corporate-stock-procedure-and-administration.

WHAT'S THE RISK? CONTRACTUAL AND INSURANCE CONSIDERATIONS FOR BANKS AND FINANCIAL INSTITUTIONS

By John M. Leonard and Regan E. Samson

John M. Leonard is a shareholder in Anderson Kill's New York office and co-chair of the firm's Financial Services Group. Regan E. Samson is an attorney in Anderson Kill's New York office and a member of the firm's Financial Services Group. Contact: jleonard@andersonkill.com or rsamson@andersonkill.com.

How can a financial institution determine which elements of its outsourced work product constitute critical activities, and what can the financial institution do to mitigate the risks that accompany that third-party critical activity? To address those questions, a trio of federal agencies (the Federal Reserve, the FDIC, and the Office of the Comptroller of the Currency) issued guidance last June.[1] Financial institutions should review their internal risk mitigation procedures in conjunction with this federal guidance to ensure that potentially unforeseen risks do not fall through the cracks.

Critical Activities

The federal guidance is just that—guidance. It is not a set of hard and fast rules, but rather guideposts to help banking organizations navigate both known and novel risks in a continuously evolving industry. For example, the federal guidance declines to make a bright-line determination regarding what, specifically, constitutes a critical activity. But it does provide a number of hallmarks of critical activities: they generally have the potential for significant customer impacts, have a significant impact on a banking organization's financial condition or operations, and would expose a financial institution to significant risk were expectations for the activity not met. Aside from these and similar principles, the guidance leaves it up to each banking organization to determine what its "critical activities" are, and which third-party relationships support those activities.

Similarly, the guidance suggests various due diligence activities but leaves the final determination regarding the extent of diligence to the banks themselves. The guidance provides an extensive list of diligence activities that financial institutions should consider, including assessing the financial condition of the vendor; evaluating the risk management protocols that the vendor has in place; assessing the insurance coverage program of the third-party; and analyzing the sub-vendors, or fourth-party vendors, that the third-party may utilize to perform its critical activities for the bank.

As evidenced above, the guidance recognizes that the complexities of banking operations also occasionally call for fourth-party vendors to complete critical activities. Here, too, banks and other financial institutions should account for the additional risks posed by adding an additional relationship into the mix. The guidance suggests that banks should assess *their* vendor's ability to assess risks posed by *its* vendor. This may include early determination of when a third-party will use a sub-vendor, oversight into the operations performed by the sub-vendor, periodic audits, and assessing whether the geographic location of the sub-vendor presents additional concerns. While banks certainly consider that risk and liability may flow up from their own vendors, they must also recognize the possibility that additional risks and liabilities may flow back from that party's vendors. Performing diligence at the outset of any relationship—including a fourth-party relationship—may minimize the exposure that banks eventually face.

Mitigating Risk from Third-Party Relationships

Given the risks that accompany third- and fourth-party relationships, banks would be wise to consider various proactive risk mitigation measures. Perhaps most obviously, banks can rely on insurance to mitigate these risks. Of course, most financial institutions already will have a robust insurance program in place to cover all sorts of risks. But based on the types of critical activities performed by vendors and subvendors, banks, along with their trusted brokers, may want to consider the breadth and scope of those insurance towers for risks such as cyber, D&O, and E&O, to name just a few.

Banks also may consider transferring risk through direct contracting with their vendors. An indemnity agreement—whether separate or incorporated into a services contract with a critical activity vendor—could shift risk away from the financial institution should a critical activity performed pursuant to that contractual relationship go awry. And because indemnity agreements can be tailored to shift varying degrees of risk, parties on both sides of a contract can have a say regarding the amount of risk they are willing to offload or accept. Limitations of liability may also function to cap the shift of risk from one party to another. Of course, just as they do when consulting brokers for their insurance programs, banks would be wise to consult in-house or outside counsel (or both) when negotiating and drafting indemnity agreements and limitations of liability. Jurisdiction, enforceability, and public policy concerns may all inform how such contractual provisions are written.

As the guidance notes, banking organizations should be familiar with the insurance coverage of their vendors to provide a potential additional layer of security against risks both known and unforeseen. Perhaps the contract between the parties specifies insurance requirements for the vendor. Those specifications may require that the financial institution be named as an additional insured under the vendor's insurance policies. Contractual partners, as well as their insurance companies, should ensure that any such requirement is met prior to any unforeseen loss occurring, both to abide by the terms of the contract and to avoid a potential coverage dispute down the road.

Conclusion

Because each banking organization has different critical activities and third-party relationships to support those activities, an individualized assessment of a bank's critical activities is necessary to mitigate risk. As new and innovative threats emerge, performing due diligence as suggested by the guidance in advance of entering into third-party relationships for critical activities can help to minimize those threats. While risk will always exist, banks have a number of tools at their disposal to assess, address, and counter these threats.

ENDNOTES:

[1] https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management.