protiviti®
Face the Future with Confidence

US Banking Regulators Finalise (Finally) Revised Third-Party Risk Management Guidance

8 June
2023

On Tuesday, 6 June 2023, the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (collectively, the agencies) issued the "Interagency Guidance on Third-Party Relationships: Risk Management."[1] This marks the long-awaited finalisation of the proposed guidance that was initially issued on 19 July 2021, with a 90-day comment period that extended until 18 October 2021. Most important, this finally brings consistency in regulatory expectations across the three primary financial regulators within the United States. The guidance applies to all institutions supervised by these agencies.

The key changes that were made from the original proposal highlight the importance of taking a right-sized approach to third-party risk management for each organisation.

Key comments that provide future clarity on approach

The agencies collectively received 82 comment letters from banking organisations, financial technology (fintech) companies and other third-party providers, trade associations, consultants, non-profits, and individuals. As is typical of regulatory guidance that has been subject to a notice and comment period, the comments received from industry participants and the agencies' responses to those comments are at least as enlightening as the guidance itself.

Key issues raised and addressed through this dialogue included the following:

- Scope of Business Arrangement remains consistent with the original proposal and continues to incorporate all types of relationships, whether contractual or not, and whether with an outside party or internal affiliate. This continues the OCC's historical perspective of taking an overly broad approach in terms of the types of relationships in

[1] "Interagency Guidance on Third-Party Relationships," Federal Reserve System, Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency, 6 June 2023: www.fdic.gov/news/financial-institution-letters/2023/fil23029.html.

scope for this guidance, contrary to industry commentors' hopes for further clarity or narrowing to limit the scope of applicability of the guidance.

- The definition of "critical activities" has been revised to emphasise flexibility, calling for each banking organisation to consider its own operations to understand those activities that would meet the "critical activity" definition. Additionally, the guidance has remained loose ("general" or "vague") in how an organisation identifies "critical activity," including whether there is a need to align with other regulatory requirements such as resolution planning for large banking organisations, as well as how examiners will evaluate whether an organisation is applying a sound methodology to designate which activities and third-party relationships receive more comprehensive oversight.
- Throughout their assessment and responses to the comment letters they received, the regulatory bodies have remained consistent in their position to allow organisations flexibility in their approach and remind them that the guidance is a principles-based approach, meaning specific examples provided are there for context and not intended to be a hard-and-fast checklist of activities. As an example, several organisations have developed subsets of their third-party risk management programs to address specific types of third parties, such as financial market utilities, telecommunication firms and professional services firms. The regulatory bodies address this topic through their commentary to say that organisations can adjust their programs to account for unique circumstances of each third-party relationship but should not take overly broad approaches to categories of third parties without considering the risks of each specific relationship.

The regulatory responses highlight that while changes were made to the proposed guidance to incorporate elements of the most recent OCC FAQ on this topic (OCC 2020-10),[2] largely the changes are intended to allow for organisations to take an approach to third-party risk management that works for their organisation's structure, governance frameworks and risk culture. This is extremely important for all organisations as they assess their current-state programs against the finalised guidance, as this also means that there isn't a silver bullet that will solve an organisation's third-party risk management needs. In other words, organisations won't be able to buy a set of checklists to manage third-party risk effectively

[2] The guidance issued by the agencies on 6 June 2023, rescinds OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29".

and have confidence that this generic approach will align to their own risk appetite and governance frameworks.

Key considerations in the guidance

While a significant portion of the final guidance is substantially similar to the proposed guidance issued in July 2021, following are the main considerations each organisation should review as it assesses the impact of the finalised guidance on its enterprise:

- Maintaining a complete inventory of third-party relationships (and as relevant, key subcontractors) is an expectation highlighted in several parts of the guidance. While this is not a new expectation (in fact, this has always been expected), how organisations manage the data associated with all "business arrangements" will be critical in demonstrating to regulators that they have a complete inventory moving forward. This is inclusive of both traditional vendor relationships as well as affiliate arrangements and other third-party relationships, potentially including referral arrangements, merchant payment processing services (where the bank's clients' clients could ultimately pose risk to the bank), subsidiaries, and joint ventures. This can also include those entities that are both customers and service providers to the organisation, whether contractual or not. As noted previously, if an organisation does create targeted frameworks for specific types of third parties (financial market utilities as an example) to streamline managing those relationships, it is important to remember that those inventories will need to be combined with overall third-party inventory, with the same data points, to demonstrate a complete and accurate inventory of all business arrangements.

- Establishing appropriate organisation structures has been a challenge for the industry since the initial wave of enhanced third-party risk management regulatory guidance in 2013.[3] The updated guidance discusses this challenge and makes note that there is no prescribed approach from an organisational structure perspective. However, in several cases the regulatory bodies note the importance of the individuals involved throughout the lifecycle having the requisite skill sets and experience. This should include experts from across various disciplines, including compliance, risk or technology, as well as legal counsel and external support where necessary. While this shouldn't be a surprise,

[3] For example, "SR 13-19 / CA 13-21: Guidance on Managing Outsourcing Risk," Board of Governors of the Federal Reserve System, 5 December 2013: www.federalreserve.gov/supervisionreg/srletters/sr1319.htm; the guidance issued by the agencies on 6 June 2023, rescinds OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance."

it's a constant reminder that finding the right organisational model to identify, manage and monitor the associated risks with each third-party relationship is crucial, and those individuals involved throughout the lifecycle can make the difference between a successful or problematic program. Larger organisations with mature risk management functions can benefit from centralising onboarding, due diligence and risk monitoring activities to create efficiencies across the organisation. This can also include dedicated teams focused on overseeing those third parties that have services that meet the "critical activity" definition. In other cases, it may be more efficient to have dedicated teams provide end-to-end oversight of specific categories of third parties, such as fintech clients in a banking-as-a-service model.

- The principles-based approach has also highlighted a key component of any successful third-party risk management program, which is integration into an organisation's overall risk management processes. This includes tailoring a third-party risk management program to align with existing risk categories and taxonomies, and with frameworks for mapping and assessing third parties to existing business processes, risks, regulatory requirements and control data (including complementary controls required by the third party to mitigate applicable risks). It also includes aligning on key metrics, risk indicators and risk reporting. Some of the critical areas that require alignment are ensuring that new third-party relationships align with the bank's risk appetite standards, and that if compliance violations or other performance issues are noted regarding a third party, those concerns are addressed in accordance with the bank's issue management standards if applicable.

- The agencies have broadened the definition of "critical activities" to allow more flexibility for how it is applied to organisations. This raises two major items to consider:

    - For several years, there has been debate in third-party risk management circles about whether "critical" is part of the inherent risk rating overall scoring scale (i.e., a scoring scale including "critical" as the top end of its range, triggering the highest level of due diligence requirements), or whether it is a separate and distinct data point that, while correlated to overall inherent risk, is captured separately and focused solely on the operational importance of the third party (i.e., the inherent risk rating could be "Very High" or "High" risk and the services are flagged as supporting "critical activities," triggering additional operational resilience program requirements) and the associated services provided to the organisation. Rather

than addressing which would be the correct interpretation, the regulatory bodies have made a point to, in effect, allow either methodology through its guidance, assuming the organisation applies a sound methodology to designate which activities and relationships receive more comprehensive oversight.[4]

- The guidance also goes out of its way to note that specific types of activities (such as those highlighted originally in OCC 2013-29) should not be considered "critical" for every organisation, but rather each organisation should determine what is critical for its own risk profile. This is important as it also relates to a concept discussed above where, for an organisation that has other requirements to fulfil around mapping critical business processes through its operational resilience program or resolution planning requirements, it should leverage established definitions and program requirements to align on how it will identify and manage "critical activities" with regard to its third parties. By allowing this flexibility, most organisations should be able to solve for the problem of having multiple "critical activities" lists within the organisation across various stakeholder groups.

- While the lifecycle stages remain consistent in the revised guidance (and OCC 2013-29 guidance, for that matter), some key details are important for organisations to note moving forward. These include the following:

  - While not explicitly called out in detail as other global regulatory guidance has in recent years,[5] the Planning section notes a requirement to outline contingency plans in the event the organisation needs to transition the activity in-house or to another third party. Organisations should expect the considerations within the Termination section of the guidance as relevant data points to evaluate in the development of their exit plans for higher risk (including critical) business arrangements.

  - The details of the Due Diligence section remain largely unchanged from previous guidance; however, the section highlights key topics that need to be considered and documented in a manner consistent with the organisation's broader risk management frameworks. These include the identification and disposition of issues noted during due diligence, as well as considerations associated with banks

[4] "Interagency Guidance on Third-Party Relationships," page 32.

[5] For example, "SS2/21 Outsourcing and third party risk management," Bank of England, 29 March 2021: www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss.

deciding to accept the risk that certain business arrangements may not meet specific criteria as defined by the organisation's third-party risk management standards (including those scenarios where documentation is not available or the third party will not provide the requested documentation). This is an important concept to consider from an audit perspective. Assessment teams will need flexibility in how they evaluate potential third-party arrangements and while documentation may not be consistent between each third party reviewed, how assessment teams arrive at their conclusions will need to be documented thoroughly and capture the circumstances of each unique assessment (which again highlights the need for properly trained team members conducting the assessments on behalf of the organisation across each risk domain).

- The guidance addresses the use of industry utilities (e.g., outsourcing specific elements of execution of the lifecycle, including due diligence or ongoing monitoring activities, to assessment services providers, or contracting with outside experts to conduct targeted or onsite assessments on behalf of the organisation) by also reconfirming that the output of those activities must be assessed within the context of the organisation's specific circumstances and performance criteria. While this is also not a new topic, it may call into question the value proposition of these entities and their associated services designed to conduct standardised assessments on behalf of multiple industry participants at once.

- Customer interaction is referenced in several sections of the guidance where it had previously not been mentioned, including several references throughout the Planning section of the lifecycle, and is embedded within other key topics such as operational resilience within the Due Diligence section. This highlights the importance of understanding which third parties have direct or indirect customer interaction and sets the expectation that this will continue to be a focus area of the regulatory bodies and how organisations are managing the associated risks of those third parties. Organisations should leverage regulatory mapping to business process data to support the identification of regulatory requirements associated with the services provided by a third party and ensure specific service level agreements are included in contracts to address these risks, among other oversight controls.

- Operational resilience is discussed in greater detail in the revised guidance, with specific scenarios highlighted for consideration, including whether contracts

should require organisations and their third parties to test business continuity plans jointly, a practice that has been more common in recent years. This reiterates the importance of connecting an operational resilience program to the third-party risk management methodologies, including the treatment for "critical activities."

- Subcontractor oversight will remain a key topic within third-party risk management, but the guidance does provide some minor reprieve in focusing future attention on assessing the third party's own third-party risk management programs versus continuing to push for banks to exercise direct oversight of fourth parties (or their "vendors' vendors").

- The finalised guidance addresses a common issue in contracting where a banking organisation may find it has limited negotiating power as it attempts to include terms, conditions or addendums to its contracts to meet its needs. We find this issue commonly comes up in arrangements with, for example, large global cloud computing or other technology providers. In these cases, organisations should determine whether the contract satisfactorily addresses the risks of using the third party, or if they would be better served using another third party or bringing the services in-house to maintain their desired risk profile. Practically speaking, however, in many cases, the selected third party may remain the best, or only, viable option. Organisations should be prepared and have built within their processes, through due diligence and contracting, the ability to identify these scenarios and have the expectation that additional mitigating controls may be required to onboard specific third parties where contractual standards may not meet the bank's traditional expectations. Examples include the large cloud computing providers where additional controls may be required internally to onboard particular third parties and/or a bank could increase its own insurance coverage to support mitigating the additional risks present based on the agreed-upon contractual language.

- Ongoing monitoring is summarised with three typical activities: review of performance monitoring reports, periodic visits and meetings to discuss performance and operational issues, and regular testing of key banking organisational controls that manage the associated third-party risks. In some cases, this last point tends to be overlooked as these activities traditionally would be connected to business-related testing of internal controls, but the output of that testing can be an early indicator of potential issues for a particular third party. As

noted above, organisations will need to consider their organisational models and who is responsible for performing the performance- and risk-related monitoring activities, recognising that there may be efficiencies for larger organisations to centralise key activities (especially for third parties tagged as "critical").

One noticeable omission from the guidance is concentration risk. While not specifically discussed, references to the topic remain within elements of the guidance, such as when it relates to a dependency on a single provider for multiple activities (Operational Resilience section of Due Diligence) and the geographic considerations related to key subcontractors. One can expect this to remain a relevant topic within third-party risk, and organisations seeking additional clarification should look north of the border to the revised OSFI B-10 guidance, which outlines in greater detail the dimensions of concentration risk that are expected to be monitored and reported for Canadian financial services organisations.

What it means

With the updated guidance now finalised, financial services organisations should assess its impact and what, if any, changes are required to current third-party risk management programs. Given how closely the final guidance now aligns to the previous OCC guidance, those organisations that are primarily regulated by the Federal Reserve or FDIC may have more work to do than national banks to bring their programs up to date.

With that said and as discussed above, with the guidance allowing flexibility in approach and being a principles-based document, organisations should focus primarily on rightsizing their approach to align with their overall risk management programs and ensuring the appropriate skill sets are included in each key lifecycle element. And remember: Sound third-party risk management is not only a risk management activity, but also can be a driver for business efficiency and cost savings and can be a competitive advantage compared to peers. When built with a business-focused mindset, the fundamentals of sound third-party risk management remain the same and are consistent with the revised guidance.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2023 *Fortune* 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About our Third-Party Risk Management services

Every organisation is different and for that reason, a one-size-fits-all approach should not be applied to your third-party risk management program.

Protiviti delivers third-party risk management (TPRM) solutions that are embedded into day-to-day business functions while aligning to industry and regulatory expectations. We identify cost savings, create efficiencies in processes and mitigate today's most critical risks.

Successful TPRM drives value by helping to focus business leaders understanding where the usage of third parties will help increase profitability while ensuring your organisation's ecosystem is built to withstand new and unexpected challenges.

If you're in a regulated environment, we help you drive compliance. If you're in a non-regulated environment, we will help increase profitability.

Contacts

Michael Brauneis
Managing Director
Global Leader, Financial Services Industry Practice
michael.brauneis@protiviti.com

Carol Beaumier
Senior Managing Director
Risk & Compliance
carol.beaumier@protiviti.com

Brian Kostek
Managing Director
Risk & Compliance
brian.kostek@protiviti.com

protiviti®