SOUTH DAKOTA
Division of Banking

1714 Lincoln Avenue, Suite 2
Pierre, SD 57501
Phone (605) 773-3421
Fax (866) 326-7504

Service Provider Due Diligence Review Guidance

All financial institutions should develop risk management processes that are commensurate with the level of risk and complexity of its third-party relationships and the institution's organizational structures. Therefore, management must document comprehensive oversight and management of third-party relationships that involve critical activities (e.g. those that could cause the institution to face significant risk if the third party fails to meet expectation, or those that could have a major impact on operations if the institution has to find an alternate third party, or if the outsourced activity has to be brought in-house. Prior to engaging a service provider, management is expected to fully investigate and document the appropriateness of selecting a particular provider over other qualified providers or performing the function in-house. Management is also expected to demonstrate through comprehensive documentation the continuous monitoring of service provider activities, the quality of services provided to customers, and any associated business or legal risk.

Initial Due Diligence Review Process

Prior to designating an outside service provider, the financial institution should document its efforts to exercise reasonable caution during the selection process, and the board and/or a designated committee should review and document approval to engage the service provider. Compatibility and performance should be considered in conjunction with the cost of the services to be provided. The scope of the review depends on the type and significance of outsourcing activity. The following criteria are some of the most common considerations; however, the listing does not supersede provisions of law or regulation, nor should it be considered exhaustive:

- Document a review of any potential conflicts of interest arising from the engagement of the service provider. The review should identify the board's analysis and assessment of the parties involved, nature of the relationships, and risks of self-dealing arising out of the conflicts of interest. It is important to note that affiliated service providers warrant heightened attention to mitigate any potential conflict of interest and self-dealing risks.
- Document an assessment of the service provider's ability to handle the volume and nature of accounts and assets to be serviced. Obtaining a list of servicer references and contact names is a customary practice.
- Document an evaluation of the service provider's legal and regulatory compliance program to determine whether it has the necessary licenses to operate and the expertise, processes, and controls to enable the financial institution to remain compliant with domestic and international laws and regulations. Check compliance status with regulators and self-regulatory organizations, if applicable.
- Document consideration of the financial strength and viability of the service provider. Financial strength provided by a parent holding company or similar organization may also be considered. This entails a review of financial statements and audit reports, and a search of pending or threatened financial or legal claims.
- If investment management is being outsourced, document a review of the service provider's investment performance (over a minimum of five to ten years, or several investment cycles). In addition, review SEC and FINRA online search tools for pertinent information with respect to investment adviser and broker-dealer service providers.

- Request and review service provider audit reports or supervisory evaluations, if available. Depending on the outsourced function, obtain AICPA Statement on Standards for Attestation Engagements Reports if conducted, or other available reports.
- Document a review of certain service provider policies, procedures, and controls. Knowledge of a service provider's business strategies, privacy policies, service philosophies, and quality control initiatives may be beneficial in choosing a service provider with standards corresponding to the financial institution's standards.
- Request and review evidence supporting the maintenance of insurance coverage by the service provider. If insurance requirements are provided in the service agreement, management should ensure these requirements are met.
- Document a review of the service provider's business continuity/disaster recovery planning and testing. A more rigorous review is warranted if management intends to rely on the service provider's planning and testing to support the financial institution's own business continuity planning.
- Document an assessment of the service provider's information security program and any business processes and technology that will be used to support the activity. When technology is necessary to support service performance and/or delivery, assess the infrastructure and application security programs, including the software development life cycle and results of vulnerability and penetration tests.
- Document a review of the service provider's incident monitoring, reporting, and escalation programs to ensure there are clearly documented processes and accountability for identifying, reporting, investigating, and managing incidents. Ensure that escalation and notification processes meet the institution's expectations and regulatory requirements.

<u>Ongoing Due Diligence Review Process</u>

In addition to performing initial service provider due diligence reviews, management has a responsibility to monitor and update the above-referenced documentation on the condition and activities of the service provider, while ensuring that the provisions of the agreement are being met. Management should at least annually update the due diligence criteria collected with respect to each service provider, documenting the review within the meeting minutes of the board and/or a designated committee. In addition to updating the above review criteria, the institution's ongoing monitoring program should incorporate the following considerations (again, this list should not be considered exhaustive):

- Adherence to the service agreement, ensuring all services, rights, and responsibilities negotiated in the agreement have been performed in a manner satisfactory to the institution.
- Desired updates to the service provider relationship, including additional services and changes to the compensation/fee structure.
- Contingency plans developed for the potential of deteriorating performance or other problems encountered with the service provider.

<u>Due Diligence Review Documentation</u>

A comprehensive service provider review program is intended to document an analysis of how the various review criteria affected management's decision to initially engage or to continue the relationship. Therefore, service provider reviews should be well documented and retained for future review by auditors and regulatory authorities. It may be useful to develop and implement a uniform format to document the various service provider reviews. Documentation should identify the criteria reviewed, the reviewer(s), and the date of review. Tthe review should be performed by individuals that are independent of the service provider. Written policies and procedures should provide adequate guidance to ensure the reviews are completed timely, properly reported, and adequately documented.