Control Risks

ROUNDTABLE March 2019

SANCTIONS COMPLIANCE & ENFORCEMENT

Today, companies have to navigate a complex global sanctions landscape. Two key trends which have emerged in recent months are an increase in targeted sanctions to achieve strategic geopolitical goals and a number of enforcement cases that indicate higher standards for sanctions-related due diligence. Given ongoing global economic and political instability, companies need to assess and enhance their sanctions compliance structure. ■

THE PANELLISTS

Henry Smith
Partner, Control Risks
T: +44 (0)20 7970 2100
E: henry.smith@controlrisks.com
www.controlrisks.com

Henry Smith is the head of the Europe and Africa business intelligence and due diligence practice at Control Risks. Mr Smith leads a team of country experts and business intelligence specialists in London, Nairobi, Johannesburg, Lagos, Berlin, Moscow, Amsterdam, Paris and Milan. He was based in the UAE for five years and led Control Risks' Iran practice.

Judith Alison Lee
Partner, Gibson, Dunn & Crutcher LLP
T: +1 (202) 887 3591
E: jalee@gibsondunn.com
www.gibsondunn.com

Judith Alison Lee is a partner in the Washington, DC office and co-chair of the firm's international trade practice group. Ms Lee practices in the areas of international trade regulation, including US Patriot Act compliance, economic sanctions and embargoes, export controls and national security reviews (CFIUS). Ms Lee also advises on issues relating to virtual and digital currencies, blockchain technologies and distributed cryptoledgers.

Eva Monard
Partner, Jones Day
T: +32 (2) 645 1510
E: emonard@jonesday.com
www.jonesday.com

Eva Monard has 10 years of experience in more than 60 anti-dumping, anti-subsidy, and safeguard investigations in over 10 jurisdictions. She advises clients on obligations under EU export control laws and sanctions, assisting them in setting up compliance policies and assessing the compliance of specific transactions with their obligations to dual-use goods and sanctions. Her practice focuses on WTO law, EU trade law, export controls, sanctions, foreign investment screening, customs law and EU competition law.

Bryce Bittner
Director of Global Trade Compliance, Textron
T: +1 (202) 637 3815
E: bbittner@textron.com
www.textron.com

Bryce Bittner is the director of global trade compliance at Textron Inc. in Washington, DC. He oversees compliance with the export control and sanctions laws for Textron's family of companies. Mr Bittner graduated from Columbia Law School and Columbia School of International and Public Affairs with a joint JD/MIA in 2006. He is admitted to the Maryland State and District of Columbia Bars.

Priya R. Aiyar
Partner, Willkie Farr & Gallagher LLP
T: +1 (202) 303 1189
E: paiyar@willkie.com
www.willkie.com

Priya Aiyar is a partner in the litigation and global trade and investment groups at Willkie Farr & Gallagher. She represents financial industry clients in a range of regulatory, compliance and enforcement matters, as well as litigation and investigations. Prior to joining Willkie, she was acting general counsel at the US Treasury Department, where she advised the secretary and other senior officials on issues related to domestic finance, international economic affairs and financial crimes enforcement.

FW: Could you provide an overview of today's global sanctions landscape? What key developments and trends have unfolded in recent months?

Monard: Today, companies have to navigate a complex global sanctions landscape. Western countries, the US and European Union (EU) in particular, have several well-established sanctions measures on myriad countries. Of these, two key relevant programmes are those on Russia and Iran. With respect to Russia, US sanctions are wider than EU sanctions, and could potentially have severe consequences for EU companies. While EU sanctions on Iran have been rather limited since the nuclear agreement was reached, the US has reimposed its Iran sanctions, which also have certain extraterritorial effects that can impact EU companies. The entire situation is exacerbated by the adoption by the EU of the Blocking Regulation, which in essence prohibits EU companies from complying with extraterritorial US sanctions.

Lee: The past 12 months have been extraordinarily busy for US sanctions policy. The year's major development was, of course, the reimposition of US nuclear-related sanctions on Iran. But there has also been a steady drumbeat of activity on other fronts, including the designation of dozens of Russian oligarchs and senior officials, as well as the gradual ratcheting up of sanctions on the Maduro government in Venezuela. Over the past year, we have also seen an increasing willingness on the part of the Office of Foreign Assets Control (OFAC) to sanction economically significant entities like Rusal and PdVSA. Moreover, approximately 1500 individuals and entities were added to the specially designated nationals (SDN) list during 2018 – 50 percent more than in any previous year – suggesting that sanctions are likely to remain a major part of the US foreign policy landscape.

Bittner: Over the last 12 months, the US has continued to actively enforce and expand its sanctions programmes. Two main trends seem to have arisen lately – an increase in targeted sanctions to achieve US strategic geopolitical goals, and several enforcement cases that indicate that OFAC is setting higher standards for how companies should conduct sanctions-related due diligence.

Aiyar: As with previous years, we are seeing a pattern of rapidly changing sanctions programmes, including the expansion of sanctions on some targets, while easing on others, as foreign policy goals shift and develop and presidential administrations transition. Recently, the Trump administration designated Petróleos de Venezuela, S.A. (PdVSA), Venezuela's state-owned oil and natural gas company, in an effort to cut the Nicolas Maduro regime off from its primary source of revenue. This is in line with the administration's goal of pressuring Maduro, whose government the US views as illegitimate, into stepping down from leading Venezuela. However, the administration recently lifted sanctions on the Russian aluminium company Rusal, the second largest aluminium supplier in the world, and its affiliates due to the divestment of its previous majority owner, Oleg Derepaska.

Smith: Geostrategic competition makes UN Security Council consensus harder to achieve, and enforcement increasingly reflects geopolitical agendas. The US has expanded the scope and number of sanctions designations, and it is increasingly weaponising them, particularly secondary sanctions, for foreign policy aims. There is a divergence, though, between the executive and Congress about when to use sanctions, and what different country-specific sanctions attempt to achieve. The EU is taking steps to insulate European trade with very important markets, namely Iran and Russia, from US sanctions, and to increase its economic independence. Differences between the US and its traditional allies in the EU are making companies' decisions about whether to comply with different sanctions regimes more complicated. Country agnostic, extraterritorial sanctions regimes are emerging. 'Magnitsky' sanctions have been adopted in the US, UK and Canada, and are under consideration in the EU. These target individuals associated with human rights abuses and corruption.

FW: Drilling down, what specific compliance and enforcement issues are companies facing in the current market? Could you highlight any recent examples of penalties applied for non-compliance?

Lee: When it comes to sanctions enforcement, we are seeing an increasing trend toward coordination among enforcement agencies. In one particularly striking example, Société Générale, in November 2018, entered into a $1.34bn global settlement with multiple regulators for processing transactions over a five-year period involving a range of sanctioned persons and jurisdictions. The settlement with Société Générale, just like the recently filed indictment against Huawei, underscores the seriousness with which US enforcement agencies view deliberate efforts to conceal transactions with sanctioned parties.

Bittner: The first trend is evidenced by OFAC sanctions on Oleg Deripaska and his companies in April 2018 and on PdVSA in January. The former, imposed on Mr Deripaska for his close relationships with the Russian Federation, resulted in a significant restructuring of En+ Group plc, UC Rusal plc and JSC EuroSibEnergo to reduce Mr Deripaska's holdings. The latter sanctions on PdVSA arose in response to political activity by president Maduro in Venezuela, although it is too soon to predict the impact these measures will have. The second trend is based on the Epsilon, Cobham and E.l.f. cases. Epsilon, which was an unusual sanctions case because it was appealed up to the DC Circuit Court, held that OFAC only needs to show that a company had a 'reason to know' that a product would be re-exported to an impermissible country or recipient, not that the product was actually re-exported to such a destination. Therefore, companies need to understand not only who their customers are, but also take reasonable steps to understand what their customers will be doing with the products. The Cobham case demonstrated that a list-

based screening software programme may not be enough to avoid sanctions risk, especially with respect to entities owned by listed entities. In this case, senior trade compliance officials at the company approved sales to a customer owned by a specially-designated national, even though the owned company had a similar name to the SDN. Lastly, the recent E.l.f. Cosmetics case involved sourcing fake eyelashes from Chinese suppliers that obtained material from North Korea. In the settlement documents, OFAC highlighted the need for companies to understand sanctions risk along their import supply chain and take measures to mitigate sanctions risk.

Smith: Firstly, it is important to understand whether third parties pose sanctions risks by virtue of their ownership and control structures, and their broader business relationships. This is typically addressed through enhanced due diligence, and as recent enforcement cases demonstrate, it needs to be applied to a company's entire supply chain. Secondly, understand the nationality of your employee base and which sanctions these employees should comply with. Thirdly, ensure currencies used in transactions – primarily the US dollar – do not inadvertently create sanctions exposure. And finally, understand whether goods and services can be provided in a specific jurisdiction without violating sanctions.

Monard: The most problematic compliance and enforcement issue for EU companies today relates to the potential for Iran-related business, where they may find themselves between a rock and a hard place. On the one hand, there are significant risks under the US Iran sanctions, and especially the extraterritorial effects thereof. This has recently been highlighted by certain high-profile cases of foreign companies facing enforcement actions in the US related to the Iran sanctions. On the other hand, the EU Blocking Regulation prohibits them from complying with some of these US Iran sanctions. They can face enforcement actions in respective EU Member States for violations of the Blocking Regulation, but can also face actions for damages by private persons.

FW: Have you observed any significant shift in enforcement trends? How aggressively are regulators punishing companies which violate the rules?

Monard: Traditionally, the enforcement of sanctions in the EU has been limited, especially as compared to the number and level of enforcement actions in the US. Similarly, enforcement actions under the Blocking Regulation have been very rare. Nevertheless, it cannot be excluded that this will change as there is an increasing focus on sanctions regimes. Moreover, the possibility for claims for damages by private parties significantly increases the risks associated with possible violations of the Blocking Regulation. Regarding the US, there does seem to be a shift in enforcement trends, with an increasing focus on violations by companies in third countries, in particular with respect to Iran. The consequences can be many, including, but not limited to, hefty fines, being cut out of the US market and potentially prison sentences.

Smith: We have been seeing greater enforcement action in the US against companies outside the financial services sector. Multinational banks processing US dollar payments were the main focus of enforcement action a few years ago, with several high-profile cases, though the subjects of enforcement are now much broader. This is partly a result of US agencies broadening who they are considering, though it is also a reflection that many multinational banks have increased their resourcing of sanctions compliance.

Lee: Through seven enforcement actions in 2018, OFAC netted over $71m in penalties. While the number of OFAC enforcement actions and penalty totals for 2018 are lower than their 2017 counterparts, 2018 was another significant year in the enforcement of US sanctions programmes. How aggressively individual companies are being punished depends heavily on the particular facts and circumstances of each case. In early February, E.l.f. Cosmetics was fined almost $1m for a handful of transactions involving North Korea, a fairly light penalty which takes into account the fact that the company self-disclosed and the conduct was not egregious. By contrast, US regulators have aggressively pursued companies found to have engaged in repeated and wilful violations of US sanctions and export controls. The most

> "IN ADDITION TO TRADITIONAL HIGH-RISK SECTORS LIKE FINANCIAL INSTITUTIONS AND INSURANCE COMPANIES, PRIVATE EQUITY (PE) FIRMS SHOULD BE PARTICULARLY MINDFUL OF THE ACTIVITIES OF THEIR INVESTMENT COMPANIES OVERSEAS."
>
> PRIYA R. AIYAR
> Willkie Farr & Gallagher LLP

striking example is ZTE, which last year faced a denial order by the US Commerce Department, which would have effectively put the company out of business, but for high-level intervention by president Trump and Chinese president Xi Jinping.

FW: Are any industries or sectors at greater risk of breaching sanctions? If so, what factors are behind this heightened exposure?

Bittner: The banking industry is always at high risk of sanctions, and in 2018 two of the largest settlements involved JPMorgan Chase and Société Générale S.A. for processing illegal transactions. However, recent enforcement cases show that any company with an extensive import supply chain or export sales channels needs to understand where its supplies are coming from, what measures its partners are taking to prevent violations of US law, to the extent they are subject to it, and who the ultimate end-users of its products will be, to the extent knowable.

Aiyar: In addition to traditional high-risk sectors like financial institutions and insurance companies, private equity (PE) firms should be particularly mindful of the activities of their investment companies overseas. Sanctions regimes can be very complex, and thus PE firms require an up-to-date understanding of sanctions and government views on policy and enforcement in order to invest wisely and maintain compliance. Every firm that does business overseas should have established and updated compliance and due diligence procedures.

Smith: There are certain sectors that are likely to pose more sanctions risks than others, due to their economic and political importance, as well as their reliance on the international financial system. Defence, energy and financial services stand out. Beyond these sanctions, business models make the greatest difference to sanctions exposure. If sales and route to market are reliant on intermediaries, such as agents and distributors, then it can be difficult for a compliance team to pre-empt, monitor and detect potential sanctions violations, including diversion, fraud and other integrity risks. If an organisation has a large population of third parties that are geographically dispersed, then this is very challenging. This means that companies in consumer goods and healthcare, despite not being sectors that are explicitly sanctioned, also need to think about sanctions risk exposure. Compliance teams need to take it upon themselves to understand their business model and to conduct appropriate risk assessments of their supply chains. This is clear from recent OFAC enforcement cases.

> THE BANKING INDUSTRY IS ALWAYS AT HIGH RISK OF SANCTIONS, AND IN 2018 TWO OF THE LARGEST SETTLEMENTS INVOLVED JPMORGAN CHASE AND SOCIÉTÉ GÉNÉRALE S.A. FOR PROCESSING ILLEGAL TRANSACTIONS.
>
> BRYCE BITTNER
> Textron

Lee: Energy companies and financial institutions are both at increased risk of violating sanctions. In the case of energy companies, it is primarily a function of the corners of the world in which they do business. Iran, Russia and Venezuela all have huge oil deposits and active US sanctions programmes. Similarly, financial institutions face heightened sanctions risks by virtue of the enormous volume of transactions they handle and the role they are expected to play in policing illicit financial flows. As a result, when financial institutions violate sanctions, they may be subject to record-setting fines, like those imposed against Société Générale and BNP Paribas. Because of the central role of the dollar in clearing transactions, financial institutions are also uniquely vulnerable to the threat of being cut off from the US market.

Monard: An area where we typically see a lack of awareness of potential risks by companies is in the context of trade in software or intangible technology transfers. Whereas companies engaging in trade of physical goods are typically more aware of sanctions-related issues, since they have to go through the entire customs process and are therefore in any event more mindful of the regulatory environment related to their exports, companies trading software or transferring technology through electronic means do not always realise that they are exporting a product and that there could be sanctions-related risks. It is always important to know your customer, and especially the location of your customer, even if you are selling software or services through electronic means. Similarly, intra-company transfers of know-how can also lead to risks under sanctions and trade controls.

FW: What are the key elements of an effective sanctions compliance programme? What steps do companies need to take to ensure they are not dealing with prohibited persons, entities or jurisdictions?

Aiyar: At the outset, businesses should have an awareness of the need for compliance with sanctions and the potential consequences of violating them. Businesses should conduct careful due diligence on investment, deal and partnership opportunities at the earliest stage of a transaction to ensure that the target has no relationship with SDNs or businesses in a sanctioned country that could potentially expose the business to a violation. In terms of compliance programmes, businesses should establish written compliance policies and procedures, screen potential partners and customers against the SDN List and other US and European sanctions lists, escalate high-risk transactions to compliance personnel for review, and firewall US persons, including US banks, from transactions that may involve a US-sanctioned country or an SDN.

Lee: A strong sanctions compliance programme generally includes a number of key features, including an organisational commitment to compliance, with support from the company's senior-most leaders, sufficient human and financial resources, well-developed compliance policies and procedures, broad education for all employees and detailed training for those employees most likely to encounter sanctions-related risks. As a minimum, companies will want to gather detailed information about their counterparties, deploy robust screening software and then regularly screen their potential counterparties against all applicable sanctions lists, including those administered by the US, the UK, the European Union and the United Nations.

Monard: It is of key importance for companies engaging in international trade to have an effective sanctions compliance system in place, which should be reviewed and reassessed on a regular basis. Sanctions compliance should be in the same group as other export control compliance and sanctions compliance, and managed by the same head. It should be managed by logistics, with the assistance of legal in all steps of the process. While having IT systems in place is essential, it is equally important to regularly train and inform staff of the compliance policy in place. This should be complemented with folders or handbooks with detailed instructions. A compliance officer should be available for staff to turn to with any questions they may have. Additionally, it is crucial that the identity of customers – and their owners, controlling entities and directors – is always verified and companies should be especially diligent when screening new customers. Finally, extensive records should always be kept in order to be in a position to demonstrate that reasonable steps were taken to ensure compliance. It is equally important that at least one individual within the company, the in-house counsel or compliance officer, keeps close track of changes in international sanctions.

Smith: An effective sanctions compliance programme has shared characteristics with other financial crime compliance programmes, including clear policies and processes and tone from the top. Responsibilities should be clear and employees enabled to deliver these. Furthermore, the programme should be responsive to changes in the organisation's business model and its external environment. This external environment is challenging, given the more regular use of sanctions by different governments and the inconsistencies between different regimes. As such, compliance teams should work closely with political risk and government affairs teams. Determining whether people and entities that you are considering a business relationship with expose you to sanctions risks is achieved through sufficiently detailed due diligence. It is critical to be clear on an entity's ownership and control structure, and ultimate beneficial owners, particularly considering the US' '50 percent rule' for entities controlled by sanctioned persons.

Bittner: Many expect OFAC to issue compliance guidelines later this year which will explain what it deems to be an effective compliance programme, but in the meantime, it is possible to make reasonable predictions from recent enforcement cases. First, the ZTE case made it very clear that lying to US government officials, or intentionally violating US export control and sanctions laws, will result in astronomical penalties. But even those companies that believe they have effective sanctions compliance programmes in the form of third-party screening software may want to consider adding tools to look deeper into ownership or control of their customers, partners and suppliers. It might also be a good idea to regularly test your screening tools to ensure that they

> "IT IS CRUCIAL THAT THE IDENTITY OF CUSTOMERS – AND THEIR OWNERS, CONTROLLING ENTITIES AND DIRECTORS – IS ALWAYS VERIFIED AND COMPANIES SHOULD BE ESPECIALLY DILIGENT WHEN SCREENING NEW CUSTOMERS."
>
> EVA MONARD
> Jones Day

are catching relevant hits, and ensure that your business partners have policies and procedures to minimise sanctions risk to the extent practicable.

FW: What strategies can companies deploy to ensure they do not engage in supplying, shipping or insuring prohibited goods, such as military and quasi-military goods?

Smith: Export-controlled items, such as military and dual use items, are explicitly defined by a series of multilateral control regimes. Companies may need to classify and screen goods against the control lists to ensure they do not violate a sanctions regime, such as an arms embargo, as well as to determine if they require an export licence for a given jurisdiction. Sanctions can also control the end users and end uses for goods, particularly dual use items that can have both civilian and military applications, a category that increasingly includes surveillance items and software that can be used for political repression. Regulators expect to see reasonable, risk-based due diligence on transactions, which often include know your customer (KYC) due diligence, training and awareness, 'red flag' assessments, routine audits and robust documentation.

Monard: Companies should have a clear understanding of all the products they supply, and of their customs and export control classification. This would allow them to identify the nature of the goods and whether they are or could be considered military or dual-use. In case companies ship or insure goods, they should request and obtain the necessary information, such as the customs and export control classification of the relevant products, in order to be in a position to be able to adequately identify the nature of the products. At the same time, when dealing with countries subject to EU arms embargoes, companies should also be aware of the end-use and end-user of the products in question, as this could also have an impact on the classification of the products.

> TECHNOLOGY IS CENTRAL TO A STRONG SANCTIONS COMPLIANCE PROGRAMME. MOST IMPORTANTLY, WIDELY AVAILABLE SOFTWARE NOW ALLOWS COMPANIES TO QUICKLY AND EASILY SCREEN THEIR COUNTERPARTIES AGAINST APPLICABLE SANCTIONS LISTS.
>
> JUDITH ALISON LEE
> Gibson, Dunn & Crutcher LLP

Lee: Overlapping regulatory requirements and compliance tools make it possible for companies to adopt procedures that simultaneously address both sanctions and export control risks. As a minimum, basic transaction diligence should be completed whenever exports of goods or services occur. Among other things, companies should determine the export control classification of goods and services, gather information about the destination and end use or end user, searching in particular for any red flags, and then carefully evaluate the applicable licensing requirements and licence exceptions.

FW: To what extent are you seeing companies utilise technology to help them obey sanctions restrictions?

Monard: Companies are increasingly using software that screens the names of persons and entities against several consolidated sanctions lists. This allows them to obtain a first indication of whether there are potential red flags regarding a potential transaction. In addition, companies are also increasingly using technology to track their goods that they have, for instance, identified as dual-use. Such technology would, for instance, flag any sales orders for such products and indicate whether a licence is required or even whether the sale can take place at all. It is, however, important to ensure that such software and technology is always up to date, and should not lead to complacency with respect to a compliance programme. Such technology should always be part of a comprehensive compliance programme and not the only element.

Lee: Technology is central to a strong sanctions compliance programme. Most importantly, widely available software now allows companies to quickly and easily screen their counterparties against applicable sanctions lists. While regulators are agnostic about precisely which screening software a company uses, we generally recommend that the software be robust enough to catch subtle variations in names and it should also be subject to frequent updates to capture the latest changes to the SDN List. Last year, JPMorgan was found to have violated US sanctions for using software that was deficient in those respects.

Bittner: In addition to the list-based screening tools that have been available for many years, companies are starting to utilise technology to assess the sanctions-related risks associated with their transactions, such as, by using subscription services and publicly-available information to identify ownership or control, main suppliers, main customers, situations of

common interest in a third party and so on. These relationships may be legal at the start of a project, but they could quickly evolve into a risky scenario if levels of ownership or control increase, or persons or entities are added to a restricted party or sectoral sanctions identification (SSI) list. We have also seen companies in the oil & gas industry create detailed maps that overlay issues that could create sanctions risk, such as water depth, projects with Russian interests, shale fields and so on. These tools allow business development teams to see the areas in the world that could have increased sanctions risk.

Smith: Banks have been using analytics to monitor their potential exposure to, and compliance with, sanctions for some time, though we have not seen this applied to the same extent by corporates. This is a reflection of the financial crime risks that banks are exposed to, the greater regulatory scrutiny banks have faced, and the sheer volume of transactions that banks need to monitor and evaluate. We see a clear role for technology to assist with sanctions compliance for corporates. This is particularly the case for companies that have large numbers of sales intermediaries and thousands of third-party relationships. For example, analytics can help look for various red flags in customer relationship management software and in accounting information that could indicate that business was taking place in sanctioned countries.

FW: Specifically, could you provide an insight into the benefits of data analysis, and how this can be leveraged to monitor and detect potential sanctions breaches?

Lee: In addition to the routine screening of counterparties against applicable sanctions lists, data analysis can be particularly useful for companies operating in high-risk sectors or jurisdictions. For example, software, together with employees well trained to use it, can monitor sales to distributors in a particular region for sudden spikes or changes. For example, if Distributor A in the UAE has been ordering 200 televisions per quarter for five years, and Distributor B in Iran has been ordering 300 televisions per quarter for five years, and Distributor A's orders suddenly increase to 500 televisions per quarter, it could signify a problem.

Smith: Relevant technology solutions include using third-party due diligence screening tools to identify higher risk entities and using data from accounting, enterprise resource planning (ERP) and customer relationship management (CRM) systems to identify indicators of sanctions exposure. This includes named entities from sanctions lists, red flag tests to detect associations with sanctioned countries, and other rules-based tests. Red flag tests need to be updated on a regular basis to reflect changes in the regulatory environment. Your findings can trigger a range of actions such as, investigation and reassessment of risk level or enhanced due diligence.

Monard: Companies typically have large amounts of data available with respect to certain transactions, such as production information, sales system and emails. It is important to find a way to analyse all relevant data in an efficient way, to be able to identify any red flags or inconsistencies. Data analysis can also be particularly useful in order to identify certain failings with respect to sanctions compliance and, in particular, to put in place adequate systems to avoid such failings from happening again. By analysing such data, compliance programmes can be streamlined and be made more effective, for instance by providing more attention to higher risk issues.

FW: Where sanctions have been lifted but subsequently reimposed, how should businesses faced with 90-day or 180-day wind-down periods to dismantle their operations respond?

Monard: In case sanctions are lifted, companies should nevertheless put in place adequate contractual language in order to protect them in case sanctions are reimposed. Moreover, especially EU companies should be mindful of potential issues related to prohibitions to comply with the extraterritorial effects of certain sanctions regimes. Key examples are the US Iran sanctions and the EU Blocking Regulation. Even though EU companies could not have easily anticipated that the US would reimpose the Iran sanctions, and that the EU would react by prohibiting compliance with certain elements, companies should tread carefully and ensure that they are fully aware of all the potential regulatory requirements that may apply to them.

> "ANALYTICS CAN HELP LOOK FOR VARIOUS RED FLAGS IN CUSTOMER RELATIONSHIP MANAGEMENT SOFTWARE AND IN ACCOUNTING INFORMATION THAT COULD INDICATE THAT BUSINESS WAS TAKING PLACE IN SANCTIONED COUNTRIES."
>
> HENRY SMITH
> Control Risks

Bittner: Companies should consider including clauses in contracts that specifically address potential changes to sanctions programmes and which allow flexibility, should an unexpected situation arise. This is sometimes included in the form of a *force majeure* clause, but this can be problematic unless a change in applicable law is expressly deemed to qualify as a *force majeure* event. Otherwise, a company may be caught in a situation in which it has to take action to comply with changing US – or other country – law which breaches the contract in a venue that does not recognise the change in law, and the company is subsequently sued in the foreign partner's domestic court for non-performance.

Smith: OFAC's request to 'wind-down' asks organisations to extricate themselves from business relationships that are covered by sanctions. However, 'wind-down' is not well-defined. The understanding is that any business with primary US sanctions exposure should stop immediately unless there is OFAC guidance to the contrary. With secondary sanctions, this is not possible due to the potential for diplomatic confrontation and the difficulty of requiring non-US companies to exit business relationships since they are not subjects of US jurisdiction. In our experience, companies should consider and plan for the possibility of wind-down when they enter a relationship with a company that could be sanctioned in the future. If due diligence or political risk forecasting indicates that a company is a candidate for sanctions, then cash flow, receivables and contractual structures need to be managed in ways that allow for a quick exit with minimal losses.

Lee: As many companies have recently experienced, following the reimposition of US nuclear-related sanctions on Iran, 90 or 180 days is not a lot of time to wind down complicated business relationships. Final deliveries of goods need to be made, payment needs to be collected and contracts need to be suspended or terminated – all in a manner that does not expose the company to litigation with their business partners or an enforcement action by OFAC. Under that set of circumstances, foreign companies doing business in the targeted jurisdiction would be well advised to get started promptly, engage sophisticated outside counsel and pay close attention to guidance and FAQs published by OFAC.

Aiyar: Businesses should first determine what transactions and activities can and cannot be conducted pursuant to wind-down periods and other general licences. Several issues arise during these periods that could expose a business to legal liability, such as contractual, employment, licensing and other matters. Businesses need to determine what they are allowed to do in the process of dealing with these potential issues and limiting exposure to liabilities. Businesses should identify and prioritise what wind-down issues require immediate attention, and which ones can be set aside for later.

FW: What essential advice would you offer to companies on developing a strong, multinational sanctions compliance programme for today's complex regulatory landscape?

Smith: Multinational organisations must consider educating their sales force and business development teams about what sanctions there are, how they can be violated, and what the personal and collective penalties are for violating them. They should also ensure their political risk and government affairs teams are working closely with the compliance function and sharing information regarding the monitoring of changes in the drivers and motivating factors for sanctions and their enforcement.

Lee: A strong sanctions compliance programme starts at the top. If there is buy-in from senior-level leadership, the resources and staffing to maintain a robust compliance programme will often follow. Companies should also regularly perform risk assessments tailored to the unique needs of their particular business – whether that be operating in certain jurisdictions or dealing with particular types of customers that are high risk – and update their policies and procedures to match. Finally, even the most sophisticated sanctions screening software will only get you so far if your employees do not know how to use it properly. Regular training is essential.

Aiyar: Companies should constantly ensure that the compliance programme is up-to-date on sanctions and additions to the SDN List. Sanctions are motivated by foreign policy, so there is a decent chance that sanctions imposed or altered by a prior administration can be lifted or reimposed by the immediately following administration, as we saw with the Trump administration reimposing sanctions on Iran that the Obama administration had eased. Businesses should not be afraid to invest in a rigorous compliance programme, as the potential penalties for violating sanctions far outweigh the costs of a properly functioning compliance programme.

Monard: It is important to set up a robust compliance programme, which is regularly reviewed and has the full backing of senior management. The legal department should be involved and have a final say on whether a potential transaction is in line with or in violation of relevant laws and regulations. It is also important to have access to legal professionals with an expert knowledge of sanctions law, who can be relied on in case of more complex issues. It is equally important that all relevant personnel are made aware of the risks and receive regular training.

FW: Looking ahead, what are your expectations for trade sanctions through 2019 and beyond? In your opinion, do businesses need to do more to enhance their sanctions compliance framework?

Bittner: It is likely that OFAC will continue to provide guidance in 2019 on what level of due diligence companies should conduct to avoid sanctions violations. While we wait to see if OFAC publishes official guidelines, companies should review recent enforcement cases, including the Epsilon, Cobham and E.l.f. cases, to assess whether they should take

steps to enhance their compliance structure or programmes.

Lee: After adding a record number of individuals and entities to the SDN List in 2018, it seems safe to assume that the Trump administration will continue to lean heavily on sanctions as an instrument of US policy in 2019. While it remains to be seen precisely where the administration will direct its energies, developments worth monitoring over the coming months include whether, on the heels of designating the state-owned oil company PdVSA, the US continues to tighten sanctions on Venezuela. Likewise, against the backdrop of simmering trade tensions between Washington and Beijing, it is possible that the US could pursue enforcement actions against major Chinese enterprises, as it has done recently with ZTE and Huawei. Large, sophisticated companies have been living with the reality that financial sanctions are an increasingly important part of the US foreign policy toolkit for a while now and have developed robust compliance programmes in response, but there is always room for improvement. As always, companies should closely monitor developments out of Washington and update their policies and procedures accordingly.

Aiyar: In the near term, we are likely to see more sanctions targeting the government of Venezuela as the Trump administration continues its efforts to pressure Nicolas Maduro into stepping down as head of state. This could include adding more individuals and entities to the SDN List. Businesses could always do more to enhance their sanctions compliance framework, but the most important things are to conduct self-audits to ensure the compliance programme is functioning properly and stays up-to-date with new and lifted sanctions and other related developments.

Monard: In light of the volatility in the past year, in particular regarding the US, Russia and Iran sanctions, and the update of the EU's Blocking Regulation, it is difficult to make clear long-term predictions. Much will depend on how things evolve on a political level. In addition, much depends on elements taking place in third countries that are often difficult to predict. For instance, the US has recently imposed additional sanctions on Venezuela. It is not unlikely that the EU may follow by also expanding its sanctions on Venezuela. Indeed, the EU is currently considering whether to do so. Similar volatility in other countries could also lead to additional sanctions. It is therefore of vital importance for companies to actively keep track of the evolution of the applicable sanctions landscape.

Smith: We expect there to be more sanctions rather than less in 2019. The US is likely to impose additional Russian sanctions, and the EU will continue to roll-over Ukraine-related sanctions, even as it jousts with the US over gas pipeline sanctions. The political situation in Venezuela is volatile. There is room for US trade and financial sanctions to escalate further if the desired political transition does not materialise, or in the event of further violent repression. The EU and other countries backing the opposition are likely to impose or increase sanctions. The US remains relatively isolated in its Iran campaign, but will continue to put pressure on the EU and other countries, as well as expand its own designations. Venezuela and Iran will remain under considerable US pressure. With regard to North Korea, significant sanctions relief remains unlikely, with talks over denuclearisation stymied by misinterpretation and mistrust. ■