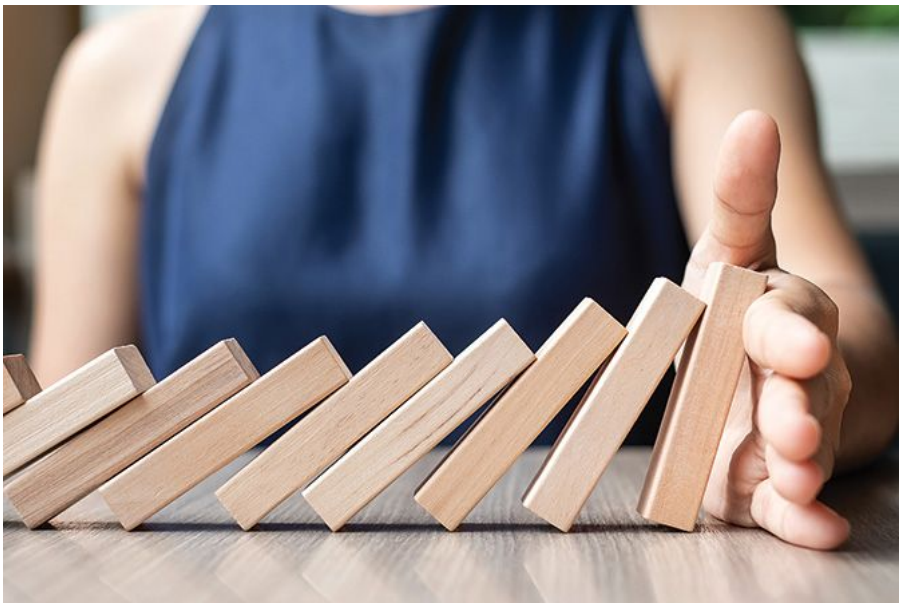
UTAH BANKER

Pub. 10 2022 Issue 4



Risk Management Of Third-Party Relationships

Published December 30, 2022

This story appears in the
Utah Banker Magazine Pub 10 2022 Issue 4

By Tracey Levandoski, CRCM, CrossCheck Compliance LLC

On July 19, 2021, the regulatory agencies issued Proposed Interagency Guidance on Third-Party Relationships: Risk Management. The proposed guidance consolidates all prior guidance, offers a detailed framework covering all stages in the life cycle of third-party relationships, and takes into account the level of risk, complexity, and size of the bank, as well as the nature of the third-party relationship. While it is unclear when the proposal will be finalized, the principles of sound third-party risk management remain the same.

Governance and Oversight

Under current guidance, the bank's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships to the same extent as if the activities were handled directly by the bank. The proposed guidance states that using third parties does not diminish the bank's responsibility to perform an activity in a safe and sound manner and in compliance with applicable laws and regulations. For evidence that the regulators will not allow a bank to outsource its accountability and responsibility to third-party providers, one only needs to read a few consent orders in which banks were held accountable for the actions of their third-party providers.

The Primary Focus of Third-Party Risk Management – Significant vs. Critical

Current guidance focuses the attention of third-party risk management on significant relationships and further defines what types of relationships should be considered significant, such as providers who:

- Introduce a new relationship or a new bank activity;
- Perform critical functions for the bank;
- Have access to sensitive customer information;
- Market bank products or services;
- Provide products or services involving subprime lending or card payment transactions; or
- Pose risks that could significantly affect earnings, capital, or the bank's reputation.

UTAH BANKER

Additionally, the nature of risk in the context of the current or planned use of a third party should be understood in conjunction with the risk areas you consider in everything else you do:

- Strategic Risk – Does the use of the third-party's services align with the bank's strategic goals?
- Reputation Risk – What risk does using the third party contribute to the bank's good name in the community?
- Operational Risk – Do the third party's processes integrate compatibly with the bank's processes?
- Transaction Risk – What is the risk of the third party's failure to perform as expected?
- Credit Risk – What is the credit risk of the third party? What credit risk does the third party introduce when using proprietary credit models for underwriting loans on the bank's behalf (for example)?
- Compliance Risk – What is the exposure if the third party violates laws or fails to comply with the bank's internal policies?

The proposed guidance is intended for all third-party relationships but is especially important for relationships that are relied on to a significant extent entail greater risk and complexity, and involve critical activities. Critical activities:

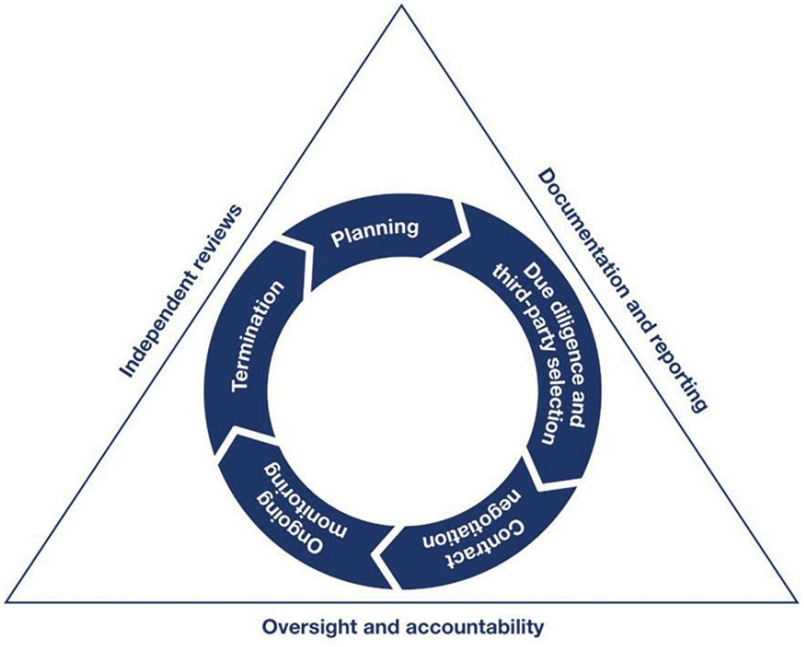
- Cause significant risks if the third party fails to meet expectations
- Have significant customer impacts
- Require significant investment in resources to implement the activity and manage the risk
- Cause a major impact on the bank's operations if an alternative must be found or the activity must be brought in-house

Regardless of the approach to defining significant or critical service providers, the bank should implement a sound methodology for designating which relationships receive more comprehensive oversight and risk management.

The Risk Management Process

Under the current guidance, the key to the effective use of a third party is to appropriately assess, measure, monitor, and control the risks associated with the relationship, which includes a risk assessment, due diligence, contract structuring and review, and ongoing oversight.

The proposed guidance significantly expands upon risk management by introducing the Third-Party Relationship Life Cycle which is depicted in the following Stages of the Risk Management Life Cycle graphic.



Source: Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency. Proposed Interagency Guidance on Third-Party Relationships: Risk Management.

UTAH BANKER

The proposed guidance significantly expands risk management by introducing the Third-Party Relationship Life Cycle. The Life Cycle starts with the first step of planning, which includes not only a risk assessment that, at a minimum, considers the risk areas described above; identifies performance criteria, internal controls, reporting needs, and necessary contractual requirements; assesses management's ability to provide adequate oversight; and contemplates the consequences of the provider's failure. In addition to the risk assessment, planning includes the commensurate steps for appropriate risk management. Planning should be a collaboration among members of management with the requisite expertise and may involve managers from across the bank's business lines, such as compliance, information technology, and legal counsel, in addition to the area directly impacted by the third party's product or service.

The next step of the Life Cycle is due diligence commensurate with the criticality of the proposed activity and level of risk identified in the risk assessment. Due diligence should include an assessment of the provider's ability to perform as expected considering its financial condition, business experience, and operational resilience; comply with the bank's policies as well as applicable federal and state laws; and operate in a safe and sound manner. In some cases, an onsite visit may be warranted.

After a provider has been selected, the contract negotiation considers service level agreements, required reporting, compliance with applicable laws and regulations, the bank's right to audit the provider, complaint and dispute resolution, and the use of subcontractors, among other provisions.

Following contract execution and provider onboarding, ongoing monitoring should be performed commensurate with the risk level determined during the planning stage. Ongoing monitoring may be similar to the initial due diligence, with an added focus on fulfilment of contract requirements, and should include an update to the risk assessment based on the results of the monitoring.

The final stage of the Life Cycle is the termination of the relationship, which should be handled efficiently to minimize the impact on operations and the bank's customers. However, termination should really be contemplated during the planning stage, including considering the implications if the provider fails to perform to expectations or, in the worst-case scenario, the provider ceases operations.

Woven into the proposed guidance is a focus on fourth parties – a third-party provider's subcontractors – and bank management must ensure that if a third-party provider uses subcontractors for any part of the bank's outsourced activities, the third party provides adequate oversight of its subcontractors. The use of subcontractors must be considered during all stages of the Life Cycle.

Oversight of the Third-Party Risk Management Program

The Third-Party Relationship Life Cycle also contemplates oversight of the third-party risk management program. While the regulators' compliance management system (CMS) examination procedures do not include provider oversight as a formal component of the CMS, they do state that compliance expectations extend to provider relationships. Therefore, third-party risk management should be incorporated into the bank's CMS, including:.

- Policies and procedures that define risk/criticality, minimum due diligence and ongoing monitoring activities based on risk, and minimum contract provisions; and address oversight of and accountability for the program
- Training for bank staff responsible for third-party oversight
- Monitoring, testing, and audit of the program
- Complaint management related to third-party providers

Third-party risk management continues to be an increasing regulatory focus. Understanding the details of sound risk management outlined in the proposed guidance and enhancing your third-party risk management program commensurate with the risk level of your bank's service provider relationships will place the bank in a more favorable position for the next regulatory examination.

Tracey is a managing director at CrossCheck Compliance LLC and a regulatory compliance and risk management professional with over 30 years of experience in the financial services industry. Prior to joining CrossCheck, Tracey was Senior Vice President, Compliance at Standard Bank & Trust, now Old National Bank; and, before that, she was Assistant Vice President, Community Bank Examinations at the Federal Reserve Bank of Chicago. She also previously held positions in compliance, accounting, and operations at community banks. Having worked as both a prudential regulator and in banking institutions, Tracey has demonstrated expertise in compliance, including extensive knowledge of lending and deposit regulations, with a recent concentration on fintech. Tracey can be reached at tlevandoski@crosscheckcompliance.com.