FEDERAL HOUSING FINANCE AGENCY

ADVISORY BULLETIN

AB 2018-08: OVERSIGHT OF THIRD-PARTY PROVIDER RELATIONSHIPS

Purpose

This advisory bulletin (AB) provides Federal Housing Finance Agency (FHFA) guidance to Fannie Mae and Freddie Mac, the Federal Home Loan Banks (FHLBanks), and the Office of Finance (OF) (collectively, the regulated entities[1]) on assessing and managing risks associated with third-party provider relationships. For the purposes of this AB, a third-party provider relationship is a business arrangement between a regulated entity and another entity that provides a product or a service.[2] When entering into third-party provider relationships, the regulated entities can be exposed to financial, operational, legal, compliance, and reputational risk. Effective risk management of third-party provider relationships is essential to the safe and sound operations of the regulated entities.

Guidance

FHFA expects each regulated entity to establish and maintain a third-party provider risk management program (program) that includes the following:

I. Governance
   - A. Responsibilities of the Board and Senior Management
   - B. Policies, Procedures, and Internal Standards
   - C. Reporting

II. Third-Party Provider Risk Management Life Cycle Phases
   - A. Risk Assessment
   - B. Due Diligence in Third-Party Provider Selection
   - C. Contract Negotiation
   - D. Ongoing Monitoring

[1] The OF is not a "regulated entity" as the term is defined by statute (*see* 12 U.S.C. 4502(20)). However, for convenience, references to the "regulated entities" in this AB should be read to also apply to the OF.
[2] This AB does not apply to business arrangements through which a FHLBank provides products or services to its members or housing associates, or to a FHLBank's business arrangements with sponsors participating in its Affordable Housing Program.

E. Termination

A regulated entity's program should enable oversight of third-party provider relationships in accordance with the level of risk presented, the nature of the relationship, the scale of the outsourced product or service, and the risk inherent in the relationship. Because of this risk-based approach, aspects of this AB may not apply to every third-party provider relationship. The regulated entities should ensure that the quality and extent of third-party provider risk management corresponds with the level of risk and the complexity of these relationships.

FHFA's general standards for safe and sound operations are set forth in the Prudential Management and Operations Standards (PMOS) at 12 CFR Part 1236 Appendix. Three relevant PMOS articulate guidelines for a regulated entity's board of directors and management to evaluate when establishing internal controls and information systems (Standard 1), overall risk management processes (Standard 8), and maintenance of adequate records (Standard 10). In addition, each regulated entity should manage its program as part of its enterprise-wide risk management program and in accordance with all relevant FHFA guidance.[3]

I. Governance

A. Responsibilities of the Board and Senior Management

The board of directors or board committee (board) should approve a policy establishing the program. The board-level policy (or management-level policies, as appropriate) should establish criteria for the acceptance and monitoring of risks related to third-party provider engagements and include enterprise-wide risk management processes that reflect the complexity of the regulated entity. Policies should assign clear roles and responsibilities to entity personnel, establish requirements for documenting decisions concerning third-party providers, and identify internal stakeholders throughout the third-party provider relationship. Internal audit, or an independent third party if specialized expertise is required, should audit the program periodically, including review of third-party assessments.

The regulated entity's board is responsible for oversight of the program, while senior management is responsible for executing the regulated entity's program and applicable policies on behalf of the board, consistent with established delegations. Each regulated entity's board should ensure that senior management has effective processes in place to manage risks related to third-party provider relationships, consistent with the regulated entity's strategic goals, organizational objectives, and risk appetite.

[3] 12 CFR 1239.11(a)

B. Policies, Procedures, and Internal Standards

The regulated entities should establish and implement risk management processes in their policies that clearly define risk categories for the oversight of third-party provider relationships. Risk categories should consider the type and degree of risk inherent in the relationship, the scope and breadth of the third-party provider relationship, the nature of the product or service provided, and the ability to find an acceptable replacement for the third-party provider. In addition to categorizing these relationships, the regulated entity should document and consistently update its inventory of third-party providers. The regulated entity's program should articulate governance standards for risk-based due diligence, monitoring, and oversight that reflect the defined risk categories. The more risk a third-party provider relationship poses to the regulated entity, the more rigorously the regulated entity should perform these activities. Documentation requirements should correspond to the risk category or the nature of the third-party provider relationship. Other factors considered in establishing a risk-based approach include third-party provider relationships that could:

- Cause a regulated entity to face significant business, operational, legal, compliance, or reputational risk if the third-party provider fails to meet its obligations;
- Require significant resources and costs to implement and manage the risk (such as a third-party provider that has an integral role in the regulated entity's operations or a financial technology firm that leverages emerging technologies); or
- Have a major effect on the regulated entity's operations if it needs to procure an alternate third-party provider or has to perform the service in house.

C. Reporting

The regulated entity should implement a reporting system that provides management sufficient information to adjust the program, including policy, resources, expertise, and controls. Management should receive periodic reports from program stakeholders about commencing new third-party provider relationships, continuing existing ones, or terminating arrangements that do not meet expectations or no longer align with the goals of the regulated entity. Regular reports to management could incorporate the documentation of phases of the third-party provider relationship, such as analysis of costs, or reputational risks found during ongoing monitoring. Reports should contain sufficient detail to adequately inform the intended audience and sufficiently support related business decisions.

To assist the board in oversight of the program, management should provide the board with regular enterprise-wide reports on the regulated entity's management of risks associated with third-party providers. Management should also notify the board of significant third-party risks, such as business interruptions and terminations for cause, or third-party provider relationships that approach the regulated entity's risk appetite limits.

II. Third-Party Provider Risk Management Life Cycle Phases

An effective program should include policies and procedures that cover all phases of the regulated entity's third-party provider relationship life cycle: Risk Assessment, Due Diligence in Third-Party Provider Selection, Contract Negotiation, Ongoing Monitoring, and Termination. The scope and duration of each phase should be consistent with the program's policy, and multiple phases may be addressed simultaneously. The documentation for each phase is also dependent on whether the phase applies and the extent to which it applies. The life cycle phases are discussed in more detail below.

A. Phase 1 – Risk Assessment

Each regulated entity's program should include processes to assess the risks associated with engaging a third-party provider to supply a product or service. These risks may include:

- The operational, compliance, legal, and reputational risks associated with having a third-party provider supply the product or service and the risk that expected benefits do not outweigh the costs;
- The breadth of the products or services that would be delivered by a third-party provider;
- Whether the regulated entity has adequate resources and expertise to monitor the third-party provider relationship;
- The complexity of the arrangement, volume of activity, potential for a third-party provider's use of subcontractors, and the technology required; and
- Potential information security risks associated with giving a third-party provider access to the regulated entity's operating location, information systems, or proprietary or personally identifiable information.

If the regulated entity establishes a third-party provider relationship, the program should provide for management of the associated risks. As necessary, the risk assessment should include a strategy for the regulated entity to procure adequate resources or expertise to mitigate the risks or justify acceptance of the identified risks. The regulated entity should review and update its risk assessment and revise risk mitigation strategies when appropriate. When documenting its risk assessment analysis, the regulated entity should indicate any risk assessment tools used in the process.

B. Phase 2 – Due Diligence in Third-Party Provider Selection

Each regulated entity should conduct due diligence on a third-party provider before entering into a contract. The degree of due diligence should be commensurate with the level of risk of the outsourced activity and the complexity of the third-party provider relationship. A regulated entity should not rely solely on its prior experience or knowledge of the third-party provider as a

substitute for an objective risk assessment of the third-party provider's ability to supply a product or service in a safe and sound manner. A regulated entity may refer to a third-party provider's independent audit, Service Organization Control (SOC) report, or recognized certifications to assess certain aspects of the third-party provider's internal risk management controls. Due diligence review should align with the severity of the risk. Due diligence results, findings, and recommendations should be documented.

Due diligence prior to entering into a third-party provider relationship should include an evaluation of financial, operational, legal, compliance, and reputational risks of engaging the proposed third-party provider. As part of the due diligence review, the regulated entity should consider:

- Whether the proposed third-party provider can offer the product or service in compliance with applicable laws and regulations, as well as the regulated entity's internal policies, procedures, and other requirements;
- The third-party provider's overall business model and how current and proposed business activities may affect the risks presented by the third-party provider;
- The third-party provider's business background, experience, and reputation;
- The financial performance, resources, and condition of the proposed third-party provider;
- The third-party provider's insurance coverage;
- The third-party provider's operational and internal controls, including information security, incident reporting and management, and business continuity programs;
- Concentration risks that may arise from relying on a third-party provider for multiple products or services or from a third-party provider's reliance on subcontractors;
- The extent to which the third-party provider relies on subcontractors to perform its obligations, the controls the subcontractor has in place, and the third-party provider's processes to oversee subcontractors that would be directly involved in the outsourced product or service;
- Any potential conflicts of interest with the directors, officers, or employees of the regulated entity concerning potential third-party providers;[4] and
- Whether there are third-party fee structures that involve potential risks, such as incentives for inappropriate risk-taking, that could arise as a result of such fee structures.

Each regulated entity's third-party provider selection process should also be designed to ensure, to the extent possible and consistent with safety and soundness, the inclusion of minority-, women-, and disabled-owned businesses.[5]

[4] 12 CFR 1239.10(a).
[5] 12 CFR 1223.2, 1223.21.

Management should review the due diligence results to determine whether the third-party provider is able to adequately provide the product or service at a level of risk acceptable to the regulated entity. If the third-party provider cannot meet the regulated entity's requirements, management should consider whether to seek an alternate provider, supply the product or service itself, or mitigate the identified risks to the extent practicable.

C. Phase 3 – Contract Negotiation

Each contract with a third-party provider should clearly specify the rights and responsibilities of each party. Consistent with the risk category involved, the regulated entity should consider what level of legal review is necessary for contracts with third-party providers and should ensure that the attorneys conducting the review for a particular contract have the appropriate subject matter expertise or work in conjunction with appropriate subject matter experts. Copies of executed contracts should be retained for reference and record-keeping purposes.

The regulated entity should consider the following when negotiating contractual provisions with third-party providers:

- The nature and scope of service;
- Duration of service;
- Performance standards and service levels;
- Experience requirements of third-party providers and their contractors;
- Cost and compensation, including the timing and procedures for payment and expense reimbursement;
- Confidentiality, use, location, and security of information;
- Business continuity and contingency plans and test results;
- Intellectual property ownership, rights, and responsibilities;
- Timely disclosure of conflicts of interest or potential conflicts of interest from the third-party provider;
- Incident reporting and management;
- Dispute resolution process (*e.g.* arbitration, mediation), termination, and remedies; and
- Internal controls and audit reports.

The regulated entity should address what constitutes nonperformance and the conditions under which the contract may be terminated by either party. The contract should also stipulate the circumstances for and responsibilities when termination occurs. If the regulated entity could no longer legally engage a third-party provider,[6] the contract should include a provision that enables the regulated entity to terminate the contract for regulatory noncompliance.

[6] *See, e.g.*, 12 CFR Part 1227.

The regulated entity should also ensure that contracts address compliance with the specific laws, regulations, and guidance applicable to the regulated entity, including the regulated entity's right to obtain necessary information to conduct ongoing risk assessments, as well as monitor performance and ensure contract compliance. Contracts should also address whether the regulated entity has the right to conduct periodic on-site reviews to verify compliance. If contracts allow for subcontracting, the regulated entity generally should seek to ensure that the primary third-party provider remains responsible for the performance of its subcontractors in accordance with the terms of the primary contract, and be notified of the identity of any material subcontractors, when appropriate.

Contracts for third-party providers should address, as appropriate, the provider's responsibility for continuation of the product or service in the event of an operational failure, such as man-made and natural disasters. Contracts should address requirements for third-party providers to back up information and maintain disaster recovery and contingency plans with sufficiently detailed operating procedures.

Other issues such as the maintenance of adequate insurance, ownership of data or licenses, privacy, and liability limitations should be considered, as applicable. For example, the regulated entity should consider potential legal and security risks to cross-border data storage, transmission, and processing.

D. Phase 4 – Ongoing Monitoring

The nature and extent of monitoring of the performance of third-party provider relationships should be commensurate with the level of risk. Management should also ensure that the regulated entity retains sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the third-party provider relationship. The approach (*e.g.*, on-site versus off-site review), depth, scope, and frequency of the monitoring and oversight activities should correspond to the risk category involved. If the regulated entity outsources any part of its monitoring and oversight, management is responsible for choosing a service provider appropriate for the entity's size, complexity, and risk environment.

Ongoing monitoring should include the due diligence activities referenced in Phase 2 that apply to the particular third-party provider relationship. Management of the regulated entity should also consider whether the third-party provider is:

- Meeting service-level agreements, performance metrics, and other contractual terms;
- Monitoring and evaluating subcontractor controls that are relevant to the contract work being performed;
- Engaged in agreements with other entities that may pose a conflict of interest or present risks;

- Performing periodic background checks; and
- Complying with applicable legal and regulatory requirements, including documenting such compliance when necessary.

Because both the level and types of risks may change over the lifetime of a third-party provider relationship, a regulated entity should ensure that its ongoing monitoring adapts accordingly. Periodic assessments should be conducted to determine whether the product or service remains necessary or relevant to the regulated entity's mission or operations. Each regulated entity should also periodically assess existing third-party provider relationships to determine whether the nature of the product or service provided has changed, resulting in the need for re-designation to a new risk category. Management should review existing third-party provider contracts to determine whether the terms and conditions address current risks associated with having the product or service supplied by the third-party provider. Where concerns are identified, the regulated entity should consider addressing those concerns by negotiating an amendment to the contract where appropriate, or revising the contract prior to a renewal.

When a regulated entity identifies concerns through ongoing monitoring, it should seek to resolve the issues at the earliest opportunity. Management should ensure procedures exist to escalate issues such as service agreement performance, material weaknesses and repeat audit findings, deterioration in financial condition, security breaches, data loss, or compliance lapses. Additionally, management should ensure that the regulated entity's controls for managing these risks from third-party provider relationships are tested regularly. Weaknesses identified that substantively increase the risk to the regulated entity should be reported to the board based on an assessment of the level of associated risk.

Any assessments and analyses performed during this phase should be documented, as well as any regular risk management and performance reports received from the third-party provider (*e.g.*, audit reports, security reviews, and reports about compliance with service-level agreements).

E. Phase 5 – Termination

The terms of each contract will govern how a regulated entity or a third-party provider may terminate the contractual relationship. A regulated entity may wish to terminate a third-party provider relationship for various reasons, including:

- Expiration, completion, or satisfaction of the contract;
- Breach of contract;
- To engage an alternate third-party provider;
- To discontinue the product or service;
- To bring the product or service in house; or

- To comply with an FHFA order directing suspension of the third-party provider relationship.

Each regulated entity should have strategies and contingency plans in place to terminate third-party provider relationships in an efficient manner that minimizes risk to the regulated entity, whether the outsourced product or service is transitioned to another third-party provider, brought in house, or discontinued. The regulated entity should consider:

- The capabilities, resources, and time frames required to transition the product or service while still managing legal, regulatory, and other risks;
- Risks associated with data retention and destruction, information system connections and access control issues, or other control concerns that require additional risk management and monitoring during and after the end of the third-party provider relationship;
- Intellectual property ownership, rights, and responsibilities, as well as the handling of any joint intellectual property developed during the course of the arrangement;
- The return of any regulated entity's information in the third-party provider's possession after voluntary or involuntary termination of the contract;
- Reputational risks to the regulated entity if the termination results from the third-party provider's inability to meet expectations; and
- Roles and assistance with transfer or wind down of the outsourced product or service upon termination.

Related Guidance

12 CFR Part 1236 Prudential Management and Operations Standards, Appendix.

Cloud Computing Risk Management, Federal Housing Finance Agency Advisory Bulletin 2018-04, August 14, 2018.

Oversight of Multifamily Seller/Servicer Relationships, Federal Housing Finance Agency Advisory Bulletin 2018-05, August 14, 2018.

Information Security Management, Federal Housing Finance Agency Advisory Bulletin 2017-02, September 28, 2017.

Internal Audit Governance and Function, Federal Housing Finance Agency Advisory Bulletin 2016-05, October 7, 2016.

Data Management and Usage, Federal Housing Finance Agency Advisory Bulletin 2016-04, September 29, 2016.

Information Technology Investment Management, Federal Housing Finance Agency Advisory Bulletin 2015-06, September 21, 2015.

Oversight of Single-Family Seller/Servicer Relationships, Federal Housing Finance Agency Advisory Bulletin, 2014-07, December 1, 2014.

Operational Risk Management, Federal Housing Finance Agency Advisory Bulletin, 2014-02, February 18, 2014.

Model Risk Management, Federal Housing Finance Agency Advisory Bulletin 2013-07, November 20, 2013.

Contingency Planning for High-Risk or High-Volume Counterparties, Federal Housing Finance Agency Advisory Bulletin 2013-01, April 1, 2013.

FHFA has statutory responsibility to ensure the safe and sound operations of the regulated entities and the Office of Finance. Advisory bulletins describe FHFA supervisory expectations for safe and sound operations in particular areas and are used in FHFA examinations of the regulated entities and the Office of Finance. Questions about this advisory bulletin should be directed to: SupervisionPolicy@fhfa.gov.