as seen in
Thomson Reuters Regulatory Intelligence

Enterprise-wide risk assessments have never been more important

Jan 17 2019 Thomas Bock and Darren Matthews

Financial services institutions have a challenging mission. Not only are they are required to manage the assets of their clients and depositors responsibly, but they are also expected to execute government policies on sanctions, trade restrictions and money laundering while countering the relentless attempts by bad actors to circumvent those same restrictions. That is on top of the threats posed by technology-enabled fraud. These obligations make an annual enterprise-wide risk assessment an absolute necessity.

Risk assessments

There are several types of risk assessments that institutions are required to conduct, depending on the regulatory requirements of the country where they do business. Usually these involve anti-money laundering, global sanctions, fraud and cyber risk assessments, but firms may also be subject to more localised regulations. Those are the four core risks that should be continually and holistically assessed. There is danger in treating these risks as separate and regional rather than interconnected and global in nature. If a firm is not examining these risks holistically, it is not only ignoring the bigger picture but also missing opportunities to leverage economies of systems, technology and people to address the frequently interconnected risks more effectively.

Only a comprehensive approach can help a financial institution identify and mitigate the most potent risks with any certainty.

How to identify and mitigate risk

Financial services firms need to design and implement the appropriate assessment methodology. This includes looking closely at their customer base, their products and services, third-party vendors, the geographies in which they operate, and where their clients operate. They drill down into the types of transactions that are facilitated through the institution on a daily basis and examine the inherent risks in the four main areas: AML, sanctions, fraud and cyber.

With a clear understanding of what risks exist, firms should look at their control environments — the controls they have in place, including people processes and technology — to help mitigate the identified risks. After identifying the risks and the control environment, firms are left with the residual risks in those important areas. By reducing the panoply of risk to a manageable set of residual risks, the institution can focus extra attention and resources on mitigating them.

Ideally, the risk assessment is just the beginning. For the purpose of a complying with regulation and mitigating remaining risk, the institution has now identified the main areas of concern where they need to focus their efforts, which includes building out a more secure control environment and conducting independent testing from a compliance perspective, or in many cases additional opportunities to train the first line of defence.

In the authors' experience, vital to a successful risk assessment is how firms interpret and utilise the results. Institutions fall short by considering the risk assessment as an exercise to be completed, when in fact completing the assessment is only the start of the process. Rather, financial institutions should see the assessment as the first step in a much longer process of analysing the results, developing learning and teachings, and focusing the enterprise on areas of risk that require more attention. There are many snippets of information you can get from a thorough risk assessment; that is where the most valuable insights come from. Analysing the data is just as important as completing the risk assessment itself.

Frequency

Another area where some institutions fall short is frequency. Banks are so inundated with business-as-usual compliance requirements that they are sorely tempted to postpone the risk assessment until a more convenient time. The trouble is, there is never is a more convenient time and past assessments grow stale over time as risks continually evolve, regulatory regimes change and the financial institution's own mission may change course. As an industry best practice, an enterprise-wide, global risk assessment has to be performed at least once a year and after a significant event such as a merger, acquisition, or upon entering a new geography.

Continued next page

Assessment process complications

Generally, there are three issues that complicate the assessment process.

- First, many banking institutions operate on a longer cycle than once a year so they put off their annual assessments. As noted, that is dangerous. If institutions let their risk assessment go for more than a year while they are developing new products across geographies, or there has been an acquisition, they are not really taking into account the additional risks that may be involved with changes to the institution's business profile.
- The second issue is the need to ensure that all the products and services offered by an institution globally are evaluated. That may sound easy to do, but if you are in 109 different countries it is very difficult to understand what one distant branch may be doing or offering its clients, but it is crucially important to understand all the different products that are being offered throughout an institution to evaluate the risk appropriately.
- The last issue is ensuring that all of the data that was gathered in the context of the risk assessment is considered in developing the final product. There is a multitude of data points that can be drawn on from transactions to customers to the geographies that you play in. Applying data analytics only enhances the value of the risk assessment, yet far too few institutions do that.

One reason for this oversight could be that the institutions do not have the appropriate skill sets to do effective data analytics, but the reality is that most banks struggle just to know truly where their data resides and how to pull it together from disparate sources, and because the data is not maintained in a central repository, it is often a challenge to know where to find the data you are looking for. It is a big ocean if you do not have a map.

This is not a criticism. There are all sorts of sizes and shapes of financial institutions. There are mid-sized banks that have 10 branches and there are global banks with hundreds of locations but they are both held to the same standards. They are viewed as the same by their regulator despite the relatively heavier burden this places on smaller institutions. That is especially true of U.S. branches of foreign banks that tend to be smaller in size but share the risks of the entire enterprise.

In the future, enterprise-wide, global risk assessments are going to be more important — not less — because of the new products than are continually being developed. For example, cryptocurrencies present a whole new world of risk exposure, and those risks are not yet fully defined. It is an evolving landscape, but one which seems to be here to stay.

Banks need to adapt to those risks and be open to onboarding different types of customers and exchange houses that are dealing in the cryptocurrency world. They should also be held to very similar standards as a typical financial institution. They should have an anti-money laundering program, strong monitoring capabilities, an experienced chief compliance officer and a cyber security program in place.

Outsourcing compliance function

Many of these crypto companies are start-ups and have little understanding of the compliance environment in the financial services industry. Their solution could be to outsource their entire compliance function to a third-party professional. Outsourcing compliance allows institutions of all sizes to rely on professional talent focused on risk day-in and day-out for not just in one institution, but many. Outsourcing does not absolve institutions of their compliance responsibilities, but a third party can help them take control of their risk and compliance responsibilities.

Final thoughts

Remember that risk is always present. It transcends institutions and industries, and with the added responsibilities of executing law enforcement and national security policy tasks, the challenge for institutions is to get it right: precision and insight has never been more important.

K2 Intelligence

Investigations · Compliance Solutions · Cyber Defense

Thomas Bock leads the regulatory compliance practice and Darren Matthews is regional head of EMEA for K2 Intelligence, a corporate investigations, regulatory compliance, and cyber defence services firm. The views expressed are their own.