Federal Deposit Insurance Corporation
550 17th Street, NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-19-2019
April 2, 2019

Technology Service Provider Contracts

Summary: The attached document describes examiner observations about gaps in financial institutions' contracts with technology service providers that may require financial institutions to take additional steps to manage their own business continuity and incident response.

Statement of Applicability to Institutions under $1 Billion in Total Assets: This FIL applies to all FDIC-supervised institutions.

Distribution:
FDIC-Supervised Financial Institutions and their Service Providers

Suggested Routing:
Chief Executive Officer
Chief Information Officer
Chief Information Security Officer

Related Topics:
FFIEC IT Outsourcing Technology Services Booklet
FFIEC IT Business Continuity Planning Booklet
FFIEC IT Information Security Booklet
FIL 44-2008, Guidance for Managing Third-Party Risk
FIL 19-2016, Technical Assistance Video on Outsourcing Technology Services
FIL 50-2001, Bank Technology Bulletin on Outsourcing
FIL 49-99, Bank Service Company Act

Attachment:
Notification of Performance of Bank Services

Contact:
Donald Saxinger, Chief, IT Supervision, DSaxinger@fdic.gov or (202) 898 – 3864

Robert A. Kahl, Sr. Examination Specialist (IT) RKahl@fdic.gov or (402) 397 – 0142

Note:
FDIC Financial Institution Letters (FILs) may be accessed from the FDIC's website at www.fdic.gov/news/news/financial/index.html.

To receive FILs electronically, please visit www.fdic.gov/about/subscriptions/fil.html.

Paper copies may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (877-275-3342 or 703-562-2200).

Highlights:

- Financial institution boards of directors and senior management are responsible for managing risks related to relationships with technology service providers.
- Effective contracts are an important risk management tool for overseeing technology service provider risks, including business continuity and incident response.
- Recent FDIC examination findings noted that some financial institution contracts with technology service providers lack sufficient detail regarding the contract parties' respective rights and responsibilities for business continuity and incident response.
- When contracts do not adequately address such risks, financial institutions remain responsible for assessing those risks and implementing appropriate mitigating controls.
- Financial institutions have a responsibility under Section 7 of the Bank Service Company Act to notify their FDIC regional office of contracts or relationships with technology service providers that provide certain services to the institution.

Financial Institution Letter
FIL-19-2019
April 2, 2019

Technology Service Provider Contracts

Background

Financial institutions often contract with technology service providers for services to the institution and its customers. Technology outsourcing relationships frequently integrate the systems and processes of the service provider and financial institution. This integration can impact how financial institutions manage their own processes such as business continuity and incident response.

When services are outsourced, a financial institution's board of directors and senior management are responsible for managing the risks posed by those services as if they were performed within the institution. Contracts are a critical tool for documenting agreement between financial institutions and their technology service providers on the levels of service required.

Observations

Examiners have noted in recent FDIC reports of examination that some financial institution contracts with technology service providers may not adequately define rights and responsibilities regarding business continuity and incident response, or provide sufficient detail to allow financial institutions to manage those processes and risks.

Some contracts do not require the service provider to maintain a business continuity plan, establish recovery standards, or define contractual remedies if the technology service provider misses a recovery standard. Other contracts did not sufficiently detail the technology service provider's security incident responsibilities such as notifying the financial institution, regulators, or law enforcement.

Additionally, some contracts do not clearly define key terms used in contractual provisions relating to business continuity and incident response. Undefined and unclear key contract terms could contribute to ambiguity in financial institution rights and service provider responsibilities, and could increase the risk that technology service provider business disruptions or security incidents will impair financial institution operations or compromise customer information.

Requirements

The Interagency Guidelines Establishing Information Security Standards, promulgated pursuant to the Gramm-Leach-Bliley Act, establish standards for safeguarding customer information.[1] Those guidelines set expectations for managing technology service provider relationships through contractual terms and ongoing monitoring. Financial institutions must account for these requirements in contracts with technology service providers.

[1] The Interagency Guidelines Establishing Information Security Standards have been incorporated into the FDIC's Rules and Regulations as Appendix B to Part 364.

Financial Institution Considerations

The FDIC encourages financial institutions, as part of their due diligence and ongoing monitoring, to ensure that business continuity and incident response risks are adequately addressed in service provider contracts. Long-term contracts and contracts that automatically renew may be at higher risk for coverage gaps.

When contracts leave gaps in business continuity and incident response, it is prudent for the financial institution to assess any resultant risks and implement compensating controls to mitigate them. For example, a financial institution may obtain supplementary business continuity documentation from the service provider, or modify the financial institution's own business continuity plan to address contractual uncertainties.

Institution management may refer to the FFIEC IT Examination Handbook, Business Continuity Booklet, or the FDIC's Guidance for Managing Third-Party Risk for additional information. These materials describe practices that can be used to mitigate risk in third-party relationships.

The FFIEC IT Examination Handbook provides guidance for business continuity management, information and cyber security, and outsourcing technology services. The guidance addresses key financial institution risk management considerations such as the need for risk assessments, due diligence, strong contract provisions, and ongoing monitoring.

The FDIC's Guidance for Managing Third-Party Risk (FIL-44-2008, issued June 6, 2008) provides additional information for managing outsourcing risk including information on contract structure, contract reviews, and service provider oversight. Among other things, the guidance discusses prudent contract provisions addressing the rights and responsibilities of each party, and service provider business continuity. The guidance also discusses the importance of financial institution periodic review of the service provider's performance for conformance with the contract. Importantly, the guidance indicates that the level of detail in contract provisions will vary with the scope and risks associated with the third-party relationship.

Other FILs noted under Related Topics provide supplementary information in the form of Technical Assistance Videos and Technology Bulletins.

Bank Service Company Act Notification Requirements

Section 7 of the Bank Service Company Act (Act) (12 U.S.C. 1867) requires depository institutions to notify, in writing, their respective federal banking agency of contracts or relationships with technology service providers that provide certain services. Services covered by Section 3 of the Act include check and deposit sorting and posting, computation and posting of interest, preparation and mailing of checks or statements, and other clerical, bookkeeping, accounting, statistical, or similar functions such as data processing, Internet banking, or mobile banking services.

To help institutions comply with the Act's notification requirements, the FDIC has developed the attached form, FDIC 6120/06 (4-99). The form is optional, and the information requested on this form may be submitted to the FDIC in any format. Notifications should be sent to the institution's FDIC regional office.