The Federal Reserve, FDIC, and OCC have released a new guide specifically tailored for community banks. This guide is a resource that will help you develop and manage third-party risk management practices. It reiterates a fundamental principle: a bank's engagement with a third party does not diminish or remove its responsibility to operate safely and soundly or to comply with legal and regulatory requirements, just as if the bank were to perform the service or activity itself.

The guide provides potential considerations, resources, and examples through each stage of the third-party risk-management life cycle. Regulators clarify that the guide is not a checklist and does not prescribe specific risk-management practices or establish safe harbors for compliance with laws or regulations. It also is not a substitute for the existing interagency guidance on third-party relationship risk management.

CCI highlights a few examples from the guide that can be helpful as you review your third-party/vendor management program.

Under the *Planning* section, the guide states, "As part of sound risk management, effective planning allows a banking organization to evaluate and consider how to manage risks before entering into a third-party relationship." CCI wants to emphasize that it is important to conduct *both* vendor and product risk assessments before entering into a new contract. Banks must ensure the new vendor falls within the bank's risk tolerance and any new product has appropriate controls in place to limit risk adequately.

Under *Due Diligence and Third-Party Selection*, the document states, "Does the third party use technologies that could introduce additional risk? Is the third party involved in ongoing litigation or other public matters of concern?" CCI wants to emphasize the importance of doing an internet search early in the discovery process to ensure that a potential new vendor does not have a history of data breaches. A vendor might have a product or service that the financial institution is sold on, but it might also have a poor track record of data security, which, ultimately, should cause the institution to look elsewhere.

Regarding the *Contract Negotiation* section, "Does the contract specify limitations on the third party's use and retention of data (including customer data) related to the activity, including its disclosure, storage, delivery to the bank, and destruction?" and "If the third party has access to bank or customer data, when and how will the bank confirm that the data has been returned or

destroyed?" It's important to have contract terms stating that the bank retains ownership of its customer data and that the vendor will destroy or return it upon termination. This matter should be resolved during the negotiation process rather than when the bank notifies the vendor that it's terminating the contract. It's essential to include this information within the contract so your institution does not receive notification from a former vendor from long ago that it had a data breach, resulting in your institution having to notify your customers and former customers of the situation that will damage both the institution's reputation and bottom line.

CCI has experts available to take care of the annual vendor management analysis and reporting at your institution. Please get in touch with us if you'd like to avoid the annual vendor management hassle and leave it up to us.

You can download the complete guide **here.**