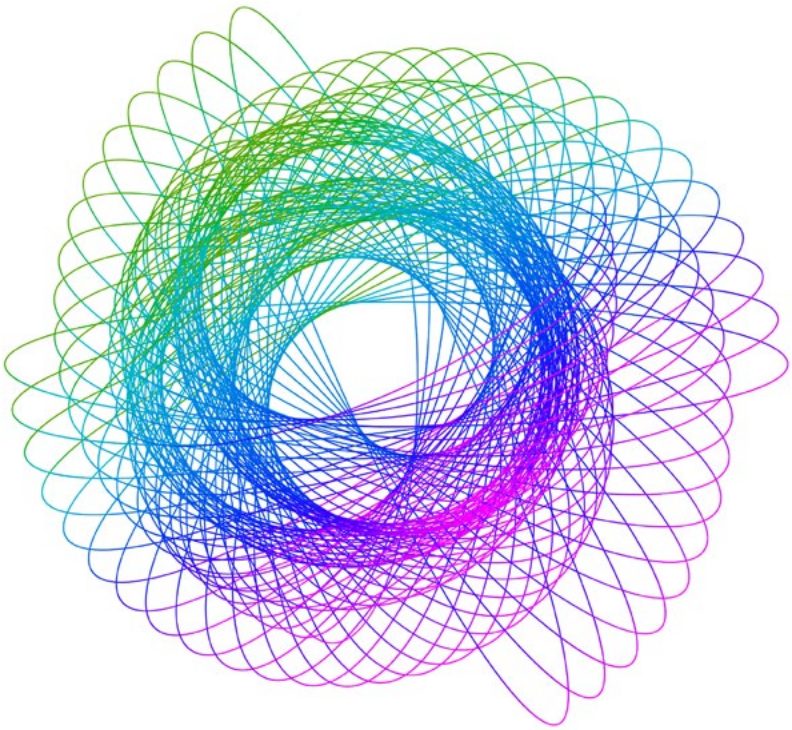
Deloitte.



Federal banking agencies propose updated guidance on third-party risk management

On July 12, 2021, the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) proposed an update to their individual guidance on third-party risk management (TPRM)[1].

This proposed guidance has been issued amid a proliferation of changes to the banking ecosystem, fueled by increased outsourcing activity. In addition, banking regulators are increasingly looking at the role of key service providers of banking organizations as noted in the Federal Financial Institution Examination Council's (FFIEC) statement on risk management for cloud computing services and the interagency proposed rule regulation for computer incident notification[2].

Banking organizations are outsourcing at an unprecedented rate to harness the advantages and wide array of innovative products, services and capabilities that third parties have to offer. While the agencies recognize those advantages, they also emphasize that banking organizations must manage the risks that third parties may pose.

This proposed guidance is intended to promote interagency consistency and modernize current supervisory views.

The jointly proposed guidance aims to:

- Modernize and integrate supervisory expectations on TPRM (leveraging in part the OCC issued Bulletin 2013-29 released in October 2013 and 2020 FAQs that were released in March 2020[3])
- Offer an updated framework based on sound risk management principles for banking organizations across the third-party risk management lifecycle to address enhanced examination and supervisory requirements that relate to third parties
- Outline requirements that observe the level of risk, complexity, and size of the banking organization as well as the nature of the third-party relationship
- Supersede each agency's existing guidance on this topic with applicability across all banking organizations supervised by the respective agencies.

Key Highlights

The Proposed Interagency Guidance on TPRM offers a framework and reemphasizes the investment many banking organizations have made in their TPRM programs. This investment is inclusive of skilled resources, effective processes and enabling technology. Although not an exhaustive list, some key incremental highlights by TPRM lifecycle component compared to the previous OCC 2013-29 guidance are provided below:

Section	Detail
Risk Management	• ***Reemphasizes*** the ***TPRM lifecycle*** and ***explicitly adds "Oversight and Accountability"*** to the lifecycle with no substantial changes to underlying principles of oversight and accountability addressed in the OCC 2013-29 guidance; this oversight extends to board and management oversight across bank-wide activities within a three lines of defense model • Provides ***more specificity*** around what is considered a ***Business Arrangement***[4] noting that neither a contract nor monetary exchange are required to be considered a third party • Includes ***incremental parameters*** for ***"right sizing"*** a banking organization's ***TPRM program***. In addition to the legacy expectation for a banking organization to have a TPRM program commensurate with the level of risk and complexity of its third-party relationships and the risk and complexity of the banking organization's operations. the risk profile of the relationship.
Planning	• Prior to contracting, banking organizations will need to ***evaluate their ability*** to ***provide adequate oversight and management*** of the proposed ***third-party relationship on an ongoing basis***. The evaluation will need to consider whether staffing levels and expertise; risk management and compliance management systems; organizational structure; policies and procedures; or internal control systems need to be adapted for the banking organization to effectively address the business arrangement.
Due Diligence and Third-Party Selection	• Banking organizations will need to consider incremental updates and new requirements to the Due Diligence and Third-Party Selection section based upon the proposed guidance. • There is incremental diligence to be considered when conducting legal, regulatory and compliance checks of third parties, specifically evaluating a ***third-party's ownership structure*** (e.g., including any beneficial ownership, whether public or private, foreign or domestic ownership) • There is added direction around the ***use of risk treatment*** and ***risk review programs to handle situations*** where a banking organization ***may not be able to obtain the desired due diligence information*** from a third party. In these situations, the guidance stresses the importance that in lieu of comprehensive information, it is the bank's responsibility to identify limitations, understand the risks, consider how to mitigate the risks, and determine whether the residual risks are acceptable. • The proposed guidance includes ***new information*** regarding a ***bank's ability to use industry utilities or consortiums***, including development organizations, other banking organizations, or joint efforts to facilitate or supplement due diligence. However, ***using external services does not diminish responsibility*** of the banking organization's board of directors or management to handle third-party relationships in a safe and sound manner and consistent with applicable laws and regulations.
Contract Negotiation	• The Contract Negotiation section includes incremental updates based upon the legacy OCC 2013-29 guidance. For example, the proposed guidance includes ***new data privacy considerations*** and notes contract mechanisms must provide a banking organization the ability to have ***unrestricted access to its data*** whether or not it is in the possession of a third party, as well as the ability to ***access native data*** and to authorize other third parties to access its data during the term of the contract.

Section	Detail
Oversight and Accountability	• The proposed guidance includes a ***new consideration regarding delegation of board responsibilities*** (e.g., approval of significant contracts or plans, oversight of the TPRM program) ***to a "designated board committee"*** (or potentially existing committee with specific mandate) reporting into the board. • In addition, the proposed guidance indicates that management should ***routinely evaluate and test TPRM controls*** and ***confirm*** the banking organization has ***enabling compliance management systems*** in place to facilitate the program.
Ongoing Monitoring	• The proposed guidance ***reemphasizes*** that the ***appropriate degree of ongoing monitoring*** activities should be ***commensurate*** with the ***level of risk and complexity*** of the third-party relationship. More comprehensive monitoring is typically necessary when the third-party relationship is higher risk (e.g., involving critical activities). Banking organizations should ***periodically re-assess existing relationships*** to determine whether the nature of an activity subsequently becomes critical..
Termination	• The proposed guidance largely reflects the legacy OCC 2013-29 guidance on the Termination stage of the TPRM lifecycle. However, it does include an ***incremental consideration*** that in the event of contract default or termination, the banking organization should ***consider other potential third-party service providers*** to which the service could be transitioned..

Conclusion

The agencies are jointly seeking comment on the proposed guidance, including whether concepts from the 2020 FAQs should be incorporated into the final version of the guidance. Comments must be received by September 17, 2021.

Regulators continue to make TPRM a key element of focus in supervisory examinations. To be prepared for when this proposed guidance goes into effect, banking organizations should monitor industry feedback once the comment period closes and:

- Evaluate current TPRM programs against the proposed interagency guidance for input into comment period;
- Determine what incremental enhancement or foundational third-party risk control uplift may be required; and,
- Formulate an implementation plan to realize control effectiveness and ultimately strengthen adherence to the proposed guidance. .

End notes:

1. Board of Governors of the Federal Reserve System (FRB), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC), "Proposed Interagency Guidance on Third-Party Relationships: Risk Management," July 28, 2021.
2. Federal Financial Institution Examination Council (FFIEC), "Joint Statement: Security in a Cloud Computing Environment," accessed July 28, 2021; Deloitte, "Financial services cloud computing regulation Cloud security risk management principles," accessed July 28, 2021; and, FRB, OCC, and FDIC, "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers," accessed July 28, 2021.
3. OCC, "Third-Party Relationships: Risk Management Guidance (Bulletin 2013-29)," accessed July 28, 2021; OCC, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," accessed July 28, 2021; OCC, "Supplemental Examination Procedures for Risk Management of Third-Party Relationships," accessed July 28, 2021; FRB, "Guidance on Managing Outsourcing Risk (SR 13-19)," accessed July 28, 2021; and,FDIC, "Guidance for Managing Third-Party Risk (FIL-44-2008)," accessed July 28, 2021.
4. The agencies state that a third-party relationship is "any business arrangement between a banking organization and another entity, by contract or otherwise." Neither a written contract nor a monetary exchange is necessary to establish a business arrangement. While determinations of business arrangements may vary depending on the facts and circumstances, third-party business arrangements generally exclude a banking organization's customers.

Contacts

Walter Hoogmoed
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Richard Rosenthal
Business & Entity Transformation Lead
Senior Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Amit Jain
Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Brian Adams
Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Srishti Dalani
Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

John Hardwick
Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Jessi Lafferty
Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Heather Beatty
Senior Consultant | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Jake Willcox
Senior Consultant | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Garrett Zeiler
Senior Consultant | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Deloitte Center for Regulatory Strategy

Irena Gecas-McCarthy
FSI Director, Deloitte Center for
Regulatory Strategy, Americas
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Austin Tuell
Manager| Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Kyle Cooke
Senior Consultant | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Deloitte.