Office of Inspector General

Office of Audits and Evaluations
Report No. EVAL-17-004

Technology Service Provider Contracts with FDIC-Supervised Institutions

February 2017

Office of Inspector General

Executive Summary

Technology Service Provider Contracts with FDIC-Supervised Institutions

Report No. EVAL-17-004
February 2017

Why We Did the Evaluation

Financial institutions (FIs) increasingly rely on technology service providers (TSPs) to provide or enable key banking functions. Every FI has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information, including when such FI customer information is maintained, processed, or accessed by a TSP. Based on results from two prior evaluations, we determined that greater scrutiny of the sufficiency of TSP contracts with FDIC-supervised institutions was warranted.

Our evaluation objective was to assess how clearly FDIC-supervised institutions' contracts with TSPs address the TSP's responsibilities related to (1) business continuity planning and (2) responding to and reporting on cybersecurity incidents. We reviewed 48 contracts between FIs and TSPs associated with 19 FIs. Our methodology relied on information collected by examiners on our behalf during the examination process. We did not contact FIs or TSPs as part of this evaluation. We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Background

In 1999, Congress enacted the Gramm-Leach-Bliley Act (GLBA). Section 501(b) required the federal banking agencies to establish appropriate standards for supervised FIs to protect customer information security and confidentiality. The standards require FIs to ensure that customer records and information are secure and kept confidential; protected against anticipated threats or hazards to their security and integrity; and protected against unauthorized access to or use, which could result in substantial harm or inconvenience to any customer.

As required by GLBA, in February 2001, the financial regulators issued *Interagency Guidelines Establishing Standards for Safeguarding Customer Information* (Interagency Guidelines) requiring development and implementation of administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These Interagency Guidelines apply to customer information maintained by or on behalf of FDIC-insured FIs. FIs are instructed to implement coordinated, comprehensive information security programs that include safeguards appropriate to each institution's size, complexity, and nature and scope of activities. The Interagency Guidelines state that FIs should:

- exercise appropriate due diligence in selecting service providers;
- contractually require their TSPs to implement appropriate measures to meet the guidelines' objectives related to protecting against unauthorized access to or use of sensitive customer information; and
- monitor contract compliance by the TSPs consistent with the institution's risk assessment to include reviewing service provider audits, test results summaries, or other equivalent evaluations.

In 2008, the FDIC issued a Financial Institution Letter (FIL) titled, *Guidance for Managing Third-Party Risk*, which emphasized that an institution's board of directors and senior management ultimately are responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships to the same extent as if the activity were handled within the institution. RMS has also reiterated these responsibilities in more recent guidance.

Executive Summary

Technology Service Provider Contracts with FDIC-Supervised Institutions

Report No. EVAL-17-004
February 2017

Evaluation Results

We did not see evidence, in the form of risk assessments or contract due diligence, that most of the FDIC-supervised FIs we reviewed fully considered and assessed the potential impact and risk that TSPs may have on the FI's ability to manage its own business continuity planning and incident response and reporting operations. Typically, FI contracts with TSPs did not clearly address TSP responsibilities and lacked specific contract provisions to protect FI interests or preserve FI rights. Contracts also did not sufficiently define key terminology related to business continuity and incident response. As a result, FI contracts with TSPs we reviewed provided FIs with limited information and assurance that TSPs (1) could recover and resume critical systems, services, and operations timely and effectively if disrupted; and (2) would take appropriate steps to contain and control incidents and report them timely to appropriate parties.

In the past 2 years, the FDIC independently and the Federal Financial Institutions Examination Council (FFIEC) members collectively took numerous steps to provide institutions comprehensive business continuity, cybersecurity, and vendor management guidance, and to enhance the FDIC and FFIEC's IT examination programs. We concluded that more time is needed to allow FDIC and FFIEC efforts to have a demonstrable and measureable impact on FI and TSP contract language. In that regard, RMS officials noted that often FI contracts with TSPs are dated and do not reflect FDIC and FFIEC efforts to strengthen cybersecurity. Although RMS does not expect FIs to renegotiate current contracts solely in response to recently issued guidance, it encourages FIs to discuss business continuity and incident response concepts, guidance, and expectations with their service providers. Finally, risks remain that FIs may attempt to transfer their inherent responsibility for FI continuity and information security to TSPs or may not be sufficiently knowledgeable about or engaged in contract management. These risks will require RMS's continued supervisory attention.

Recommendations

Notwithstanding the FDIC's efforts, we recommend that RMS continue to communicate to FIs the importance of (1) fully considering and assessing the risks that TSPs present, (2) ensuring that contracts with TSPs include specific detailed provisions that address FI-identified risks and protect FI interests, and (3) clearly defining key contract terms that would be important in understanding FI and TSP rights and responsibilities. We also recommend that, at an appropriate time, RMS study and assess to what extent FIs have effectively addressed the above issues. The FDIC concurred with our recommendations and proposed actions responsive to the recommendations to be completed by October 2018.

Contents

	Page
Background	2
Evaluation Results	5
FI Analyses Do Not Fully Consider Business Continuity and Incident Response Risks Presented by TSPs	5
Key Contract Provisions Provide Limited Coverage of the TSP's Business Continuity Planning and Incident Response and Reporting Responsibilities	7
Key Contract Terms Lack Clear and Specific Definition	11
The FDIC Has Implemented Numerous Initiatives to Address Cybersecurity Risks	11
FI Third-Party Relationship Risks Remain and Will Require Continued Supervisory Attention	12
Recommendations	13
Corporation Comments and OIG Evaluation	14
Appendices	
1. Objective, Scope, and Methodology	15
2. Third-Party RMA Process	18
3. Key Contract Provisions	19
4. Key Contract Terms	20
5. Key Terminology Usage	21
6. FDIC and FFIEC Initiatives	22
7. Acronyms and Abbreviations	23
8. Corporation Comments	24
9. Summary of the Corporation's Corrective Actions	28
Tables	
1. Contract Coverage of Business Continuity	9
2. Contract Coverage of Incident Response and Reporting	10
3. FIs' Total Assets and Prior IT Composite Rating	17
Figure	
Key Terminology Usage	21

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226

Office of Audits and Evaluations
Office of Inspector General

DATE: February 14, 2017

MEMORANDUM TO: Doreen R. Eberley, Director
Division of Risk Management Supervision

/Signed/
FROM: E. Marshall Gentry
Assistant Inspector General for Evaluations

SUBJECT: *Technology Service Provider Contracts with FDIC-Supervised Institutions* (Report No. EVAL-17-004)

Financial institutions (FIs) increasingly rely on technology service providers (TSPs) to deliver or enable key banking functions. Every FI has an affirmative and continuing obligation to respect customer privacy and to protect the security and confidentiality of customers' nonpublic personal information, including when such FI customer information is maintained, processed, or accessed by a TSP. FIs also have an operational interest in maintaining or quickly restoring systems and business operations in the event of a disruption or a business continuity event impacting the FI or its TSPs.

When an FI relies upon third parties to provide operational services, it also relies on those service providers to have sufficient recovery capabilities for the services they perform on behalf of the FI. Business continuity and incident response contract provisions allow an FI to coordinate its risk management processes with the service provider's operations. FIs with information security program limitations or unclear contract language face increased risk that business disruptions or security incidents will negatively impact business operations or compromise customer information. Based on two prior OIG evaluations' results and an environment of increasingly frequent and significant cybersecurity incidents, we determined that an assessment of the sufficiency of TSP contracts with FDIC-supervised institutions was warranted.

Our objective was to assess how clearly FDIC-supervised institutions' contracts with TSPs address the TSPs responsibilities related to (1) business continuity planning and (2) responding to and reporting on cybersecurity incidents. We reviewed 48 contracts between FIs and TSPs associated with 19 FIs. Our methodology relied on information collected by examiners on our behalf during the examination process. We did not contact FIs or TSPs as part of this evaluation. We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Appendix 1 of this report includes additional details on our objective, scope, and methodology. Additional appendices include acronyms and abbreviations, the Corporation's comments on a draft of this report, and a summary of the Corporation's corrective actions.

Background

In 1999, Congress enacted the Gramm-Leach-Bliley Act (GLBA). Section 501(b) of the GLBA required the federal banking agencies to establish appropriate standards, for supervised FIs, to protect customer information security and confidentiality. The standards require FIs to ensure that customer records and information are secure and kept confidential; protected against anticipated threats or hazards to their security and integrity; and protected against unauthorized access to or use, which could result in substantial harm or inconvenience to any customer.

As required by GLBA, in February 2001, the financial regulators issued *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, codified to 12 C.F.R. Part 364 (Interagency Guidelines). Appendix B to Part 364 addresses standards required by GLBA for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These Interagency Guidelines apply to customer information maintained by or on behalf of FDIC-insured FIs. FIs are instructed to implement coordinated, comprehensive information security programs that include safeguards appropriate to each institution's size, complexity, and nature and scope of activities.

The Interagency Guidelines state that FIs should:

- exercise appropriate due diligence in selecting service providers;[1]
- contractually require their TSPs to implement appropriate measures to meet the Interagency Guidelines objectives related to protecting against unauthorized access to or use of sensitive customer information;[2] and
- monitor contract compliance by the TSPs consistent with the institution's risk assessment, to include reviewing service provider audits, test results summaries, or other equivalent evaluations.

The FDIC's Financial Institution Letter (FIL) titled, *Guidance for Managing Third-Party Risk*, dated June 2008, emphasizes that an institution's board of directors and senior management ultimately are responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships to the same extent as if the activity were handled within the institution. RMS has also reiterated these responsibilities in more recent guidance.

---

[1] Interagency Guidelines Appendix B defines a service provider as "any person or entity that maintains, processes, or otherwise is permitted access to customer information or consumer information through its provision of services directly to the bank."

[2] Personally identifiable information is any information about an individual that can be used to distinguish or trace that individual's identity, or any other personal information which is linked or linkable to that individual. Sensitive customer information is a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name or password or password and account number.

Business Continuity Planning

Business continuity planning involves developing an enterprise-wide business continuity plan and prioritizing business objectives and critical operations essential for recovery. This enterprise-wide framework should consider how every critical process, business unit, department, and system will respond to disruptions and which recovery solutions should be implemented.

A business continuity plan establishes the basis for FIs or TSPs to recover and resume business processes when operations have been disrupted unexpectedly. These plans involve a continuous, process-oriented approach that includes a business impact analysis, a risk assessment, risk management, and risk monitoring and testing. Because FIs play a crucial role in the overall economy, service disruptions should be minimized in order to maintain public trust and confidence in the financial system. Without an enterprise-wide business continuity plan that considers all critical business elements, an institution may not be able to resume customer service at an acceptable level or within reasonable timeframes.

As such, FI management should incorporate business continuity considerations into its business model's overall design to proactively mitigate the risk of service disruptions. When an FI relies upon third parties to provide operational services, it also relies on those service providers to have sufficient recovery capabilities for the specific services they perform on behalf of the FI. Specific business continuity contract provisions allow an FI to coordinate its risk management processes with the service provider's operations and plans.

Business Continuity Plan. According to Appendix J of the FFIEC IT booklet titled, *Business Continuity Planning*, dated February 2015, when using third-party service providers, FI management should ensure adequate business resiliency through:

- Third-Party Management, which involves due diligence procedures, regular monitoring, and strategic, integrative considerations with third-party servicers;
- Third-Party Capacity, which considers third parties' abilities to deliver essential services under adverse scenarios, in addition to possible alternatives in the event of third-party failure;
- Testing with Third-Party TSPs, which involves testing the business continuity resilience among the FI and third-party service providers, in addition to the review of test results and remediation of any observed weaknesses; and
- Cyber Resilience, which involves identification and mitigation of cyber threats to data and operational infrastructure, as well as effective incident response procedures to cyber attacks.

Incident Response Program

A security incident is the attempted or successful unauthorized access, use, modification, or destruction of information systems or customer data. If a security incident occurs, the FI's computer systems could potentially fail and FI operations or confidential information could be impacted or compromised. An incident response program specifies the actions to be taken when the FI suspects or detects that unauthorized individuals gained access to customer information systems, and includes providing appropriate reports to regulatory and law enforcement agencies.

An FI is expected to be able to address an unauthorized access incident to customer information in systems maintained by its service providers. Therefore, FI and TSP contracts should require the service provider to take appropriate actions to address unauthorized access incidents to the FI's customer information, including notifying the FI.

Supplement A to Part 364 Appendix B, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, interprets GLBA section 501(b). Pursuant to Supplement A, when an FI becomes aware of an unauthorized access to sensitive customer information incident, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that customer information misuse has occurred or is reasonably possible, the institution should notify the affected customer as soon as possible.

Minimum Components for an Incident Response Program. The Interagency Guidelines provide that the minimum components of an FI's incident response program should contain procedures for:

- Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused;
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence;
- Notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;
- Notifying appropriate law enforcement authorities and filing a timely Suspicious Activity Report in situations involving federal criminal violations; and
- Notifying customers when warranted.

Supplement A also instructs each institution to address unauthorized access to customer information incidents in customer information systems maintained by its service providers. The guidance states that an FI's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the FI's customer information, including notifying the FI of any such incident as soon as possible, to enable the FI to expeditiously implement its response program. Additionally, where an unauthorized access to customer information incident involves customer information systems maintained by an FI's service provider, the FI remains responsible for notifying its customers and regulator. However, an FI has discretion to authorize or contract with its service provider to notify the FI's customers or regulator on its behalf.

Evaluation Results

FI Analyses Do Not Fully Consider Business Continuity and Incident Response Risks Presented by TSPs

Supervisory guidance provides that the key to the effective use of a third party in any capacity is for the FI's management to appropriately assess, measure, monitor, and control the risks associated with a contractual relationship. While engaging another entity may assist management and the board in achieving strategic goals, such an arrangement reduces management's direct control and introduces risks. As discussed earlier, the FI retains responsibility for activities performed through third-party relationships, which increases the need for strong oversight. Accordingly, institutions should establish and maintain an effective risk management process for initiating and overseeing outsourced operations.

FI Oversight Responsibilities. The FDIC's June 2008 FIL provides that the FI's board of directors should initially approve, oversee, and review at least annually significant third-party arrangements. Results of oversight activities for material third-party arrangements should be periodically reported to the FI's board or designated committee, and identified weaknesses should be documented and promptly addressed. The guidance also serves as a resource for implementing a third-party risk management program by providing a general framework that boards and senior management may use. The guidelines are not mandatory, but management should ensure that sufficient procedures and policies are in place to control third-party relationship risks.

An effective third-party risk management process has four elements:

- Risk assessment,
- Due diligence in selecting a third-party service provider,
- Contract structuring and review, and
- Ongoing monitoring.

Each element should consider the risks and managerial responsibilities associated with business continuity, information security and customer privacy, and subcontractor use. Taken together, these elements compose the FI's risk management analysis (RMA) of the third-party relationship. Appendix 2 of this report discusses the third-party risk management process further.

Although results varied widely, we did not see evidence, in the form of risk assessments or contract due diligence, that most of the FDIC-supervised FIs we reviewed fully considered and

assessed the potential impact and risk that TSPs and their subcontractors[3] could have on the FI's ability to manage its own business continuity planning and incident response and reporting operations. Although most FIs documented a TSP risk assessment matrix[4] that assessed the product or service criticality and considered the TSP's access to customers' personally identifiable information, almost half of the FIs lacked evidence that the FIs performed a comprehensive due diligence assessment[5] prior or subsequent to the contract's ratification. From the documentation of the 19 FIs that we reviewed:

OIG Methodology. To assess each FI's TSP RMA process, we requested and considered any pre-contract due diligence analysis, contract structuring review, prior or current risk assessment review, and internal risk rating the FI performed. We also requested each FI's TSP subcontractor RMA, if applicable.

We did not evaluate the FDIC's examination review process surrounding the FIs' TSP risk management oversight or process for initiating and overseeing outsourced operations.

- Fifteen (79 percent) completed a risk assessment matrix, which considered the TSP's criticality and access to sensitive or personally identifiable information in determining an internal risk rating.
- Ten (53 percent) performed a pre-contract and/or an annual due diligence review that covered the TSP's risk management systems and performance.
- Eight (42 percent) completed both a TSP risk assessment matrix and a due diligence review, as recommended by supervisory guidance.
- Seven (37 percent) only completed a risk assessment matrix.
- Two (11 percent) only performed a pre-contract and/or annual due diligence review.
- Two (11 percent) provided nothing.

The June 2008 FIL states that significant contracts should prohibit TSPs from subcontracting their obligations to another entity unless the FI determines that such subcontracting would be consistent with the due diligence standards used to select the TSP. Contracts associated with 18 of the 19 FIs that we reviewed (95 percent) allowed service providers to subcontract assigned work.[6] However, only 4 of 19 FIs documented consideration of subcontractor use within their

[3] Similar to TSPs, TSP subcontractors pose potential risk that is dependent on the significance of services provided and degree of access to sensitive and confidential information.
[4] A TSP risk assessment matrix is 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 FI.
[5] A TSP due diligence assessment involves a review of all available information about a potential third party, focusing on the entity's financial condition, its specific relevant experience, its knowledge of applicable laws and regulations, its reputation, and the scope and effectiveness of its operations and controls.
[6] We reviewed 48 contracts associated with the 19 FIs. Forty-one of those contracts allowed service providers to use subcontractors.

TSP due diligence and risk assessment matrices. Three of those FIs contractually allowed and one FI disallowed subcontractor use. The other 15 FIs (80 percent) that contractually allowed subcontractor use did not document subcontractor considerations within their TSP risk assessment matrix or due diligence reviews.[7]

The quality and sophistication of both the FIs' risk assessment matrices and due diligence reviews varied greatly. While many FIs completed short simplistic checklists or listings, a few FIs performed comprehensive reviews. For example, one FI's risk assessment matrix analyzed the relationship's financial, compliance, strategic, reputation, and operational/transaction risks.[8] Another FI provided a comprehensive due diligence review that considered the TSP's financial condition, service organization control (SOC) report,[9] payment card industry data security standard compliance, insurance coverage, business continuity plan, cyber security plan, penetration and vulnerability testing, compliance program, customer complaints, and information security program.[10]

Regardless of the risk assessment methodology used, FIs typically identified critical service providers and documented those that had access to sensitive or personally identifiable information. For example, 17 FIs (89 percent) identified service criticality and 13 FIs (68 percent) identified TSP access to personally identifiable information as a potential risk. However, as discussed later in this report, the contracts did not always include provisions to effectively address these risks.

Key Contract Provisions Provide Limited Coverage of the TSP's Business Continuity Planning and Incident Response and Reporting Responsibilities

Supervisory guidance recognizes that after an FI completes an initial risk assessment, selects a third party, and performs a comprehensive due diligence analysis, FI management should ensure the specific expectations and obligations of both the FI and the third party are outlined in a written contract prior to entering into the arrangement.[11] Supervisory guidance also discusses various contract provisions that should be considered based on the nature and significance of the third-party relationship. Appendix 3 of this report provides further details of key contract provisions pertinent to an FI's business continuity planning and incident response and reporting processes.

---

[7] Examiners confirmed that minimal or no additional subcontractor analysis or documentation was available for those FIs and reported that FI management believed that there were no subcontractors being used. We did not attempt to verify with TSPs whether they were using subcontractors.

[8] The FI is located in the New York Region with total assets less than $1 billion. The FI's risk assessment matrix and contract were dated in 2015.

[9] SOC reports are internal control reports on the services provided by a service organization that provide information to assess and address the risks associated with an outsourced service. SOC reports come in variations (SOC-1, SOC-2, and SOC-3) that provide differing levels of assurance.

[10] The FI is located in the Kansas City Region with total assets greater than $1 billion. The FI performed due diligence in 2015 based, in part, on a 2011 contract.

[11] Supervisory guidance states that the level of detail in contract provisions will vary with the scope and risks associated with the third-party relationship.

Most contracts explicitly stated the need for TSPs to adhere to GLBA's regulatory requirements; however, the contracts did not provide details necessary to allow FIs to manage their own business continuity planning and incident response and reporting efforts through TSP operations. Most contracts also had limited discussions of these concepts within other parts of the contract such as contract provisions related to performance standards, service level agreements, and reports. Typically, contracts for larger FIs and core service providers contained more detailed contract provisions.

OIG Methodology. We requested contracts with TSPs that the FIs considered critical and that had access to sensitive or personally identifiable information. Our selection process targeted contracts that would need to establish FIs' rights and TSP responsibilities for business continuity and incident response and reporting. To assess each contract, we requested FDIC examiners provide the FI's TSP RMA. We reviewed the analysis to verify the applicability and need for potential business continuity and incident response provisions. We then reviewed key contract provisions to assess the FI's consideration of business continuity planning and incident response and reporting.

Business Continuity

About half of the contracts we reviewed explicitly included business continuity provisions. Contracts often addressed key business continuity issues recommended by supervisory guidance in the following ways.

- More than half of the contracts required the maintenance of security standards that ensured data reliability, protection, and availability; often affirming compliance with GLBA, but only at a general level and not specifically tied to the TSP's business continuity plans.

- More than half of the contracts also required some TSP reporting, typically limited to providing financial statement audit reports and independent third-party reviews, such as SOC reports.[12] In many cases, the TSP's reporting responsibilities did not include management information system monitoring reports, performance reports, internal control reviews, security and business resumption testing, and regulatory examination reports.

FDIC TSP Contract Study. Similar to our results, RMS's June 2014 TSP Contract Study concluded that a large percentage of the contracts reviewed did not adequately address business continuity, and that contracts typically contained a TSP commitment to protect sensitive FI customer information by implementing appropriate measures designed to meet the objectives of the GLBA Interagency Guidelines.

[12] Within our report titled *The FDIC's Supervisory Approach to Cyberattack Risks*, dated March 2015, we reported that vendors frequently provided FIs with SOC reports that provided lower levels of assurance. For example, vendors frequently provided a category SOC-1 assessment of the service provider's financial statement controls, as opposed to the more comprehensive SOC-2 or SOC-3 assessment of the service provider's controls relevant to the security, availability, processing integrity of the service organization's systems, and the privacy or confidentiality of the information the system processes.

- Nearly half of the contracts we reviewed did not require the TSP to establish a business continuity plan. Those that did so did not elaborate on the TSP's responsibilities for maintaining continuous risk management processes, risk scenario events, integrative considerations between multiple components and service providers (internal and external dependencies), and capacity in supporting required processing and restoring services to multiple clients under adverse scenarios. Some contracts also limited the TSP's business continuity responsibilities in the event of a disaster.

- Few contracts established or defined clear performance standards, and few of those established performance metrics and remedies for failures to meet such standards. A notable exception was a contract that specified a 24-hour data recovery point objective and a 72-hour recovery time objective after a declared disaster.[13]

Table 1 summarizes how key contract provisions in 48 FI contracts with TSPs that we reviewed addressed TSP business continuity terms.

Table 1: Contract Coverage of Business Continuity

Contract Provision	Detailed Discussion of Business Continuity		High-Level Discussion of Business Continuity		No Discussion of Business Continuity	
	Number	Percent	Number	Percent	Number	Percent
Business Continuity	20	42%	5	10%	23	48%
Performance Standards	5	10%	5	10%	38	80%
Service Level Agreements	15	31%	25	52%	8	17%
Internal Controls	16	33%	15	31%	17	36%
Audits	21	44%	6	12%	21	44%
Reports	19	39%	8	17%	21	44%

Source: OIG analysis of examination documentation.

Contract provisions that more specifically detail key business continuity issues could provide FIs greater assurance that critical systems, services, and operations will be recovered and resumed timely and effectively when operations have been unexpectedly disrupted.

Incident Response and Reporting

Most of the contracts explicitly included security and confidentiality provisions related to incident response and reporting. Contracts often addressed key incident response and reporting issues recommended by supervisory guidance in the following ways:

- Most contracts addressed the TSP's responsibility for information security and confidentiality and GLBA compliance by requiring the TSP to notify FIs of unauthorized intrusions that may materially affect the FI or its customers. However, contracts did not discuss the TSP's responsibilities for assessing and responding to a potential incident, determining the potential effect on the FI and its customers, or the reporting and notification processes to regulatory and law enforcement authorities.

[13] The FI is located in the Dallas Region with total assets less than $250 million. The contract was dated in 2010.

- While service level agreements often discussed cybersecurity incident response and reporting plans, very few contracts detailed incident response and recovery metrics or specified the use of independent forensic expertise.

- More than half of the contracts defined performance standards related to providing the FI notice of an unauthorized intrusion or security breach, but few contracts established criteria to assess the nature and scope of potential incidents; or to contain and control such incidents, which could preserve evidence. A more thorough contract obligated the TSP to:
    - assess the incident's nature and scope;
    - conduct a reasonable investigation to identify information and systems accessed;
    - determine the likelihood that the incident could result in substantial harm or inconvenience, or that the accessed information would be misused;
    - promptly notify the FI of the incident details;
    - promptly take appropriate steps to prevent further misuse of information; and,
    - provide the FI with periodic updates on the investigation until resolved.[14]

- Contracts typically did not provide remedies for the failure to meet incident response and reporting standards.

Table 2 summarizes how key contract provisions in 48 FI contracts with TSPs that we reviewed addressed incident response and reporting terms.

Table 2: Contract Coverage of Incident Response and Reporting

Contract Provision	Detailed Discussion of Incident Response		High-Level Discussion of Incident Response		No Discussion of Incident Response	
	Number	Percent	Number	Percent	Number	Percent
Security and Confidentiality	31	65%	10	21%	7	14%
Performance Standards	11	23%	22	46%	15	31%
Service Level Agreements	9	19%	26	54%	13	27%
Internal Controls	14	29%	20	42%	14	29%
Audits	10	21%	16	33%	22	46%
Reports	12	25%	15	31%	21	44%

Source: OIG analysis of examination documentation.

Contract provisions that more specifically detail key incident response and reporting issues could provide FIs greater assurance that information systems and confidential data are properly protected. Also, in the event of a security incident, institution and customer damage could be minimized through incident containment and proper information system restoration.

[14] The FI is located in the Kansas City Region with total assets less than $1 billion. The contract was dated in 2011.

Key Contract Terms Lack Clear and Specific Definition

We reviewed regulatory and supervisory guidance and identified certain key terms related to business continuity and incident response and reporting. We noted these terms are not explicitly defined in the guidance. Subjective terms such as potential breach, unauthorized access, containment, material impact, and timely notification may be subject to differing interpretations, and require further clarification within the contract. Appendix 4 of our report provides a listing of key contract terms that we identified that were often undefined, and their corresponding regulatory or supervisory context. Most contracts that we reviewed did not specifically use certain key terms found in guidance, or clearly define key terms. In certain cases, the contracts provided limited definitions tied to broad generalizations or general regulatory references. Appendix 5 of this report illustrates the terms reviewed, contract use, and the degree of explanation of those terms in contracts that we reviewed.

> **OIG Methodology.** To assess each contract, we reviewed regulatory and supervisory guidance for key regulatory terms that were undefined in the context of business continuity and incident response and reporting concepts. We then reviewed our sampled contracts for each term's usage and level of clarification.

In a few instances, contracts provided more thorough definitions. For example, although contracts did not specifically define the term "adverse event," six contracts used the similar term "disaster" and provided detailed definitions based on the respective FIs' unique business lines and operations. Among those contracts, the term was defined as (1) any unplanned impairment or interruption of those systems, resources or processes that enable standard performance of the applicable service's functionality; (2) an event that will cause an outage of the computer facilities in excess of 24 hours, or (3) an event or occurrence which renders the center unable to provide a customer with normal service for a prolonged period of time or those situations which the center deems to be a disaster.

TSPs appear to have drafted most of the contracts we reviewed. Many of the contracts appeared to be based on standardized forms with generic FI customer descriptions, and high-level provisions that lacked specificity needed to protect the FI's information and resource needs. In addition, several contracts placed an emphasis on the FIs' responsibility to protect TSP system and application confidentiality, and a few contracts explicitly limited TSP responsibility and liability for ensuring business continuity and cybersecurity.

Unclear contract terminology leaves FI rights and TSP responsibilities subjective and open to interpretation, may not protect FI interests, and makes it more difficult for FIs to manage business continuity planning and incident response and reporting operations, introducing greater operational and reputational risk.

The FDIC Has Implemented Numerous Initiatives to Address Cybersecurity Risks

In the past 2 years, the FDIC independently and the FFIEC members collectively took numerous steps to provide institutions comprehensive business continuity, cybersecurity, and vendor

management guidance, and to enhance the FDIC and FFIEC's IT examination programs. Appendix 6 of this report provides further details on these initiatives. The initiatives focus on enhancing institution awareness, regulatory authority and guidance, and the examination process. They include a cybersecurity awareness program, a vendor management technical assistance video, a *Supervisory Insights* article, FFIEC guidance, new IT examination procedures, proposed TSP rules, and a 2016 Horizontal Interconnectedness Review.[15] The FDIC's 2015 and 2016 performance goals identified and detailed many of these initiatives.

Of particular note, in February 2015, the FFIEC issued Appendix J to the *Business Continuity Planning* booklet titled, *Strengthening the Resilience of Outsourced Technology Services*. As presented earlier in this report, that appendix discusses four key elements of business continuity planning that an FI should address to ensure that its TSPs are providing resilient technology services.

RMS stated that due to the volume of initiatives implemented during 2015 and 2016, more time was needed to see a demonstrable and measureable impact on FIs and TSPs. RMS noted that many FI contracts with TSPs are dated and may not reflect the impact of the recent FDIC and FFIEC initiatives. Eighty-one percent of our sampled contracts originated before January 2015. For the nine contracts that originated after January 2015, we did not observe a significant difference in the specificity of contract provisions. Although RMS does not expect FIs to renegotiate current contracts solely in response to recently issued guidance, it encourages FIs to discuss business continuity and incident response concepts, guidance, and expectations with their service providers. However, as presented earlier in this report, annual due diligence reviews and ongoing contract monitoring documentation appeared limited. Following an appropriate amount of time to allow FIs to implement guidance, it may be prudent for RMS to study or evaluate FIs' implementation of RMS and FFIEC guidance, especially with respect to the sufficiency and specificity of contract language between FIs and TSPs.

FI Third-Party Relationship Risks Remain and Will Require Continued Supervisory Attention

There are numerous risks that may arise from an FI's use of third parties. Some of the risks are associated with the underlying activity itself, similar to the risks faced by an institution directly conducting the activity. Other potential risks arise from or are heightened by the involvement of a third party. These risks include strategic, reputation, operational, and transactional risks.

Based on this evaluation, prior work, and examiner interviews that we have performed, we identified the following potential risks that could impact the sufficiency of FI contracts with TSPs:

[15] A horizontal review is an evaluation of one process or activity across several groups or departments within an enterprise. The FDIC periodically performs external horizontal reviews that focus on a targeted risk factor within a population of supervised institutions.

- Despite FFIEC and FDIC guidance reiterating that the FI retains responsibility for activities performed through third-party relationships, a risk exists that an FI will transfer or delegate its risk management responsibilities to a service provider. Some FIs that we reviewed appeared to have risk management procedures that they did not follow or fully implement.

- FIs may not have sufficient contracting and IT knowledge, expertise, or resources to gauge risks presented by TSPs; structure contracts to or otherwise address those risks; and oversee ongoing contracts. Over-reliance on service providers coupled with a lack of appropriate contract management expertise weakens an FI's control environment, which may impact business continuity and incident response planning efforts.

- FIs may not be sufficiently engaged in writing and negotiating contracts to ensure their rights and TSP responsibilities are clearly defined. TSPs appear to be drafting the contracts and ensuring that their rights are protected more than the FIs.

These risks are not new to RMS but will require the division's continued supervisory attention.

Recommendations

As a result of the observations and risks identified in this report, current external risk environment, and degree of information technology interconnectedness, we recommend that the Director, RMS:

(1) Continue to communicate to FIs the importance of:

- Fully considering and assessing the risks that TSPs could have on the FI's ability to manage its own business continuity and incident response planning efforts;

- Ensuring that contracts with TSPs include specific provisions that address FI-identified risks, protect FI interests, and provide details necessary to allow FIs to manage their own business continuity planning and incident response and reporting efforts through TSP operations; and

- Clearly defining key contract terms that would be important in understanding FI and TSP rights and responsibilities in the event of a business disruption or computer security incident particularly for those contracts that FIs identify as critical or that have access to sensitive or personally identifiable information.

(2) Following an appropriate amount of time for FIs to implement guidance, conduct a follow-on study, such as a horizontal review of FIs, to assess to what extent the issues included in recommendation 1 are being effectively addressed by FIs.

Corporation Comments and OIG Evaluation

The Director, RMS, provided a response, dated January 26, 2017, to a draft of this report. The response is presented in its entirety in Appendix 8. The Director concurred with the two recommendations, proposed actions responsive to the recommendations, and targeted completion dates from June 30, 2018 through October 1, 2018. These recommendations will remain open until the planned actions are completed. A summary of the Corporation's corrective actions is presented in Appendix 9.

Objective, Scope, and Methodology

Objective

Our evaluation objective was to assess how clearly FDIC-supervised institutions' contracts with TSPs address the TSP's responsibilities related to (1) business continuity planning and (2) responding to and reporting on cybersecurity incidents.

We performed our work from April 2016 to September 2016 at the FDIC's offices in Washington D.C. and Arlington, Virginia, in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Scope and Methodology

The scope of this evaluation included evaluating current contracts between FIs and TSPs that were designated as "critical" or "high" risk to the FI's operations. We sampled these contracts from FDIC-supervised FIs scheduled to be examined from April 1, 2016 to May 31, 2016. In our view, focusing on this particular group provided a reasonable way to isolate our attention on those TSPs and corresponding contracts that pose the greatest operational and reputational risk. Typically, these institutions only represent a small percentage of the FI's service providers.

To address our evaluation objective, we performed the following procedures and techniques:

- Researched applicable criteria such as the Interagency Guidelines and FFIEC guidance, and relevant FILs, Regional Directors Memoranda, and Examination Documentation modules. Based on this research, we identified key contract provisions and terms that corresponded to business continuity planning and cybersecurity incident response and reporting rights and responsibilities, and developed a data collection instrument for assessing key sources of guidance, including the following:
    - Appendix B to Part 364—*Interagency Guidelines Establishing Information Security Standards*.
    - FFIEC IT Examination Handbook.
    - March 2016 FIL titled, *Technical Assistance Video on Outsourcing Technology Services*. (FIL-19-2016)
    - November 2015 FIL titled, *Cybersecurity Awareness Resources*. (FIL-55-2015)
    - July 2015 FIL titled, *Cybersecurity Assessment Tool*. (FIL-28-2015)
    - April 2014 FIL titled, *Technology Outsourcing: Informational Tools for Community Bankers Documents*. (FIL-13-2014)
    - June 2008 FIL titled, *Third-Party Risk Guidance for Managing Third-Party Risk*. (FIL-44-2008)
    - June 2008 RD Memorandum titled, *Guidance for Managing Third-Party Risk*.
    - September 2014 Examination Documentation Module titled, *Third-Party Risk*.

Objective, Scope, and Methodology

- Considered prior FDIC OIG work including:
  - *The FDIC's Supervisory Approach to Cyberattack Risks* (EVAL-15-003), dated March 2015, which identified variations in the quality and depth of FI risk assessments and other IT security program elements.
  - *Case Study of a Computer Security Incident Involving a Technology Service Provider* (EVAL-16-002), dated February 2016, which concluded, among other things, that the contract language between the TSP and its client FIs could have better defined terms related to incident response and specified notification requirements.

- Considered other regulatory agencies and the U.S. Government Accountability Office work, recent legislative proposal actions, the FDIC's 2015 Annual Report and Assurance Statement, and the 2015 and 2016 FDIC performance goals.

- From a universe of all FDIC-supervised FI IT examinations initiated from April 1, 2016 to May 31, 2016, implemented a multistage non-statistical sampling process that first identified FIs subject to review, and then identified and sampled current contracts designated as "critical" or "high" risk TSPs either by the FI or FDIC examiner-in-charge. We selected FIs to ensure institution diversity based on IT composite rating, total asset size, and regional location and TSPs to ensure a variety of service providers and services.

- Reviewed sampled contracts' key provisions and terms for consideration of business continuity planning and cybersecurity incident response and reporting rights and responsibilities using our data collection instrument. Testing considered the FI's business continuity plan, incident response program, and TSP RMA, including pre-contract due diligence analysis, current risk assessment review, and internal risk rating, when available. We designed our testing methodology and data collection instrument to answer the following:
  - Does the FI's TSP RMA consider business continuity planning, incident response, and subcontractor use?
  - How do key contract provisions address business continuity planning?
  - How do key contract provisions address incident response and reporting?
  - How do the contracts define key terms?

- Collected and analyzed data collected on an aggregate and segmented basis, and analyzed and determined the impact of potentially mitigating factors, based on the FI's pre-contract due diligence. Segmented data analysis considered the following factors:
  - FI's total assets,
  - FI's prior IT composite rating,
  - TSP's prior IT composite rating,
  - TSP's examination priority ranking,
  - Supervisory region, and

- Services provided.

Our methodology relied on information collected by examiners on our behalf during the examination process. We did not contact the FIs or TSPs as part of this evaluation.

Sampling Methodology

We non-statistically sampled 28 FIs from an evaluation universe of 265 institutions and revised the sample to 19 FIs based on the evaluation's interim results. The evaluation universe comprised all FDIC-supervised FI IT examinations initiated from April 1, 2016 to May 31, 2016. The FI sample represented each region and included all 14 FIs previously rated 3, 4, or 5 and 14 FIs previously rated 1 or 2. Moreover, 13 FIs in our sample had total assets less than $250 million and 15 FIs had total assets $250 million and above as of December 2015.

From these FIs, we sampled 48 TSP contracts that FIs designated as "critical" or "high" risk. To ensure a diverse sample, we selected contracts involving a variety of service providers and services. The contract sampling process focused on existing contracts available during the sampled FDIC-supervised FI IT examinations. FDIC examiners identified and gathered our targeted sample source documents. As needed, we obtained other TSP background information from the Regional Automated Document Distribution (RADD) and Virtual Supervisory Information on the Net (ViSION) applications. Table 3 provides the distribution of the sample universe, initial sample selection, and revised sample population by the prior IT composite rating and total asset size. Non-statistical samples are judgmental and results cannot be projected to the universe of institutions.

Table 3: FIs' Total Assets and Prior IT Composite Rating

Prior IT Composite Rating	FI Total Assets				Total	FI Sample	Revised FI Sample
	Less than $250 million	$250 to $499 million	$500 to $999 million	$1 billion or more			
1	26	12	7	19	64	6	5
2	123	35	7	22	187	8	8
3	10	1	1	1	13	13	5
4	1	0	0	0	1	1	1
5	0	0	0	0	0	0	0
Total	160	48	15	42	265		
FI Sample	13	5	4	6		28	
Revised FI Sample	8	5	1	5			19

Source: OIG analysis of RMS's scheduled IT examinations.

Our initial and revised FI sample sizes were deemed sufficiently large enough to meet the evaluation's objective considering observable characteristics and data variance, universe size and composition, and available time and resources. As needed, we exchanged some initially selected FIs for others within the sample universe to accommodate completed IT examination schedules. In addition, we reduced the FI sample based on the assignment's interim results. We believed that these changes would not materially impact the evaluation's results and conclusions.

Third-Party RMA Process

Third-Party RMA Process. The FDIC's June 2008 FIL, *Guidance for Managing Third-Party Risk*, states that an effective third-party RMA process has four basic elements:

- **Risk assessment.** The initial risk assessment process encompasses the cost/benefit and risk/reward analysis of the proposed relationship, and the relationship's overall fit within the FI's strategic plan and business strategy. The process should identify performance criteria, internal controls, reporting needs, and contractual requirements that are critical to the FI's ongoing assessment and control of specific identified risks. In particular, the process should assess information security and customer privacy requirements.

- **Due diligence in selecting a third party**. A comprehensive due diligence process involves a review of available information about a third party that focuses, in part, on the scope and effectiveness of its operations and controls. The review should assess internal controls, systems and data security, privacy protections, and audit coverage; business resumption strategy and contingency plans; and the use of other third-party subcontractors. Not only should due diligence be performed prior to selecting a third party, but it should also be performed periodically during the course of the relationship, particularly when considering a renewal of a contract.

- **Contract structuring and review.** After selecting a third party, management should ensure that the specific expectations and obligations of both the FI and the third party are outlined in a written contract prior to entering into the arrangement. Certain key provisions should be considered as a contract is structured, with the applicability of each dependent upon the nature and significance of the third-party relationship.

- **Oversight**. Institutions should maintain adequate oversight of third-party activities and adequate quality control over those products and services provided through third-party arrangements in order to minimize exposure to potential significant financial loss, reputation damage, and supervisory action. An oversight program will generally include monitoring of the third party's quality of service, risk management practices, financial condition, and applicable controls and reports.

Key Contract Provisions

Key Contract Provisions	Description
Audits	Audit rights and expectations, and access to audit information.
Business Resumption and Contingency Plans	Data and systems backup processes, protections, and resumption plans.
Internal controls	Process and system controls.
Performance Standards	Minimum service level requirements and remedies for failure to meet standards.
Regulatory Compliance	Explicit recognition of regulatory requirements.
Reports	Access to reporting information.
Scope of Service	Overall rights and responsibilities, required activities, timeframes, and assignment of responsibilities.
Security and Confidentiality	Responsibilities and controls over FI data and personally identifiable information.
Service Level Agreements	Detailed performance expectations.
Subcontracting and Assignment	Transfer rights to third (or more) parties.
Termination and Default	Contract default events and potential remedies.

Source: OIG analysis of FFIEC and FDIC online resources.

Key Contract Terms

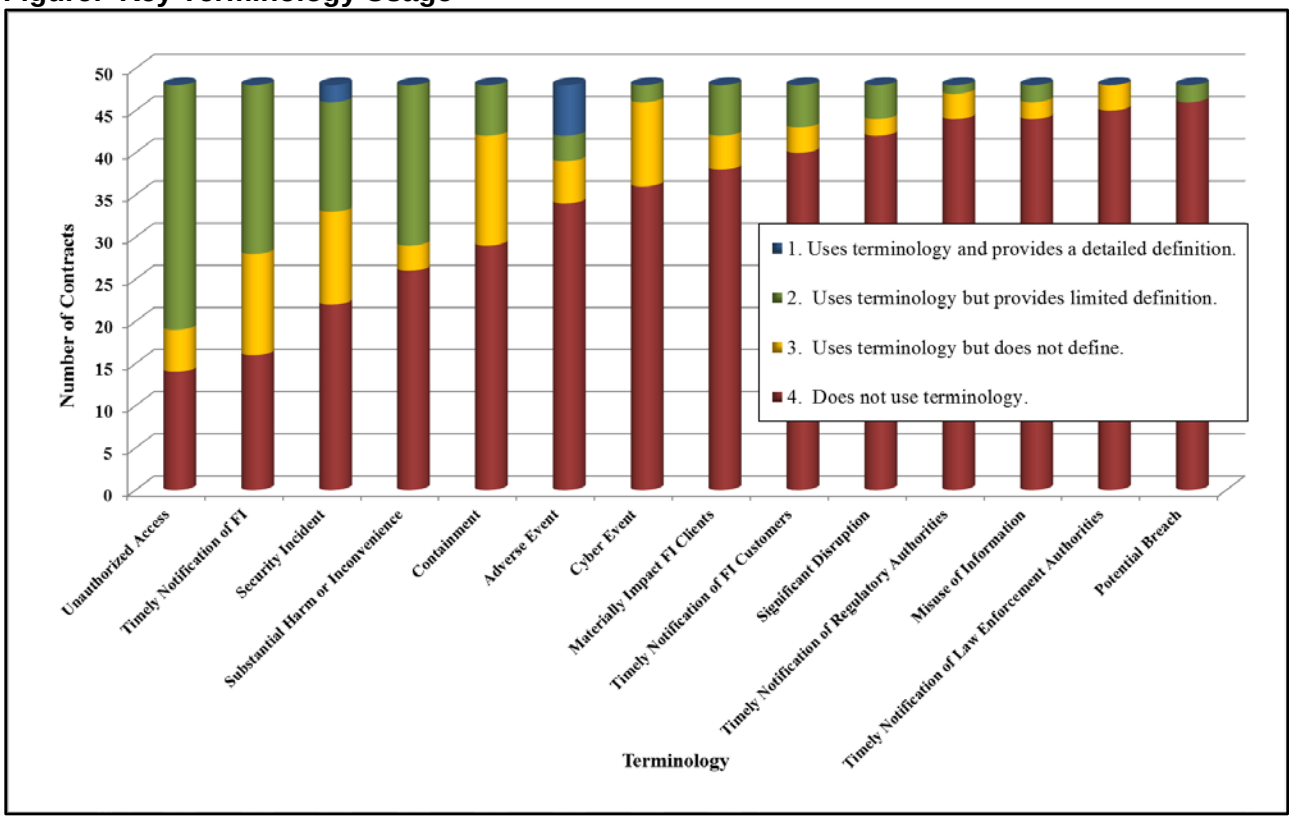
Key Terminology	Contextual Reference
Adverse Event	An FI should be able to recover critical IT systems for all types of adverse events (e.g., natural disaster, infrastructure failure, technology failure, availability of staff, or cyber attack.)
Containment	A response program should contain procedures for taking appropriate steps to contain the incident.
Cyber Event	FIs and TSPs need to incorporate the potential impact of a cyber event into their business continuity planning process. A cyber event may include malware, insider threats, data or systems destruction and corruption, distributed denial of service attack or communication infrastructure disruption, and simultaneous attack on an FI and its TSPs.
Materially Impact FI Clients	The contract should include notification responsibilities for situations where breaches in security result in unauthorized intrusions to the TSP that may materially affect FI clients.
Misuse of Information	If the circumstances of the unauthorized access lead the institution to determine that misuse of the information is reasonably possible, it should notify all customers in the group.
Potential Breach	Any breaches in the security and confidentiality of information, including a potential breach resulting from an unauthorized intrusion, should be required to be fully and promptly disclosed to the FI.
Security Breach or Violation	Each institution shall report to its board at least annually. The report should discuss material matters related to security breaches or violations.
Significant Disruption	It is incumbent on FIs and TSPs to identify and prepare for potentially-significant disruptive events, including those that may have a low probability of occurring but would have a high impact.
Substantial Harm or Inconvenience	Interagency Guidelines describes response programs to address unauthorized access that could result in substantial harm or inconvenience to a customer.
Timely Notification	FI and TSP contracts should require the service provider to take appropriate actions to address incidents of unauthorized access to the FI's customer information, including notification to the institution as soon as possible of any such incident. In addition, FIs are responsible for notifying their primary Federal regulator as soon as possible, notifying appropriate law enforcement authorities consistent with Suspicious Activity Report regulations, and notifying customers when warranted. Timely notification of customers is important to manage an institution's reputation risk.
Unauthorized Access	Interagency Guidelines describes response programs that an FI should develop to address unauthorized access to or use of customer information.

Source: OIG analysis of FFIEC and FDIC online resources.

Key Terminology Usage

Regulatory and supervisory guidance uses certain key terms that are not explicitly defined in the context of business continuity and incident response and reporting concepts. The figure below illustrates the degree of explanation of these terms in contracts we reviewed.

Figure: Key Terminology Usage



Source: OIG analysis of examination documentation.

FDIC and FFIEC Initiatives

FDIC and FFIEC Initiatives. Recent FDIC and FFIEC initiatives include the following:

- **Cybersecurity Awareness Program.** The FFIEC initiated a cybersecurity awareness program to improve FI management and board awareness of growing cybersecurity risks and the need to identify, assess, and mitigate these risks. In June 2015, the FFIEC agencies issued the *FFIEC Cybersecurity Assessment Tool*, to help institutions identify their inherent cyber risk and determine their cybersecurity preparedness.

- **Vendor Management Technical Assistance Video.** The FDIC published several technical assistance videos related to cybersecurity and vendor management. Recently, in March 2016, the FDIC released a vendor management video titled, *Vendor Management – Outsourcing Technology Services*, to assist FI directors and senior management in developing a comprehensive vendor management risk-assessment program.

- **Supervisory Insights Article.** In 2015, the FDIC published a supervisory insights article titled, *A Framework for Cybersecurity*. The article discussed the cyber threat landscape and how FI and TSP information security programs could be enhanced to address evolving cybersecurity risks.

- **FFIEC Guidance.** The FFIEC has initiated efforts to update the IT Examination Handbook. Recently, the FFIEC has updated certain IT booklets that provide outsourcing guidance including, the FFIEC's Business Continuity Planning booklet, dated February 2015; the FFIEC's Management booklet, dated November 2015; and the FFIEC's Information Security booklet, dated September 2016. Appendix J to the Business Continuity Planning booklet stresses the importance of addressing and incorporating cybersecurity elements when establishing and monitoring third-party relationships.

- **IT Risk Examination Program.** In June 2016, the FDIC issued new IT examination procedures designed to enhance identification, assessment, and validation of IT and operations risk. In March 2016, the FDIC also initiated a pilot program that utilized a cybersecurity examination tool.

- **Proposed TSP Rules.** The FDIC is sponsoring a proposed rule that would establish TSP standards and provide a basic framework of expectations and requirements, and a proposed rule, with the FRB and OCC, to establish an enhanced framework of heightened standards for certain institutions based on asset size and service provided.

- **2016 Horizontal Interconnectedness Review.** The federal banking agencies established a horizontal review program that focuses on how large significant service providers manage systemic interconnectivity risks. In the future, RMS would like to perform a study to assess FI and TSP interconnectivity.

Acronyms and Abbreviations

Acronym / Abbreviation	Explanation
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FDICIA	Federal Deposit Insurance Corporation Improvement Act
FFIEC	Federal Financial Institutions Examination Council
FI	Financial Institution
FIL	Financial Institution Letter
GLBA	Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act
IT	Information Technology
OIG	Office of Inspector General
RADD	Regional Automated Document Distribution
RD	Regional Director
RMS	Division of Risk Management Supervision
SOC	Service Organization Control
TSP	Technology Service Provider
ViSION	Virtual Supervisory Information on the Net

Corporation Comments

FDIC
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Division of Risk Management Supervision

January 26, 2017

TO: E. Marshall Gentry
Assistant Inspector General for Evaluation

FROM: Doreen R. Eberley **/Signed/**
Director, Division of Risk Management Supervision

SUBJECT: Draft Evaluation Report Entitled, *Technology Service Provider Contracts with FDIC Supervised Institutions* (Assignment No. 2016-021)

Thank you for the opportunity to review and comment on the report by the Office of the Inspector General for the Federal Deposit Insurance Corporation, entitled, *Technology Service Provider Contracts with FDIC's Supervised Institutions* (Report). The Division of Risk Management Supervision (RMS) appreciated the thoroughness of the evaluation and the recommendations for mitigating the risks that may arise from a financial institution's use of a third party. RMS agrees with the two recommendations made in the Report, and has taken numerous steps to provide institutions comprehensive business continuity, cybersecurity, and vendor management guidance, and to enhance our information technology (IT) examination programs.

The OIG's evaluation objectives were to assess how clearly FDIC-supervised institutions' contracts with technology service providers address the technology service provider's responsibilities related to:

1. business continuity planning; and
2. responding to and reporting on cybersecurity incidents.

In your evaluation you reviewed 48 contracts between financial institutions and technology service providers that were designated as "critical' or "high" risk to the financial institutions operations. The resulting report contains two recommendations. RMS concurs with each recommendation and has provided a more specific response to each below.

<u>OIG Audit Recommendation 1</u>: *Continue to communicate to FIs the importance of:*

- *Fully considering and assessing the risks that TSPs could have on the FI's ability to manage its own business continuity and incident response planning efforts;*

  Ensuring that contracts with TSPs include specific provisions that address FI identified risks, protect FI interests, and provide details necessary to allow FIs to manage their own business continuity planning and incident response and reporting efforts through TSP operations; and

Corporation Comments

- *Clearly defining key contract terms that would be important in understanding FI and TSP rights and responsibilities in the event of a business disruption or computer security incident particularly for those contracts that FIs identify as critical or that have access to sensitive or personally identifiable information.*

  RMS will continue to communicate the importance of effective contracts between financial institutions and technology service providers through our supervision program which includes:
  - guidance,
  - examination procedures,
  - examinations, and
  - off-site monitoring.

  Guidance: The FDIC is currently participating in two Federal Financial Institutions Examination Council (FFIEC) projects to provide supervisory guidance to financial institutions concerning their relationships with technology service providers: updating the FFIEC Business Continuity Planning and Outsourcing Booklets. RMS is of the opinion that OIG Recommendation No. 1 can be addressed in the revisions to these booklets that are currently in process. However, since these are FFIEC projects, specific language addressing the recommendations of the Report, will have to be agreed to by all the FFIEC agencies.

  In addition, the federal banking agencies are seeking to address the issue of appropriate recovery time objectives in the event of a disruption or cyber event in the Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards that was published for public comment on October 26, 2016. Comments are due to the agencies shortly.

  Also, the FDIC has made a video available on its website to assist community banks in developing a comprehensive vendor management program when outsourcing technology services at https://www.fdic.gov/regulations/resources/director/virtual/vendor.html and reissued guidance papers. See enclosed Financial Institution Letter (FIL).

  Examination Procedures: RMS updated the information technology and operations risk (IT) examination procedures to provide a more efficient, risk-focused approach. The Information Technology Risk Examination (InTREx) Program will allow for the continued communication of the importance of strong contracts between financial institutions and technology service providers. One of the Management evaluation factors in InTREx is, "The adequacy of contracts and management's ability to monitor relationships with third-party servicers."

OIG Audit Recommendation 2: *Following an appropriate amount of time for FIs to implement guidance, conduct a follow-on study, such as a horizontal review of FIs, to assess to what extent the issues included in recommendation 1 are being effectively addressed.*

  Examinations: The recently implemented InTREx Program will allow for a horizontal review of the adequacy of contracts and management's ability to monitor relationships with

2

Corporation Comments

third-party servicers. Among the examination procedures included the program are an evaluation of the vendor management program established at each financial institution to monitor service provider and vendor relationships (both domestic and foreign-based). Included in the evaluation:

- Coverage of service providers and vendors, including affiliates, in the risk assessment process
- Foreign-based risks, as applicable
- Ongoing monitoring, which may include review of the following:
  - Financial statements
  - Controls assessments, such as SSAE 16 SOC Reports (Statement on Standards for Attestation Engagement Service Organization Control Reports)
  - Information security program
  - Cybersecurity preparedness and resilience
  - Incident response
  - Internal/external audit reports
  - Regulatory reports
  - Affiliate relationships (e.g., Federal Reserve Regulation W)
  - Consumer compliance
  - Onsite reviews
  - Participation in user groups
  - Business continuity program, including integrated testing with the institution's plan
  - Service level agreement compliance
  - Vendor awareness of emerging technologies
  - Report to Board of Directors

Off-site Monitoring: FIL 43-2016, informed FDIC supervised financial institutions that InTREx would be used for all IT and operations risk examinations beginning October 1, 2016. At the end of the 18-month examination cycle which began October 1, 2016, we will prepare a full horizontal review to assess to what extent the issues included in recommendation one of the Report are being effectively addressed, and plan any additional actions based on that review.

3

Corporation Comments

FDIC

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

Financial Institution Letter
FIL-13-2014
April 7, 2014

Technology Outsourcing: Informational Tools for Community Bankers

Summary: The three attached FDIC Technology Outsourcing documents are being re-issued as an informational resource to community banks on how to select service providers, draft contract terms, and oversee multiple service providers when outsourcing for technology products and services. The documents are not examination procedures or official guidance but, rather, informational tools.

Statement of Applicability to Institutions with Less than $1 Billion in Total Assets: This Financial Institution Letter (FIL) applies to all FDIC-supervised institutions.

Suggested Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Security Officer

Attachments:
- Effective Practices for Selecting a Service Provider
- Tools to Manage Technology Providers' Performance Risk: Service Level Agreements
- Techniques for Managing Multiple Service Providers.

Related Topics:
- FFIEC Handbook on Outsourcing Technology Services (June 2004) http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf
- FDIC Guidance for Managing Third-Party Risk (FIL-44-2008) www.fdic.gov/news/news/financial/2008/fil08044.html
- Technology Bulletin on Outsourcing (FIL-50-2001) www.fdic.gov/news/news/financial/2001/fil0150.html

Contact:
Donald Saxinger, Senior Examination Specialist, at dsaxinger@fdic.gov or (703) 254-0214

Note:
FDIC Financial Institution Letters (FILs) may be accessed from the FDIC's Web site at http://www.fdic.gov/news/news/financial/2014/.

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

Paper copies of may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (1-877-275-3342 or 703-562-2200).

Highlights:

- The attached three documents, first issued on June 4, 2001, contain practical ideas for banks to consider when they engage in technology outsourcing.
- These documents are intended to assist community bankers by providing information on:
  - Effective Practices for Selecting a Service Provider,
  - Tools to Manage Technology Providers' Performance Risk: Service Level Agreements, and
  - Techniques for Managing Multiple Service Providers.
- The attached documents are for informational purposes only and are not considered to be official examination guidance.
- Examination guidance and additional information on vendor management can be found in the FFIEC IT Examination Handbook, *Outsourcing Technology Services*. This guidance focuses on four key areas: risk assessment, service provider selection, contract terms, and oversight of outsourcing arrangements.

Summary of the Corporation's Corrective Actions

This table presents management's response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	RMS will continue to communicate the importance of effective contracts between FIs and TSPs through its supervision program, which includes guidance, examination procedures, examinations, and off-site monitoring.	June 30, 2018	N/A	Yes	Open
2	RMS will prepare a full horizontal review to assess to what extent the issues included in recommendation one of the report are being effectively addressed, and plan any additional actions based on that review.	October 1, 2018	N/A	Yes	Open

[a] Resolved – (1) Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but alternative action meets the intent of the recommendation.
(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Recommendations will be closed when (a) Corporate Management Control notifies the OIG that corrective actions are complete or (b) in the case of recommendations that the OIG determines to be particularly significant, when the OIG confirms that corrective actions have been completed and are responsive.