considering the investments made by EU businesses in Iran since the JCPOA was signed, this could lead to an enhanced enforcement appetite in the EU to protect those investments[11]. One thing is for sure: what the Blocking Regulation and re-imposition of US secondary sanctions does appear to have achieved is to have added to the banks' burdens the need to maintain an effective sanctions compliance programme in light of the ever-shifting sanctions regulations. In the past, many UK/European financial institutions have sought to comply with both EU and US laws but are now faced with a dilemma as to how to proceed—particularly in any transactions with an Iranian connection.

3.5 The EU's appeal to the US asking for certain EU exemptions from Iran sanctions in relation, inter alia, to pharmaceutical products, healthcare, and maintaining banking and financing channels has been rejected[12]. Germany, France, and the UK have created a special financial channel to facilitate trade with Iran despite the re-imposition of US sanctions on Iran. The countries have created a "special purpose vehicle", or SPV, called Instex to enable international trade with Iran, although at the time of writing in January 2019, it is unclear how it will work in practice or indeed whether it will work[13]. However, the future of the regime created by the

---

[9] UK Finance. (11 July 2018). The EU Blocking Regulation—Issues and Considerations for the financial services sector. Retrieved from https://www.ukfinance.org.uk

[10] Allen & Overy. Iran sanctions and the EU Blocking Regulation: Navigating legal conflict. Retrieved from http://www.allenovery.com/publications/en-gb/lrrfs/cross-border/Pages/Iran-sanctions-and-the-EU-Blocking-Regulation-Navigating-legal-conflict.aspx

[11] Allen & Overy. Iran sanctions and the EU Blocking Regulation: Navigating legal conflict. Retrieved from http://www.allenovery.com/publications/en-gb/lrrfs/cross-border/Pages/Iran-sanctions-and-the-EU-Blocking-Regulation-Navigating-legal-conflict.aspx

[12] The Telegraph. (16 July 2018). Mike Pompeo rejects EU appeal for exemptions in sanctions against Iran. Retrieved from https://www.telegraph.co.uk/news/2018/07/16/mike-pompeo-rejects-eu-appeal-exemptions-sanctions-against-iran/

[13] Gov.UK. (31 January 2019). New mechanism to facilitate trade with Iran: joint statement. Retrieved from https://www.gov.uk/government/news/joint-statement-on-the-new-mechanism-to-facilitate-trade-with-iran

Blocking Regulation is in flux. This latest development in EU sanctions highlights the ever-shifting sands of sanctions regulations and the need for auditors to monitor how these changes and emerging risks affect their financial institution.

3.6 Auditors of UK/EU banks should find out what, if anything, their institution is doing about this issue.

- Does your firm know if it has exposure to Iran that falls within the crosshairs of US secondary sanctions?
- If your sanctions policy permits doing business with an Iranian nexus then this is an emerging risk area that must be monitored.
- What is your bank financial crime compliance team proposing to do about the exposure?

Possible approaches to this dilemma include obtaining an authorisation from the European Commission to enable firms to comply with both the Blocking Regulation and the targeted US secondary sanctions. The bar for obtaining these licenses is considered very high, however, which indicates that the EC is unlikely to issue these generously, as that would undermine the very purpose of the Blocking Regulation[14]. Alternatively, firms may opt to reject any particular transactions with an Iranian link relating to concerns other than the US secondary sanctions targeted by the Blocking Regulation, such as credit risk or money laundering concerns. Or, firms may choose to approach each scenario on a case-by-case basis given that US secondary sanctions do not prohibit EU persons from undertaking any/all activities with Iran—merely those activities that are targeted by the relevant US secondary sanctions as listed within the Blocking Regulation[15]. In the current environment, auditors of UK/EU banks with sanctions exposure to Iran should keep a close watch on this issue through engagement with colleagues in their bank's anti-financial crime team and by monitoring relevant UK, EU, and US government websites, to understand what approach is being taken and whether it is within their bank's risk appetite. This is a dynamic area with frequent change and needs to be a prominent aspect of the continuous auditing programme for each audit to be effective. Auditors should also add this topic to their quarterly business monitoring plan.

4. Key controls within an effective sanctions compliance programme and how to test them

Audit functions should identify and test controls that mitigate inherent sanctions risks to ensure that their firms are taking adequate steps to mitigate their exposure. This section outlines key controls that typically make up an effective sanctions compliance programme, as well as setting

[14] Allen & Overy. Iran sanctions and the EU Blocking Regulation: Navigating legal conflict. Retrieved from http://www.allenovery.com/publications/en-gb/lrrfs/cross-border/Pages/Iran-sanctions-and-the-EU-Blocking-Regulation-Navigating-legal-conflict.aspx

[15] Allen & Overy. Iran sanctions and the EU Blocking Regulation: Navigating legal conflict. Retrieved from http://www.allenovery.com/publications/en-gb/lrrfs/cross-border/Pages/Iran-sanctions-and-the-EU-Blocking-Regulation-Navigating-legal-conflict.aspx

out end-to-end test strategies and sampling approaches designed to help auditors assure that higher sanction risks are being satisfactorily mitigated.

4.1 Governance, organisational structure, and management information

A firm should maintain effective governance of the bank's sanctions compliance programme, which allows for the management of its sanctions risk in a timely and effective manner. Sanctions issues should be communicated and escalated across the firm, including all internal and external sanctions breaches, in a timely manner. Senior and knowledgeable staff should be appointed to sanctions roles with clear and appropriate reporting lines to escalate sanctions issues. Accurate, timely, and actionable sanctions-related management information is produced and reviewed to facilitate effective oversight of sanctions matters.

4.1.1 Test-approach considerations

- Review the terms of reference for each of the key committees, where sanctions issues are discussed, and verify that the committee has appropriate representation from senior management; that roles and responsibilities are appropriately documented; and that committees are required to meet sufficiently regularly to effectively oversee sanctions issues and that escalation processes to other senior committees have been established.
    - Obtain and review the minutes and meeting packs for a sample of key committee meetings, for example for the three most recent meetings, to assess whether the committee is operating effectively, as designed.

- Evaluate whether the procedures for communication, escalation, and reporting of sanctions matters across the firm have been implemented and facilitate a robust process outlining the types of information that require escalation and reporting, including potential internal and external breaches; roles and responsibilities for escalation and reporting top-down and bottom-up; and any applicable time frames.
    - Confirm that appropriate tools are in place to facilitate the bank-wide communication, escalation, and reporting processes, and that the procedures and processes are understood.
    - Test a sample of internal and external breaches and determine whether these have been escalated and reported as per the requirements in the bank’s procedures for communication, escalation, and reporting sanctions matters.

- Assess whether roles and responsibilities have been appropriately assigned, taking into account the level of seniority, experience, and knowledge necessary to carry out the sanctions officer role. Considering the following:
    - Someone is directly accountable for sanctions with appropriate seniority.
    - Areas of responsibility are clearly delineated.

- Review the sanctions target operating model in place and determine with senior staff whether there are sufficient personnel with the required skills in key sanctions roles.

- Assess whether key performance indicators (KPI) / key risk indicators (KRI) metrics and management information (MI) provide coverage of key sanctions risk areas and allow senior management to assess key controls, manage sanctions risk, and monitor compliance with risk appetite.

    - Review a sample of minutes and meeting packs of relevant meetings and committee discussions and evaluate the design of sanctions KPIs/KRIs to establish whether they allow for informed decision-making.

4.2 Risk appetite and risk assessment

Audit functions must review their firm's documented risk appetite statement, which should set out the level of risk (using both qualitative and quantitative measures) the institution is willing to accept to meet its business objectives, whilst also meeting the firm's global legal and regulatory obligations[16]. In addition, auditors must check that the bank has a sanctions risk assessment process in place, as part of an enterprise-wide risk assessment process, that measures the level of residual sanctions risk the bank is exposed to in order to highlight areas where corrective action is required to enable the bank to manage its sanctions risk exposure effectively.

4.2.1 Test approach considerations

- Obtain and review the Sanctions Risk Appetite Statement to confirm that it is clearly defined, and sets out a measurable risk tolerance and risk appetite for all material aspects of sanctions risk in accordance with the firm's enterprise risk management framework.
    - Obtain a sample of monthly risk appetite metrics to ensure that they are reported at executive committee meetings for discussion and are scrutinised. Where risk appetite level thresholds are exceeded, assesses whether there is swift and appropriate corrective action and associated reporting.

- Assess whether the sanctions risk assessment is conducted at least annually, on a stand-alone basis, or as part of an enterprise-wide financial crime risk assessment process.

- Review the risk assessment methodology to confirm:
    - It mandates the use of reliable data sources and is based on sound principles (e.g. mathematical, statistical, etc) and requires measurement of the inherent risk, control environment, and residual risk in line with the firm's structure (e.g. at country, line of business, or regional level, etc).

[16] US Office of the Comptroller of the Currency. (2014). OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations. Retrieved from https://www.occ.treas.gov/news-issuances/news-releases/2014/nr-occ-2014-117a.pdf

- Review the risk assessment inputs and outputs to confirm:
    - The methodology relating to inherent risk, control assessment, and residual risk produces inherent risk, control, and residual risk ratings across the assessment units that are consistent, comprehensive, and relevant to all stakeholders (i.e. local, line of business, regional, and global stakeholders).

4.3 Sanctions policies and procedures

Firms should have a "global" or "group-wide" sanctions policy that is aligned to its sanctions risk appetite and that is applicable globally across the firm. It may sometimes be appropriate for country-level sanctions policies to be developed, for example, for those jurisdictions that have additional sanctions requirements over and above the global sanctions policy. Procedures should be in place to support implementation of and compliance with policy requirements across the firm.

4.3.1 Test approach considerations

- Review the sanctions policy and supporting procedures to assure that they cover all key elements of a sanctions programme and reflect industry standards, the firm's risk appetite, and regulatory requirements and guidance.

- Ensure that the latest version of the policy is easily accessible to staff.

- Obtain a list of recent regulatory updates and check that these have been incorporated into the latest sanctions policy.

- Assess the governance process that ensures the sanctions policies and procedures are kept up-to-date and cascaded across the firm.

4.4 Staff training programme

Banks should provide annual sanctions training to all relevant employees. In addition, staff who perform functions considered higher risk for sanctions, such as roles that entail customer contact, processing customer transactions, or otherwise evaluating customer data, should be provided with additional targeted role-specific training which supplements the annual sanctions training.

4.4.1 Test approach considerations

- Assess the training plans for annual sanctions training and sanctions training for high-risk roles to ensure that this training is delivered to all eligible employees at an appropriate frequency.

- Review the training materials to ensure that they are sufficiently detailed and effective, and that they include a test with a pass grade in order to demonstrate comprehension.

- Verify that training material has been reviewed by the in-house legal department or external counsel to ensure that training contents comply with the legal and regulatory obligations with respect to sanctions.

- Evaluate how the completion of the training is tracked as well as the follow-up process for any training that was not completed within the prescribed time frames, including any consequences.

- Confirm that all eligible staff have received training within required time frames and, when staff has not been trained, that they are scheduled for future training. Or, explain why training will not be provided, and/or that appropriate follow-up has occurred with individuals who failed to complete mandated sanctions training.

- Obtain a list of employees who have been determined to be in a high-risk role, select a sample, and determine whether they have been correctly classified and whether they received appropriate training, within required time frames.

4.5 Sanctions screening and list management

Banks should screen new and existing customers and transactions against sanctions lists, on a risk-basis. Automated screening systems should be used as a key control, depending on the nature, scale, and complexity of the organisation, its jurisdictional footprint, its customer base, types of products and services, volume of transactions, and distribution channels[17]. Where automated screening systems are used, the bank should periodically test the integrity and effectiveness of these systems to ensure they remain effective. The bank should maintain a process for ensuring that all necessary external global and local sanctions lists and watch lists that are used in the screening process are complete, up-to-date, reflect changes made by relevant authorities, and are deployed correctly and in a timely manner, across the bank where required, to ensure that the bank screens against all applicable lists required by law and the bank's sanctions policy.

4.5.1 Test approach considerations

- Assess whether the firm uses appropriate screening processes given the nature, scale, and complexity of the organisation, its jurisdictional footprint, its customer base, types of products and services, volume of transactions, and distribution channels.

[17] Per the Wolfsberg Group's Wolfsberg Guidance on Sanctions Screening (2019), sanctions screening "is the comparison of one string of text against another to detect similarities which would suggest a possible match. It compares data sourced from an FI's operations, such as customer and transactional records, against lists of names and other indicators of sanctioned parties or locations". Retrieved from https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

    - Identify any businesses or locations where sanctions screening is undertaken manually and prioritise testing of these manual controls in locations with exposure to higher sanctions risks.

- Assess whether the design of the screening process complies with the firm's sanctions policy. For example, if the sanctions policy mandates the daily screening of new-to-bank and existing customers, ultimate beneficial owners and controllers, vendors, staff, and all cross-border transactions against specific lists issued by competent authorities, assess whether the screening process (manual or automated) is designed to do this.
    - Customise this test depending on the requirements of the firm's sanctions policy to ensure a comprehensive assessment[18].

- If available, review the bank's sanctions product risk assessment to ensure that all transfers of value have been risk-assessed to determine which ones should be subjected to automated sanctions screening.

- Review the process by which lists are selected for screening based on the firm's risk appetite, products, services, volume of transactions, customers, jurisdictions in which they operate, and distribution channels. As a minimum, UK and European banks that operate in Europe and offer US dollar-denominated products and services screen against lists produced by HM Treasury (HMT) in the UK, the EU, the UN, and OFAC. The bank may also be required to screen against other lists if they operate in countries that issue local lists.

- Check that the bank screens against all required lists. Although screening for politically exposed persons (PEPs) is outside the scope of this paper, the EU Money Laundering Directives now require identification of domestic PEPs as part of the CDD process and many firms use their sanctions screening system to also screen and identify PEPs within their customer book.

- Review controls over the firm's automated screening systems' filters to ensure that they are configured to screen against the correct lists and that these lists are complete, updated frequently to reflect changes made by relevant competent authorities, and deployed correctly and in a timely manner, across the bank where required.

- Assess controls over internal "good guy" lists (sometimes referred to as "white" lists), "grey" lists (sometimes referred to as "black" lists), and other exclusion rules to ensure that only authorised staff can modify these lists, that changes to the list are subject to "four-eye" input controls, and that the exclusion rules are revalidated periodically.

[18] Auditors should utilise the latest industry guidance on sanctions screening issued by the Wolfsberg Group to benchmark their institution's approach to sanctions screening. The Wolfsberg Group. (2019). Wolfsberg Guidance on Sanctions Screening. Retrieved from https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

- If input and review controls over lists are ineffective, review the "good guy" list to ensure that it does not contain sanctioned parties.

- Assess the process used by the business or financial crime compliance to test the integrity and effectiveness of name and transaction screening systems and completeness of sanctions lists, and whether this is tested at an appropriate depth and frequency.

    - To independently assess screening system efficacy to ensure that the systems generate alerts where required, auditors can create test files that contain names on sanctions lists and run them through the test environment of the firm's screening system filters to check that they are configured correctly and that alerts are generated where expected. If the audit team does not have the capability to do this type of testing in-house, it should consider using a specialist third-party vendor.

- Review data feeds into screening systems to ensure that customer and transactional data is transferred completely, accurately, and in a timely manner from upstream banking systems.
    - Review the quality of data that is fed into screening systems to identify any data quality issues that may impair screening efficacy. For example, missing or truncated names or addresses will impact name-screening efficacy. Missing or truncated originator or beneficiary information in payment messages will impact transaction screening efficacy.

- Review data controls to ensure that all alerts generated by the screening system are logged and tracked to resolution.

- Assess the use of machine learning technology in screening systems—if used as a sanctions analytics layer—to reduce the need to manually investigate false-positive alerts. The machine learns from historical dispositioning of alerts, triages the alerts, and reapplies learning to auto-close alerts, thereby presenting only the highly productive alerts for human review.

    - Ensure that the business back-tests auto-closed alerts at least monthly to ensure that the machine logic continues to be applied effectively.
    - Select a sample of auto-closed alerts and verify that the alerts that were auto-closed have minimal sanctions exposure and were therefore auto-closed appropriately and in accordance with auto-closure rules. If the audit team does not have the skills to do this type of testing in-house, it should consider using a specialist third-party vendor.

4.6 Alert investigation and escalations

Banks should investigate all screening alerts[19] within prescribed time frames or service level agreements (SLAs) and determine whether potential sanctions matches have been identified by reviewing all relevant internal and external data sources. Supporting records should be retained to demonstrate that such investigations are reasonably complete and adequately documented by detailing what has been checked, the outcome of those checks, and how they have informed the bank's actions. Monthly management information (MI) and metrics should be produced that report on the volume of alert investigations, including alerts that have not been investigated and those that remain open beyond agreed SLAs. The bank should identify backlogs in name and transaction screening alerts in a timely manner and escalate them to senior management. The bank should also produce management information to report progress on the resolution of backlogs, maintain appropriate remediation processes, and provide sufficient resources to promptly address backlogs as well as their root causes.

4.6.1 Test approach considerations

- Test the effective investigation of name screening and transaction screening alerts by obtaining a sample of alerts, including false positives, escalations, and true matches against sanctions and grey lists. For each level of the investigation process, assess whether procedures were followed and the correct outcomes achieved. Include an assessment of whether:
    - there is a clear and accurate audit trail of the investigation, outcome, and rationale;
    - the outcome for each alert is appropriate;
    - where alerts require escalation, they are escalated to the next level in a timely manner;
    - where true matches are identified, the true match process is followed and the customer's sanctions risk profile is reviewed and updated;
    - retained documents are easily accessible and retrievable; and
    - the bank complies with record-keeping requirements prescribed by the local competent authority or the sanctions policy.

- Interview investigators to assess whether they understand when they are required to block or freeze assets and when they should reject payments. Also assess whether they are familiar with the concept of sanctions circumvention and whether they have received training that would enable them to spot attempts to circumvent/evade sanctions. For

[19] Sanctions alert investigation processes can comprise of various stages. Some banks have three stages at Level 1, Level 2, and Level 3. Level 1 and Level 2 alert investigators undertake a four-eye maker/checker review of all alerts generated by the name screening or payment screening system. Level 1 alert investigators will follow procedures that guide them on how to assess whether or not each alert is a "true match" against a sanctions list. They use information within the body of the alert and other information relating to the term(s) that generated the alert, which could be for example a sanctioned country, a customer name, a counterparty name, a vessel name or dual-use goods that generated the alert. Once they have concluded on the likelihood of the match being a "true match" or a "false positive" against a sanctioned country, entity or individual or activity, they will escalate the alert to the next level for confirmation of their conclusion. The Level 2 investigators will independently re-perform the investigation. If they agree with the Level 1 conclusion of a "false positive", the alert is closed and no further action is taken. However, if Level 2 disagrees with Level 1's conclusion or agrees the alert is likely to be a "true match", the alert is escalated to Level 3 for a final decision. Level 3 investigators undertake the final stage of the investigations process to confirm whether an alert generated a true match or not and tend to be sanctions specialists with more advanced knowledge of sanctions regimes.

example, attempts by customers to resubmit payments that have previously been rejected by the bank by structuring them in a way to attempt to evade the bank's sanctions detection controls. See Section 4.7 below on circumvention controls.

- Verify that the bank produces and reviews at least monthly management information and metrics to monitor the effectiveness of the sanctions alert investigation process to identify and manage alert backlogs, as this represents open risk to the firm.

- If there are backlogs, query how long they have existed, how they are being addressed, and how they will be prevented.

- Consider the following criteria when selecting a risk-based sample of sanctions screening alerts to test. Note that this is not an exhaustive or prescriptive list and that audit teams should also take specific in-country risk factors into account for their sampling. Audit teams should consider using in-house data analytics teams or a specialist third-party vendor to review the data efficiently to identify the risk-based samples:
    - Alerts closed as "no match" within an overly short or overly long adjudication time;
    - For alerts closed as true matches, identify any relevant prior or later alerts and assess the respective adjudication decisions (to assess whether these alerts were closed as "no match" in error);
    - Customers who have a high number of payment screening alerts with regard to their accounts;
    - Payment alerts linked to customers with blocked accounts;
    - Alerts on customers with known sanctions exposure; and
    - Look for likely "resubmitted" payments that may be attempts to circumvent sanctions screening controls.

4.7 Circumvention controls

Banks should seek to detect and prevent sanctions evasion through the use of interdiction rules on transaction screening systems to flag potential attempts to resubmit previously rejected payments. Banks should complete a thorough investigation of any potential attempt made to evade sanctions controls which is documented by the sanctions team in conjunction with the legal department (where applicable) and includes the circumstances of the attempt and the involvement of any bank staff and entities. Confirmed sanctions evasion attempts identified by the bank should be reported to the relevant competent authorities as applicable.

4.7.1 Test approach considerations

- Understand what interdiction rules are in place in transaction screening systems to detect resubmitted payments and assess the process for regularly reviewing the rules to ensure that they are effective, accurate, and implemented in a timely manner to relevant customer accounts.

- Obtain a population of sanctions payment screening alerts for a period (12 months is recommended) and select a sample of blocked or rejected payments.
    - Test whether interdiction rules have been applied to all of the accounts of all of the relevant customers, and whether these rules generated resubmission alerts where appropriate, by looking at the customer's transactional history.

- Obtain a population of resubmission alerts and select a sample of these. Test the alerts to assess whether they have been adjudicated correctly and timely. Where a genuine resubmission/sanctions evasion attempt is identified, assess actions taken by the bank, including appropriate internal escalation and reporting, customer transactional lookbacks, customer exit consideration, and external reporting to the relevant competent authorities where applicable.

4.8 Handling true matches, freezing assets, and reporting obligations

The bank ensures that when a true sanctions match is identified, it is escalated across the bank, assets are frozen and reported externally to local authorities – consistent with legal and regulatory requirements.

4.8.1 Test approach considerations

- Establish whether there have been any sanctions policy violations or matches. Check that these issues have been escalated to the sanctions officer in line with policy, logged, and reported to appropriate authorities in line with legal and regulatory requirements.
    - Select a sample of customers and transactions that have been confirmed as being an individual or entity on a sanctions list or have violated specific activity-based or country sanctions, and assess whether the bank has taken appropriate follow-up actions as required by the relevant competent authority.

- Where there is no sanctions programme requirement in place to freeze assets, check that the sanctions officer directs the bank to act in accordance to the requirements of the bank's sanctions policy.

- Review the process for the management of blocked accounts and assess if this is in line with bank procedures and local regulatory requirements.

- Review the transactional activity for a sample of blocked or frozen accounts to assess whether they are effectively blocked or frozen.

- Assess the process for unblocking or unfreezing accounts, and if this is appropriate.

4.9 Non-screening sanctions controls

Banks should conduct an annual sanctions risk assessment of products and assess the effectiveness of non-screening sanctions controls where products are not subject to automated sanctions screening. Banks should implement a risk-based approach to customer due diligence (CDD) processes which facilitate the identification and assessment of sanctions risk, including changes in risk exposure through event-driven and periodic CDD reviews. The bank should retain a copy of the customer license for relevant transactions, with confirmation that the transactions are consistent with the terms and time frame of the license. If a bank breaches sanctions regulations, it should make timely disclosures to competent authorities in line with legal and regulatory requirements and take appropriate mitigating actions (such as root cause analysis to understand why the breach occurred, to identify required corrective actions, and transaction lookbacks to quantify the extent of the sanctions breach in relation to these customers).

4.9.1 Test approach considerations

- Review the bank's sanctions product risk assessment. For those products or services with high sanctions risk, determine whether risk is mitigated by screening or non-screening controls. Consider whether products or services allow higher-risk activities, such as cross-border movements of value or anonymity to any parties involved.

- Check that the bank's CDD procedures require the collection and recording in the core banking system of the minimum data points mandated in the sanctions policy to facilitate effective name sanctions screening.

- Confirm that the policies and procedures for CDD outline the key information to be collected for the assessment of sanctions risks of all customers:
    - Customer name and address
    - UBO and controller information for entities
    - Customer business activity/nature of business
    - Source of wealth/source of funds
    - Country of operation(s) including parent company and/or subsidiaries
    - Counterparties to transactions/deals
    - Any activity the customer has in relation to sanctioned countries (e.g. location of counterparties)

- Confirm whether CDD or sanctions procedures provide guidance on how to identify and assess both direct sanctions exposure as well as indirect sanctions exposure, and how that sanctions exposure should be calculated by the business.

- Determine if sanctions risks are effectively reflected in the customer risk rating methodology applied as part of the CDD process.

- Confirm that where a higher sanctions risk is identified during the CDD process, an appropriate enhanced due diligence process and related procedure is in place.

- Test a risk-based sample of customer files and verify that sanctions risk has been assessed appropriately and any indicia of sanctions risk have been identified and addressed by the business.

- Determine whether procedures are in place requiring a CDD review of a customer where sanctions-related events occur—for example, information on a rejected, blocked, or returned payment, received suggesting the customer's sanctions risk has changed, or the customer and/or connected parties are added to a sanctions list. Establish the circumstances where enhanced due diligence (EDD) is required, including a lookback review of a customer's transactional history.

- Identify whether any customers within the customer file sample should have been subject to a sanctions event-driven review, based on the criteria detailed within the procedures. For customers that should have been subject to an event-driven review, review the customer file and confirm that an effective review was undertaken by the business.

- Review procedures related to reporting regulatory sanctions breaches and evaluate whether this is sufficiently detailed, setting out roles and responsibilities, when to make a report, what information/documents are required to be retained, when to perform a transactional "lookback", and the escalation and approval path to be followed.

- Obtain a log of reports of regulatory sanctions breaches in the last 12 months and select a sample to check that procedures have been followed.

- For a risk-based customer file selection, consider selecting clients from the populations listed below. Note that this is not an exhaustive or prescriptive list and that audit teams should also take specific in-country risk factors into account for their sampling. Audit teams should consider using in-house data analytics teams or a specialist third-party vendor to review the data efficiently to identify the risk-based samples:
    - Non-resident customers based in high-risk countries bordering sanctioned countries
    - Customers who operate in high-risk industries or in dual-use goods
    - Customers with known sanctions exposure
    - Corporate customers operating in jurisdictions that permit business with sanctioned countries or that share a border with sanctioned countries
    - Customers who have had rejected/blocked payments or generated multiple sanctions alerts
    - Customers considered for exit due to sanctions exposure and who were subsequently retained
    - Customers with missing KYC information critical for effective sanctions screening

- Include high-, medium-, and low-risk rated customers; new-to-bank relationships; and more established relationships and customers from different business lines, depending on the scope of the audit

4.10 Lookbacks when sanctions matches occur using risk-based approach

Banks should perform comprehensive lookbacks of previous transactions involving a customer involved in a sanctions breach which is sufficiently retrospective and far-reaching to identify any other activity that may breach the bank's sanctions policy or applicable laws and regulations.

4.10.1 Test approach considerations

- Through interviews and reviews of the policy and procedure documents, establish when a lookback should be performed and what this entails. Assess if this is appropriate.

- Select a sample of payments that are adjudicated as true matches (either from the record of true matches or the population of transactions screening alerts) and review the transactional history of the customers to identify whether any previous payments relating to the sample of customers are in breach and whether these were identified by the lookback, if one was performed. Consider using in-house data analytics teams or a specialist third-party vendor to review the data efficiently to identify potential breaches.

5.0 Conclusion

In the current environment, auditors of UK/EU banks with sanctions exposure to Iran should keep a close watch on developments with the EU Blocking Regulation moving forward in order to understand what approach one's firm is taking and undertake audit work to ensure that it is within the bank's risk appetite. To test the effectiveness of a firm's sanctions compliance programme, auditors should adopt an approach that utilises risk-based samples designed to test a bank's sanctions compliance controls end-to-end to ensure that they are fit for managing and mitigating sanctions risks so that the firm remains within the risk appetite. Audit teams should consider using in-house data analytics teams or a specialist third-party vendor to review the data efficiently to identify the risk-based samples. Sanctions regulations are a dynamic area with frequent changes, so this topic needs to be a prominent aspect of the audit department's quarterly business monitoring plan to ensure that each sanctions-related audit is effective.

6.0 Sources

1. Council on Foreign Relations. (17 August 2017). What Are Economic Sanctions? Retrieved from https://www.cfr.org/backgrounder/what-are-economic-sanctions

2. and 4. Eversheds Sutherland. (2018). European Union Global Sanctions Guide. Retrieved from https://sanctionsguide.eversheds-sutherland.com/countries/the-european-union/#map-europe-title

3. US Office of Foreign Asset Control FAQs. Retrieved from https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_general.aspx#basic

5. Refinitiv.com. (2019). Fines for banks that breached US sanctions. Retrieved from https://www.refinitiv.com/en/resources/infographics/fines-banks-breached-us-sanctions

6. Reuters. (30 June 2014). U.S. imposes record fine on BNP in sanctions warning to banks. Retrieved from https://www.reuters.com/article/us-bnp-paribas-settlement/u-s-imposes-record-fine-on-bnp-in-sanctions-warning-to-banks-idUSKBN0F52HA20140701

7. Financial Conduct Authority. (January 2019). Financial Crime Guide: A firm's guide to countering financial crime risks. Retrieved from https://www.handbook.fca.org.uk/handbook/FCG/1/1.html

8. Federal Financial Institutions Examination Council. (2014). Bank Secrecy Act / Anti-Money Laundering Examination Manual. Retrieved from https://www.ffiec.gov/default.htm

9. UK Finance. (11 July 2018). The EU Blocking Regulation—Issues and Considerations for the financial services sector. Retrieved from https://www.ukfinance.org.uk

10., 11., 14., and 15. Allen & Overy. Iran sanctions and the EU Blocking Regulation: Navigating legal conflict. Retrieved from http://www.allenovery.com/publications/en-gb/lrrfs/cross-border/Pages/Iran-sanctions-and-the-EU-Blocking-Regulation-Navigating-legal-conflict.aspx

12. The Telegraph. (16 July 2018). Mike Pompeo rejects EU appeal for exemptions in sanctions against Iran. Retrieved from https://www.telegraph.co.uk/news/2018/07/16/mike-pompeo-rejects-eu-appeal-exemptions-sanctions-against-iran/

13. Gov.UK. (31 January 2019). New mechanism to facilitate trade with Iran: joint statement. Retrieved from https://www.gov.uk/government/news/joint-statement-on-the-new-mechanism-to-facilitate-trade-with-iran

16. US Office of the Comptroller of the Currency. (2014). OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations. Retrieved from https://www.occ.treas.gov/news-issuances/news-releases/2014/nr-occ-2014-117a.pdf

17. and 18. The Wolfsberg Group. (2019). Wolfsberg Guidance on Sanctions Screening. Retrieved from https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf