Getting to grips with international sanctions

Q: With talk of sanctions always in the news, what do risk managers need to know and should they be concerned?

A: The threat of adverse publicity, investigations, high fines, criminal liability and consequential reputational damage has brought sanctions to the top of agenda for many risk managers.

In May, the US Department of Justice sentenced a financial institution headquartered in Paris for violations of US economic sanctions targeting Sudan, Iran and Cuba. The sentencing made headlines because it was the first time that a financial institution has been convicted and sentenced for breaches of US financial sanctions and it was the largest ever fine imposed in a criminal case. The sentencing included a five-year term of probation, an order to forfeit $8,84bn (€7.9bn) to the US and a fine of $140m.

Financial sanctions involve restrictions on trade and financial activity to address a foreign and security policy objective. Modern sanctions take various forms, such as travel bans, arms embargoes and freezing the assets of listed individuals or entities. Financial sanctions can also be comprehensive, imposing restrictions on the international trade and economic activity of an entire country.

For risk managers trying to better understand sanctions compliance, several issues should be explored as a starting point.

Which programmes apply?

Many countries operate autonomous sanctions programmes and risk managers should therefore ensure that their firms and businesses are compliant with the national sanctions laws in the country in which they are based. The EU implements UN sanctions into EU regulations that directly apply to all EU countries. EU sanctions apply to EU nationals wherever they are located, entities incorporated within the EU and any person or business in respect of any business done in whole or part within the EU.

A further layer of complexity arises in circumstances where an organisation may be affected not only by domestic and EU regulations but also by foreign sanctions programmes. For example, an insurer based in an EU member state might be affected by US sanctions because its business is owned and controlled by a US parent. US citizens might be employed in an European business that might engage in activities that are prohibited by US sanctions.

Greatest risk of exposure and prohibited activities

Risk managers need to conduct a risk assessment of the potential areas where their businesses might be exposed to sanctions. This could be influenced by the countries in which their firms do business or the nationality of the clients or those supplying services to their business.

Typically, sanctions will prohibit making funds or economic resources available to, or dealing with funds or economic resources belonging to or controlled by, sanctioned companies and individuals. Recent sectoral sanctions have restricted activities in specific areas such as oil and gas, access to capital markets. Sanctions have also restricted the provision of (re)insurance services to persons, entities and governments on sanctions lists.

Preventing breaches

It is good practice to identify when you are dealing with a listed individual or entity, either by implementing bulk screening or manually screening individuals or entities against the applicable sanctions lists, (which are generally available online). Registering to receive automated alerts is an effective way to keep on top of frequent updates to sanctions lists and legislation.

It is vital to be aware of when employees are about to engage in business that involves a sanctioned country. Communications highlighting countries subject to sanctions can be effective in raising awareness and this should be supported by a process for notifying potential sanctions matters to a central point within the organisation. Notifications provide an opportunity to review the potential risk that your organisation might conduct a prohibited activity and to advise on the best course of action.

When assessing sanctions risk, relevant factors include the nationality of all parties to the transaction, the place of incorporation and ownership of your business, the involvement of US interests (US dollars, goods of US origin). It is a good idea to standardise how this information is obtained through a paper questionnaire or electronic form.

If you have identified that you are dealing with a sanctioned party and/or your transaction or services are likely to involve a prohibited activity, withdrawing from the transaction or supply of services is not the only option. It is possible to apply for a licence from the national competent authority responsible for the administration of sanctions in the country in which you are based. If a licence is granted, it will authorise you to undertake an activity that is otherwise prohibited.

One last important area to note is that circumventing financial sanctions or enabling or facilitating an action that has the effect of circumventing sanctions is generally prohibited.

What next?

Sanctions are becoming more complex and governments are producing new ways to fashion 'smart' sanctions that address specific policy goals. This trend can be witnessed in the sectoral sanctions against Russia by the US, EU and other countries and the US president Barack Obama's recent Executive Order establishing a new sanctions regime for "significant malicious cyber-enabled activities." These co-called cyber sanctions target hackers and those complicit in cyber attacks on the US or who benefit from trade secrets, knowing that they are derived from illegal cyber activity. This recent activity points to the conclusion that this is an ever-burgeoning area of interest for risk managers, particularly those based in multinational businesses or who do business internationally.

Che Odlum is the compliance manager – financial crime and sanctions at DLA Piper UK LLP