WHITE PAPER

MORE THAN JUST SANCTIONS

HOW FINANCIAL INSTITUTIONS ARE IMPACTED BY THE SANCTIONS ON RUSSIA AND BELARUS

Financial institutions face significant legal, regulatory, operational and reputation risks related to their implementation of sanctions on Russia and Belarus and the world events that have led to these sanctions. These risks have implications across the financial crime compliance program and, more broadly, the entire organisation.

Foto: imanstu, iStock

protiviti®

Global Business Consulting

»Sanctions risk assessments will need to be updated to reflect changes in inherent risk and potentially the control environment.«

CORNELIA TOMCZAK
DIRECTOR PROTIVITI GERMANY

Not all financial institutions will face the same challenges managing these risks. Size, complexity, organisational structure, product and service offerings, and geographic footprint will be among the influencing factors. But many will find their ability to manoeuvre in this uncharted territory severely tested in the months to come.

SANCTIONS COMPLIANCE

Interpreting the many rounds of sanctions issued by governments across the globe, often with little or limited implementation guidance, will require significant investments of time and effort by compliance officers, counsel and other advisors. First and second line personnel will need to team to review client arrangements that are or may be subject to the sanctions, which in some instances may number in the tens of thousands.

Sanctions teams – many needing reinforcements – will be busy investigating and dispositioning increased numbers of alerts – both productive and non-productive. This process will require thorough, documented due diligence to evidence that a good faith effort has been made to interpret all the sanctions programs correctly, both as they apply to sanctioned parties and to related parties – directly and indirectly. Sanctions quality control teams will also need to step up their efforts, given a higher volume of activity, to review and validate the accuracy, comprehensiveness and rationale for dispositions.

For the true sanction hits, sanctions teams will need to comply with reporting and record-keeping obligations that may mean satisfying the requirements of multiple authorities in several jurisdictions and will also need, in certain circumstances, to deal with licensing requirements. And sanctions risk assessments will need to be updated to reflect changes in inherent risk and potentially the control environment.

As significant and numerous as these undertakings are, they do not come close to addressing all the attendant risks in the current environment.

OTHER IMPACTS

Here are some other – though not all – ways financial institutions are being impacted by current developments.

Risk strategy and appetite:
In just a few weeks, the world's geopolitical landscape has been radically altered, and will likely continue to change over the coming weeks and months in ways we cannot anticipate as the world presses forward into unprecedented times. Boards of directors and executive management will need to reassess and gain consensus quickly on their new risk strategies and risk appetites. Their deliberation must extend beyond consideration of the legal, regulatory and operational risks to a broader, and perhaps even more challenging, evaluation of reputation risk. The fundamental questions that need to be asked in every boardroom are:

- → Is it enough to just comply with legal and regulatory requirements or will others – customers, shareholders, regulators, as examples – expect us to do more?
- → What is our plan for rationalising, memorialising and disseminating our decisions?
- → What unintended consequences can we anticipate as a result of decisions we are making today?
- → In due time, when regulators or others look at the actions we took during these times, will they ask us, 'What were we thinking when we made that decision?'

»Changes in risk strategy and appetite will have a cascading effect.«

CORNELIA TOMCZAK

Changes in risk strategy and appetite will have a cascading effect, requiring changes to policies and procedures, country, customer and enterprise risk assessments, customer onboarding standards, transaction and surveillance monitoring, front- and back-office operations, training, testing, and more.

Management oversight:

Accountability and responsibility will need to be clear across the organisation, both for implementing the sanctions and for effecting changes to risk strategy and appetite. Project plans and status reporting will be important for keeping the board of directors, executive management and process owners apprised of the actions being taken. They will also prove valuable in demonstrating the organisation's good faith effort to its regulators and other stakeholders.

Staffing needs:

Capacity of account management teams, compliance, operations/back office (e.g. wire rooms, letter of credit processing), and even technology teams required to make system changes to support compliance and policy adherence will be stressed in some organisations. Therefore, having a good grasp of baseline volumes, trending and productivity will be an important input to establishing staffing needs during these turbulent times.

Staff training/awareness:

Changes in legal and regulatory requirements and in risk strategy/risk appetite need to be communicated clearly and in a timely manner to all three lines of defence. Ensuring that the first line understands the risks and the importance of their role is critically important to not soliciting or onboarding new customers or processing transactions that pose unacceptable risk. Socialising clear and concise internal communications on compliance and other required changes and expectations of targeted team members will be important for promoting awareness and establishing accountability. Personnel reassigned temporarily to back-fill in areas outside of their normal responsibilities will need more in-depth training and job aids to perform effectively.

Event-driven customer reviews:

Organisations that decide to adjust their risk strategies and appetites will need to perform event-driven reviews of their customers to identify those falling outside the organisation's updated tolerance. Where available, contextual monitoring tools can provide valuable information on relationships that should trigger customer reviews.

New review criteria (what are the data elements critical to the review?) will need to be established and decisions will need to be made about how these criteria are to be applied uniformly in global organisations. In some cases, this exercise is likely to expose or exacerbate weaknesses in organisations' customer due diligence programs, such as inadequate understanding of the breadth of a customer's business, operations and geographic reach. Conditions and procedures will need to be delineated for customer offboarding. Additionally, organisations will need to consider whether a suspicious activity/transaction report is warranted for customers that are exited.

PEP, negative news screening:
As quickly as events are unfolding, some institutions may decide they need to modify screening criteria, increase the frequency of PEP and negative news screening, and/or add resources to evaluate screening results in a timely manner. In some organisations, the Financial Intelligence Unit may be responsible for considering the importance and impact of these screening results, along with the market and law enforcement intelligence that it gathers.

Operations/back-office support:
Operations and back-office personnel responsible for processing transactions will need customised training on the requirements that apply to the specific products for which they are responsible and will need access to real-time support of legal and compliance departments to prevent processing delays.

Transaction monitoring:
Transaction monitoring systems and protocols may not only need to be revised, with greater focus on certain customer types, jurisdictions, products and services, to align with risk strategy and appetite modifications, but they also need to be assessed to ensure ongoing effectiveness in identifying potential evasion of applicable sanctions. As various regulatory bodies continue to draft guidance on updated risk scenarios and red flags, compliance programs should review and incorporate relevant scenarios and rules into their monitoring programs and document risk-to-rule mappings to help rationalise changes. In some cases, this may require conducting ad hoc queries of transaction activity until new rules and scenarios can be developed, tested and implemented.

Investigation of potential suspicious activity:
Investigation departments and teams may quickly find themselves overwhelmed with a spike in the number of cases as they are forced to deal not only with their standard workload, but also sanctions investigation cases, review of customer relationships to be terminated, and, likely, an uptick in internal referrals as front line and operations/back-office personnel raise more questions about the activity they are seeing.

> »It is important to have a defined process to deal with these breaches.«
>
> CORNELIA TOMCZAK

Control framework:
Depending on the program changes made, the control framework may require tactical changes in the first and second lines as well as changes in assurance activities, such as internal audit, second line testing and model validation.

Third-party risk management:
For those financial institutions that rely on third parties for any part of their sanctions or AML compliance programs, extreme care will need to be taken to ensure that third-party providers are made aware of program changes and are complying.

Handling of potential inadvertent breaches of sanctions regulations:
There is room for interpretation concerning specific sanctions regulations requirements. Moreover, decision-making parties may not always have current and complete client and transactional information at that point in time they must decide to release a transaction. Therefore, inadvertent sanction breaches may occur. If so, it is important to have a defined process to deal with these breaches. This process should include requirements for escalation, investigation, look back, determination of mitigating measures and reporting to a competent regulator, as warranted. Organisations should also take steps to capture and share the lessons learned from these breaches to prevent recurrence.

IN CLOSING

This all seems overwhelming, especially considering business as usual (BAU) activities must continue uninterrupted. Cyber security experts have warned that while the world is focused on detecting and preventing Russian cyber attacks, other bad actors, alone or through collaboration with the Russians, may seek to take advantage of the situation. It is not unreasonable to extend this same thinking to money laundering and terrorist financing – bad actors may well look to exploit real or perceived gaps in BAU compliance efforts given other priorities.

While there are few silver linings in the pandemic, it did reenforce something we have known for a long time – since Plato wrote The Republic in 380 BC, to be precise: Necessity is the mother of invention. Maybe now, when the impact of financial crime compliance across organisations has never been more obvious, is the time to start thinking more creatively about how we manage our efforts to fight financial crime in the future – how we can be more predictive and analytical, collaborate across an organisation and across the industry, and pivot more quickly to respond to world events.

ABOUT PROTIVITI'S FINANCIAL CRIMES PRACTICE

Protiviti's Financial Crimes practice specialises in helping financial institutions satisfy their regulatory obligations and reduce their financial crime exposure using a combination of AML/CTF and sanctions risk assessment, control enhancements, 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.

CONTACT US!

CORNELIA TOMCZAK
Director Protiviti Germany
+49 172 2891382
cornelia.tomczak@protiviti.de

BERNADINE REESE
Managing Director Protiviti UK
+44 (0)207 0247 589
bernadine.reese@protiviti.co.uk

www.protiviti.de

protiviti® Global Business Consulting