OCC Bulletin 2020-10 | March 5, 2020

Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29

To

Chief Executive Officers of All National Banks, Federal Savings Associations, and Federal Branches and Agencies; Department and Division Heads; All Examining Personnel; and Other Interested Parties

Summary

The Office of the Comptroller of the Currency (OCC) is issuing frequently asked questions (FAQ) to supplement OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," issued October 30, 2013. These FAQs are intended to clarify the OCC's existing guidance and reflect evolving industry trends.

This new bulletin rescinds OCC Bulletin 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," issued on June 7, 2017. The FAQs from OCC Bulletin 2017-21 have been incorporated unchanged into this new bulletin, except for question No. 24, which was updated to reflect current AICPA Service Organization Control report information. The FAQ numbers from OCC Bulletin 2017-21 are noted in parentheses throughout this bulletin.

Note for Community Banks

This bulletin applies to community banks.[1]

Highlights

Topics addressed in the new FAQs include

- the terms "third-party relationship" and "business arrangement."
- when cloud computing providers are in a third-party relationship with a bank.
- when data aggregators are in a third-party relationship with a bank.
- risk management when the bank has limited negotiating power in contractual arrangements.

- critical activities and how a bank can determine the risks associated with third-party relationships.
- bank management's responsibilities regarding a third party's subcontractors.
- reliance on and use of third party-provided reports, certificates of compliance, and independent audits.
- risk management when third party has limited ability to provide the same level of due diligence-related information as larger or more established third parties.
- risk management when using a third-party model or when using a third party to assist with model risk management.
- use of third-party assessment services in managing third-party relationship risks.
- a board's approval of contracts.
- risk management when obtaining alternative data from a third party.

Background

OCC Bulletin 2013-29 addresses risk management of third-party relationships. The OCC expects a bank to practice effective risk management regardless of whether the bank performs an activity internally or through a third party. A bank's use of third parties does not diminish the bank's responsibility to perform the activity in a safe and sound manner and in compliance with applicable laws and regulations. A bank's third-party risk management should be commensurate with the level of risk and complexity of its third-party relationships; the higher the risk of the individual relationship, the more robust the third-party risk management should be for that relationship. It is up to bank management to determine the risks associated with each of the bank's third-party relationships.

Frequently Asked Questions

1. **What is a third-party relationship? (originally FAQ No. 1 in OCC Bulletin 2017-21)**
   OCC Bulletin 2013-29 defines a third-party relationship as any business arrangement between the bank and another entity, by contract or otherwise.

   Bank management should conduct in-depth due diligence and ongoing monitoring of each of the bank's third-party service providers that support critical activities. The OCC realizes that although banks may want in-depth information, they may not receive all the information they seek on each critical third-party service provider, particularly from new companies. When a bank does not receive all the information it seeks about third-party service providers that support the bank's critical activities, the OCC expects the bank's board of directors and management to
   - develop appropriate alternative ways to analyze these critical third-party service providers.
   - establish risk-mitigating controls.
   - be prepared to address interruptions in delivery (for example, use multiple payment systems, generators for power, and multiple telecommunications lines in and out of critical sites).
   - make risk-based decisions that these critical third-party service providers are the best service providers available to the bank despite the fact that the bank cannot acquire all the information it wants.
   - retain appropriate documentation of all their efforts to obtain information and related decisions.

- ensure that contracts meet the bank's needs.

2. **What is a "business arrangement?"**
   OCC Bulletin 2013-29 states that a third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise. The term "business arrangement" is meant to be interpreted broadly and is synonymous with the term third-party relationship. A footnote in OCC Bulletin 2013-29 provides examples of business arrangements (third-party relationships), such as activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements in which the bank has an ongoing relationship or may have responsibility for the associated records. Neither a written contract nor a monetary exchange is necessary to establish a business arrangement; all that is necessary is an agreement between the bank and the third party. Business arrangements generally exclude bank customers.

   Traditionally, banks use the terms "vendor" or "outsource" to describe business arrangements and often use these terms instead of third-party relationships. A "vendor" is typically an individual or company offering something for sale, and banks may "outsource" a bank function or task to another company. A bank's relationships with vendors or entities to which banks outsource bank functions or activities do not represent the only types of business arrangements.

   Since the publication of OCC Bulletin 2013-29, business arrangements have expanded and become more varied and, in some cases, more complex. The OCC has received requests for clarification regarding business arrangements and how those arrangements relate to OCC Bulletin 2013-29. The following are some examples:
   - **Referral arrangements:** A referral arrangement is a continuing agreement between a bank and another party (e.g., bank, corporate entity, or individual) in which the bank refers potential customers (or "leads") to the other party in exchange for some form of compensation. The compensation may also be non-financial such as cross-marketing. The bank has a business arrangement with the party receiving the bank's referral.
   - **Appraisers and appraisal management companies:** Some banks maintain an approved panel or list of individual appraisers. When an appraisal is requested, the bank enters into an agreement with an individual appraiser. This establishes a business arrangement between the bank and the individual appraiser. Banks may also outsource the process of engaging real estate appraisers to appraisal management companies. In such an instance, a bank has a business arrangement with the appraisal management company that the bank uses.[2]
   - **Professional service providers:** Service providers such as law firms, consultants, or audit firms often provide professional services to banks. A bank that receives these professional services has a business arrangement with the professional service provider.[3]
   - **Maintenance, catering, and custodial service companies:** There are many companies that a bank or a line of business may need to provide a product or service either to the bank or to the bank's customers. The bank has a business arrangement with each of these types of companies.[4]

3. **Does a company that provides a bank with cloud computing have a third-party relationship with the bank? If so, what are the third-party risk management expectations?**
   Consistent with OCC Bulletin 2013-29, a bank that has a business arrangement with a cloud service provider has a third-party relationship with the cloud service provider. Third-party risk management for cloud computing

services is fundamentally the same as for other third-party relationships. The level of due diligence and oversight should be commensurate with the risk associated with the activity or data using cloud computing. Bank management should keep in mind that specific technical controls in cloud computing may operate differently than in more traditional network environments.

When using cloud computing services, bank management should have a clear understanding of, and should document in the contract, the controls that the cloud service provider is responsible for managing and those controls that the bank is responsible for configuring and managing. Regardless of the division of control responsibilities between the cloud service provider and the bank, the bank is ultimately responsible for the effectiveness of the control environment.

A bank may have a third-party relationship with a third party that has subcontracted with a cloud service provider to house systems that support the third-party service provider. As with other third-party relationships, bank management should conduct due diligence to confirm that the third party can satisfactorily oversee and monitor the cloud service subcontractor.[5] In many cases, independent reports, such as System and Organization Controls (SOC) reports, may be leveraged for this purpose.[6]

4. **If a data aggregator [7] collects customer-permissioned data from a bank, does the data aggregator have a third-party relationship with the bank? If so, what are the third-party risk management expectations?**
A data aggregator typically acts at the request of and on behalf of a bank's customer without the bank's involvement in the arrangement. Banks typically allow for the sharing of customer information, as authorized by the customer, with data aggregators to support customers" choice of financial services. Whether a bank has a business arrangement with the data aggregator depends on the level of formality of any arrangements that the bank has with the data aggregator for sharing customer-permissioned data.

   A bank that has a business arrangement with a data aggregator has a third-party relationship, consistent with the existing guidance in OCC Bulletin 2013-29. Regardless of the structure of the business arrangement for sharing customer-permissioned data, the level of due diligence and ongoing monitoring should be commensurate with the risk to the bank. In many cases, banks may not receive a direct service or benefit from these arrangements. In these cases, the level of risk for banks is typically lower than with more traditional business arrangements. Banks still have a responsibility, however, to manage these relationships in a safe and sound manner with consumer protections.

   Information security and the safeguarding of sensitive customer data should be a key focus for a bank's third-party risk management when a bank is contemplating or has a business arrangement with a data aggregator. A security breach at the data aggregator could compromise numerous customer banking credentials and sensitive customer information, causing harm to the bank's customers and potentially causing reputation and security risk and financial liability for the bank.

   If a bank is not receiving a direct service from a data aggregator and if there is no business arrangement, banks still have risk from sharing customer-permissioned data with a data aggregator. Bank management should perform due diligence to evaluate the business experience and reputation of the data aggregator to gain assurance that the data aggregator maintains controls to safeguard sensitive customer data.

The following are examples of different types of interactions that banks might have with data aggregators.

- **Agreements for banks" use of data aggregation services:**[8] A business arrangement exists when a bank contracts or partners with a data aggregator to use the data aggregator's services to offer or enhance a bank product or service. Due diligence, contract negotiation, and ongoing monitoring should be commensurate with the risk, similar to the bank's risk management of other third-party relationships.
- **Agreements for sharing customer-permissioned data:** Many banks are establishing bilateral agreements with data aggregators for sharing customer-permissioned data, typically through an application programming interface (API).[9] Banks typically establish these agreements to share sensitive customer data through an efficient and secure portal. These business arrangements, using APIs, may reduce the use of less effective methods, such as screen scraping, and can allow bank customers to better define and manage the data they want to share with a data aggregator and limit access to unnecessary sensitive customer data.

  When a bank establishes a contractual relationship with a data aggregator to share sensitive customer data (with the bank customer's permission), the bank has established a business arrangement as defined in OCC Bulletin 2013-29. In such an arrangement, the bank's customer authorizes the sharing of information and the bank typically is not receiving a direct service or financial benefit from the third party. As with other business arrangements, however, banks should gain a level of assurance that the data aggregator is managing sensitive bank customer information appropriately given the potential risk.
- **Screen scraping:** A common method for data aggregation is screen scraping, in which a data aggregator uses the customer's credentials (that the customer has provided) to access the bank's website as if it were the customer. The data aggregator typically uses automated scripts to capture various data, which is then provided to the customer or a financial technology (fintech) application that serves the customer or some other business. Relevant agreements concerning customer-permissioned information sharing are generally between the customer and the financial service provider or the data aggregator and do not involve a contractual relationship with the bank.

  While screen-scraping activities typically do not meet the definition of business arrangement, banks should engage in appropriate risk management for this activity. Screen-scraping can pose operational and reputation risks. Banks should take steps to manage the safety and soundness of the sharing of customer-permissioned data with third parties. Banks" information security monitoring systems, or those of their service providers, should identify large-scale screen scraping activities. When identified, banks should take appropriate steps to identify the source of these activities and conduct appropriate due diligence to gain reasonable assurance of controls for managing this process. These efforts may include research to confirm ownership and understand business practices of the firms; direct communication to learn security and governance practices; review of independent audit reports and assessments; and ongoing monitoring of data-sharing activities.

5. **What type of due diligence and ongoing monitoring should be conducted when a bank enters into a contractual arrangement in which the bank has limited negotiating power?**
   Some companies do not allow banks to negotiate changes to their standard contract, do not share their business resumption and disaster recovery plans, do not allow site visits, or do not respond to a bank's due diligence questionnaire. In these situations, bank management is limited in its ability to conduct the type of due diligence,

contract negotiation, and ongoing monitoring that it normally would, even if the third-party relationship involves or supports a bank's critical activities.

When a bank does not receive all the information it is seeking about a third party that supports the bank's critical activities, bank management should take appropriate actions to manage the risks in that arrangement. Such actions may include

- determining if the risk to the bank of having limited negotiating power is within the bank's risk appetite.
- determining appropriate alternative methods to analyze these critical third parties (e.g., use information posted on the third party's website).
- being prepared to address interruptions in delivery (e.g., use multiple payment systems, generators for power, and multiple telecom lines in and out of critical sites).
- performing sound analysis to support the decision that the specific third party is the most appropriate third party available to the bank.
- retaining appropriate documentation of efforts to obtain information and related decisions.
- confirming that contracts meet the bank's needs even if they are not customized contracts.

6. **How should banks structure their third-party risk management process? (originally FAQ No. 3 in OCC Bulletin 2017-21)**
   There is no one way for banks to structure their third-party risk management process. OCC Bulletin 2013-29 notes that the OCC expects banks to adopt an effective third-party risk management process commensurate with the level of risk and complexity of their third-party relationships. Some banks have dispersed accountability for their third-party risk management process among their business lines. Other banks have centralized the management of the process under their compliance, information security, procurement, or risk management functions. No matter where accountability resides, each applicable business line can provide valuable input into the third-party risk management process, for example, by completing risk assessments, reviewing due diligence questionnaires and documents, and evaluating the controls over the third-party relationship. Personnel in control functions such as audit, risk management, and compliance programs should be involved in the management of third-party relationships. However a bank structures its third-party risk management process, the board is responsible for overseeing the development of an effective third-party risk management process commensurate with the level of risk and complexity of the third-party relationships. Periodic board reporting is essential to ensure that board responsibilities are fulfilled.
7. **OCC Bulletin 2013-29 defines third-party relationships very broadly and reads like it can apply to lower-risk relationships. How can a bank reduce its oversight costs for lower-risk relationships? (originally FAQ No. 2 from OCC Bulletin 2017-21)**
   Not all third-party relationships present the same level of risk. The same relationship may present varying levels of risk across banks. Bank management should determine the risks associated with each third-party relationship and then determine how to adjust risk management practices for each relationship. The goal is for the bank's risk management practices for each relationship to be commensurate with the level of risk and complexity of the third-party relationship. This risk assessment should be periodically updated throughout the relationship. It should not be a one-time assessment conducted at the beginning of the relationship.

   The OCC expects banks to perform due diligence and ongoing monitoring for all third-party relationships. The

level of due diligence and ongoing monitoring, however, may differ for, and should be specific to, each third-party relationship. The level of due diligence and ongoing monitoring should be consistent with the level of risk and complexity posed by each third-party relationship. For critical activities, the OCC expects that due diligence and ongoing monitoring will be robust, comprehensive, and appropriately documented. Additionally, for activities that bank management determines to be low risk, management should follow the bank's board-established policies and procedures for due diligence and ongoing monitoring.

8. **OCC Bulletin 2013-29 states that the OCC expects more comprehensive and rigorous oversight and management of third-party relationships that involve critical activities. What third-party relationships involve critical activities?**

   OCC Bulletin 2013-29 indicates that critical activities include significant bank functions (e.g., payments, clearing, settlements, and custody) or significant shared services (e.g., information technology) or other activities that

   - could cause a bank to face significant risk if the third party fails to meet expectations.
   - could have significant customer impacts.
   - require significant investment in resources to implement the third-party relationship and manage the risk.
   - could have a major impact on bank operations if the bank needs to find an alternate third party or if the outsourced activity has to be brought in-house.

   As part of ongoing monitoring, bank management should periodically assess existing third-party relationships to determine whether the nature of the activity performed constitutes a critical activity. Some banks assign a criticality or risk level to each third-party relationship, whereas others identify critical activities and those third parties associated with the critical activities. Either approach is consistent with the risk management principles in OCC Bulletin 2013-29. Not every relationship involving critical activities is necessarily a critical third-party relationship. Mere involvement in a critical activity does not necessarily make a third party a critical third party. It is common for a bank to have several third-party relationships that support the same critical activity (e.g., a major bank project or initiative), but not all of these relationships are critical to the success of that particular activity. Regardless of a bank's approach, the bank should have a sound methodology for designating which third-party relationships receive more comprehensive and rigorous oversight and risk management.

9. **How should bank management determine the risks associated with third-party relationships?**

   OCC Bulletin 2013-29 recognizes that not all third-party relationships present the same level of risk or criticality to a bank's operations. Risk does not depend on the size of the third-party relationship. For example, a large service provider delivering office supplies might be low risk; a small service provider in a foreign country that provides information technology services to a bank's call center might be considered high risk.

   Some banks categorize their third-party relationships by similar risk characteristics and criticality (e.g., information technology service providers; portfolio managers; catering, maintenance, and groundkeeper providers; and security providers). Bank management then applies different standards for due diligence, contract negotiation, and ongoing monitoring based on the risk profile of the category. By differentiating its third-party service providers by category, risk profile, or criticality, the bank may be able to gain efficiencies in due diligence, contract negotiation, and ongoing monitoring.

   Bank management should determine the risks associated with each third-party relationship or category of relationship. A bank's third-party risk management should be commensurate with the level of risk and complexity

of its third-party relationships; the higher the risk of the individual or category of relationships, the more robust the third-party risk management should be for that relationship or category of relationships. A bank's policies regarding the extent of due diligence, contract negotiation, and ongoing monitoring for third-party relationships should show differences that correspond to different levels of risk.

10. **Is a fintech company arrangement considered a critical activity? (originally FAQ No. 7 from OCC Bulletin 2017-21)**
    A bank's relationship with a fintech company may or may not involve critical bank activities, depending on a number of factors. OCC Bulletin 2013-29 provides criteria that a bank's board and management may use to determine what critical activities are. It is up to each bank's board and management to identify the critical activities of the bank and the third-party relationships related to these critical activities. The board (or committees thereof) should approve the policies and procedures that address how critical activities are identified. Under OCC Bulletin 2013-29, critical activities can include significant bank functions (e.g., payments, clearing, settlements, and custody), significant shared services (e.g., information technology), or other activities that
    - could cause the bank to face significant risk if a third party fails to meet expectations.
    - could have significant bank customer impact.
    - require significant investment in resources to implement third-party relationships and manage risks.
    - could have major impact on bank operations if the bank has to find an alternative third party or if the outsourced activities have to be brought in-house.

    The OCC expects banks to have more comprehensive and rigorous management of third-party relationships that involve critical activities.

11. **What are a bank management's responsibilities regarding a third party's subcontractors?**
    Third parties often enlist the help of suppliers, service providers, or other organizations. OCC Bulletin 2013-29 refers to these entities as subcontractors, which are also referred to as fourth parties.

    As part of due diligence and ongoing monitoring, bank management should determine whether a third party appropriately oversees and monitors its subcontractors. OCC Bulletin 2013-29 includes information about the types of activities bank management should conduct regarding how the bank's third parties oversee and monitor subcontractors.

    Third parties can fail to manage their subcontractors with the same rigor that the bank would have applied if it had engaged the subcontractor directly. To demonstrate its oversight of its subcontractors, a third party may provide a bank with independent reports or certifications. For example, as explained in FAQ No. 23, a SOC 1, type 2, report may be particularly useful, as standards of the American Institute of Certified Public Accountants require the auditor to determine and report on the effectiveness of the client's internal controls over financial reporting and associated controls to monitor relevant subcontractors. In other words, the SOC 1 report may provide bank management useful information for purposes of evaluating whether the third party has effective oversight of its subcontractors.

    During due diligence, bank management should evaluate the volume and types of subcontracted activities and the subcontractors" geographic locations. Bank management should determine the third party's ability to identify and control risks from its use of subcontractors and to determine if the subcontractor's quality of operations is

satisfactory and if the subcontractor has sufficient controls no matter where the subcontractor's operations reside.

Contracts should stipulate when and how the third party will notify the bank of its intent to use a subcontractor as well as how the third party will report to the bank regarding a subcontractor's conformance with performance measures, periodic audit results, compliance with laws and regulations, and other contractual obligations of the third party.

Key areas of consideration for ongoing monitoring may include

- the nature and extent of changes to the third party's reliance on, exposure to, or performance of subcontractors.
- location of subcontractors and bank data.
- whether subcontractors provide services for critical activities.
- whether subcontractors have access to sensitive customer information.
- the third party's monitoring and control testing of subcontractors.

The bank's inventory of third-party relationships should identify the third parties that use subcontractors. This is particularly important for a bank's third-party relationships that support the bank's critical activities or for higher-risk third parties.

12. **When multiple banks use the same third-party service providers, can they collaborate[10] to meet expectations for managing third-party relationships specified in OCC Bulletin 2013-29? (originally FAQ No. 4 from OCC Bulletin 2017-21)**
If they are using the same service providers to secure or obtain like products or services, banks may collaborate[11] to meet certain expectations, such as performing the due diligence, contract negotiation, and ongoing monitoring responsibilities described in OCC Bulletin 2013-29. Like products and services may, however, present a different level of risk to each bank that uses those products or services, making collaboration a useful tool but insufficient to fully meet the bank's responsibilities under OCC Bulletin 2013-29. Collaboration can leverage resources by distributing costs across multiple banks. In addition, many banks that use like products and services from technology or other service providers may become members of user groups. Frequently, these user groups create the opportunity for banks, particularly community banks, to collaborate with their peers on innovative product ideas, enhancements to existing products or services, and customer service and relationship management issues with the service providers. Banks that use a customized product or service may not, however, be able to use collaboration to fully meet their due diligence, contract negotiation, or ongoing responsibilities.

Banks may take advantage of various tools designed to help them evaluate the controls of third-party service providers. In general, these types of tools offer standardized approaches to perform due diligence and ongoing monitoring of third-party service providers by having participating third parties complete common security, privacy, and business resiliency control assessment questionnaires. After third parties complete the questionnaires, the results can be shared with numerous banks and other clients. Collaboration can result in increased negotiating power and lower costs to banks during the contract negotiation phase of the risk management life cycle.

Some community banks have joined an alliance to create a standardized contract with their common third-party service providers and improve negotiating power.

13. **When collaborating to meet responsibilities for managing a relationship with a common third-party service provider, what are some of the responsibilities that each bank still needs to undertake individually to meet the expectations in OCC Bulletin 2013-29? (originally FAQ No. 5 from OCC Bulletin 2017-21)**
While collaborative arrangements can assist banks with their responsibilities in the life cycle phases for third-party risk management, each individual bank should have its own effective third-party risk management process tailored to each bank's specific needs. Some individual bank-specific responsibilities include defining the requirements for planning and termination (e.g., plans to manage the third-party service provider relationship and development of contingency plans in response to termination of service), as well as
    - integrating the use of product and delivery channels into the bank's strategic planning process and ensuring consistency with the bank's internal controls, corporate governance, business plan, and risk appetite.
    - assessing the quantity of risk posed to the bank through the third-party service provider and the ability of the bank to monitor and control the risk.
    - implementing information technology controls at the bank.
    - ongoing benchmarking of service provider performance against the contract or service-level agreement.
    - evaluating the third party's fee structure to determine if it creates incentives that encourage inappropriate risk taking.
    - monitoring the third party's actions on behalf of the bank for compliance with applicable laws and regulations.
    - monitoring the third party's disaster recovery and business continuity time frames for resuming activities and recovering data for consistency with the bank's disaster recovery and business continuity plans.
14. **Can a bank rely on reports, certificates of compliance, and independent audits provided by entities with which it has a third-party relationship?**
In conducting due diligence and ongoing monitoring, bank management may obtain and review various reports (e.g., reports of compliance with service-level agreements, reports of independent reviewers, certificates of compliance with International Organization for Standardization (ISO) standards,[12] or SOC reports).[13] The person reviewing the report, certificate, or audit should have enough experience and expertise to determine whether it sufficiently addresses the risks associated with the third-party relationship.

    OCC Bulletin 2013-29 explains that bank management should consider whether reports contain sufficient information to assess the third party's controls or whether additional scrutiny is necessary through an audit by the bank or other third party at the bank's request. More specifically, management may consider the following:
    - Whether the report, certificate, or scope of the audit is enough to determine if the third-party's control structure will meet the terms of the contract.
    - Whether the report, certificate, or audit is consistent with widely recognized standards.

    For some third-party relationships, such as those with cloud providers that distribute data across several physical locations, on-site audits could be inefficient and costly. The American Institute of Certified Public Accountants has developed cloud-specific SOC reports based on the framework advanced by the Cloud Security Alliance. When available, these reports can provide valuable information to the bank. The Principles for Financial Market

Infrastructures are international standards for payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories. One key objective of the Principles for Financial Market Infrastructures is to encourage clear and comprehensive disclosure by financial market utilities, which are often in third-party relationships with banks. Financial market utilities typically provide disclosures to explain how their businesses and operations reflect each of the applicable Principles for Financial Market Infrastructures. Banks that have third-party relationships with financial market utilities can rely on these disclosures. Banks can also rely on pooled audit reports, which are audits paid for by a group of banks that use the same company for similar products or services.

15. **What collaboration opportunities exist to address cyber threats to banks as well as to their third-party relationships? (originally FAQ No. 6 from OCC Bulletin 2017-21)**
Banks may engage with a number of information-sharing organizations to better understand cyber threats to their own institutions as well as to the third parties with whom they have relationships. Banks participating in information-sharing forums have improved their ability to identify attack tactics and successfully mitigate cyber attacks on their systems. Banks may use the Financial Services Information Sharing and Analysis Center (FS-ISAC), the U.S. Computer Emergency Readiness Team (US-CERT), InfraGard, and other information-sharing organizations to monitor cyber threats and vulnerabilities and to enhance their risk management and internal controls. Banks also may use the FS-ISAC to share information with other banks.

16. **Can a bank engage with a start-up fintech company with limited financial information? (originally FAQ No. 8 from OCC Bulletin 2017-21)**
OCC Bulletin 2013-29 states that banks should consider the financial condition of their third parties during the due diligence stage of the life cycle before the banks have selected or entered into contracts or relationships with third parties. In assessing the financial condition of a start-up or less established fintech company, the bank may consider a company's access to funds, its funding sources, earnings, net cash flow, expected growth, projected borrowing capacity, and other factors that may affect the third party's overall financial stability. Assessing changes to the financial condition of third parties is an expectation of the ongoing monitoring stage of the life cycle. Because it may be receiving limited financial information, the bank should have appropriate contingency plans in case the start-up fintech company experiences a business interruption, fails, or declares bankruptcy and is unable to perform the agreed-upon activities or services.

    Some banks have expressed confusion about whether third-party service providers need to meet a bank's credit underwriting guidelines. OCC Bulletin 2013-29 states that depending on the significance of the third-party relationship, a bank's analysis of a third party's financial condition may be as comprehensive as if the bank were extending credit to the third-party service provider. This statement may have been misunderstood as meaning a bank may not enter into relationships with third parties that do not meet the bank's lending criteria. There is no such requirement or expectation in OCC Bulletin 2013-29.

17. **Some third parties, such as fintechs, start-ups, and small businesses, are often limited in their ability to provide the same level of due diligence-related information as larger or more established third parties. What type of due diligence and ongoing monitoring should be applied to these companies?**
OCC Bulletin 2013-29 states that banks should consider the financial condition of their third parties during due diligence and ongoing monitoring. When third parties, such as fintechs, start-ups, and small businesses, have limited due diligence information, the bank should consider alternative information sources. The bank may consider a company's access to funds, its funding sources, earnings, net cash flow, expected growth, projected

borrowing capacity, and other factors that may affect the third party's overall financial stability. Assessing changes to the financial condition of third parties is an expectation of the ongoing monitoring component of the bank's risk management. When a bank can only obtain limited financial information, the bank should have contingency plans in case this third party experiences a business interruption, fails, or declares bankruptcy and is unable to perform the agreed-upon activities or services.

Bank management has the flexibility to apply different methods of due diligence and ongoing monitoring when a company may not have the same level of corporate infrastructure as larger or more established companies. During due diligence and before signing a contract, bank management should assess the risks posed by the relationship and understand the third party's risk management and control environment. The scope of due diligence and the due diligence method should vary based on the level of risk of the third-party relationship. While due diligence methods may differ, it is important for management to conclude that the third party has a sufficient control environment for the risk involved in the arrangement.

18. **How can a bank offer products or services to underbanked or underserved segments of the population through a third-party relationship with a fintech company? (originally FAQ No. 9 from OCC Bulletin 2017-21)**
Banks have collaborated with fintech companies in several ways to help meet the banking needs of underbanked or underserved consumers. Banks may partner with fintech companies to offer savings, credit, financial planning, or payments in an effort to increase consumer access. In some instances, banks serve only as facilitators for the fintech companies" products or services with one of the products or services coming from the banks. For example, several banks have partnered with fintech companies to establish dedicated interactive kiosks or automated teller machines (ATM) with video services that enable the consumer to speak directly to a bank teller. Frequently, these interactive kiosks or ATMs are installed in retail stores, senior community centers, or other locations that do not have branches to serve the community. Some fintech companies offer other ways for banks to partner with them. For example, a bank's customers can link their savings accounts with the fintech company's application, which can offer incentives to the bank's customers to save for short-term emergencies or achieve specific savings goals.

    In these examples, the fintech company is considered to have a third-party relationship with the bank that falls under the scope of OCC Bulletin 2013-29.

19. **What should a bank consider when entering a marketplace lending arrangement with nonbank entities? (originally FAQ No. 10 from OCC Bulletin 2017-21)**
When engaging in marketplace lending activities, a bank's board and management should understand the relationships among the bank, the marketplace lender, and the borrowers; fully understand the legal, strategic, reputation, operational, and other risks that these arrangements pose; and evaluate the marketplace lender's practices for compliance with applicable laws and regulations. As with any third-party relationship, management at banks involved with marketplace lenders should ensure the risk exposure is consistent with their boards" strategic goals, risk appetite, and safety and soundness objectives. In addition, boards should adopt appropriate policies, inclusive of concentration limitations, before beginning business relationships with marketplace lenders.

    Banks should have the appropriate personnel, processes, and systems so that they can effectively monitor and control the risks inherent within the marketplace lending relationship. Risks include reputation, credit, concentrations, compliance, market, liquidity, and operational risks. For credit risk management, for example,

banks should have adequate loan underwriting guidelines, and management should ensure that loans are underwritten to these guidelines. For compliance risk management, banks should not originate or support marketplace lenders that have inadequate compliance management processes and should monitor the marketplace lenders to ensure that they appropriately implement applicable consumer protection laws, regulations, and guidance. When banks enter into marketplace lending or servicing arrangements, the banks" customers may associate the marketplace lenders" products with those of the banks, thereby introducing reputation risk if the products underperform or harm customers. Also, operational risk can increase quickly if the operational processes of the banks and the marketplace lenders do not include appropriate limits and controls, such as contractually agreed-to loan volume limits and proper underwriting.

To address these risks, banks" due diligence of marketplace lenders should include consulting with the banks" appropriate business units, such as credit, compliance, finance, audit, operations, accounting, legal, and information technology. Contracts or other governing documents should lay out the terms of service-level agreements and contractual obligations. Subsequent significant contractual changes should prompt reevaluation of bank policies, processes, and risk management practices.

20. **Does OCC Bulletin 2013-29 apply when a bank engages a third party to provide bank customers the ability to make mobile payments using their bank accounts, including debit and credit cards? (originally FAQ No. 11 from OCC Bulletin 2017-21)**
When using third-party service providers in mobile payment environments, banks are expected to act in a manner consistent with OCC Bulletin 2013-29. Banks often enter into business arrangements with third-party service providers to provide software and licenses in mobile payment environments. These third-party service providers also provide assistance to the banks and the banks" customers (for example, payment authentication, delivering payment account information to customers" mobile devices, assisting card networks in processing payment transactions, developing or managing mobile software (apps) or hardware, managing back-end servers, or deactivating stolen mobile phones).

    Many bank customers expect to use transaction accounts and credit, debit, or prepaid cards issued by their banks in mobile payment environments. Because almost all banks issue debit cards and offer transaction accounts, banks frequently participate in mobile payment environments even if they do not issue credit cards. Banks should work with mobile payment providers to establish processes for authenticating enrollment of customers" account information that the customers provide to the mobile payment providers.

21. **May a community bank outsource the development, maintenance, monitoring, and compliance responsibilities of its compliance management system? (originally FAQ No. 12 from OCC Bulletin 2017-21)**
Banks may outsource some or all aspects of their compliance management systems to third parties, so long as banks monitor and ensure that third parties comply with current and subsequent changes to consumer laws and regulations. Some banks outsource maintenance or monitoring or use third parties to automate data collection and management processes (for example, to file compliance reports under the Bank Secrecy Act or for mortgage loan application processing or disclosures). The OCC expects all banks to develop and maintain an effective compliance management system and provide fair access to financial services, ensure fair treatment of customers, and comply with consumer protection laws and regulations. Strong compliance management systems include appropriate policies, procedures, practices, training, internal controls, and audit systems to manage and monitor compliance processes as well as a commitment of appropriate compliance resources.

22. **How should bank management address third-party risk management when using a third-party model or a third party to assist with model risk management?**
The principles in OCC Bulletin 2013-29 are relevant when a bank uses a third-party model or uses a third party to assist with model risk management, as are the principles in OCC Bulletin 2011-12, 'sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management." Accordingly, third-party models should be incorporated into the bank's third-party risk management and model risk management processes. Bank management should conduct appropriate due diligence on the third-party relationship and on the model itself.

If the bank lacks sufficient expertise in-house, a bank may decide to engage external resources (i.e., a third party) to help execute certain activities related to model risk management and the bank's ongoing third-party monitoring responsibilities. These activities could include model validation and review, compliance functions, or other activities in support of internal audit. Bank management should understand and evaluate the results of validation and risk control activities that are conducted by third parties. Bank management typically designates an internal party to

- verify that the agreed upon scope of work has been completed by the third party.
- evaluate and track identified issues and ensure they are addressed.
- make sure completed work is incorporated into the bank's model risk management and third-party risk management processes.

Bank management should conduct a risk-based review of each third-party model to determine whether it is working as intended and if the existing validation activities aresufficient. Banks should expect the third party to conduct ongoing performance monitoring and outcomes analysis of the model, disclose results to the bank, and make appropriate modifications and updates to the model over time, if applicable.

Many third-party models can be customized by a bank to meet its needs. A bank's customization choices should be documented and justified as part of the validation. If third parties provide input data or assumptions, the relevance and appropriateness of the data or assumptions should be validated. Bank management should periodically conduct an outcomes analysis of the third-party model's performance using the bank's own outcomes.

Many third parties provide banks with reports of independent certifications or validations of the third-party model. Validation reports provided by a third-party model provider should identify model aspects that were reviewed, highlighting potential deficiencies over a range of financial and economic conditions (as applicable), and determining whether adjustments or other compensating controls are warranted. Effective validation reports include clear executive summaries, with a statement of model purpose and a synopsis of model validation results, including major limitations and key assumptions. Validation reports should not be taken at face value. Bank management should understand any of the limitations experienced by the validator in assessing the processes and codes used in the models.

As part of the planning and termination phases of the third-party risk management life cycle, the bank should have a contingency plan for instances when the third-party model is no longer available or cannot be supported by the third party. Bank management should have as much knowledge in-house as possible, in case the third party or the bank terminates the contract, or if the third party is no longer in business.

23. **Can banks obtain access to interagency technology service providers" (TSP) reports of examination? (originally FAQ No. 13 from OCC Bulletin 2017-21)**
    TSP reports of examination[14] are available only to banks that have contractual relationships with the TSPs at the time of the examination. Because the OCC's (and other federal banking regulators") statutory authority is to examine a TSP that enters into a contractual relationship with a regulated financial institution, the OCC (and other federal banking regulators) cannot provide a copy of a TSP's report of examination to financial institutions that are either considering outsourcing activities to the examined TSP or that enter into a contract after the date of examination.

    Banks can request TSP reports of examination through the banks" respective OCC supervisory office. TSP reports of examination are provided on a request basis. The OCC may, however, proactively distribute TSP reports of examination in certain situations because of significant concerns or other findings to banks with contractual relationships with that particular TSP.

    Although a bank may not share a TSP report of examination or the contents therein with other banks, a bank that has not contracted with a particular TSP may seek information from other banks with information or experience with a particular TSP as well as information from the TSP to meet the bank's due diligence responsibilities.

24. **Can a bank rely on a third party's Service Organization Control (SOC) report, prepared in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 18 (SSAE 18)? (originally FAQ No. 14 from OCC Bulletin 2017-21**
    In meeting its due diligence and ongoing monitoring responsibilities, a bank may review a third party's SOC 1 report prepared in accordance with SSAE 18 to evaluate the third party's client(s)" internal controls over financial reporting, including policies, processes, and internal controls. If a third party uses subcontractors (also referred to as fourth parties), a bank may find the third party's SOC 1 type 2 report particularly useful, as SSAE 18 requires the auditor to determine and report on the effectiveness of controls the third party has implemented to monitor the controls of the subcontractor. In other words, the SOC 1 type 2 report will address the question as to whether the third party has effective oversight of its subcontractors. A bank should consider whether an SOC 1 type 2 report contains sufficient information and is sufficient in scope to assess the third party's risk environment or whether additional audit or review is required for the bank to properly assess the third party's control environment.

25. **How may a bank use third-party assessment services (sometimes referred to as third-party utilities)?**
    Third-party assessment service companies have been formed to help banks with third-party risk management, including due diligence and ongoing monitoring. These companies offer banks a standardized questionnaire with responses from a variety of third parties (particularly information technology-related companies). The benefit of this arrangement is that the third party can provide the same information to many banks using a standardized questionnaire. Banks often pay a fee to the utility to receive the questionnaire. The utility may provide other services in addition to the questionnaire. This form of collaboration can help banks gain efficiencies in due diligence and ongoing monitoring. When a bank uses a third-party utility, it has a business arrangement with the utility, and the utility should be incorporated into the bank's third-party risk management process.

    Bank management should understand how the information contained within the utility report covers the specific services that the bank has obtained from the third party and meets the bank's due diligence and ongoing monitoring needs. For example, in some cases a standardized questionnaire may not be enough if the third party

is supporting a critical activity at the bank, as the information requested on the questionnaire may not be specific to the bank. In these circumstances, bank management may need additional information from the third party.

26. **How does a bank's board of directors approve contracts with third parties that involve critical activities?** OCC Bulletin 2013-29 indicates that a bank's board should approve contracts with third parties that involve critical activities. This statement was not meant to imply that the board must read or be involved with the negotiation of each of these contracts. The board should receive sufficient information to understand the bank's strategy for use of third parties to support products, services, and operations and understand key dependencies, costs, and limitations that the bank has with these third parties. This allows the board to understand the benefits and risks associated with engaging third parties for critical services and knowingly approve the bank's contracts. The board may use executive summaries of contracts in their review and may delegate actual approval of contracts with third parties that involve critical activities to a board committee or senior management.
27. **How should a bank handle third-party risk management when obtaining alternative data from a third party?** Banks may be using or contemplating using a broad range of alternative data in credit underwriting, fraud detection, marketing, pricing, servicing, and account management.[15] For the purpose of this FAQ, alternative data mean information not typically found in the consumer's credit files at the nationwide consumer reporting agencies or customarily provided by consumers as part of applications for credit.[16]

    When contemplating a third-party relationship that may involve the use of alternative data by or on behalf of the bank, bank management should[17]

    - conduct due diligence on third parties before selecting and entering into contracts. The degree of due diligence should be commensurate with the risk to the bank from the third-party relationship.
    - ensure that alternative data usage comports with safe and sound operations. Appropriate data controls include rigorous assessment of the quality and suitability of data to support prudent banking operations. Additionally, the OCC's model risk management guidance contains important principles, including those that may leverage alternative data.
    - analyze relevant consumer protection laws and regulations to understand the opportunities, risks, and compliance requirements before using alternative data. Based on that analysis, data that present greater compliance risk warrant more robust compliance management. Robust compliance management includes appropriate testing, monitoring, and controls to ensure that compliance risks are understood and addressed.
    - conduct ongoing monitoring on third parties in a manner and with a frequency commensurate with the risk to the bank from the third-party relationship.
    - discuss its plans with an OCC portfolio manager, examiner-in-charge, or supervisory office if the use of alternative data from a third-party relationship constitutes a substantial deviation from the bank's existing business plans or material changes in the bank's use of alternative data.

Further Information

Please contact Lazaro Barreiro, Director for Governance and Operational Risk Policy, Operational Risk Division, at (202) 649-6550.

Grovetta N. Gardineer
Senior Deputy Comptroller for Bank Supervision Policy

Related Link

- OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"

---

[1] As used in this bulletin, "banks" refers collectively to national banks, federal savings associations, and federal branches and agencies of foreign banking organizations.

[2] For more information, refer to OCC Bulletin 2019-43, "Appraisals: Appraisal Management Company Registration Requirements."

[3] Refer to OCC Bulletin 2003-12, "Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing: Revised Guidelines on Internal Audit and its Outsourcing."

[4] If a bank considers these activities to be low risk, management should refer to FAQ No. 7 in this bulletin for more information about the extent of due diligence, contract negotiation, and ongoing monitoring that should be conducted for third-party relationships that support or involve low-risk bank activities.

[5] Refer to FAQ No. 11 in this bulletin for more information about a third party's subcontractors.

[6] Refer to FAQ No. 14 in this bulletin for more information on bank reliance on reports, certificates of compliance, and independent audits provided by entities with which the bank has a third-party relationship.

[7] Data aggregators are entities that access, aggregate, share, or store consumer financial account and transaction data that they acquire through connections to financial services companies. Aggregators are often intermediaries between the financial technology (fintech) applications that consumers use to access their data and the sources of data at financial services companies. An aggregator may be a generic provider of data to consumer fintech application providers and other third parties, or the aggregator may be part of a company providing branded and direct services to consumers. Refer to U.S. Department of the Treasury report "A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation" for more information on data aggregators.

[8] Refer to OCC Bulletin 2001-12, "Bank-Provided Account Aggregation Services: Guidance to Banks" (national banks) for more information on direct relationships. While the OCC has not made OCC Bulletin 2001-12 applicable to federal savings associations, federal savings associations may nonetheless find the information in the bulletin relevant.

[9] An API refers to a set of protocols that links two or more systems to enable communication and data exchange between them. An API for a particular routine can easily be inserted into code that uses that API in the software. An example would be the Financial Data Exchange's "FDX API Standard."

[10] Refer to OCC News Release 2015-1, "Collaboration Can Facilitate Community Bank Competitiveness, OCC Says," January 13, 2015.

[11] Any collaborative activities among banks must comply with antitrust laws. Refer to the Federal Trade Commission and U.S. Department of Justice's "Antitrust Guidelines for Collaborations Among Competitors."

[12] Refer to ISO 22301:2012, 'societal Security – Business Continuity Management Systems – Requirements," for more information regarding the ISO's standards for business continuity management.

[13] For more information on types of audits and control reviews, refer to appendix B of the "Internal and External Audits" booklet of the *Comptroller's Handbook*.

[14] The OCC conducts examinations of services provided by significant TSPs based on authorities granted by the Bank Service Company Act, 12 USC 1867. These examinations typically are conducted in coordination with the Board of Governors of the Federal Reserve Board, Federal Deposit Insurance Corporation, and other banking agencies with similar authorities. The scope of examinations focuses on the services provided and key technology and operational controls communicated in the *FFIEC Information Technology Examination Handbook* and other regulatory guidance.

[15] Existing OCC and interagency guidance potentially applicable to alternative data includes "Policy Statement on Discrimination in Lending" (59 Fed. Reg. 18266 (April 15, 1994)); OCC Bulletin 1997-24, "Credit Scoring Models: Examination Guidance"; OCC Bulletin 2011-12, 'sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management"; OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management"; and OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles."

[16] Refer to OCC Bulletin 2019-62, "Consumer Compliance: Interagency Statement on the Use of Alternative Data in Credit Underwriting," for more information about compliance risk management considerations regarding the use of alternative data. Also refer to Consumer Financial Protection Bureau (CFPB), "Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process," 82 Fed. Reg. 11183 (February 21, 2017).

[17] The information in this list is consistent with the Interagency Policy Statement on the Use of Alternative Data in Credit Underwriting.

Topic(s): CORPORATE & RISK GOVERNANCE (CARG) THIRD PARTY RISK MANAGEMENT