Clarification on the Responsibilities of the Board of Directors February 26, 2021: As described in SR letter 21-4 / CA letter 21-2, "Inactive or Revised SR Letters Related to Federal Reserve Expectations for Boards of Directors," this SR letter was revised as of February 26, 2021 to better reflect the Federal Reserve's guidance for boards of directors in SR letter 21-3 / CA letter 21-1, "Supervisory Guidance on Board of Directors' Effectiveness," and SR letter 16-11, "Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than $100 Billion." No other material changes were made to this letter.

Guidance on Managing Outsourcing Risk

Division of Banking Supervision and Regulation
Division of Consumer and Community Affairs
Board of Governors of the Federal Reserve System

December 5, 2013

Table of Contents

I. Purpose

In addition to traditional core bank processing and information technology services, financial institutions[1] outsource operational activities such as accounting, appraisal management, internal audit, human resources, sales and marketing, loan review, asset and wealth management, procurement, and loan servicing. The Federal Reserve is issuing this guidance to financial institutions to highlight the potential risks arising from the use of service providers and to describe the elements of an appropriate service provider risk management program. This guidance supplements existing guidance on technology service provider (TSP) risk,[2] and applies to service provider relationships where business functions or activities are outsourced. For purposes of this guidance, "service providers" is broadly defined to include all entities[3] that have entered into a contractual relationship with a financial institution to provide business functions or activities.

II. Risks from the Use of Service Providers

The use of service providers to perform operational functions presents various risks to financial institutions. Some risks are inherent to the outsourced activity itself, whereas others are introduced with the involvement of a service provider. If not managed effectively, the use of service providers may expose financial institutions to risks that can result in regulatory action, financial loss, litigation, and loss of reputation. Financial institutions should consider the following risks before entering into and while managing outsourcing arrangements.

- *Compliance risks* arise when the services, products, or activities of a service provider fail to comply with applicable U.S. laws and regulations.
- *Concentration risks* arise when outsourced services or products are provided by a limited number of service providers or are concentrated in limited geographic locations.

[1] For purposes of this guidance, a "financial institution" refers to state member banks, bank and savings and loan holding companies (including their nonbank subsidiaries), and U.S. operations of foreign banking organizations.

[2] Refer to the *FFIEC Outsourcing Technology Services Booklet* (June 2004) at http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx.

[3] Entities may be a bank or nonbank, affiliated or non-affiliated, regulated or non-regulated, or domestic or foreign.

- *Reputational risks* arise when actions or poor performance of a service provider causes the public to form a negative opinion about a financial institution.
- *Country risks* arise when a financial institution engages a foreign-based service provider, exposing the institution to possible economic, social, and political conditions and events from the country where the provider is located.
- *Operational risks* arise when a service provider exposes a financial institution to losses due to inadequate or failed internal processes or systems or from external events and human error.
- *Legal risks* arise when a service provider exposes a financial institution to legal expenses and possible lawsuits.

III. Role of Senior Management

The use of service providers does not relieve a financial institution of the responsibility to ensure that outsourced activities are conducted in a safe-and-sound manner and in compliance with applicable laws and regulations. Senior management should establish policies governing the use of service providers that are appropriate for the range and risks of the institution's outsourced activity and organizational structure. These policies should establish a service provider risk management program that addresses risk assessments and due diligence, standards for contract provisions and considerations, ongoing monitoring of service providers, and business continuity and contingency planning.

Senior management is responsible for ensuring that policies for the use of service providers are appropriately executed. This includes overseeing the development and implementation of an appropriate risk management and reporting framework that includes elements described in this guidance. Senior management is also responsible for providing the institution's board of directors with sufficient information about outsourcing arrangements so that the board can understand the risks posed by these arrangements.

IV. Service Provider Risk Management Programs

A financial institution's service provider risk management program should be risk-focused and provide oversight and controls commensurate with the level of risk presented by the outsourcing arrangements in which the financial institution is engaged. It should focus on outsourced activities that have a substantial impact on a financial institution's financial condition; are critical to the institution's ongoing operations; involve sensitive customer information or new bank products or services; or pose material compliance risk.

The depth and formality of the service provider risk management program will depend on the criticality, complexity, and number of material business activities being outsourced. A community banking organization may have critical business activities being outsourced, but the number may be few and to highly reputable service providers. Therefore, the risk management program may be simpler and use less elements and considerations. For those financial institutions that may use hundreds or thousands of service providers for numerous business activities that have material risk, the financial institution may find that they need to use many more elements and considerations of a service provider risk management program to manage the higher level of risk and reliance on service providers.

While the activities necessary to implement an effective service provider risk management program can vary based on the scope and nature of a financial institution's outsourced activities, effective programs usually include the following core elements:

A. Risk assessments;

B. Due diligence and selection of service providers;

C. Contract provisions and considerations;

D. Incentive compensation review;

E. Oversight and monitoring of service providers; and

F. Business continuity and contingency plans.

A. Risk Assessments

Risk assessment of a business activity and the implications of performing the activity in-house or having the activity performed by a service provider are fundamental to the decision of whether or not to outsource. A financial institution should determine whether outsourcing an activity is consistent with the strategic direction and overall business strategy of the organization. After that determination is made, a financial institution should analyze the benefits and risks of outsourcing the proposed activity as well as the service provider risk, and determine cost implications for establishing the outsourcing arrangement. Consideration should also be given to the availability of qualified and experienced service providers to perform the service on an ongoing basis. Additionally, management should consider the financial institution's ability and expertise to provide appropriate oversight and management of the relationship with the service provider.

This risk assessment should be updated at appropriate intervals consistent with the financial institution's service provider risk management program. A financial institution should revise its risk mitigation plans, if appropriate, based on the results of the updated risk assessment.

B. Due Diligence and Selection of Service Providers

A financial institution should conduct an evaluation of and perform the necessary due diligence for a prospective service provider prior to engaging the service provider. The depth and formality of the due diligence performed will vary depending on the scope, complexity, and importance of the planned outsourcing arrangement, the financial institution's familiarity with prospective service providers, and the reputation and industry standing of the service provider. Throughout the due diligence process, financial institution technical experts and key stakeholders should be engaged in the review and approval process as needed. The overall due diligence process includes a review of the service provider with regard to:

1. Business background, reputation, and strategy;
2. Financial performance and condition; and
3. Operations and internal controls.

1. Business Background, Reputation, and Strategy

Financial institutions should review a prospective service provider's status in the industry and corporate history and qualifications; review the background and reputation of the service provider and its principals; and ensure that the service provider has an appropriate background check program for its employees.

The service provider's experience in providing the proposed service should be evaluated in order to assess its qualifications and competencies to perform the service. The service provider's business model, including its business strategy and mission, service philosophy, quality initiatives, and organizational policies should be evaluated. Financial institutions should also consider the resiliency and adaptability of the service provider's business model as factors in assessing the future viability of the provider to perform services.

Financial institutions should check the service provider's references to ascertain its performance record, and verify any required licenses and certifications. Financial institutions should also verify whether there are any pending legal or regulatory compliance issues (for example, litigation, regulatory actions, or complaints) that are associated with the prospective service provider and its principals.

2. Financial Performance and Condition

Financial institutions should review the financial condition of the service provider and its closely-related affiliates. The financial review may include:

- The service provider's most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity and operating results.

- The service provider's sustainability, including factors such as the length of time that the service provider has been in business and the service provider's growth of market share for a given service.
- The potential impact of the financial institution's business relationship on the service provider's financial condition.
- The service provider's commitment (both in terms of financial and staff resources) to provide the contracted services to the financial institution for the duration of the contract.
- The adequacy of the service provider's insurance coverage.
- The adequacy of the service provider's review of the financial condition of any subcontractors.
- Other current issues the service provider may be facing that could affect future financial performance.

3. Operations and Internal Controls

Financial institutions are responsible for ensuring that services provided by service providers comply with applicable laws and regulations and are consistent with safe-and-sound banking practices. Financial institutions should evaluate the adequacy of standards, policies, and procedures. Depending on the characteristics of the outsourced activity, some or all of the following may need to be reviewed:

- Internal controls;
- Facilities management (such as access requirements or sharing of facilities);
- Training, including compliance training for staff;
- Security of systems (for example, data and equipment);
- Privacy protection of the financial institution's confidential information;
- Maintenance and retention of records;
- Business resumption and contingency planning;
- Systems development and maintenance;
- Service support and delivery;
- Employee background checks; and
- Adherence to applicable laws, regulations, and supervisory guidance.

C. Contract Provisions and Considerations

Financial institutions should understand the service contract and legal issues associated with proposed outsourcing arrangements. The terms of service agreements should be defined in written contracts that have been reviewed by the financial institution's legal counsel prior to execution. The characteristics of the business activity being outsourced and the service provider's strategy for providing those services will determine the terms of the contract. Elements of well-defined contracts and service agreements usually include:

- ***Scope:*** Contracts should clearly define the rights and responsibilities of each party, including:
  - Support, maintenance, and customer service;
  - Contract timeframes;
  - Compliance with applicable laws, regulations, and regulatory guidance;
  - Training of financial institution employees;
  - The ability to subcontract services;
  - The distribution of any required statements or disclosures to the financial institution's customers;
  - Insurance coverage requirements; and
  - Terms governing the use of the financial institution's property, equipment, and staff.
- ***Cost and compensation:*** Contracts should describe the compensation, variable charges, and any fees to be paid for non-recurring items and special requests. Agreements should also address which party is responsible for the payment of any legal, audit, and examination fees related to the activity being performed by the service provider. Where applicable, agreements should address the party responsible for the expense, purchasing, and maintenance of any equipment, hardware, software or any other item related to the activity being performed by the service provider. In addition, financial institutions should ensure that any incentives (for example, in the form of variable charges, such as fees and/or commissions) provided in contracts do not provide potential incentives to take imprudent risks on behalf of the institution.
- ***Right to audit:*** Agreements may provide for the right of the institution or its representatives to audit the service provider and/or to have access to audit reports. Agreements should define the types of audit reports the financial institution will receive and the frequency of the audits and reports.
- ***Establishment and monitoring of performance standards:*** Agreements should define measurable performance standards for the services or products being provided.

- ***Confidentiality and security of information:*** Consistent with applicable laws, regulations, and supervisory guidance, service providers should ensure the security and confidentiality of both the financial institution's confidential information and the financial institution's customer information. Information security measures for outsourced functions should be viewed as if the activity were being performed by the financial institution and afforded the same protections. Financial institutions have a responsibility to ensure service providers take appropriate measures designed to meet the objectives of the information security guidelines within Federal Financial Institutions Examination Council (FFIEC) guidance[4], as well as comply with section 501(b) of the Gramm-Leach-Bliley Act. These measures should be mapped directly to the security processes at financial institutions, as well as be included or referenced in agreements between financial institutions and service providers.

  Service agreements should also address service provider use of financial institution information and its customer information. Information made available to the service provider should be limited to what is needed to provide the contracted services. Service providers may reveal confidential supervisory information only to the extent authorized under applicable laws and regulations.[5]

  If service providers handle any of the financial institution customer's Nonpublic Personal Information (NPPI), the service providers must comply with applicable privacy laws and regulations.[6] Financial institutions should require notification from service providers of any breaches involving the disclosure of NPPI data. Generally, NPPI data is any nonpublic personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) derived using any personally identifiable financial information that is not publicly available.[7] Financial institutions and their service providers who maintain, store, or process NPPI data are responsible for that information and any disclosure of it. The security of, retention of, and access to NPPI data should be addressed in any contracts with service providers.

  When a breach or compromise of NPPI data occurs, financial institutions have legal requirements that vary by state and these requirements should be made part of the contracts between the financial institution and any service provider that provides storage, processing, or transmission of NPPI data. Misuse or unauthorized disclosure of confidential customer data by service providers may expose financial institutions to liability or action by a federal or state regulatory agency. Contracts should clearly authorize and disclose the roles and responsibilities of financial institutions and service providers regarding NPPI data.

---

[4] For further guidance regarding vendor security practices, refer to the *FFIEC Information Security Booklet* (July 2006) at http://ithandbook.ffiec.gov/it-booklets/information-security.aspx.

[5] *See* 12 CFR Part 261.

[6] *See* 12 CFR Part 1016.

[7] *See* 12 U.S.C. 6801(b).

- ***Ownership and license:*** Agreements should define the ability and circumstances under which service providers may use financial institution property inclusive of data, hardware, software, and intellectual property. Agreements should address the ownership and control of any information generated by service providers. If financial institutions purchase software from service providers, escrow agreements may be needed to ensure that financial institutions have the ability to access the source code and programs under certain conditions.[8]

- ***Indemnification:*** Agreements should provide for service provider indemnification of financial institutions for any claims against financial institutions resulting from the service provider's negligence.

- ***Default and termination:*** Agreements should define events of a contractual default, list of acceptable remedies, and provide opportunities for curing default. Agreements should also define termination rights, including change in control, merger or acquisition, increase in fees, failure to meet performance standards, failure to fulfill the contractual obligations, failure to provide required notices, and failure to prevent violations of law, bankruptcy, closure, or insolvency. Contracts should include termination and notification requirements that provide financial institutions with sufficient time to transfer services to another service provider. Agreements should also address a service provider's preservation and timely return of financial institution data, records, and other resources.

- ***Dispute resolution:*** Agreements should include a dispute resolution process in order to expedite problem resolution and address the continuation of the arrangement between the parties during the dispute resolution period.

- ***Limits on liability:*** Service providers may want to contractually limit their liability. Financial institutions should determine whether the proposed limitations are reasonable when compared to the risks to the institution if a service provider fails to perform.[9]

- ***Insurance:*** Service providers should have adequate insurance and provide financial institutions with proof of insurance. Further, service providers should notify financial institutions when there is a material change in their insurance coverage.

- ***Customer complaints:*** Agreements should specify the responsibilities of financial institutions and service providers related to responding to customer complaints. If service providers are responsible for customer complaint resolution, agreements

---

[8] Escrow agreements are established with vendors when buying or leasing products that have underlying proprietary software. In such agreements, an organization can only access the source program code under specific conditions, such as discontinued product support or financial insolvency of the vendor.

[9] Refer to SR letter 06-4, "Interagency Advisory on the Unsafe and Unsound Use of Limitations on Liability Provisions in External Audit Engagement Letters," regarding restrictions on the liability limitations for external audit engagements at http://www.federalreserve.gov/boarddocs/srletters/2006/SR0604.htm.

should provide for summary reports to the financial institutions that track the status and resolution of complaints.

- ***Business resumption and contingency plan of the service provider:*** Agreements should address the continuation of services provided by service providers in the event of operational failures. Agreements should address service provider responsibility for backing up information and maintaining disaster recovery and contingency plans. Agreements may include a service provider's responsibility for testing of plans and providing testing results to financial institutions.

- ***Foreign-based service providers:*** For agreements with foreign-based service providers, financial institutions should consider including express choice of law and jurisdictional provisions that would provide for the adjudication of all disputes between the two parties under the laws of a single, specific jurisdiction. Such agreements may be subject to the interpretation of foreign courts relying on local laws. Foreign law may differ from U.S. law in the enforcement of contracts. As a result, financial institutions should seek legal advice regarding the enforceability of all aspects of proposed contracts with foreign-based service providers and the other legal ramifications of such arrangements.

- ***Subcontracting:*** If agreements allow for subcontracting, the same contractual provisions should apply to the subcontractor. Contract provisions should clearly state that the primary service provider has overall accountability for all services that the service provider and its subcontractors provide. Agreements should define the services that may be subcontracted, the service provider's due diligence process for engaging and monitoring subcontractors, and the notification and approval requirements regarding changes to the service provider's subcontractors. Financial institutions should pay special attention to any foreign subcontractors, as information security and data privacy standards may be different in other jurisdictions. Additionally, agreements should include the service provider's process for assessing the subcontractor's financial condition to fulfill contractual obligations.

D. Incentive Compensation Review

Financial institutions should also ensure that an effective process is in place to review and approve any incentive compensation that may be embedded in service provider contracts, including a review of whether existing governance and controls are adequate in light of risks arising from incentive compensation arrangements. As the service provider represents the institution by selling products or services on its behalf, the institution should consider whether the incentives provided might encourage the service provider to take imprudent risks. Inappropriately structured incentives may result in reputational damage, increased litigation, or other risks to the financial institution. An example of an inappropriate incentive would be one where variable fees or commissions encourage the service provider to direct customers to products with higher profit margins without due consideration of whether such products are suitable for the customer.

E. Oversight and Monitoring of Service Providers

To effectively monitor contractual requirements, financial institutions should establish acceptable performance metrics that the business line or relationship management determines to be indicative of acceptable performance levels. Financial institutions should ensure that personnel with oversight and management responsibilities for service providers have the appropriate level of expertise and stature to manage the outsourcing arrangement. The oversight process, including the level and frequency of management reporting, should be risk-focused. Higher risk service providers may require more frequent assessment and monitoring and may require financial institutions to designate individuals or a group as a point of contact for those service providers. Financial institutions should tailor and implement risk mitigation plans for higher risk service providers that may include processes such as additional reporting by the service provider or heightened monitoring by the financial institution. Further, more frequent and stringent monitoring is necessary for service providers that exhibit performance, financial, compliance, or control concerns. For lower risk service providers, the level of monitoring can be lessened.

Financial condition: Financial institutions should have established procedures to monitor the financial condition of service providers to evaluate their ongoing viability. In performing these assessments, financial institutions should review the most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity and operating results. If a service provider relies significantly on subcontractors to provide services to financial institutions, then the service provider's controls and due diligence regarding the subcontractors should also be reviewed.

***Internal controls*:** For significant service provider relationships, financial institutions should assess the adequacy of the provider's control environment. Assessments should include reviewing available audits or reports such as the American Institute of Certified Public Accountants' Service Organization Control 2 report.[10] If the service provider delivers information technology services, the financial institution can request the FFIEC Technology Service Provider examination report from its primary federal regulator. Security incidents at the service provider may also necessitate the institution to elevate its monitoring of the service provider.

Escalation of oversight activities: Financial institutions should ensure that risk management processes include triggers to escalate oversight and monitoring when service providers are failing to meet performance, compliance, control, or viability expectations. These procedures should include more frequent and stringent monitoring and follow-up on identified issues, on-site control reviews, and when an institution should exercise its right to audit a service provider's adherence to the terms of the agreement. Financial institutions should develop criteria for engaging alternative outsourcing arrangements and terminating the service provider contract in the event that identified issues are not adequately addressed in a timely manner.

[10] Refer to www.AICPA.org.

F. Business Continuity and Contingency Considerations

Various events may affect a service provider's ability to provide contracted services. For example, services could be disrupted by a provider's performance failure, operational disruption, financial difficulty, or failure of business continuity and contingency plans during operational disruptions or natural disasters. Financial institution contingency plans should focus on critical services provided by service providers and consider alternative arrangements in the event that a service provider is unable to perform.[11] When preparing contingency plans, financial institutions should:

- Ensure that a disaster recovery and business continuity plan exists with regard to the contracted services and products;
- Assess the adequacy and effectiveness of a service provider's disaster recovery and business continuity plan and its alignment to their own plan;
- Document the roles and responsibilities for maintaining and testing the service provider's business continuity and contingency plans;
- Test the service provider's business continuity and contingency plans on a periodic basis to ensure adequacy and effectiveness; and
- Maintain an exit strategy, including a pool of comparable service providers, in the event that a contracted service provider is unable to perform.

G. Additional Risk Considerations

Suspicious Activity Report (SAR) reporting functions: The confidentiality of suspicious activity reporting makes the outsourcing of any SAR-related function more complex. Financial institutions need to identify and monitor the risks associated with using service providers to perform certain suspicious activity reporting functions in compliance with the Bank Secrecy Act (BSA). Financial institution management should ensure they understand the risks associated with such an arrangement and any BSA-specific guidance in this area.

***Foreign-based service providers*:** Financial institutions should ensure that foreign-based service providers are in compliance with applicable U.S. laws, regulations, and regulatory guidance. Financial institutions may also want to consider laws and regulations of the foreign-based provider's country or regulatory authority regarding the financial institution's ability to perform on-site review of the service provider's operations. In addition, financial institutions should consider the authority or ability of home country supervisors to gain access to the financial institution's customer information while examining the foreign-based service provider.

---

[11] For further guidance regarding business continuity planning with service providers, refer to the *FFIEC Business Continuity Booklet* (March 2008) at http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx.

Internal audit: Financial institutions should refer to existing guidance on the engagement of independent public accounting firms and other outside professionals to perform work that has been traditionally carried out by internal auditors.[12] The Sarbanes-Oxley Act of 2002 specifically prohibits a registered public accounting firm from performing certain non-audit services for a public company client for whom it performs financial statement audits.

Risk management activities: Financial institutions may outsource various risk management activities, such as aspects of interest rate risk and model risk management. Financial institutions should require service providers to provide information that demonstrates developmental evidence explaining the product components, design, and intended use, to determine whether the products and/or services are appropriate for the institution's exposures and risks.[13] Financial institutions should also have standards and processes in place for ensuring that service providers offering model risk management services, such as validation, do so in a way that is consistent with existing model risk management guidance.

---

[12] Refer to SR 13-1, "Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing," specifically the section titled, "Depository Institutions Subject to the Annual Audit and Reporting Requirements of Section 36 of the FDI Act" at http://www.federalreserve.gov/bankinforeg/srletters/sr1301.htm.
Refer also to SR 03-5, "Amended Interagency Guidance on the Internal Audit Function and its Outsourcing," particularly the section titled, "Institutions Not Subject to Section 36 of the FDI Act that are Neither Public Companies nor Subsidiaries of Public Companies" at http://www.federalreserve.gov/boarddocs/srletters/2003/sr0305.htm.

[13] Refer to SR 11-7, "Guidance on Model Risk Management" which informs financial institutions of the importance and risk to the use of models and the supervisory expectations that financial institutions should adhere to. http://www.federalreserve.gov/bankinforeg/srletters/sr1107.htm