Third Party Risk

Introduction

The board of directors and senior management of an insured depository institution (institution) are ultimately 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. The use of third-party relationships does not relinquish responsibility of the board of directors and management. The institution's officials are expected to have a clearly defined system of risk management controls built into the management system that governs the institution's compliance operations, including controls over activities conducted by affiliates and third-party vendors. The more significant the third party program, the more important it is that the institution conduct regular periodic reviews of the adequacy of its oversight and controls over third-party relationships.

Examiners should evaluate all applicable activities conducted through third-party relationships as though the activities were performed by the institution itself. It must be emphasized that while an institution may properly seek to mitigate the risks of third-party relationships through the use of indemnity agreements with third parties, such agreements do not insulate the institution from its ultimate responsibility to conduct banking-related activities in a safe and sound manner and in compliance with applicable consumer protection laws and regulations, including fair lending laws and regulations (for example, the Equal Credit Opportunity Act (ECOA) and the Fair Housing Act).

These examination procedures provide additional context and guidance for compliance examiners when evaluating an institution's third-party relationships. These procedures include a description of potential risks arising from third-party relationships and provide examiners with insight on how to assess compliance risk for third-party business relationships.

A third-party relationship could be considered "significant" if:

- the institution's relationship with the third party is a new relationship or involves implementing new institution activities;
- the relationship has a material effect on the institution's revenues or expenses;
- the third party performs critical functions;
- the third party stores, accesses, transmits, or performs transactions on sensitive customer information;
- the third-party relationship significantly increases the institution's geographic market;
- the third party provides a product or performs a service involving lending or card payment transactions;
- the third party poses risks that could materially affect the institution's earnings, capital, or reputation;
- the third party provides a product or performs a service that covers or could cover a large number of consumers;
- the third party provides a product or performs a service that implicates several or higher risk consumer protection regulations;
- the third party is involved in deposit taking arrangements such as affinity arrangements; or
- the third party markets products or services directly to institution customers that could pose a risk of financial loss to the individual.

Background

For purposes of this guidance, the term "third party" is broadly defined to include all entities that have entered into a business relationship with the institution, whether the third party is a bank or a nonbank, affiliated or not affiliated, regulated or nonregulated, a wholly- or partially-owned subsidiary, or a domestic or a foreign institution.

Institutions generally enter into third-party relationships by outsourcing[1] certain operational functions to a third party or by using a third party to make products and services available that the institution does not originate. Also, institutions may enter into arrangements with third parties in which the institution funds directly or indirectly through a line of credit certain products originated by a third party. As the financial services industry continues to evolve, some institutions are also using third parties for functions that are either new or have traditionally been performed in-house, ***e.g.***, outsourcing the institution's compliance management system (CMS) audit function.

The use of third parties can aid institution management in attaining strategic objectives by increasing revenues or reducing costs. The use of a third party also serves as a vehicle for management to access greater expertise or efficiency for a particular activity. Appropriately managed third-party relationships can enhance competitiveness, provide diversification, and ultimately strengthen the safety and soundness and CMS of the institution. However, third-party arrangements also present risks if not properly managed. Specifically, failure to manage these risks can expose an institution to supervisory action, financial loss, litigation, and

1 The term "outsourcing" is a vernacular expression that refers to a company or business that contracts or subcontracts a service or function to a third party that might otherwise be performed by in-house employees. Institutions may use the terms "outsourcing" and "third-party" interchangeably. However, examiners should remember that services and functions outsourced by an institution contain varying degrees of risk. Therefore, when reviewing for third-party risk, examiners should request a listing of all functions and services outsourced to ensure that appropriate relationships that have third-party risk are captured for review.

reputational damage. To that end, the decision about whether to use a third party should be considered by an institution's board of directors and management, taking into account the circumstances unique to the potential relationship.

Institutions have also been presented with increasing opportunities to enter into contractual arrangements with foreign-based third-party service providers to fulfill outsourcing needs. Examiners should evaluate these relationships with, at least, the same level of vigilance and scrutiny as with domestic third-party service providers (see discussion of Country Risk below).

These examination procedures provide a framework for examining the effectiveness of an institution's CMS as it relates to the policies and procedures for overseeing, managing, and controlling third-party relationships. More importantly, this guidance supplements, but does not replace, previously issued information on third-party risk and is intended to aid in the examination of third-party arrangements.[2]

Potential Risks Arising from Third-Party Relationships

There are numerous risks that may arise from an institution'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. Failure to prevent or mitigate these risks can expose an institution to supervisory action, financial loss, litigation, and reputation damage, and may even impair the institution's ability to establish new or service existing customer relationships.

Not all of the following risks will be applicable to every third-party relationship; however, complex or significant arrangements may have definable risks in most areas. The institution's board of directors and senior management should understand the nature of these risks in the context of the institution's current or planned use of third parties and in establishing and evaluating the institution's risk oversight and control systems. The following summary of risks is not considered all-inclusive.

"Compliance Risk" Compliance risk is the risk arising from violations of laws, rules, or regulations, or from noncompliance with the institution's internal policies or procedures or business standards. This risk exists when the products or activities of a third party are not consistent with governing laws, rules, regulations, policies, or ethical standards. For example, some third parties may engage in product marketing practices that are deceptive in violation of Section 5 of the Federal Trade Commission Act, or lending practices that are discriminatory in violation of the ECOA and the Consumer Financial Protection Bureau's Regulation B. The ability of the third party to maintain the privacy of customer records and to implement an appropriate information security and disclosure program is another compliance concern. Liability could potentially extend to the institution when third parties experience security breaches involving customer information in violation of the safeguarding requirements of customer information, as set out in Federal Deposit Insurance Corporation (FDIC) and Federal Trade Commission regulations. Compliance risk is exacerbated when an institution has inadequate oversight, monitoring, or audit functions over third-party relationships.

"Reputation Risk" Reputation risk is the risk arising from negative public opinion. Third-party relationships that result in dissatisfied customers, unexpected customer financial loss, interactions not consistent with institution policies, inappropriate recommendations, security breaches resulting in the disclosure of customer information, and violations of laws and regulations are all examples that could harm the reputation and standing of the institution. Any negative publicity involving the third party, whether or not the publicity is related to the institution's use of the third party, could result in reputation risk.

"Strategic Risk" Strategic risk is the risk arising from adverse business decisions, or the failure to implement appropriate business decisions in a manner that is consistent with the institution's strategic goals. The use of a third party to perform banking functions or to offer products or services that do not help the institution achieve corporate strategic goals and provide an adequate return on investment exposes the institution to strategic risk.

"Operational Risk" Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, systems, or external events. Third-party relationships often integrate the internal processes of other organizations with the institution's processes and can increase the overall operational complexity.

"Transaction Risk" Transaction risk is the risk arising from problems with service or product delivery. A third-party's failure to perform as expected by customers or the institution due to reasons such as inadequate capacity, technological failure, human error, or fraud, exposes the institution to transaction risk. The lack of an effective business resumption plan and appropriate contingency plans increase transaction risk. Weak control over technology used in the third-party arrangement may result in threats to security and the integrity of systems and resources. These issues could result in unauthorized transactions or the inability to transact business as expected.

2 Financial Institution Letter 44-2008 dated June 6, 2008, entitled *Third Party Risk, Guidance for Managing Third-Party Risk*

"Credit Risk" Credit risk is the risk that a third party, or any other creditor necessary to the third-party relationship, is unable to meet the terms of the contractual arrangements with the institution or to otherwise financially perform as agreed. The basic form of credit risk involves the financial condition of the third party itself. Some contracts provide that the third party ensures some measure of performance related to obligations arising from the relationship, such as loan origination programs. In these circumstances, the financial condition of the third party is a factor in assessing credit risk. Credit risk also arises from the use of third parties that market or originate certain types of loans, solicit and refer customers, conduct underwriting analysis, or set up product programs for the institution. Appropriate monitoring of the financial activity of the third party is necessary to ensure that credit risk is understood and remains within board-approved limits.

"Country Risk" Country risk is the exposure to the economic, social and political conditions and events in a foreign country that may adversely affect the ability of the foreign-based third-party service provider (FBTSP) to meet the level of service required by the arrangement, resulting in harm to the institution. In extreme cases, this exposure could result in the loss of data, research and development efforts, or other assets. Contracting with a FBTSP exposes an institution to country risk, a unique characteristic of these arrangements. Managing country risk requires the ability to gather and assess information regarding a foreign government's policies, including those addressing information access, as well as local political, social, economic, and legal conditions.

"Other Risks" The types of risk introduced by an institution's decision to use a third party cannot be fully assessed without a complete understanding of the resulting arrangement. Therefore, a comprehensive list of potential risks that could be associated with a third-party relationship is not possible. In addition to the risks described above, third-party relationships may also subject the institution to liquidity, interest rate, price, legal, and foreign currency translation risks.

With the wide array of risks that may occur, the following includes some pragmatic examples of concerns that can surface if there is lack of appropriate oversight and monitoring of third-party relationships and associated CMSs:

- Where the institution lends its name or regulated entity status to products and services originated by others or activities predominantly conducted by others, and those vendors engage in practices that may be considered predatory, abusive, or unfair and deceptive to consumers;
- When possible violations of fair lending and consumer protection laws and regulations occur, particularly when the actual involvement of the institution and the third party is invisible to the customer;
- Where the third-party relationships do not meet the expectation of the institution's customers;
- Where, due to the third party, the customer experiences poor service, disruption of service, financial loss resulting from not understanding product or service risks or alternatives, and inferior choices stemming from lack of disclosure(s);
- When privacy of consumer and customer records is not adequately protected;
- Where the third party is unable to deliver products or services due to fraud, error, inadequate capacity, or technology failure, and where there is a lack of effective business resumption and contingency planning for such situations;
- Where a problem or issue lies with a service being rendered by a third party that went undetected by the institution because an appropriate audit or monitoring program was not in place for the third-party relationship; and
- Where the third party is the auditor for the institution's CMS and management failed to properly oversee and manage the scope and intensity of these audits to ensure reviews were comprehensive or covered areas of significant risk.

Compliance Management System Review

The key to the effective and successful use of a third party in any capacity is for the institution's management to appropriately assess, measure, monitor, and control the risks associated with the relationship and weave that process into its CMS. While engaging another entity may aid management and the board in achieving strategic goals, such an arrangement reduces management's direct control. Therefore, the use of a third party increases the need for robust oversight of the process from start to finish. This guidance provides four main elements of an effective third-party risk compliance management process:

1. *Risk Assessment* – The process of assessing risks and options for controlling third-party arrangements.
2. *Due Diligence in Selecting a Third Party* – The process of selecting a qualified entity to implement the activity or program.
3. *Contract Structuring and Review* – The process of ensuring that the specific expectations and obligations of both the institution and the third party are outlined in a written contract prior to entering into the arrangement—a contract should act as a map to the relationship and define its structure.
4. *Oversight* – The process of reviewing the operational and financial performance of third-party activities over those products and services performed through third-party arrangements on an ongoing basis, to ensure that the third

party meets and can continue to meet the terms of the contractual arrangement.

While these four elements apply to any third-party activities, the precise use of this process is predicated upon the nature of the third-party relationship, the scope and magnitude of the activity, and the risks identified. These examination procedures are not intended to result in an expansion or a decrease in the use of third parties by institutions, but to provide a framework for assessing, measuring, monitoring, and controlling risks associated with third parties. A comprehensive risk management process, which includes management of any third-party relationships, will enable management to ensure that the third party is operating in a manner consistent with federal and state laws, rules, and regulations, including those intended to protect consumers. With that, the aforementioned four elements will serve as the nexus for examining the effectiveness of an institution's oversight and management of third-party relationships.

Examination Objectives

1. Determine if the financial institution has any "significant" third-party relationships;
2. Determine the adequacy of the institution's CMS, including policies and procedures, internal controls, training, monitoring, and internal and external auditing procedures associated with third-party relationships to ensure consistent and ongoing compliance with all applicable consumer protection laws and regulations;
3. Determine whether activities conducted through third parties are compliant with applicable consumer protection laws, fair lending regulations, and internal policies; and
4. Determine appropriate corrective action when third-party risk issues are identified or deficiencies are noted.

Examination Procedures

Pre-Examination Planning

Examiners should follow the general Compliance Examination procedures pertaining to pre-examination planning, found in the FDIC's Compliance Examination Manual, to gather as much information as possible about an institution's involvement in any third-party arrangement. Examiners must consider these relationships when assessing the quality of the institution's CMS. The following includes the steps that examiners should generally follow in gathering information on an institution's third-party relationships:

1. During the initial contact with the institution and through the Compliance Information and Document Request (CIDR), identify the presence of any third-party relationships;
2. During the initial contact with the institution and through the CIDR, identify planned or newly initiated third-party relationships;
3. Obtain and review copies of current contracts and relevant records that management utilizes to manage third-party relationships. Examples of relevant records may include, but are not limited to, audit reports, engagement letters, contracts, references, marketing scripts, due diligence documentation, advertisements (***e.g.***, paper, electronic, and e-mail), promotional materials, disclosures, documentation of monitoring efforts, training material, policies, and procedural manuals;
4. Review prior Compliance and Risk Management examination reports along with institution file correspondence for information concerning any adverse material effect the third-party relationship(s) has on compliance with consumer protection laws and regulations that may affect safe and sound operations. It may be possible to risk scope certain aspects of the Compliance review depending on timing and depth of the Risk Management Review; and
5. Review any consumer complaints received against the institution and/or third-party provider(s).[3]

Risk Assessment

1. Determine if management, prior to entering the third-party relationship, ensured that the proposed third-party relationship is consistent with the institution's strategic planning and overall business strategy.
2. Determine if management, prior to entering the third-party relationship, analyzed the strategic risk the institution is willing to enter into given its size, resources, capacity, and number of employees.
3. Determine if management, prior to entering the third-party relationship, analyzed the benefits, costs, legal aspects, and the potential risks associated with the third party under consideration.
4. Determine if management performed a risk/reward analysis, comparing the proposed third-party relationship to other methods of performing the activity or product offering, including the use of other vendors or in-house staff. For such matters, the analysis should be considered integral to the institution's overall strategic planning, and should thus be performed by senior management and reviewed by the board or an appropriate committee.
5. Determine if institution personnel have the requisite knowledge and skills to adequately perform the risk analysis. Certain aspects of the risk assessment phase may include the use of internal or external auditors, compliance officers, technology officers, and legal counsel. This phase should also identify performance criteria, internal controls, reporting needs, and contractual requirements that would

3 Resources: www.bbb.org (Better Business Bureau); websites/blogs such as www.Ripoffreport.com and www.complaints.com; and state attorney general offices.

be critical to the ongoing assessment and control of specific identified risks. For example, if the activity involves consumer products or services, the board and management should establish a clear solicitation and origination strategy that allows for an assessment of performance, as well as mid-course corrections.

6. Determine if management reviewed whether the third-party's activities could be viewed as predatory, discriminatory, abusive, unfair, or deceptive to consumers.
7. Determine if management reviewed its ability to provide adequate oversight and management of the proposed third-party relationship on an ongoing basis.
8. Determine if management has a process in place for elevating new or significant third-party relationships and issues to the board and appropriate committee for review and approval.

Due Diligence in Selecting a Third Party

1. Determine if management conducted an adequate due diligence that included 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, as applicable. The scope and depth of due diligence should be directly related to the importance and magnitude of the third-party relationship. (Note: Due diligence should be performed not only prior to selecting a third-party relationship, but also periodically during the course of the relationship, particularly when considering a renewal of a contract.) The evaluation of a third party may include the following items:
   - Audited financial statements, annual reports, Securities and Exchange Commission filings, and other available financial information;
   - Significance of the proposed contract on the third-party's financial condition;
   - Experience and ability in implementing and monitoring the proposed activity;
   - Business reputation, including any complaints filed;
   - Span of business operations in which the third party is engaged;
   - Qualifications and experience of the company's principals;
   - Strategies and goals, including service philosophies, quality initiatives, efficiency improvements, and employment policies;
   - Existence of any significant complaints or litigation (past and pending), or supervisory actions against the company or its owners or principals;
   - Ability to perform the proposed functions using current systems or the need to make additional investment;
   - Use of other parties or subcontractors by the third party;
   - Scope of internal controls, systems and data security, privacy protections, and audit coverage;
   - Business resumption strategy and contingency plans;
   - Knowledge of and background and experience with consumer protection and civil rights laws and regulations;
   - Underwriting criteria;
   - Adequacy of management information systems;
   - Insurance coverage;
   - Marketing materials to determine how the institution's name will be associated with the product;
   - Websites; and
   - Vendor and institution management responsibilities.

Contract Structuring and Review

1. Determine if management ensures that the specific expectations and obligations of both the institution and the third party are outlined in a written contract prior to entering into the arrangement. Any material or significant contract with a third party should prohibit assignment, transfer, or subcontracting by the third party of its obligations unless the institution appropriately determines that such activity is consistent with its due diligence responsibilities.
2. Determine if the board provides approval prior to entering into any material third-party arrangements. When reviewing this area, questions that compliance examiners may want to consider are: (1) Are board members fully aware of the risks, issues, and responsibilities associated with the third-party relationship under consideration?; (2) Do any board members have close ties to or have a vested interest in the third-party relationship under consideration?; (3) Did the Directorate abrogate their responsibilities during the review and approval of any material third-party relationship?; (4) Were board members provided access to the due diligence findings and were findings accurately presented?; and (5) Do minutes exist of Board meetings where the third-party arrangements were addressed?
3. Determine if appropriate legal counsel reviewed significant contracts prior to finalization.
4. Determine if clearly defined performance standards are included to serve as a basis for measuring the performance of the third party. Determine if management periodically reviews the performance measures to ensure consistency with its overall objectives. Performance standards may also be used as a factor in the compensation or fee paid to the third party. Institutions should employ compensation programs that are consistent with consumer protection laws and sound banking practices.[4]
5. Determine if the contract addresses the following:
   - Outlines the fees to be paid, including fixed compensation, variable charges, and any fees to be paid for nonrecurring items or special requests. Other items that should be addressed, if applicable, are the cost and responsibility for purchasing and maintaining any equipment, hardware, software, or other item related to the activity. Additionally, the contract should address obligations for retaining documentation for compensation arrangements, as appropriate. Also, the party responsible for payment of any legal or audit expenses should be identified.
   - Specifies the type and frequency of management information reports to be received from the third party. Routine reports may include performance, audits, financial, security, consumer complaint, and business resumption testing reports. Determine if management considers mandating exception-based reports that would serve as notification of any changes or problems that could affect the nature of the relationship or pose a risk to the institution.
   - Specifies the institution's right to audit the third party (or engage an independent auditor) as needed to monitor performance under the contract. Management should ensure that the third-party's internal control environment as it relates to the service or product being provided to the institution is sufficiently audited or monitored. Does the contract specify the scope of audits that will be performed? Do audits capture all compliance-related risk?
   - Prohibits the third party and its agents from using or disclosing the institution's information, except as necessary to perform the functions designated by the contract, or as otherwise permitted by law. For example, any non-public personal information of the institution's customers must be handled in a manner consistent with the institution's own privacy policy and in accordance with applicable privacy laws and regulations. Any breaches in the security and confidentiality of information should be fully and promptly disclosed to the institution.
   - Specifies whether the institution or the third party has the duty to respond to any complaints received by the third party from customers of the institution. If the third party is responsible for such responses, a copy of any complaint and the response should be forwarded to the institution. The contract should also provide for periodic summary reports detailing the status and resolution of complaints along with a trend analysis on types of complaints. Additionally, the contract should address record retention provisions for retaining relevant consumer complaint records.
   - Addresses the third-party's responsibility for continuation of services provided for in the contractual arrangement in the event of an operational failure, including both man-made and natural disasters. The third party should have appropriate protections for backing up information and also maintain disaster recovery and contingency plans with sufficiently detailed operating procedures. Results of testing of these plans should be provided to the institution.

4 The FDIC enforces laws and regulations that prohibit the use of compensation arrangements that encourage third-party originators to inappropriately steer borrowers into higher cost products or avoid mortgage lending in low-income neighborhoods where home prices are lower. Compensation arrangements should not create unintended incentives to engage in unfair or deceptive acts or practices, particularly with respect to product sales, loan originations, and collections; or be tailored to circumvent other applicable consumer protection laws and regulations, including fair lending laws and regulations.

- Specifies what circumstances constitute default, identifies remedies, and allows for a reasonable opportunity to cure a default. Similarly, termination rights should be identified in the contract, especially for material third-party arrangements and relationships involving rapidly changing technology or circumstances. For example, termination rights may be sought for various conditions, such as inability to prevent violations of consumer protection laws and regulations.
- Includes a dispute resolution process for the purpose of resolving problems expeditiously. Continuation of the arrangement between the parties during the dispute should also be addressed.
- Addresses ownership issues and the third-party's right to use the institution's property, including intellectual property such as the institution's name and logo, trademark, and other copyrighted material. It should also address ownership and control of any records generated by the third party.
- Provides indemnification provisions that require the third party to hold the institution harmless from liability as a result of negligence by the third party, and vice versa. The existence of indemnification provisions will not be a mitigating factor where deficiencies indicate the need to seek corrective actions. For example, where violations of consumer protection laws and regulations are present, the FDIC's consideration of remedial/enforcement measures will be made irrespective of the existence of indemnification clauses in third-party contracts.

Board and Management Oversight

1. Determine if the board initially approved significant third-party arrangements, and what the Board considered in reaching that approval. Additionally, determine if the board oversees and reviews, at least annually, significant third-party arrangements, and reviews these arrangements and written agreements whenever there is a material change to the program.
2. Determine if management periodically reviews the third party's operations in order to verify that they are consistent with the terms of the written agreement and that risks are being controlled. The institution's CMS should also ensure continuing compliance with applicable consumer protection laws and regulations, as well as internal policies and procedures.
3. Determine if management allocates sufficient qualified staff to monitor significant third-party relationships and provides the necessary oversight. Specifically, management should consider designating an individual or committee to coordinate the oversight activities with respect to significant relationships, and involve their compliance management function and, as necessary, other operational areas such as audit.[5]
   - 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.
4. Determine if management is following the institution's policies and procedures for terminating or probating third-party relationships, based on findings from audits and performance monitoring.
5. Determine if the results of oversight activities for material third-party arrangements are periodically reported to the institution's board of directors or designated committee. Identified weaknesses should be documented and promptly addressed.
6. Determine if the institution maintains documents and records on all aspects of the third-party relationship, including valid contracts, business plans, risk analyses, due diligence, and oversight activities (including reports to the board or delegated committees and documents regarding any dispute resolution) and for what period of time.

Institution-Affiliated Party

Institutions can also outsource activities to third parties, or otherwise make use of products or services provided by third parties, via a subsidiary or affiliate referred to as an Institution-Affiliated Party (IAP).[6] By statute, an IAP is defined as:

- Any director, officer, employee, or controlling stockholder (other than a bank holding company) of, or agent for, an insured depository institution;
- Any other person who has filed or is required to file a change-in-control notice with their primary Federal banking regulator;
- Any shareholder (other than a bank holding company), consultant, joint venture partner, and any other person as determined by the appropriate Federal banking agency (by regulation or case-by-case) who participates in the conduct of the affairs of an insured depository institution; or
- Any independent contractor (including any attorney, appraiser, or accountant) who knowingly or recklessly participates in:
  - any violation of any law or regulation;
  - any breach of fiduciary duty; or

5 The extent of oversight of a particular third-party relationship will depend upon the potential risks and the scope and magnitude of the arrangement.

6 Despite the use of the word "person" and other similar vernaculars in the definition, an institution-affiliated party can be an individual or institution itself.

- any unsafe or unsound practice, which caused or is likely to cause more than a minimal financial loss to, or a significant adverse effect on, the insured depository institution.

The designation of a third party as an IAP is significant when the FDIC is considering bringing enforcement action against a third party, because the FDIC's direct enforcement jurisdiction over third parties generally is limited to insured State nonmember banks, foreign institutions having an insured branch, and their IAPs. Examiners should be mindful of the possible existence of this status during examinations and utilize the same examination principles and level of caution for reviewing the institution's management of these third-party relationships.

If significant ambiguity exists when trying to ascertain if the third party is an IAP, a case-by-case analysis may be warranted, in consultation with the FDIC's Legal Division, before proceeding with the examination of the third party. The FDIC's examination authority over third parties is broader than enforcement jurisdiction.

Refer to the IAP examination procedures[7] for further information and guidance on examining and potentially bringing enforcement action against a person or entity that may be an IAP.

Transaction Sampling and Testing

Based on the examiner's conclusions about the institution's CMS, a determination should be made about the extent of transaction testing or file review necessary to complete the Compliance Examination. The severity of the CMS weaknesses and risks present should dictate the intensity of transaction testing. The determination and level of transaction testing should be tailored to weaknesses identified in the CMS as it relates to specific third-party relationships, focusing on those areas that present the greatest degree of risk to the institution or to consumers. The following are examples of items that should be reviewed, as applicable:

- Advertisement and marketing documentation;
- New product development documentation;
- Procedural manuals, including those for servicing, collections, and safeguarding customer information;
- Employee training records;
- Audit/monitoring report findings;
- Customer disclosures, notices, agreements, and periodic statements for each product and service reviewed;
- Account statements;
- Contracts with third parties;
- Compensation programs;
- Promotional materials;
- Telemarketing scripts; and
- Recorded calls for telemarketing or collections.

Documentation of Examination Findings

At the conclusion of the examination, examiners should document their conclusions about the institution's third-party relationships in the Risk Profile and Scope Memorandum, examination work papers, and Report of Examination, as appropriate. The Third Party Check List (VII-5.10 to VII-5.20) is provided to aid examiners in reviewing third-party relationships and documenting examination findings.

Institutions that fail to comply with applicable laws and regulations, or fail to establish or observe appropriate policies and procedures should be subject to criticism in the Report of Examination and appropriate corrective action.

Consultations

Because of the wide range of facts, activities, and issues that can arise in the context of third-party relationships, as well as the multitude of consumer protection regulations that can be impacted, the examiner should consult the Regional Office when possible issues or concerns are identified at a Compliance Examination.

Appropriate corrective action, including enforcement action, may be pursued for deficiencies related to a third-party relationship, including IAP activities that pose compliance management concerns or result in violations of applicable consumer protection laws and regulations.

Examiners are reminded that indemnity or other contractual provisions with third parties cannot insulate the institution from regulatory corrective action.

7 Examination procedures for IAPs can be found in Section X-5.1, Bank Subsidiaries and Affiliates, of the Compliance Examination Manual.

References

FIL-32-2009:Third-Party Referrals Promising Above-Market Rates on Certificates of Deposit

FIL-44-2008:Third-Party Risk: Guidance for Managing Third-Party Risk

FIL-03-2012: Payment Processor Relationships Revised Guidance

FIL-41-2014: FDIC Clarifying Supervisory Approach to Institutions Establishing Account Relationships with Third-Party Payment Processors

FIL-5-2015: Statement on Providing Banking Services

This job aid can be utilized for examining the effectiveness of a financial institution's (institution) compliance management system as it relates to the procedures for overseeing, managing, and controlling third-party relationships. Complete only those aspects of the job aid that specifically relate to the area being reviewed and retain those completed sections in the compliance examination work papers.

When reviewing a institution's self-monitoring controls and oversight of third-party relationships, a "No" answer indicates a possible exception/deficiency/violation and should be further investigated and explained in the Risk Profile and Scope Memorandum, examination work papers, and report of examination, as appropriate. If a line item is not applicable within the area of review, indicate "NA."

	Yes	No	N/A	Comments
Risk Assessment				
1. Did management, prior to entering the third-party relationship, ensure that the proposed third-party relationship is consistent with the institution's strategic planning and overall business strategy?				
2. Did management, prior to entering the third-party relationship, analyze the strategic risk the institution is willing to enter into given its size, resources, capacity, and number of employees?				
3. Did management, prior to entering the third-party relationship, analyze the benefits, costs, legal aspects, and the potential risks associated with the third party under consideration?				
4. Did management perform a risk/reward analysis, comparing the proposed third-party relationship to other methods of performing the activity or product offering, including the use of other vendors or in-house staff?				
5. Do institution personnel have the requisite knowledge and skills to adequately perform the risk analysis?				
• Does this phase identify performance criteria, internal controls, reporting needs, and contractual requirements that would be critical to the ongoing assessment and control of specific identified risks?				

	Yes	No	N/A	Comments
Risk Assessment (cont.)				
6. Did management review whether the third-party's activities could be viewed as predatory, discriminatory, abusive, unfair, or deceptive to consumers, particularly if products and services offered through the institution have fees, interest rates, or other terms that the third party could not otherwise offer on its own?				
• Are there any differences in fees, interest rates, or other terms for products and services offered to area consumers versus non-area consumers through third-party arrangements?				
7. Did management review its ability to provide adequate oversight and management of the proposed third-party relationship on an ongoing basis?				
• Is the institution's compliance management system (CMS) adapted to effectively address the third-party relationship and appropriately respond to emerging issues and compliance deficiencies?				
8. Does management have a process in place for elevating new or significant third-party relationships and issues to the board and appropriate committee for review and approval?				
Due Diligence in Selecting a Third Party				
1. Did management conduct an adequate due diligence that included 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, as applicable?				

	Yes	No	N/A	Comments
Due Diligence in Selecting a Third Party (cont.)				
2. Did management review the following items when evaluating the third party, as applicable?				
• Audited financial statements, annual reports, Securities and Exchange Commission filings, and other available financial information;				
• Significance of the proposed contract on the third party's financial condition;				
• Experience and ability in implementing and monitoring the proposed activity;				
• Business reputation;				
• Span of business operations in which the third party is engaged;				
• Qualifications and experience of the company's principals:				
• Strategies and goals, including service philosophies, quality initiatives, efficiency improvements, and employment policies;				
• Existence of any significant complaints or litigation (past and pending), or regulatory actions against the company or its owners or principals;				
• Ability to perform the proposed functions using current systems or the need to make additional investment;				
• Use of other parties or subcontractors by the third party;				
• Scope of internal controls, systems and data security, privacy protections, and audit coverage;				
• Business resumption strategy and contingency plans;				
• Knowledge of, and background and experience with, consumer protection and civil rights laws and regulations;				
• Underwriting criteria;				
• Adequacy of management information systems;				
• Insurance coverage;				

	Yes	No	N/A	Comments
Due Diligence in Selecting a Third Party (cont.)				
• Marketing materials to determine how the institution's name will be associated with the product;				
• Websites; and				
• Vendor and institution management responsibilities.				
Contract Structuring and Review				
1. Did management ensure that the specific expectations and obligations of both the institution and the third party are outlined in a written contract prior to entering into the arrangement?				
2. Did the board provide the appropriate level of review and approval prior to entering into any material third-party arrangements?				
3. Did appropriate legal counsel review significant contracts prior to finalization?				
4. Are the following topics considered as the contract is structured, with the applicability of each dependent upon the nature and significance of the third-party relationship?				
• Timeframe covered by the contract;				
• Frequency, format, and specifications of the service or product to be provided;				
• Other services to be provided by the third party, such as software support and maintenance, training of employees, and customer service;				
• Requirement that the third party comply with all applicable consumer protection laws, regulations, and regulatory guidance;				
• If a third party vendor is found culpable for violations, does the contract address responsibility for making appropriate customer restitution, paying any civil money penalty, etc.;[1]				

1 Examiners should be cognizant that the FDIC believes that an institution cannot contractually transfer its liability to a third party. If an institution is found to be derelict in its obligation to monitor the third-party's activities, the FDIC will impose a civil money penalty against the institution.

	Yes	No	N/A	Comments
Contract Structuring and Review (cont.)				
• Requirement governing which parties must retain records relating to agreements and activities conducted pursuant to the relationship, for at least a minimum required period;				
• Authorization for the institution and the appropriate federal and state regulatory agency to have access to records of the third party as are necessary or appropriate to evaluate compliance with consumer protection and fair lending laws and regulations;				
• Identification of which party will be responsible for delivering any required customer disclosures and in what format;				
• Terms and conditions relating to any compensation, monetary or otherwise, to be paid in connection with products or services rendered as a result of the third-party relationship;				
• Insurance coverage to be maintained by the third party;				
• Terms relating to any use of institution premises, equipment, data, or employees; • Permissibility/prohibition of the third party to assign, transfer, or subcontract its obligations with respect to the material or significant contract, and any notice/approval requirements;				
• Notification protocols when software or other relevant product modifications are made;				
• Protocols for reporting and handling breaches of security;				
• Authorization for the institution to monitor and periodically review the third party for compliance with its agreement; and				
• Indemnification.				

	Yes	No	N/A	Comments
Contract Structuring and Review (cont.)				
5 Are clearly defined performance standards included to serve as a basis for measuring the performance of the third party?				
• Does management periodically review the performance measures to ensure consistency with its overall objectives?				
• Does the institution employ a compensation program that is consistent with consumer protection laws and sound banking practices?				
6. Does the contract outline the fees to be paid, including fixed compensation, variable charges, and any fees to be paid for nonrecurring items or special requests?				
• Does the contract address, if applicable, the cost and responsibility for purchasing and maintaining any equipment, hardware, software, or other item related to the activity?				
• Does the contract address obligations for retaining documentation for compensation arrangements, as appropriate?				
• Does the contract identify the party responsible for payment of any legal or audit expenses?				
7. Does the contract specify the type and frequency of management information reports to be received from the third party?				
• Does management consider mandating exception-based reports that would serve as notification of any changes or problems that could affect the nature of the relationship or pose a risk to the institution?				

	Yes	No	N/A	Comments
Contract Structuring and Review (cont.)				
8. Does the contract specify the institution's right to audit the third party (or engage an independent auditor) as needed to monitor performance under the contract?				
• Does management ensure that the third party's internal control environment as it relates to the service or product being provided to the institution is sufficiently audited or monitored?				
• Does the contract specify the scope of audits that will be performed?				
• Do audits capture all compliance-related risk?				
9. Does the contract prohibit the third party and its agents from using or disclosing the institution's information, except as necessary to perform the functions designated by the contract, or as otherwise permitted by law?				
• Are any breaches in the security and confidentiality of information fully and promptly disclosed to the institution?				
10. Does the contract specify whether the institution or the third party has the duty to respond to any complaints received by the third party from customers of the institution?				
• If the third party is responsible for such responses, is a copy of any complaint and the response forwarded to the institution?				
• Does the contract provide for periodic summary reports detailing the status and resolution of complaints along with any trend analysis on types of complaints?				
• Does the contract address record retention provisions for retaining relevant consumer complaint records?				
11. Does the contract address the third-party's responsibility for continuation of services provided for in the contractual arrangement in the event of an operational failure, including both man-made and natural disasters?				
• Are the results of testing of these plans provided to the institution?				

	Yes	No	N/A	Comments
Contract Structuring and Review (cont.)				
12. Does the contract specify what circumstances constitute default, identify remedies, and allow for a reasonable opportunity to cure a default?				
• Are termination rights identified in the contract, especially for material third-party arrangements and relationships involving rapidly changing technology or circumstances?				
13. Does the contract include a dispute resolution process for the purpose of resolving problems expeditiously?				
• Does the contract address the continuation of the arrangement between the parties during the dispute?				
14. Does the contract address ownership issues and the third-party's right to use the institution's property, including intellectual property such as the institution's name and logo, trademark, and other copyrighted material?				
• Does the contract address ownership and control of any records generated by the third party?				
15. Does the contract provide indemnification provisions that require the third party to hold the institution harmless from liability as a result of negligence by the third party, and vice versa?				
Board and Management Oversight				
1. Did the board initially approve the significant third-party relationship and what the Board considered in reaching that approval?				
• Does the board oversee and review at least annually significant third-party arrangements, and review these arrangements and written agreements whenever there is a material change to the program?				
2. Does management periodically review the third party's operations in order to verify that they are consistent with the terms of the written agreement and that risks are being controlled?				
3. Does management allocate sufficient qualified staff to monitor significant third-party relationships and provide the necessary oversight?				

	Yes	No	N/A	Comments
Board and Management Oversight (cont.)				
4. Does performance monitoring (i.e., third-party's quality of service, risk management practices, financial condition, and applicable controls and reports) include any of the following, as applicable?				
• Evaluate the overall effectiveness of the third-party relationship and the consistency of the relationship with the institution's strategic goals;				
• Review any licensing or registrations to ensure the third party can legally perform its services (e.g., non-deposit products);				
• Evaluate the third-party's financial condition at least annually, including its owners and principals. Financial review should be as comprehensive as the credit risk analysis performed on the institution's borrowing relationships. Audited financial statements should be required for significant third-party relationships;				
• Review the adequacy of the third party's insurance coverage;				
• Ensure that the third party's financial obligations to others are being met;				
• Review audit reports or other reports of the third party, and follow up on significant complaints and any needed corrective actions;				
• Review the adequacy and adherence to the third-party's policies relating to internal controls and security issues. This practice may also include performing on-site quality assurance reviews, targeting adherence to specified policies and procedures (e.g., visiting customer call centers to observe and verify sales, customer service, collection call procedures, and listening to verification recordings);				

	Yes	No	N/A	Comments
Board and Management Oversight (cont.)				
• Monitor for compliance with applicable consumer protection laws, rules, and regulations (e.g., reviewing/checking scripts, consumer disclosures, appropriate compensation, advertisements and other promotional materials, procedures for safeguarding customer information, etc.);				
• Review the third-party's business resumption contingency planning and testing;				
• Assess the effect and risks of any change in key third-party personnel involved in the relationship with the institution;				
• Review reports relating to the third-party's performance in the context of contractual requirements and performance standards, with appropriate follow-up as needed;				
• Determine the adequacy and reach of any training afforded to employees of the institution and the third party as it relates to applicable consumer protection laws and regulations, including fair lending laws and regulations;				
• Administer any testing programs for third parties with direct interaction with customers;				
• Review customer complaints about the products and services provided by the third party and the resolution of the complaints on a periodic basis; and				
• Meet as needed with representatives of the third party to discuss performance and operational issues.				

	Yes	No	N/A	Comments
Board and Management Oversight (cont.)				
5. Does management follow the institution's policies and procedures for terminating or probating third-party relationships, based on findings from audits and performance monitoring?				
6. Are the results of oversight activities for material third-party arrangements periodically reported to the institution's board of directors or designated committee?				
• Are identified weaknesses documented and promptly addressed?				
7. Does the institution maintain documents and records on all aspects of the third-party relationship, including valid contracts, business plans, risk analyses, due diligence, and oversight activities (including reports to the board or delegated committees and documents regarding any dispute resolution) and for what period of time?				
Summary Comment – Findings				