protiviti®
Global Business Consulting

SANCTIONS SERIES

Sanctions Risk Assessment: A Key Risk Management Tool

By Francesco Monini and Alberto Aniasi

Faced with the growing complexity of the geopolitical landscape, governments have been using financial sanctions increasingly as foreign policy tools to respond to developments as wide ranging as regional conflicts and wars, terrorism, and human slavery.

In today's highly charged geopolitical environment, sanctions compliance is a focus not only for financial institutions and regulatory authorities, but also for investors, the media and the public.

It is critical for financial institutions (FIs) to assess their exposure to sanctions-related risks and the adequacy of their control systems, both to avoid fines and penalties and to safeguard the institution's reputation.

FIs have been long accustomed to performing Anti-Money Laundering (AML) risk assessments under a regulatory framework that is more mature and globally aligned than the framework for managing sanctions. It was not until 2019 that the Office of Foreign Assets Control (OFAC), one of the most advanced sanctions

WHAT IS SANCTIONS COMPLIANCE RISK?

Probability of an individual or entity violating sanctions laws, directly or indirectly, through circumstances, layering, or other means. This violation may lead to legal or regulatory penalties, financial loss, or damage to reputation caused by the FIs' failure to comply with sanctions laws, rules, and regulatory compliance.

Source: OFAC Framework for Compliance Commitments

regimes, published its Framework for Compliance Commitments that highlighted the need for ongoing sanctions risk assessments. Since the release of OFAC's guidance, other regulatory bodies have expressed expectations, formally or through the examination process, that a sanctions risk assessment is foundational to an effective sanctions compliance program. Therefore, it is critical that a financial institution (FI) can articulate its sanctions risk assessment methodology and demonstrate the linkage between the risk assessment and its sanctions control framework.

A sanctions risk assessment (SRA) requires the evaluation of risks, controls, policies and procedures, data and information feeds, and alert review practices. The identification of gaps in critical controls and adoption of best practices can drive improvements in an institution's screening system and processes as well as in financial crime risk management. Typically, FIs seek to identify and quantify the inherent risk of a legal entity and its customers, products, services and geographic reach. They assign an inherent risk rating (generally using a three – or four-point scale of high, moderate, low, or high, medium/high, medium/low, or low). Next, they assess the effectiveness of controls designed to mitigate these risks by assigning a rating to identified control deficiencies (i.e., "not significant," "slightly significant," "fairly significant," "very significant"). An overall risk rating is then assigned based on assessment of inherent risk and the control environment. For institutions with multiple legal entities, a roll-up exercise provides a view of the organisation's consolidated sanctions risk. The accuracy and value of the SRA depends on many factors, described in further detail in the sections below.

Hot Topics for SRAs: Goods, Circumvention, Cryptocurrency

Arriving at the right answer often depends on asking the right questions, which in a risk assessment exercise corresponds with collecting complete and reliable data.

For example, FIs are expected to take a proactive approach toward managing the sanctions risks associated with specific goods, circumvention of activities, and cryptocurrency. To identify potential exposure, the following items need to be evaluated:

1. Specific Goods

a. **High Risk Sectors:** any sector that produces goods, software or technology (collectively referred to as "dual-use items") that can be used for civilian and military purposes, including the production of weapons of mass destruction.

b. **Banned Sectors:** specific industries or industry sectors that are often targeted with sanctions; these will vary depending on the circumstances but may include financial services, energy and/or luxury goods.

Control Framework: Consider strengthening controls over the acceptance and monitoring of trade-related business to include, for example, vessel tracking technology.

2. Circumvention

a. **Circumvention Hubs:** jurisdictions not currently subject to sanctions but friendly to sanctioned jurisdictions which might be used to avoid sanctions.

b. **Front Companies:** companies formed (often, but not exclusively in circumvention hubs) to disguise their ties to sanctioned parties.

Control Framework: Through analytics, determine whether there have been increases in new accounts and transaction activity with jurisdictions known to be friendly to sanctioned jurisdictions; ensure rigorous approach to identifying beneficial owners of shell companies and other potential front companies and consider, depending on the perceived level of exposure, using link analysis tools designed to detect hidden relationships.

3. Cryptocurrencies

a. **Anonymity:** the pseudo-anonymity of cryptocurrency has made it an attractive medium for sanctions evasion.

Control framework to consider: Ensure that due diligence and customer risk rating schemes appropriately consider the impact of the use of cryptocurrencies; develop and maintain advanced monitoring capabilities to identify and mitigate the risks of possible sanctions evasion.

Realising the Full Potential of the SRA

Forward-Looking and Actionable

A future-oriented perspective is essential for control frameworks to guide business decisions rather than just highlight past issues. Analysing industry trends, anticipating emerging scenarios, and integrating non-financial data into the risk assessment facilitate the identification of evolving threats and emerging opportunities. The most advanced frameworks even allow for simulations based on hypothetical scenarios that can drive business decisions.

If properly designed and interpreted, an advanced risk assessment exercise allows an FI to identify areas where there is a combination of significant exposure to sanctions and little mitigation from the control system. Being aware of where residual risk poses a greater threat, management can more confidently deploy resources for maximum effect.

Additionally, cross-functional collaboration between different business functions is crucial to exploit the full potential of a risk assessment exercise. The most direct connection is probably with an FI's risk appetite statements, which, in accordance with industry best practice and regulatory expectations, need to be clearly linked with the results of the FI's risk assessments. This forward-

looking perspective, fueled by an analysis of emerging trends and threats, can position FIs strategically to manage long-term risk successfully.

Clear and Concise Output

To ensure optimal usage of the SRA, it is important to obtain sufficient support and sponsorship. It is not enough to extract relevant metrics. The metrics must be easily understandable to stakeholders, including senior management and the board of directors, who did not participate in the risk assessment exercise and are not involved in sanctions risk management on a daily basis. Given demands on time for these individuals, it is imperative to convey two or three key messages that can be quickly and easily understood.

KEY MESSAGES FOR SENIOR MANAGEMENT AND THE BOARD

The financial institution's management body should be responsible for approving the financial institution's overall strategy for compliance with restrictive measures and for overseeing its implementation. All the members of the management body should be aware of the exposure of the financial institution to restrictive measures and its vulnerability to circumvention of restrictive measures.

Source: EBA Consultation Paper 2023/42

Best practices highlight the importance of simplifying and clarifying information to draw attention to key issues that require action. It's crucial to provide clear messages and avoid overloading these stakeholders with unnecessary information. To prevent this, it's essential to have concise reporting with only a few slides and include case studies that help them understand better the issues and requirements.

Attention should be focused on summarising the key messages and categorising issues as either relevant to the requirement or a deviation from policy. It's vital to communicate whether there has been a confirmed or probable breach, as this basic KPI immediately catches senior management and the board's attention.

Computational Methods and Advanced Technology

Efficiency: Leverage AML Risk Indicators for Sanctions Purposes

Learnings from AML risk assessment exercises can provide indispensable information for identifying and mitigating illicit activities. An obvious but important question is whether there are synergies between AML and sanctions risk assessments that can be used to minimise the need for additional data collection. Our experience suggests the answer to this question is "Yes" as it applies to consideration of inherent risk.

In many instances, the same risk indicators used for determining AML risks can be replicated for the SRA by assigning them a different weight. Geographic exposure plays a significant role in assessing both AML and sanctions risk. Certain products and services, such as trade finance, also have an impact on determining inherent risk. Even customer types come into play. For instance, an assessment of high-net-worth clients can be leveraged for both AML and sanctions.

Leveraging the AML risk assessment is highly recommended for financial institutions seeking to enhance their anti-financial crime strategies. This approach will improve the effectiveness of risk assessment exercises and will yield significant benefits, such as:

- **Risk Customisation:** An FI's self-assessment process can be customised by adjusting the weights of AML indicators to create the SRA component. This customisation allows for a tailored approach that includes the bank's specific characteristics and the particular features of each indicator. This is particularly useful when an indicator exhibits characteristics that make it risky from a sanctions perspective.
- **Adaptation to Sanctions-Specific Threats:** Depending on the prevailing legislation, attention must also be directed towards different criteria as some indicators are specific just for sanctions risk. For example, specific geographic areas might include countries considered higher risk for AML or sanctions purposes. Different perspectives may emerge from control system vulnerabilities, such as the assessment of screening capabilities.

Effectiveness: Using Advanced Statistics and Artificial Intelligence

As risks to the financial sector expand, so do the tools for identifying and managing these risks. Using statistical learning and artificial intelligence (AI) – in particular, machine learning – techniques can significantly enhance the accuracy of risk assessment at different stages of the process.

The use of these tools and methodologies brings several advantages, including:

1. The ability to handle large volumes of disparate data sets.
2. Identifying complex and implicit patterns and correlations within the data that may not be immediately evident through conventional statistical analysis.
3. Fine-tuning over time: methodologies can improve performance as they are updated with new data, reducing the need for human intervention to update risk assessment models.
4. Processing and analysing data at a significantly faster pace than traditional statistical methods: this can enable the generation of insights almost in real-time, allowing for timely decision making.

5. Adaptability to handle new types of data and risk scenarios: adaptability makes these tools and methodologies particularly useful in rapidly evolving environments, where they can effectively manage emerging data types and evolving risk scenarios.

To be sure, it is also necessary to consider the investments required, both in terms of economic resources to be deployed and in terms of staff upskilling. In this respect, there is no one-size-fits-all model: a solution can be purchased or developed in-house and, whatever the choice, technology will need to be tailored according to the specific risk profile of the FI. Economies of scale can be achieved by adopting tools that cover more than just sanctions-related obligations, for example. In almost all cases, technology can be adapted to address other risks and threats facing FIs, such as fraud and cyber risk.

Steps to Consider

FIs can take several proactive steps to improve their sanctions risk assessments:

Governance

- Define clear roles and responsibilities among the group, divisions/sub-holdings, legal entities and branches.
- Report results effectively and submit key message points to senior management and the board.

Methodology

- Refine calculation methods continuously to reflect the changing environment.
- Assess control frameworks on an ongoing basis and incorporate findings of the second and third lines of defence as well as regulators.
- Consider a comprehensive approach toward financial crime that combines other areas of risk management (e.g., bribery and corruption risks, fraud). Experience suggests there is considerable overlap between perpetrators of different types of financial crimes.

Data Quality

- Review processes, methods and guidelines to guarantee the consistency and accuracy of data.
- Implement both methodological and operational improvements to enhance data quality, and subsequently the reliability of assessments/evaluations.

Digitalisation

Invest in technology to support the sanctions controls framework: i) automation of time-consuming processes, ii) uploading and storing data in a dedicated database, iii) optimisation of human-intensive activities such as coherence checks and specific controls review and, iv) calculating and reporting the results. While there are obvious costs to investing in technology, over the long term these investments translate into greater operational efficiency and effectiveness.

Tool Development and Implementation, Vendor Selection

Among the key considerations when investing in or developing digital support are:

- **In-Depth Needs Analysis:** meticulously analyse requirements to gain a comprehensive understanding of the functional and regulatory necessities for the tools in question.
- **Custom Development:** depending on the size of an FI, consider bespoke or customisable software solutions that allow optimised processes and regulatory compliance.
- **Vendor Evaluation:** perform a rigorous assessment of potential vendors, considering technical expertise, industry experience, robust security practices, and post-implementation support.
- **Continuous Updates:** maintain a rigorous monitoring process of regulatory and technological developments to ensure that tools and vendors consistently align with the latest standards and industry best practices.
- **Cross-competencies:** consider vendors and professional services that can offer both best-in-class technological and regulatory compliance support to ensure adequate risk and regulatory coverage.

The bottom line: Gone are the days when an FI's SRA considered only the direct exposure of the FI and its clients to sanctioned jurisdictions, entities and individuals. SRAs today need to be multifaceted, actionable and dynamic

About the Authors

Francesco Monini is a Managing Director at Protiviti's Milan office, leading the FSI Audit & Compliance practice. In this capacity he supports numerous Italian and international companies in managing projects in Anti-Financial Crime, Compliance, Internal Audit and Risk Management. Francesco has gained Sanctions experience in part through managing projects in the banking and payments industries. Francesco is a board member of the ACAMS Italy chapter.

Alberto Aniasi is a Manager in Protiviti's Financial Services practice in Milan, with experience in the Financial Services industry, Project Management, Data Analytics and Modelling. Starting in Protiviti's London office, he has worked with several leading global financial institutions developing and implementing Sanctions risk models and control systems.

About Protiviti's Financial Crime Practice

Protiviti's Financial Crime practice specialises in helping financial institutions satisfy their regulatory obligations and reduce their financial crime risk exposure using a combination of anti-money laundering/combating the financing of terrorism and sanctions risk assessment, control enhancement, and change capability to deliver effective operational risk and compliance frameworks. Our team of specialists assists organisations with protecting their brand and reputation by proactively advising on their vulnerability to financial crime, fraud and corruption, professional misconduct, and other financial business risk issues.