OCC Bulletin 2013-29 | October 30, 2013

Third-Party Relationships: Risk Management Guidance

To

Chief Executive Officers and Chief Risk Officers of All National Banks and Federal Savings Associations, Technology Service Providers, Department and Division Heads, All Examining Personnel, and Other Interested Parties

Summary

This bulletin provides guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third-party relationships. A third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise.[1]

The Office of the Comptroller of the Currency (OCC) expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party. A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.[2]

This bulletin rescinds OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," and OCC Advisory Letter 2000-9, "Third-Party Risk." This bulletin supplements and should be used in conjunction with other OCC and interagency issuances on third-party relationships and risk management listed in appendix B. In connection with the issuance of this bulletin, the OCC is applying to federal savings associations (FSA) certain guidance applicable to national banks, as indicated in appendix B.

Highlights

- A bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.
- A bank should ensure comprehensive risk management and oversight of third-party relationships involving critical activities.
- An effective risk management process throughout the life cycle of the relationship includes

- plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party.
- proper due diligence in selecting a third party.
- written contracts that outline the rights and responsibilities of all parties.
- ongoing monitoring of the third party's activities and performance.
- contingency plans for terminating the relationship in an effective manner.
- clear roles and responsibilities for overseeing and managing the relationship and risk management process.
- Documentation and reporting that facilitates oversight, accountability, monitoring, and risk management.
- Independent reviews that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks.

Note for Community Banks

This guidance applies to all banks with third-party relationships. A community bank should adopt risk management practices commensurate with the level of risk and complexity of its third-party relationships. A community bank's board and management should identify those third-party relationships that involve critical activities and ensure the bank has risk management practices in place to assess, monitor, and manage the risks.

Background

Banks continue to increase the number and complexity of relationships with both foreign and domestic third parties, such as

- outsourcing entire bank functions to third parties, such as tax, legal, audit, or information technology operations.
- outsourcing lines of business or products.
- relying on a single third party to perform multiple activities, often to such an extent that the third party becomes an integral component of the bank's operations.
- working with third parties that engage directly with customers.[3]
- contracting with third parties that subcontract activities to other foreign and domestic providers.
- contracting with third parties whose employees, facilities, and subcontractors may be geographically concentrated.
- working with a third party to address deficiencies in bank operations or compliance with laws or regulations.

The OCC is concerned that the quality of risk management over third-party relationships may not be keeping pace with the level of risk and complexity of these relationships. The OCC has identified instances in which bank management has

- failed to properly assess and understand the risks and direct and indirect costs involved in third-party relationships.
- failed to perform adequate due diligence and ongoing monitoring of third-party relationships.
- entered into contracts without assessing the adequacy of a third party's risk management practices.

- entered into contracts that incentivize a third party to take risks that are detrimental to the bank or its customers, in order to maximize the third party's revenues.
- engaged in informal third-party relationships without contracts in place.

These examples represent trends whose associated risks reinforce the need for banks to maintain effective risk management practices over third-party relationships.

Risk Management Life Cycle

The OCC expects a bank to have risk management processes that are commensurate with the level of risk and complexity of its third-party relationships and the bank's organizational structures. Therefore, the OCC expects more comprehensive and rigorous oversight and management of third-party relationships that involve ***critical activities***—significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that

- could cause a bank to face significant risk[4] 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 has to find an alternate third party or if the outsourced activity has to be brought in-house.

An effective third-party risk management process follows a continuous life cycle for all relationships and incorporates the following phases:

Planning:

Developing a plan to manage the relationship is often the first step in the third-party risk management process. This step is helpful for many situations but is necessary when a bank is considering contracts with third parties that involve critical activities.

Due diligence and third-party selection: Conducting a review of a potential third party before signing a contract[5] helps ensure that the bank selects an appropriate third party and understands and controls the risks posed by the relationship, consistent with the bank's risk appetite.

Contract negotiation:

Developing a contract that clearly defines expectations and responsibilities of the third party helps to ensure the contract's enforceability, limit the bank's liability, and mitigate disputes about performance.

Ongoing monitoring: Performing ongoing monitoring of the third-party relationship once the contract is in place is essential to the bank's ability to manage risk of the third-party relationship.

Termination:

Developing a contingency plan to ensure that the bank can transition the activities to another third party, bring the activities in-house, or discontinue the activities when a contract expires, the terms of the contract have been satisfied, in response to contract default, or in response to changes to the bank's or third party's business strategy.

In addition, a bank should perform the following throughout the life cycle of the relationship as part of its risk management process:

Oversight and accountability:

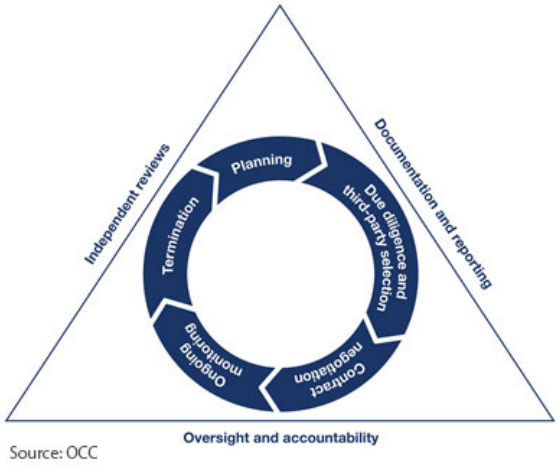
Assigning clear roles and responsibilities for managing third-party relationships and integrating the bank's third-party risk management process with its enterprise risk management framework enables continuous oversight and accountability.

Documentation and reporting: Proper documentation and reporting facilitates oversight, accountability, monitoring, and risk management associated with third-party relationships.

Independent reviews:

Conducting periodic independent reviews of the risk management process enables management to assess whether the process aligns with the bank's strategy and effectively manages risk posed by third-party relationships.

Figure 1: Risk Management Life Cycle



Source: OCC

Before entering into a third-party relationship, senior management should develop a plan to manage the relationship. The management plan should be commensurate with the level of risk and complexity of the third-party relationship and should

- discuss the risks inherent in the activity.
- outline the strategic purposes (e.g., reduce costs, leverage specialized expertise or technology, augment resources, expand or enhance operations), legal and compliance aspects, and inherent risks associated with using third parties, and discuss how the arrangement aligns with the bank's overall strategic goals, objectives, and risk appetite.
- assess the complexity of the arrangement, such as the volume of activity, potential for subcontractors, the technology needed, and the likely degree of foreign-based third-party support.
- determine whether the potential financial benefits outweigh the estimated costs to control the risks (including estimated direct contractual costs and indirect costs to augment or alter bank processes, systems, or staffing to properly manage the third-party relationship or adjust or terminate existing contracts).

- consider how the third-party relationship could affect other strategic bank initiatives, such as large technology projects, organizational changes, mergers, acquisitions, or divestitures.
- consider how the third-party relationship could affect bank and dual employees[6] and what transition steps are needed to manage the impacts when the activities currently conducted internally are outsourced.
- assess the nature of customer interaction with the third party and potential impact the relationship will have on the bank's customers—including access to or use of those customers' confidential information, joint marketing or franchising arrangements, and handling of customer complaints—and outline plans to manage these impacts.
- assess potential information security implications including access to the bank's systems and to its confidential information.
- consider the bank's contingency plans in the event the bank needs to transition the activity to another third party or bring it in-house.
- assess the extent to which the activities are subject to specific laws and regulations (e.g., privacy, information security, Bank Secrecy Act/Anti-Money Laundering (BSA/AML), fiduciary requirements).
- consider whether the selection of the third party is consistent with the bank's broader corporate policies and practices including its diversity policies and practices.
- detail how the bank will select, assess, and oversee the third party, including monitoring the third party's compliance with the contract.
- be presented to and approved by the bank's board of directors when critical activities are involved.

Due Diligence and Third-Party Selection

A bank should conduct due diligence on all potential third parties before selecting and entering into contracts or relationships. A bank should not rely solely on experience with or prior knowledge of the third party as a proxy for an objective, in-depth assessment of the third party's ability to perform the activity in compliance with all applicable laws and regulations and in a safe and sound manner.

The degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. More extensive due diligence is necessary when a third-party relationship involves critical activities. On-site visits may be useful to understand fully the third party's operations and capacity. If the bank uncovers information that warrants additional scrutiny, it should broaden the scope or assessment methods of the due diligence as needed.

The bank should consider the following during due diligence:

Strategies and Goals

Review the third party's overall business strategy and goals to ensure they do not conflict with those of the bank. Consider how the third party's current and proposed strategic business arrangements (such as mergers, acquisitions, divestitures, joint ventures, or joint marketing initiatives) may affect the activity. Also consider reviewing the third party's service philosophies, quality initiatives, efficiency improvements, and employment policies and practices.

Legal and Regulatory Compliance

Evaluate the third party's legal and regulatory compliance program to determine whether the third party has the necessary licenses to operate and the expertise, processes, and controls to enable the bank to remain compliant with

domestic and international laws and regulations. Check compliance status with regulators and self-regulatory organizations as appropriate.

Financial Condition

Assess the third party's financial condition, including reviews of the third party's audited financial statements. Evaluate growth, earnings, pending litigation, unfunded liabilities, and other factors that may affect the third party's overall financial stability. Depending on the significance of the third-party relationship, the bank's analysis may be as comprehensive as if extending credit to the third party.

Business Experience and Reputation

Evaluate the third party's depth of resources and previous experience providing the specific activity. Assess the third party's reputation, including history of customer complaints or litigation. Determine how long the third party has been in business, its market share for the activities, and whether there have been significant changes in the activities offered or in its business model. Conduct reference checks with external organizations and agencies such as the industry associations, Better Business Bureau, Federal Trade Commission, state attorneys general offices, state consumer affairs offices, and similar foreign authorities. Check U.S. Securities and Exchange Commission or other regulatory filings. Review the third party's Websites and other marketing materials to ensure that statements and assertions are in-line with the bank's expectations and do not overstate or misrepresent activities and capabilities. Determine whether and how the third party plans to use the bank's name and reputation in marketing efforts.

Fee Structure and Incentives

Evaluate the third party's normal fee structure and incentives for similar business arrangements to determine if the fee structure and incentives would create burdensome upfront fees or result in inappropriate risk taking by the third party or the bank.

Qualifications, Backgrounds, and Reputations of Company Principals

Ensure the third party periodically conducts thorough background checks on its senior management and employees as well as on subcontractors who may have access to critical systems or confidential information. Ensure that third parties have policies and procedures in place for removing employees who do not meet minimum background check requirements.

Risk Management

Evaluate the effectiveness of the third party's risk management program, including policies, processes, and internal controls. Where applicable, determine whether the third party's internal audit function independently and effectively tests and reports on the third party's internal controls. Evaluate processes for escalating, remediating, and holding management accountable for concerns identified during audits or other independent tests. If available, review Service Organization Control (SOC) reports, prepared in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 16 (SSAE 16). Consider whether these reports contain sufficient information to assess the third party's risk or whether additional scrutiny is required through an audit by the bank or other third party at the bank's request. Consider any certification by independent third parties for compliance with domestic or international internal control standards (e.g., the National Institute of Standards and Technology and the International Standards Organization).

Information Security

Assess the third party's information security program. Determine whether the third party has sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities. When technology is necessary to support service delivery, assess the third party's infrastructure and application security programs, including the software development life cycle and results of vulnerability and penetration tests. Evaluate the third party's ability to implement effective and sustainable corrective actions to address deficiencies discovered during testing.

Management of Information Systems

Gain a clear understanding of the third party's business processes and technology that will be used to support the activity. When technology is a major component of the third-party relationship, review both the bank's and the third party's information systems to identify gaps in service-level expectations, technology, business process and management, or interoperability issues. Review the third party's processes for maintaining accurate inventories of its technology and its subcontractors. Assess the third party's change management processes to ensure that clear roles, responsibilities, and segregation of duties are in place. Understand the third party's performance metrics for its information systems and ensure they meet the bank's expectations.

Resilience

Assess the third party's ability to respond to service disruptions or degradations resulting from natural disasters, human error, or intentional physical or cyber attacks. Determine whether the third party maintains disaster recovery and business continuity plans that specify the time frame to resume activities and recover data. Review the third party's telecommunications redundancy and resilience plans and preparations for known and emerging threats and vulnerabilities, such as wide-scale natural disasters, distributed denial of service attacks, or other intentional or unintentional events. Review the results of business continuity testing and performance during actual disruptions.

Incident-Reporting and Management Programs

Review the third party's incident reporting and management programs to ensure there are clearly documented processes and accountability for identifying, reporting, investigating, and escalating incidents. Ensure that the third party's escalation and notification processes meet the bank's expectations and regulatory requirements.

Physical Security

Evaluate whether the third party has sufficient physical and environmental controls to ensure the safety and security of its facilities, technology systems, and employees.

Human Resource Management

Review the third party's program to train and hold employees accountable for compliance with policies and procedures. Review the third party's succession and redundancy planning for key management and support personnel. Review training programs to ensure that the third party's staff is knowledgeable about changes in laws, regulations, technology, risk, and other factors that may affect the quality of the activities provided.

Reliance on Subcontractors

Evaluate the volume and types of subcontracted activities and the subcontractors' geographic locations. Evaluate the third party's ability to assess, monitor, and mitigate risks from its use of subcontractors and to ensure that the same

level of quality and controls exists no matter where the subcontractors' operations reside. Evaluate whether additional concentration-related risks may arise from the third party's reliance on subcontractors and, if necessary, conduct similar due diligence on the third party's critical subcontractors.

Insurance Coverage

Verify that the third party has fidelity bond coverage to insure against losses attributable to dishonest acts, liability coverage for losses attributable to negligent acts, and hazard insurance covering fire, loss of data, and protection of documents. Determine whether the third party has insurance coverage for its intellectual property rights, as such coverage may not be available under a general commercial policy. The amounts of such coverage should be commensurate with the level of risk involved with the third party's operations and the type of activities to be provided.

Conflicting Contractual Arrangements With Other Parties

Obtain information regarding legally binding arrangements with subcontractors or other parties in cases where the third party has indemnified itself, as such arrangements may transfer risks to the bank. Evaluate the potential legal and financial implications to the bank of these contracts between the third party and its subcontractors or other parties.

Senior management should review the results of the due diligence to determine whether the third party is able to meet the bank's expectations and whether the bank should proceed with the third-party relationship. If the results do not meet expectations, management should recommend that the third party make appropriate changes, find an alternate third party, conduct the activity in-house, or discontinue the activity. As part of any recommended changes, the bank may need to supplement the third party's resources or increase or implement new controls to manage the risks. Management should present results of due diligence to the board when making recommendations for third-party relationships that involve critical activities.

Contract Negotiation

Once the bank selects a third party, management should negotiate a contract that clearly specifies the rights and responsibilities of each party to the contract. Additionally, senior management should obtain board approval of the contract before its execution when a third-party relationship will involve critical activities. A bank should review existing contracts periodically, particularly those involving critical activities, to ensure they continue to address pertinent risk controls and legal protections. Where problems are identified, the bank should seek to renegotiate at the earliest opportunity.

Contracts should generally address the following:

Nature and Scope of Arrangement

Ensure that the contract specifies the nature and scope of the arrangement. For example, a third-party contract should specifically identify the frequency, content, and format of the service, product, or function provided. Include in the contract, as applicable, such ancillary services as software or other technology support and maintenance, employee training, and customer service. Specify which activities the third party is to conduct, whether on or off the bank's premises, and describe the terms governing the use of the bank's information, facilities, personnel, systems, and equipment, as well as access to and use of the bank's or customers' information. When dual employees will be used, clearly articulate their responsibilities and reporting lines.[7]

Performance Measures or Benchmarks

Specify performance measures that define the expectations and responsibilities for both parties including conformance with regulatory standards or rules. Such measures can be used to motivate the third party's performance, penalize poor performance, or reward outstanding performance. Performance measures should not incentivize undesirable performance, such as encouraging processing volume or speed without regard for accuracy, compliance requirements, or adverse effects on customers. Industry standards for service-level agreements may provide a reference point for standardized services, such as payroll processing. For more customized activities, there may be no standard measures. Instead, the bank and third party should agree on appropriate measures.

Responsibilities for Providing, Receiving, and Retaining Information

Ensure that the contract requires the third party to provide and retain timely, accurate, and comprehensive information such as records and reports that allow bank management to monitor performance, service levels, and risks. Stipulate the frequency and type of reports required, for example: performance reports, control audits, financial statements, security reports, BSA/AML and Office of Foreign Asset Control (OFAC) compliance responsibilities and reports for monitoring potential suspicious activity, reports for monitoring customer complaint activity, and business resumption testing reports.

Ensure that the contract sufficiently addresses

- the responsibilities and methods to address failures to adhere to the agreement including the ability of both parties to the agreement to exit the relationship.
- the prompt notification of financial difficulty, catastrophic events, and significant incidents such as information breaches, data loss, service or system interruptions, compliance lapses, enforcement actions, or other regulatory actions.
- the bank's materiality thresholds and procedures for notifying the bank in writing whenever service disruptions, security breaches, or other events pose a significant risk to the bank.
- notification to the bank before making significant changes to the contracted activities, including acquisition, subcontracting, off-shoring, management or key personnel changes, or implementing new or revised policies, processes, and information technology.
- notification to the bank of significant strategic business changes, such as mergers, acquisitions, joint ventures, divestitures, or other business activities that could affect the activities involved.
- the ability of the third party to resell, assign, or permit access to the bank's data and systems to other entities.
- the bank's obligations to notify the third party if the bank implements strategic or operational changes or experiences significant incidents that may affect the third party.

The Right to Audit and Require Remediation

Ensure that the contract establishes the bank's right to audit, monitor performance, and require remediation when issues are identified. Generally, a third-party contract should include provisions for periodic independent internal or external audits of the third party, and relevant subcontractors, at intervals and scopes consistent with the bank's in-house functions to monitor performance with the contract. A bank should include in the contract the types and frequency of audit reports the bank is entitled to receive from the third party (e.g., financial, SSAE 16, SOC 1, SOC 2, and SOC 3 reports, and security reviews). Consider whether to accept audits conducted by the third party's internal or external auditors. Reserve the bank's right to conduct its own audits of the third party's activities or to engage an

independent party to perform such audits. Audit reports should include a review of the third party's risk management and internal control environment as it relates to the activities involved and of the third party's information security program and disaster recovery and business continuity plans.

Responsibility for Compliance With Applicable Laws and Regulations

Ensure the contract addresses compliance with the specific laws, regulations, guidance, and self-regulatory standards applicable to the activities involved, including provisions that outline compliance with certain provisions of the Gramm-Leach-Bliley Act (GLBA) (including privacy and safeguarding of customer information); BSA/AML; OFAC; and Fair Lending and other consumer protection laws and regulations. Ensure that the contract requires the third party to maintain policies and procedures which address the bank's right to conduct periodic reviews so as to verify the third party's compliance with the bank's policies and expectations. Ensure that the contract states the bank has the right to monitor on an ongoing basis the third party's compliance with applicable laws, regulations, and policies and requires remediation if issues arise.

Cost and Compensation

Fully describe compensation, fees, and calculations for base services, as well as any fees based on volume of activity and for special requests. Ensure the contracts do not include burdensome upfront fees or incentives that could result in inappropriate risk taking by the bank or third party. Indicate which party is responsible for payment of legal, audit, and examination fees associated with the activities involved. Consider outlining cost and responsibility for purchasing and maintaining hardware and software. Specify the conditions under which the cost structure may be changed, including limits on any cost increases.

Ownership and License

State whether and how the third party has the right to use the bank's information, technology, and intellectual property, such as the bank's name, logo, trademark, and copyrighted material. Indicate whether any records generated by the third party become the bank's property. Include appropriate warranties on the part of the third party related to its acquisition of licenses for use of any intellectual property developed by other third parties. If the bank purchases software, establish escrow agreements to provide for the bank's access to source code and programs under certain conditions (e.g., insolvency of the third party).

Confidentiality and Integrity

Prohibit the third party and its subcontractors from using or disclosing the bank's information, except as necessary to provide the contracted activities or comply with legal requirements. If the third party receives bank customers' personally identifiable information, the contract should ensure that the third party implements and maintains appropriate security measures to comply with privacy regulations and regulatory guidelines. Specify when and how the third party will disclose, in a timely manner, information security breaches that have resulted in unauthorized intrusions or access that may materially affect the bank or its customers. Stipulate that intrusion notifications include estimates of the effects on the bank and specify corrective action to be taken by the third party. Address the powers of each party to change security and risk management procedures and requirements, and resolve any confidentiality and integrity issues arising out of shared use of facilities owned by the third party. Stipulate whether and how often the bank and the third party will jointly practice incident management plans involving unauthorized intrusions or other breaches in confidentiality and integrity.

Business Resumption and Contingency Plans

Ensure the contract provides for continuation of the business function in the event of problems affecting the third party's operations, including degradations or interruptions resulting from natural disasters, human error, or intentional attacks. Stipulate the third party's responsibility for backing up and otherwise protecting programs, data, and equipment, and for maintaining current and sound business resumption and contingency plans. Include provisions—in the event of the third party's bankruptcy, business failure, or business interruption—for transferring the bank's accounts or activities to another third party without penalty.

Ensure that the contract requires the third party to provide the bank with operating procedures to be carried out in the event business resumption and disaster recovery plans are implemented. Include specific time frames for business resumption and recovery that meet the bank's requirements, and when appropriate, regulatory requirements. Stipulate whether and how often the bank and the third party will jointly practice business resumption and disaster recovery plans.

Indemnification

Consider including indemnification clauses that specify the extent to which the bank will be held liable for claims that cite failure of the third party to perform, including failure of the third party to obtain any necessary intellectual property licenses. Carefully assess indemnification clauses that require the bank to hold the third party harmless from liability.

Insurance

Stipulate that the third party is required to maintain adequate insurance, notify the bank of material changes to coverage, and provide evidence of coverage where appropriate. Types of insurance coverage may include fidelity bond coverage, liability coverage, hazard insurance, and intellectual property insurance.

Dispute Resolution

Consider whether the contract should establish a dispute resolution process (arbitration, mediation, or other means) to resolve problems between the bank and the third party in an expeditious manner, and whether the third party should continue to provide activities to the bank during the dispute resolution period.

Limits on Liability

Determine whether the contract limits the third party's liability and whether the proposed limit is in proportion to the amount of loss the bank might experience because of the third party's failure to perform or to comply with applicable laws. Consider whether a contract would subject the bank to undue risk of litigation, particularly if the third party violates or is accused of violating intellectual property rights.

Default and Termination

Ensure that the contract stipulates what constitutes default, identifies remedies and allows opportunities to cure defaults, and stipulates the circumstances and responsibilities for termination. Determine whether it includes a provision that enables the bank to terminate the contract, upon reasonable notice and without penalty, in the event that the OCC formally directs the bank to terminate the relationship. Ensure the contract permits the bank to terminate the relationship in a timely manner without prohibitive expense. Include termination and notification

requirements with time frames to allow for the orderly conversion to another third party. Provide for the timely return or destruction of the bank's data and other resources and ensure the contract provides for ongoing monitoring of the third party after the contract terms are satisfied as necessary. Clearly assign all costs and obligations associated with transition and termination.

Customer Complaints

Specify whether the bank or third party is responsible for responding to customer complaints. If it is the third party's responsibility, specify provisions that ensure that the third party receives and responds timely to customer complaints and forwards a copy of each complaint and response to the bank. The third party should submit sufficient, timely, and usable information to enable the bank to analyze customer complaint activity and trends for risk management purposes.

Subcontracting

Stipulate when and how the third party should notify the bank of its intent to use a subcontractor. Specify the activities that cannot be subcontracted or whether the bank prohibits the third party from subcontracting activities to certain locations or specific subcontractors. Detail the contractual obligations—such as reporting on the subcontractor's conformance with performance measures, periodic audit results, compliance with laws and regulations, and other contractual obligations. State the third party's liability for activities or actions by its subcontractors and which party is responsible for the costs and resources required for any additional monitoring and management of the subcontractors. Reserve the right to terminate the contract without penalty if the third party's subcontracting arrangements do not comply with the terms of the contract.

Foreign-Based Third Parties

Include in contracts with foreign-based third parties choice-of-law covenants and jurisdictional covenants that provide for adjudication of all disputes between the parties under the laws of a single, specific jurisdiction. Understand that such contracts and covenants may be subject, however, to the interpretation of foreign courts relying on local laws. Foreign courts and laws may differ substantially from U.S. courts and laws in the application and enforcement of choice-of-law covenants, requirements on banks, protection of privacy of customer information, and the types of information that the third party or foreign governmental entities will provide upon request. Therefore, seek legal advice to ensure the enforceability of all aspects of a proposed contract with a foreign-based third party and other legal ramifications of each such arrangement.

OCC Supervision

In contracts with service providers, stipulate that the performance of activities by external parties for the bank is subject to OCC examination oversight, including access to all work papers, drafts, and other materials. The OCC treats as subject to 12 USC 1867(c) and 12 USC 1464(d)(7), situations in which a bank arranges, by contract or otherwise, for the performance of any applicable functions of its operations. Therefore, the OCC generally has the authority to examine and to regulate the functions or operations performed or provided by third parties to the same extent as if they were performed by the bank itself on its own premises.[8]

Ongoing Monitoring

Ongoing monitoring for the duration of the third-party relationship is an essential component of the bank's risk management process. More comprehensive monitoring is necessary when the third-party relationship involves critical activities. Senior management should periodically assess existing third-party relationships to determine whether the nature of the activity performed now constitutes a critical activity.

After entering into a contract with a third party, bank management should dedicate sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the third party commensurate with the level of risk and complexity of the relationship. Regular on site visits may be useful to understand fully the third party's operations and ongoing ability to meet contract requirements. Management should ensure that bank employees that directly manage third-party relationships monitor the third party's activities and performance. A bank should pay particular attention to the quality and sustainability of the third party's controls, and its ability to meet service-level agreements, performance metrics and other contractual terms, and to comply with legal and regulatory requirements.

The OCC expects the bank's ongoing monitoring of third-party relationships to cover the due diligence activities discussed earlier. Because both the level and types of risks may change over the lifetime of third-party relationships, a bank should ensure that its ongoing monitoring adapts accordingly. This monitoring may result in changes to the frequency and types of required reports from the third party, including service-level agreement performance reports, audit reports, and control testing results. In addition to ongoing review of third-party reports, some key areas of consideration for ongoing monitoring may include assessing changes to the third party's

- business strategy (including acquisitions, divestitures, joint ventures) and reputation (including litigation) that may pose conflicting interests and impact its ability to meet contractual obligations and service-level agreements.
- compliance with legal and regulatory requirements.
- financial condition.
- insurance coverage.
- key personnel and ability to retain essential knowledge in support of the activities.
- ability to effectively manage risk by identifying and addressing issues before they are cited in audit reports.
- process for adjusting policies, procedures, and controls in response to changing threats and new vulnerabilities and material breaches or other serious incidents.
- information technology used or the management of information systems.
- ability to respond to and recover from service disruptions or degradations and meet business resilience expectations.
- reliance on, exposure to, or performance of subcontractors; location of subcontractors; and the ongoing monitoring and control testing of subcontractors.
- agreements with other entities that may pose a conflict of interest or introduce reputation, operational, or other risks to the bank.
- ability to maintain the confidentiality and integrity of the bank's information and systems.
- volume, nature, and trends of consumer complaints, in particular those that indicate compliance or risk management problems.
- ability to appropriately remediate customer complaints.

Bank employees who directly manage third-party relationships should escalate to senior management significant issues or concerns arising from ongoing monitoring, such as an increase in risk, material weaknesses and repeat audit findings, deterioration in financial condition, security breaches, data loss, service or system interruptions, or compliance lapses. Additionally, management should ensure that the bank's controls to manage risks from third-party relationships are tested regularly, particularly where critical activities are involved. Based on the results of the ongoing monitoring and internal control testing, management should respond to issues when identified including escalating significant issues to the board.

Termination

A bank may terminate third-party relationships for various reasons, including

- expiration or satisfaction of the contract.
- desire to seek an alternate third party.
- desire to bring the activity in-house or discontinue the activity.
- breach of contract.

Management should ensure that relationships terminate in an efficient manner, whether the activities are transitioned to another third party or in-house, or discontinued. In the event of contract default or termination, the bank should have a plan to bring the service in-house if there are no alternate third parties. This plan should cover

- capabilities, resources, and the time frame required to transition the activity while still managing legal, regulatory, customer, and other impacts that might arise.
- risks associated with data retention and destruction, information system connections and access control issues, or other control concerns that require additional risk management and monitoring during and after the end of the third-party relationship.
- handling of joint intellectual property developed during the course of the arrangement.
- reputation risks to the bank if the termination happens as a result of the third party's inability to meet expectations.

The extent and flexibility of termination rights may vary with the type of activity.

Oversight and Accountability

The bank's board of directors (or a board committee) and senior management are responsible for overseeing the bank's overall risk management processes. The board, senior management, and employees within the lines of businesses who manage the third-party relationships have distinct but interrelated responsibilities to ensure that the relationships and activities are managed effectively and commensurate with their level of risk and complexity, particularly for relationships that involve critical activities:[9]

Board of Directors

- Ensure an effective process is in place to manage risks related to third-party relationships in a manner consistent with the bank's strategic goals, organizational objectives, and risk appetite.

- Approve the bank's risk-based policies that govern the third-party risk management process and identify critical activities.
- Review and approve management plans for using third parties that involve critical activities.
- Review summary of due diligence results and management's recommendations to use third parties that involve critical activities.
- Approve contracts with third parties that involve critical activities.
- Review the results of management's ongoing monitoring of third-party relationships involving critical activities.
- Ensure management takes appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring.
- Review results of periodic independent reviews of the bank's third-party risk management process.

Senior Bank Management

- Develop and implement the bank's third-party risk management process.
- Establish the bank's risk-based policies to govern the third-party risk management process.
- Develop plans for engaging third parties, identify those that involve critical activities, and present plans to the board when critical activities are involved.
- Ensure appropriate due diligence is conducted on potential third parties and present results to the board when making recommendations to use third parties that involve critical activities.
- Review and approve contracts with third parties. Board approval should be obtained for contracts that involve critical activities.
- Ensure ongoing monitoring of third parties, respond to issues when identified, and escalate significant issues to the board.
- Ensure appropriate documentation and reporting throughout the life cycle for all third-party relationships.
- Ensure periodic independent reviews of third-party relationships that involve critical activities and of the bank's third-party risk management process. Analyze the results, take appropriate actions, and report results to the board.
- Hold accountable the bank employees within business lines or functions who manage direct relationships with third parties.
- Terminate arrangements with third parties that do not meet expectations or no longer align with the bank's strategic goals, objectives, or risk appetite.
- Oversee enterprise-wide risk management and reporting of third-party relationships.

Bank Employees Who Directly Manage Third-Party Relationships

- Conduct due diligence of third parties and report results to senior management.
- Ensure that third parties comply with the bank's policies and reporting requirements.
- Perform ongoing monitoring of third parties and ensure compliance with contract terms and service-level agreements.
- Ensure the bank or the third party addresses any issues identified.

- Escalate significant issues to senior management.
- Notify the third party of significant operational issues at the bank that may affect the third party.
- Ensure that the bank has regularly tested controls in place to manage risks associated with third-party relationships.
- Ensure that third parties regularly test and implement agreed-upon remediation when issues arise.
- Maintain appropriate documentation throughout the life cycle.
- Respond to material weaknesses identified by independent reviews.
- Recommend termination of arrangements with third parties that do not meet expectations or no longer align with the bank's strategic goals, objectives, or risk appetite.

Documentation and Reporting

A bank should properly document and report on its third-party risk management process and specific arrangements throughout their life cycle. Proper documentation and reporting facilitates the accountability, monitoring, and risk management associated with third parties and typically includes

- a current inventory of all third-party relationships, which should clearly identify those relationships that involve critical activities and delineate the risks posed by those relationships across the bank.[10]
- approved plans for the use of third-party relationships.
- due diligence results, findings, and recommendations.
- analysis of costs associated with each activity or third-party relationship, including any indirect costs assumed by the bank.
- executed contracts.
- regular risk management and performance reports required and received from the third party (e.g., audit reports, security reviews, and reports indicating compliance with service-level agreements).
- regular reports to the board and senior management on the results of internal control testing and ongoing monitoring of third parties involved in critical activities.
- regular reports to the board and senior management on the results of independent reviews of the bank's overall risk management process.

Independent Reviews

Senior management should ensure that periodic independent reviews are conducted on the third-party risk management process, particularly when a bank involves third parties in critical activities. The bank's internal auditor or an independent third party may perform the reviews, and senior management should ensure the results are reported to the board. Reviews may include assessing the adequacy of the bank's process for

- ensuring third-party relationships align with the bank's business strategy.
- identifying, assessing, managing, and reporting on risks of third-party relationships.
- responding to material breaches, service disruptions, or other material issues.

- identifying and managing risks associated with complex third-party relationships, including foreign-based third parties and subcontractors.
- involving multiple disciplines across the bank as appropriate during each phase of the third-party risk management life cycle.[11]
- ensuring appropriate staffing and expertise to perform due diligence and ongoing monitoring and management of third parties.
- ensuring oversight and accountability for managing third-party relationships (e.g., whether roles and responsibilities are clearly defined and assigned and whether the individuals possess the requisite expertise, resources, and authority).
- ensuring that conflicts of interest or appearances of conflicts of interest do not exist when selecting or overseeing third parties.
- identifying and managing concentration risks that may arise from relying on a single third party for multiple activities, or from geographic concentration of business due to either direct contracting or subcontracting agreements to the same locations.

Senior management should analyze the results of independent reviews to determine whether and how to adjust the bank's third-party risk management process, including policy, reporting, resources, expertise, and controls. Additionally, the results may assist senior management's understanding of the effectiveness of the bank's third-party risk management process so that they can make informed decisions about commencing new or continuing existing third-party relationships, bringing activities in-house, or discontinuing activities. Management should respond promptly and thoroughly to significant issues or concerns identified and escalate to the board if the risk posed is approaching the bank's risk appetite limits.

Supervisory Reviews of Third-Party Relationships

The OCC expects bank management to engage in a robust analytical process to identify, measure, monitor, and control the risks associated with third-party relationships and to avoid excessive risk taking that may threaten a bank's safety and soundness. A bank's failure to have an effective third-party risk management process that is commensurate with the level of risk, complexity of third-party relationships, and organizational structure of the bank may be *an unsafe and unsound banking practice.*

When reviewing third-party relationships, examiners should

- assess the bank's ability to oversee and manage its relationships.
- highlight and discuss material risks and any deficiencies in the bank's risk management process with the board of directors and senior management.
- carefully review the bank's plans for appropriate and sustainable remediation of such deficiencies, particularly those associated with the oversight of third parties that involve critical activities.
- follow existing guidance for citing deficiencies in supervisory findings and reports of examination, and recommend appropriate supervisory actions. These actions may range from citing the deficiencies in Matters Requiring Attention to recommending formal enforcement action.
- consider the findings when assigning the management component of the Federal Financial Institutions Examination Council's (FFIEC) Uniform Financial Institutions Rating System (CAMELS ratings).[12] Serious deficiencies

may result in management being deemed less than satisfactory.

- reflect the associated risks in their overall assessment of the bank's risk profile.

When circumstances warrant, the OCC may use its authority to examine the functions or operations performed by a third party on the bank's behalf. Such examinations may evaluate safety and soundness risks, the financial and operational viability of the third party to fulfill its contractual obligations, compliance with applicable laws and regulations, including consumer protection, fair lending, BSA/AML and OFAC laws, and whether the third party engages in unfair or deceptive acts or practices in violation of federal or applicable state law. The OCC will pursue appropriate corrective measures, including enforcement actions, to address violations of law and regulations or unsafe or unsound banking practices by the bank or its third party. The OCC has the authority to assess a bank a special examination or investigation fee when the OCC examines or investigates the activities of a third party for the bank.

Further Information

"For further information, contact John Eckert, Director, Operational Risk and Core Policy at (202) 649-7163 or john.eckert@occ.treas.gov, or (202) 649-6550.

John C. Lyons Jr.
Senior Deputy Comptroller and Chief National Bank Examiner

APPENDIX A: Risks Associated With Third-Party Relationships

Use of third parties reduces management's direct control of activities and may introduce new or increase existing risks, specifically, operational, compliance, reputation, strategic, and credit risks and the interrelationship of these risks. Increased risk most often arises from greater complexity, ineffective risk management by the bank, and inferior performance by the third party. Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for an expanded discussion of banking risks and their definitions.

Operational Risk

Operational risk is present in all products, services, functions, delivery channels, and processes. Third-party relationships may increase a bank's exposure to operational risk because the bank may not have direct control of the activity performed by the third party.

Operational risk can increase significantly when third-party relationships result in concentrations. Concentrations may arise when a bank relies on a single third party for multiple activities, particularly when several of the activities are critical to bank operations. Additionally, geographic concentrations can arise when a bank's own operations and that of its third parties and subcontractors are located in the same region or are dependent on the same critical power and telecommunications infrastructures.

Compliance Risk

Compliance risk exists when products, services, or systems associated with third-party relationships are not properly reviewed for compliance or when the third party's operations are not consistent with laws, regulations, ethical standards, or the bank's policies and procedures. Such risks also arise when a third party implements or manages a

product or service in a manner that is unfair, deceptive, or abusive to the recipient of the product or service. Compliance risk may arise when a bank licenses or uses technology from a third party that violates a third party's intellectual property rights. Compliance risk may also arise when the third party does not adequately monitor and report transactions for suspicious activities to the bank under the BSA or OFAC. The potential for serious or frequent violations or noncompliance exists when a bank's oversight program does not include appropriate audit and control features, particularly when the third party is implementing new bank activities or expanding existing ones, when activities are further subcontracted, when activities are conducted in foreign countries, or when customer and employee data is transmitted to foreign countries.

Compliance risk increases when conflicts of interest between a bank and a third party are not appropriately managed, when transactions are not adequately monitored for compliance with all necessary laws and regulations, and when a bank or its third parties have not implemented appropriate controls to protect consumer privacy and customer and bank records. Compliance failures by the third party could result in litigation or loss of business to the bank and damage to the bank's reputation.

Reputation Risk

Third-party relationships that do not meet the expectations of the bank's customers expose the bank to reputation risk. Poor service, frequent or prolonged service disruptions, significant or repetitive security lapses, inappropriate sales recommendations, and violations of consumer law and other law can result in litigation, loss of business to the bank, or negative perceptions in the marketplace. Publicity about adverse events surrounding the third parties also may increase the bank's reputation risk. In addition, many of the products and services involved in franchising arrangements expose banks to higher reputation risks. Franchising the bank's attributes often includes direct or subtle reference to the bank's name. Thus, the bank is permitting its attributes to be used in connection with the products and services of a third party. In some cases, however, it is not until something goes wrong with the third party's products, services, or client relationships, that it becomes apparent to the third party's clients that the bank is involved or plays a role in the transactions. When a bank is offering products and services actually originated by third parties as its own, the bank can be exposed to substantial financial loss and damage to its reputation if it fails to maintain adequate quality control over those products and services and adequate oversight over the third party's activities.

Strategic Risk

A bank is exposed to strategic risk if it uses third parties to conduct banking functions or offer products and services that are not compatible with the bank's strategic goals, cannot be effectively monitored and managed by the bank, or do not provide an adequate return on investment. Strategic risk exists in a bank that uses third parties in an effort to remain competitive, increase earnings, or control expense without fully performing due diligence reviews or implementing the appropriate risk management infrastructure to oversee the activity. Strategic risk also arises if management does not possess adequate expertise and experience to oversee properly the third-party relationship.

Conversely, strategic risk can arise if a bank does not use third parties when it is prudent to do so. For example, a bank may introduce strategic risk when it does not leverage third parties that possess greater expertise than the bank does internally, when the third party can more cost effectively supplement internal expertise, or when the third party is more efficient at providing a service with better risk management than the bank can provide internally.

Credit Risk

Credit risk may arise when management has exercised ineffective due diligence and oversight of third parties that market or originate certain types of loans on the bank's behalf, resulting in low-quality receivables and loans. Ineffective oversight of third parties can also result in poor account management, customer service, or collection activities. Likewise, where third parties solicit and refer customers, conduct underwriting analysis, or set up product programs on behalf of the bank, substantial credit risk may be transferred to the bank if the third party is unwilling or unable to fulfill its obligations.

Credit risk also may arise from country or sovereign exposure. To the extent that a bank engages a foreign-based third party, either directly or through subcontractors, the bank may expose itself to country risk.

APPENDIX B: References

Additional guidance about third-party relationships and risk management practices can be found in the following documents.[13]

OCC Guidance

Issuance	Date	Subject	Description/Applicability to FSAs
Comptroller's Handbook	Various	Asset Management series	Each of the booklets in the Comptroller's Handbook Asset Management series provides guidance on oversight of third-party providers. **Applies to FSAs.**
Comptroller's Handbook	September 2013	Other Real Estate Owned	Provides guidance on managing foreclosed properties, including risk management of third-party relationships. **Applies to FSAs.**
Comptroller's Handbook	April 2012	SAFE Act	Provides procedures for examining mortgage loan originator (MLO) activities for compliance with the Secure & Fair Enforcement & Licensing Act of 2008, which mandates a nationwide licensing and registration system for residential MLOs. MLOs may be employees of a bank or third-party vendors. **Applies to FSAs.**
Comptroller's Handbook	May 2011	Servicemembers Civil Relief Act of 2003 (SCRA)	Provides guidance on SCRA requirements applicable to banks and servicers, as a large number of banks outsource loan-servicing functions such as credit administration to third-party servicers.
Comptroller's Handbook	December 2010	Truth in Lending Act	Provides guidance to banks and servicers on the content and timing of disclosures; interest rate calculations; and prohibited activities.
Comptroller's Handbook	September 2010	Real Estate Settlement Procedures	Provides guidance to banks and servicers on the content and timing of pre-settlement and settlement disclosures to borrowers and on prohibited practices.
Comptroller's Handbook	January 2010	Fair Lending	Provides guidance on indicators of potential disparate treatment in loan servicing and loss mitigation; use of vendor-designed credit scorecards; and guidance on evaluating third parties.
Comptroller's Handbook	April 2003	Internal and External Audits	Provides guidelines for banks that outsource internal audit.
Comptroller's Handbook	December 2001	Merchant Processing	Provides guidance on risk management of third-party processors.
Comptroller's Handbook	February 1994	Retail Nondeposit Investment Sales	Provides guidance on risk management and board oversight of third-party vendors selling nondeposit investment products. (See OCC Bulletin 1994-13)

Alert 2012-16	December 21, 2012	Information Security: Distributed Denial of Service Attacks and Customer Account Fraud	Highlights the risks related to these attacks; raises awareness for banks to be prepared to mitigate associated risks. Preparation may include ensuring sufficient resources in conjunction with pre-contracted third-party servicers that can assist in managing the internet-based traffic flow. **Applies to FSAs.**
Alert 2001-4	April 24, 2001	Network Securities Vulnerabilities	Alerts banks to review contracts with service providers to ensure that security maintenance and reporting responsibilities are clearly described.
News Release 2013-116	July 17, 2013	OCC Statement Regarding Oversight of Debt Collection and Debt Sales	Appendix provides guidance on the due diligence and ongoing monitoring of third parties to which banks sell consumer debt. **Applies to FSAs.**
News Release 2012-93	June 21, 2012	Regulators Issue Joint Guidance to Address Mortgage Servicer Practices that Affect Servicemembers	Provides guidance to banks and mortgage servicers, including ensuring that their employees are adequately trained about the options available for homeowners with permanent change of station orders. **Applies to FSAs.**
Bulletin 2013-10	March 29, 2013	Flood Disaster Protection Act: Interagency Statement on Effective Dates of Certain Provisions of the Biggert–Waters Act and Impact on Proposed Interagency Questions and Answers	Provides guidance to lenders or their servicers regarding the contents of notifications to borrowers about flood insurance renewals, force placement to ensure continuity of coverage, use of private flood insurance policies, related insurance fees, and escrow accounts. Provides summaries of new requirements for disclosure contents and timing. **Applies to FSAs.**
Bulletin 2011-39	September 22, 2011	Fair Credit Reporting and Equal Credit Opportunity Acts—Risk-Based Pricing Notices: Final Rules	Provides guidance on notification requirements (timing, content) when adverse credit decision relies on a credit score, including those generated by third-party vendors (i.e., consumer reporting agencies). **Applies to FSAs.**
Bulletin 2011-30	July 6, 2011	Counterparty Credit Risk Management: Interagency Supervisory Guidance	Addresses some of the weaknesses highlighted by the recent financial crisis and reinforces sound governance of counterparty credit risk (CCR) management practices through prudent board and senior management oversight and an effective CCR management framework. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2011-29	June 30, 2011	Foreclosure Management: Supervisory Guidance	Discusses third-party vendor management and reaffirms expectations that management should properly structure, carefully conduct, and prudently manage relationships with third-party vendors, including outside law firms assisting in the foreclosure process. **Applies to FSAs.**
Bulletin 2011-27	June 28, 2011	Prepaid Access Programs: Risk Management Guidance and Sound Practices	Highlights the risks and provides risk management guidance concerning prepaid access programs. **Applies to FSAs.**
Bulletin 2011-26	June 28, 2011	Authentication in an Internet Banking Environment: Supplement	Reinforces the guidance's risk management framework and updates expectations regarding banks' authentications systems and practices whether they

			are provided internally or by a technology service provider. **Applies to FSAs.**
Bulletin 2011-12	April 4, 2011	Sound Practices for Model Risk Management: Supervisory Guidance	Includes guidance on the use of third-party models. **Applies to FSAs.**
Bulletin 2011-11	March 29, 2011	Risk Management Elements: Collective Investment Funds and Outsourcing Arrangements	Expands upon long-standing guidance on sound risk management and beneficiary/participant protections for bank-offered collective investment funds (CIF). The focus is on supervisory concerns that arise if a bank delegates responsibility for a bank CIF to a third-party service provider, such as a registered investment adviser. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2010-42	December 10, 2010	Sound Practices for Appraisals and Evaluations: Interagency Appraisal and Evaluation Guidelines	Provides guidance regarding a bank's responsibility for selecting appraisers and people performing evaluations based on their competence, experience, and knowledge of the market and type of property being valued. **Applies to FSAs.**
Bulletin 2010-30	August 16, 2010	Reverse Mortgages: Interagency Guidance	Provides guidance on managing the compliance and reputation risks when making, purchasing, or servicing reverse mortgages through a third party, such as a mortgage broker or correspondent. **Applies to FSAs.**
Bulletin 2010-7	February 18, 2010	Tax Refund Anticipation Loans: Guidance on Consumer Protection and Safety and Soundness	Provides guidance to enhance, clarify, and increase awareness regarding the measures the OCC expects to see in place for tax refund-related products offered by banks, including issues related to reliance on third-party tax return preparers who interact with consumers.
Bulletin 2010-1	January 8, 2010	Interest Rate Risk: Interagency Advisory on Interest Rate Risk Management	Includes guidance on selection, control frameworks, and validation of third-party asset liability management models. **Applies to FSAs.**
Bulletin 2009-15	May 22, 2009	Investment Securities: Risk Management and Lessons Learned	Provides guidance for banks that use the services of third parties who compile and provide investment analytics for bank management.
Bulletin 2008-12	April 24, 2008	Payment Processors: Risk Management Guidance	Provides guidance to banks regarding relationships with third-party processors and requirements for effective due diligence, underwriting, and monitoring. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2008-5	March 6, 2008	Conflicts of Interest: Risk Management Guidance—Divestiture of Certain Asset Management Businesses	Provides guidance for banks that contemplate divestiture of affiliated funds and associated advisers, whether directly, or through their broader corporate organizations.
Bulletin 2008-4	February 2, 2008	Flood Disaster Protection Act: Flood Hazard Determination Practices	Provides guidance to banks that outsource flood hazard determinations to third-party servicers to ensure that appropriate information is used when performing flood determinations and that revision dates be included in the determination form. **Applies to FSAs with the issuance of this bulletin.**

Bulletin 2006-47	December 13, 2006	Allowance for Loan and Lease Losses (ALLL): Guidance and Frequently Asked Questions (FAQs) on the ALLL	Includes guidance for when some or the entire loan review function and the validation of the ALLL methodology is outsourced to a qualified external party, and identifies the minimum objectives of a loan review program. **Applies to FSAs.**
Bulletin 2006-39	September 1, 2006	Automated Clearing House Activities: Risk Management Guidance	Provides guidance for banks and examiners on managing the risks of automated clearing house (ACH) activity, which can include new and evolving types of ACH transactions as well as new participants in the ACH network, including certain merchants and third parties known as third-party senders. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2005-35	October 12, 2005	Authentication in an Internet Banking Environment: Interagency Guidance	Highlights requirements for banks to use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a technology service provider. **Applies to FSAs.**
Bulletin 2005-27	August 4, 2005	Real Estate Settlement Procedures Act (RESPA): Sham Controlled Business Arrangements	Provides guidance on determining if a RESPA settlement service provider (often a third-party servicer or vendor) is a "controlled business arrangement" and therefore entitled to certain exemptions. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2005-22	May 16, 2005	Home Equity Lending: Credit Risk Management Guidance	Sets forth regulatory expectations for enhanced risk management practices, including management of third-party originations. **Applies to FSAs.**
Bulletin 2005-13	April 14, 2005	Response Programs for Unauthorized Access to Customer Information and Customer Notice: Final Guidance: Interagency Guidance	Provides guidance on banks implementing a response program to address unauthorized access to customer information maintained by the institution or its service providers. **Applies to FSAs.**
Bulletin 2005-1	January 12, 2005	Proper Disposal of Consumer Information: Final Rule	Sets standards for information security. Requires agreements with service providers on disposal. Describes duties of users of consumer reports regarding identity theft. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2004-47	October 27, 2004	FFIEC Guidance: Risk Management for the Use of Free and Open Source Software (FOSS)	Provides guidance for institutions considering using or deploying FOSS regardless of whether it will be provided internally or by a third-party service provider. **Applies to FSAs.**
Bulletin 2004-20	May 10, 2004	Risk Management of New, Expanded, or Modified Bank Products and Services: Risk Management Process	Reminds banks of the risk management process they should follow to prudently manage the risks associated with new, expanded, or modified bank products and services, including those provided by third parties.
Bulletin 2003-15	April 23, 2003	Weblinking: Interagency Guidance on Weblinking Activity	Provides guidance to institutions that develop and maintain their own Websites, as well as institutions that use third-party service providers for this function. **Applies to FSAs.**

Bulletin 2003-12	March 17, 2003	Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing: Revised Guidance on Internal Audit and Its Outsourcing	Reflects developments within the financial, audit, and regulatory industries, particularly the Sarbanes–Oxley Act of 2002 that established numerous independence parameters for audit firms that provide external audit, outsourced internal audit, and other non-audit services for financial institutions. **Applies to FSAs.**
Bulletin 2002-16	May 15, 2002	Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance	Provides guidance on managing the risks that may arise from outsourcing relationships with foreign-based third-party service providers, and addresses the need for banks to establish relationships with foreign-based third-party service providers in a way that does not diminish the ability of the OCC to timely access data or information needed for supervisory activities. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2002-03	January 15, 2002	Real Estate Settlement Procedures Act: Examiner Guidance —Mark-ups of Settlement Service Fees	Provides guidance on determining if a RESPA settlement service provider (often a third-party servicer or vendor) is charging more for a settlement service provided by a third party than is actually paid to the third party and the third party is not involved in the mark-up, which is prohibited by RESPA Section 8(b) (implemented by Regulation X) in most but not all states. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2001-51	December 12, 2001	Privacy of Consumer Financial Information: Small Bank Compliance Guide	Includes guidance for banks to evaluate agreements with nonaffiliated third parties that involve the disclosure of consumer information. **Applies to FSAs.**
Bulletin 2001-12	February 28, 2001	Bank-Provided Account Aggregation Services: Guidance to Banks	Includes guidance for banks that offer aggregation services through third-party service providers.
Bulletin 2001-8	February 15, 2001	Guidelines Establishing Standards for Safeguarding Customer Information: Final Guidelines	Alerts banks that oversight program of service providers should include confirmation that the providers have implemented appropriate measures designed to meet the objectives of the guidelines. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2000-25	September 8, 2000	Privacy Laws and Regulations: Summary of Requirements	Includes guidance for banks to evaluate agreements with third parties that involve the disclosure of consumer information. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2000-14	May 15, 2000	Infrastructure Threats—Intrusion Risks: Message to Bankers and Examiners	Provides guidance on how to prevent, detect, and respond to intrusions into bank computer systems, including outsourced systems.
Bulletin 1999-14	March 29, 1999	Real Estate Settlement Procedures Act: Statement of Policy —Lender Payments to Mortgage Brokers	Provides guidance on services normally performed in loan origination, including those often performed by a third-party servicer or vendor. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 1998-3	March 17, 1998	Technology Risk Management:	Includes a short description of a bank's responsibility with regard to outsourcing its technology products and

		Guidance for Bankers and Examiners	services. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 1996-48	September 3, 1996	Stored Value Card Systems: Information for Bankers and Examiners	Provides basic information to assist banks in identifying and managing risks involved in stored value systems. **Applies to FSAs with the issuance of this bulletin.**
Advisory Letter 2004-6	May 6, 2004	Payroll Card Systems	Advises banks engaged in payroll cards systems involving nonbank third parties to fully comply with OCC guidance on third-party relationships.
Advisory Letter 2002-3	March 22, 2002	Guidance on Unfair or Deceptive Acts or Practices	Describes legal standards and provides guidance on unfair or deceptive acts and practices. Cross references other OCC guidance on: selecting a third-party vendor; monitoring vendor performance; maintaining proper documentation about vendor management; review of contractual arrangements; compensation concerns; monitoring consumer complaints; payment procedures; and loan collection activities.
Advisory Letter 2000-11	November 27, 2000	Title Loan Programs	Alerts banks to OCC concerns over title loan programs, including the involvement of third-party vendors.
Advisory Letter 2000-10	November 27, 2000	Payday Lending	Alerts banks to OCC concerns over payday lending programs, including the involvement of third-party vendors. **Applies to FSAs.**
Banking Circular 181	August 2, 1984	Purchases of Loans in Whole or in Part-Participations	Describes prudent purchases of loans from and loan participations with third parties. **Applies to FSAs with the issuance of this bulletin.**

FFIEC Handbooks

Issuance	Date	Subject	Description
FFIEC Bank Secrecy Act/ Anti-Money Laundering Examination Manual	April 29, 2010	Bank Secrecy Act and Anti-Money Laundering	Provides guidance on identifying and controlling risks associated with money laundering and terrorist financing, including third-party payment processors and professional service providers.
FFIEC Information Technology Examination Handbook	Various	"Outsourcing Technology Services" and "Supervision of Technology Service Providers"	Provides guidance on managing risks associated with the outsourcing of IT services. Several other booklets of the FFIEC IT Examination Handbook also provide guidance addressing third-party relationships.

[1] Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where the bank has an ongoing relationship or may have responsibility for the associated records. Affiliate relationships are also subject to sections 23A and 23B of the Federal Reserve Act (12 USC 371c and 12 USC 371c-1) as implemented in Regulation W (12 CFR 223). Third-party relationships generally do not include customer relationships.

[2] An OCC-supervised bank that provides services to another OCC-supervised bank is held to the same standards of due diligence, controls, and oversight as is a non-bank entity.

[3] For example, in franchising arrangements, the bank lends its name or regulated entity status to activities originated or predominantly conducted by others. Thus, the bank is permitting its attributes to be used in connection with the products and services of a third party. The risks to the bank from these franchising arrangements vary based on the terms of the agreement between the bank and the third party and the nature of the services offered. When a bank is offering products and services originated by third parties as its own, the bank can be exposed to substantial financial loss and damage to its reputation if it fails to

maintain adequate quality control over those products and services and adequate oversight over the third-party activities. Risk may also increase when the third party relies on the bank's regulated entity status and offers services or products through the bank with fees, interest rates, or other terms that cannot be offered by the third party directly.

[4] Refer to appendix A for a discussion of risks associated with third-party relationships.

[5] Except for nondisclosure agreements that may be required in order for the bank to conduct due diligence.

[6] Dual employees are employed by both the bank and the third party.

[7] If the bank enters into a written arrangement under which a broker registered under the securities laws offers brokerage services on or off the premises of the bank, the bank should ensure that the arrangement qualifies for the exception in the Securities and Exchange Act of 1934, 15 USC 78c(a)(4)(B)(i), and Regulation R, 12 CFR 218.700-701 and 17 CFR 247.700-701, for third-party brokerage arrangements. Otherwise, the bank may be required to register as a securities broker under the federal securities laws. The bank also should ensure compliance with regulatory requirements if bank employees receive fees for referrals to the third-party broker.

[8] Before conducting an examination of a third party that is a functionally regulated affiliate (FRA), the OCC is required to give notice to and consult with the FRA's primary regulator and, to the fullest extent possible, avoid duplication of examination activities, reporting requirements, and requests for information. See 12 USC 1831v.

[9] When a third-party relationship involves critical activities, a bank may need to consider appointing a senior officer to provide oversight of that relationship.

[10] Under 12 USC 1867(c)(2), national banks are required to notify the OCC of the existence of a servicing relationship. FSAs are subject to similar requirements set forth in 12 USC 1464(d)(7)(D)(ii) and 12 USC 1867(c)(2). The OCC implements this notification requirement by requiring banks to maintain a current inventory of all third-party relationships and make it available to examiners upon request.

[11] In addition to the functional business units, this may include information technology, identity and access management, physical security, information security, business continuity, compliance, legal, risk management, and human resources.

[12] The CAMELS rating is an overall assessment of a bank based on six individual ratings; the word CAMELS is an acronym for these individual elements of regulatory assessment (capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk).

[13] All guidance applies to national banks. Guidance not currently applicable to FSAs (as noted in this appendix) is undergoing review through the OCC's policy integration efforts.

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