Appendix A: Examination Procedures

EXAMINATION OBJECTIVE: Assess the effectiveness of the institution's risk management process as it relates to the outsourcing of information systems and technology services.

- Tier I objectives and procedures relate to the institution's implementation of a process for identifying and managing outsourcing risks.
- Tier II objectives and procedures provide additional validation and testing techniques as warranted by risk to verify the effectiveness of the institution's process on individual contracts.

Tier I and Tier II are intended to be a tool set examiners will use when selecting examination procedures for their particular examination. Examiners should use these procedures as necessary to support examination objectives.

TIER I OBJECTIVES AND PROCEDURES

Objective 1: Determine the appropriate scope for the examination.

1. Review past reports for weaknesses involving outsourcing. Consider:

- Regulatory reports of examination of the institution and service provider(s); and
- Internal and external audit reports of the institution and service provider(s) (if available).

2. Assess management's response to issues raised since the last examination. Consider:

- Resolution of root causes rather than just specific issues; and
- Existence of any outstanding issues.

3. Interview management and review institution information to identify:

- Current outsourcing relationships, including cloud computing relationships, and changes to those relationships since the last examination. Also identify any:
  - Material service provider subcontractors,
  - Affiliated service providers,
  - Foreign-based third party providers;
- Current transaction volume in each function outsourced;
- Any material problems experienced with the service provided;
- Service providers with significant financial or control related weaknesses; and
- When applicable, whether the primary regulator has been notified of the outsourcing relationship as required by the Bank Service Company Act or Home Owners' Loan Act.

Objective 2: Evaluate the quantity of risk present from the institution's outsourcing arrangements.

1. Assess the level of risk present in outsourcing arrangements. Consider risks pertaining to:

- Functions outsourced;
- Service providers, including, where appropriate, unique risks inherent in foreign-based service provider arrangements; and
- Technology used.

2. If the institution engages in cloud computing, determine whether:

- The cloud computing service is or will be hosted internally or outsourced to a third party provider (hosted externally).

- Resources are shared within a single organization or across various clients of the service provider. (Resources can be shared at the network, host, or application level).
- The institution has the ability to increase or decrease resources on demand without involving the service provider (on-demand self-service).
- Massive scalability in terms of bandwidth or storage is available to the institution.
- The institution can rapidly deploy or release resources.
- The financial institution pays only for those resources which are actually used (pay-as-you go pricing)

3. If the institution engages in cloud computing, identify the type(s) of service model that is or will be used:

- Software as a Service (SaaS) - application software is hosted in the cloud; commonly used for email applications such as Hotmail or Gmail, time reporting systems, customer relationship management (CRM) systems such as SalesForce, etc.;
- Platform as a Service (PaaS) - development platform such as Java, .Net, etc. for developing systems is hosted in the cloud;
- Infrastructure as a Service (IaaS) - infrastructure resources such as data processing, data storage, network systems, etc. are provided via the cloud; or
- Data as a Service (DaaS) - data is provided or accessed via the cloud such as access to LexisNexis data, Google data, and Amazon data

4. If the institution engages in cloud computing, identify the type of deployment model to be used:

- Private Cloud - hosted for or by a single entity on a private network; can be hosted internally or outsourced but is most often operated internally; only those within the entity share the resources;
- Community Cloud - hosted for a limited number of entities with a common purpose; access is generally restricted; most often used in a regulated environment where entities have common requirements;
- Hybrid Cloud - data or applications are portable and permit private and public clouds to connect; or,
- Public Cloud - available to the general public; owned and operated by a third party service provider

Objective 3: Evaluate the quality of risk management

1. Evaluate the outsourcing process for appropriateness given the size and complexity of the institution. The following elements are particularly important:

- Institution's evaluation of service providers consistent with scope and criticality of outsourced services; and
- Requirements for ongoing monitoring.

2. Evaluate the requirements definition process.

- Ascertain that all stakeholders are involved; the requirements are developed to allow for subsequent use in request for proposals (RFPs), contracts, and monitoring; and actions are required to be documented; and
- Ascertain that the requirements definition is sufficiently complete to support the future

control efforts of service provider selection, contract preparation, and monitoring.

3. Evaluate the service provider selection process.

- Determine that the RFP adequately encapsulates the institution's requirements and that elements included in the requirements definition are complete and sufficiently detailed to support subsequent RFP development, contract formulation, and monitoring;
- Determine that any differences between the RFP and the submission of the selected service provider are appropriately evaluated, and that the institution takes appropriate actions to mitigate risks arising from requirements not being met; and
- Determine whether due diligence requirements encompass all material aspects of the service provider relationship, such as the provider's financial condition, reputation (e.g., reference checks), controls, key personnel, disaster recovery plans and tests, insurance, communications capabilities and use of subcontractors.

4. Evaluate the process for entering into a contract with a service provider. Consider whether:

- The contract contains adequate and measurable service level agreements;
- Allowed pricing methods do not adversely affect the institution's safety and soundness, including the reasonableness of future price changes;
- The rights and responsibilities of both parties are sufficiently detailed;
- Required contract clauses address significant issues, such as financial and control reporting, right to audit, ownership of data and programs, confidentiality, subcontractors, continuity of service, etc;
- Legal counsel reviewed the contract and legal issues were satisfactorily resolved; and
- Contract inducement concerns are adequately addressed.

5. If the institution engages in cloud processing, determine that inherent risks have been comprehensively evaluated, control mechanisms have been clearly identified, and that residual risks are at acceptable levels. Ensure that

- Action plans are developed and implemented in instances where residual risk requires further mitigation.
- Management updates the risk assessment as necessary.
- The types of data in the cloud have been identified (social security numbers, account numbers, IP addresses, etc.) and have established appropriate data classifications based on the financial institution's policies.
- The controls are commensurate with the sensitivity and criticality of the data.
- The effectiveness of the controls are tested and verified.
- Adequate controls exist over the hypervisor if a virtual machine environment supports the cloud services.
- All network traffic is encrypted in the cloud provider's internal network and during transition from the cloud to the institution's network.
- All data stored on the service providers systems are being encrypted with unique keys that only authenticated users from this institution can access.
- Unless the institution is using private cloud model, determine what controls the institution or service provider established to mitigate the risks of multitenancy.
- If a financial institution is using the Software as a Service (SaaS) model, determine whether regular backup copies of the data are being made in a format that can be read by the financial institution. (Backup copies made by the service provider may not be

readable.)

- Ensure that the financial institution's business continuity plan addresses contingencies for the cloud computing service. Determine whether the financial institution has an exit strategy and de-conversion plan or strategy for the cloud services.
- Determine whether the cloud service provider has an internal IT audit staff with adequate knowledge and experience or an adequate contractual arrangement with a qualified third-party audit firm.

6. Evaluate the institution's process for monitoring the risk presented by the service provider relationship. Ascertain that monitoring addresses:

- Key service level agreements and contract provisions;
- Financial condition of the service provider;
- General control environment of the service provider through the receipt and review of appropriate audit and regulatory reports;
- Service provider's disaster recovery program and testing;
- Information security;
- Insurance coverage;
- Subcontractor relationships including any changes or control concerns;
- Foreign third party relationships; and
- Potential changes due to the external environment (i.e., competition and industry trends).

7. Determine whether the following policies and processes have been revised in light of the need for increased controls brought about by the implementation of cloud computing:

- The Information Security Risk Assessment;
- The Technology Outsourcing (Vendor Management) Policy;8. Review the policies regarding periodic ranking of service providers by risk for decisions regarding the intensity of monitoring (i.e., risk assessment). Decision process should:
- The Information Security Policy;
- The Security Incident or Customer Notification Policy;
- The Business Continuity Plan

8. Review the policies regarding periodic ranking of service providers by risk for decisions regarding the intensity of monitoring (i.e., risk assessment). Decision process should:

- Include objective criteria;
- Support consistent application;
- Consider the degree of service provider support for the institution's strategic and critical business needs, and
- Specify subsequent actions when rankings change.

9. Evaluate the financial institution's use of user groups and other mechanisms to monitor and influence the service provider.

Objective 4: Discuss corrective action and communicate findings

1. Determine the need to complete Tier II procedures for additional validation to support conclusions related to any of the Tier I objectives.

2. Review preliminary conclusions with the EIC regarding:

- Violations of law, rulings, regulations;
- Significant issues warranting inclusion in the Report as matters requiring attention or recommendations; and
- Potential impact of your conclusions on the institution's risk profile and composite or component IT ratings.

3. Discuss findings with management and obtain proposed corrective action for significant deficiencies.

4. Document conclusions in a memo to the EIC that provides report ready comments for the Report of Examination and guidance to future examiners.

5. Organize work papers to ensure clear support for significant findings by examination objective.

TIER II OBJECTIVES AND PROCEDURES

A. IT REQUIREMENTS DEFINITION

1. Review documentation supporting the requirements definition process to ascertain that it appropriately addresses:

- Scope and nature;
- Standards for controls;
- Minimum acceptable service provider characteristics;
- Monitoring and reporting;
- Transition requirements;
- Contract duration, termination, and assignment' and
- Contractual protections against liability.

B. DUE DILIGENCE

1. Assess the extent to which the institution reviews the financial stability of the service provider:

- Analyzes the service provider's audited financial statements and annual reports;
- Assesses the provider's length of operation and market share;
- Considers the size of the institution's contract in relation to the size of the company;
- Reviews the service provider's level of technological expenditures to ensure on-going support; and
- Assesses the impact of economic, political, or environmental risk on the service provider's financial stability.

2. Evaluate whether the institution's due diligence considers the following:

- References from current users or user groups about a particular vendor's reputation and performance;
- The service provider's experience and ability in the industry;
- The service provider's experience and ability in dealing with situations similar to the institution's environment and operations;

- The quality and effectiveness of any cost/benefit analyses. Determine whether the analysis considered the incremental costs of the additional monitoring, operations responsibilities, and protections that may be required of the financial institution.
- The cost for additional system and data conversions or interfaces presented by the various vendors;
- Shortcomings in the service provider's expertise that the institution would need to supplement in order to fully mitigate risks;
- The service provider's proposed use of third parties, subcontractors, or partners to support the outsourced activities;
- The service provider's ability to respond to service disruptions;
- Key service provider personnel that would be assigned to support the institution;
- The service provider's ability to comply with appropriate federal and state laws. In particular, ensure management has assessed the providers' ability to comply with federal laws (including GLBA and the USA PATRIOT Act); and
- Country, state, or locale risk.

C. SERVICE CONTRACT

1. Verify that legal counsel reviewed the contract prior to closing.

- Ensure that the legal counsel is qualified to review the contract particularly if it is based on the laws of a foreign country or other state; and
- Ensure that the legal review includes an assessment of the enforceability of local contract provisions and laws in foreign or out-of-state jurisdictions.

2. Verify that the contract appropriately addresses:

- Scope of services;
- Performance standards;
- Pricing;
- Controls;
- Financial and control reporting;
- Right to audit;
- Ownership of data and programs;
- Confidentiality and security;
- Regulatory compliance;
- Indemnification;
- Limitation of liability;
- Dispute resolution;
- Contract duration;
- Restrictions on, or prior approval for, subcontractors;
- Termination and assignment, including timely return of data in a machine-readable format;
- Insurance coverage;
- Prevailing jurisdiction (where applicable);
- Choice of Law (foreign outsourcing arrangements);

- Regulatory access to data and information necessary for supervision; and
- Business Continuity Planning.

3. Review service level agreements to ensure they are adequate and measurable. Consider whether:

- Significant elements of the service are identified and based on the institution's requirements;
- Objective measurements for each significant element are defined;
- Reporting of measurements is required;
- Measurements specify what constitutes inadequate performance; and
- Inadequate performance is met with appropriate sanctions, such as reduction in contract fees or contract termination.

4. Review the institution's process for verifying billing accuracy and monitoring any contract savings through bundling.

D. MONITORING SERVICE PROVIDER RELATIONSHIP(S)

1. Evaluate the institution's periodic monitoring of the service provider relationship(s), including:

- Timeliness of review, given the risk from the relationship;
- Changes in the risk due to the function outsourced;
- Changing circumstances at the service provider, including financial and control environment changes;
- Conformance with the contract, including the service level agreement; and
- Audit reports and other required reporting addressing business continuity, security, and other facets of the outsourcing relationship.

2. Review risk rankings of service providers to ascertain:

- Objectivity;
- Consistency; and
- Compliance with policy.

3. Review actions taken by management when rankings change, to ensure policy conformance when rankings reflect increased risk.

4. Review any material subcontractor relationships identified by the service provider or in the outsourcing contracts. Ensure:

- Management has reviewed the control environment of all relevant subcontractors for compliance with the institution's requirements definitions and security guidelines; and
- The institution monitors and documents relevant service provider subcontracting relationships including any changes in the relationships or control concerns.

Platform as a Service (PaaS) - development platform such as Java, .Net, etc. for developing systems is hosted in the cloud;

- Infrastructure as a Service (IaaS) - infrastructure resources such as data processing, data storage, network systems, etc. are provided via the cloud; or,
- Data as a Service (DaaS) - data is provided or accessed via the cloud such as access to

LexisNexis data, Google data, and Amazon data.