OUTLINE FOR REVIEW

Outsourcing

Technology Services

INFOSIGHT

www.InfoSightInc.com

FOR FINANCIAL INSTITUTIONS

Review of Outsourcing Technology Services

I. **Risk Assessment and Requirements**
   a. Quantity of risk considerations
   b. Requirements definition

II. **Service Provider Selection**
   a. Request for proposal
   b. Due diligence

III. **Contract Issues**
   a. Service level agreements
   b. Pricing methods
   c. Bundling
   d. Contract inducement concerns

IV. **Ongoing Monitoring**
   a. Key service level agreements and contract provisions
   b. Financial condition of service providers
   c. General control environment of the service provider
   d. Potential changes due to the external environment

V. **Cloud Computing Relationships**
   a. General considerations
   b. Service model used
   c. Deployment model used
   d. Revision of policies and processes
   e. Due diligence
   f. Vendor management
   g. Audit
   h. Information security
   i. Legal, regulatory, and reputation considerations
   j. Business continuity planning

Tier 1

Risk Assessment and Requirements

Evaluate the quantity of risk present from the institution's 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

Evaluate the requirements definition process –

- Ascertain that all stakeholders are involved; the requirements are developed to allow for subsequent use in RFPs, contracts, and monitoring, and actions are required to be documented;
- Ascertain that the requirements definition is sufficiently complete to support the future control efforts of service provider selection, contract preparation, and monitoring

Service Provider Selection

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 risk arising from requirements not being met; and

- Determine whether due diligence requirements encompass all material aspects of the service provider relationship such as the following:
    a) Financial condition;
    b) Reputation (reference checks);
    c) Controls;
    d) Key personnel;
    e) Disaster recovery plans and tests;
    f) Insurance;
    g) Communications capabilities; and
    h) Use of subcontractors

Contract Issues

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:
    a) Financial and control reporting;
    b) Right to audit;
    c) Ownership of data and programs;
    d) Confidentiality;
    e) Subcontractors;
    f) Continuity of service
- The contract was reviewed by Legal
- Contract inducement concerns are adequately addressed

Ongoing Monitoring

Evaluate the 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 (competition and industry trends)

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
- Specify subsequent actions when rankings change

Evaluate the use of user groups and other mechanisms to monitor and influence the service provider.

Cloud Computing Relationships

If engaged 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)

Identify the type(s) of service model that is or will be used: (layers in a cloud)

- Software as Services (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), system 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

Identify the type of deployment model that is or will 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 operating 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

If the institution engages in cloud processing, determine that the 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; (schedules the amount of access that guest OSes have, used to split physical computer resources)

- Native hypervisor – sits directly on the hardware platform, better performance for individual users
- Embedded hypervisors – integrated into a processor on a separate chip. Used by service providers to gain performance improvements
- Hosted hypervisors – runs as distinct software layer above both the hardware and the OS. Useful in both private and public clouds to gain performance improvements.

- 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 the institution can access;
- Unless the institution is using a private cloud model, determine what controls the institution or service provider established to mitigate the risks of **multi-tenancy** (multiple tenants (applications) either inside or outside the enterprise that needs its own secure and exclusive virtual computing environment. This environment can encompass all or some select layers of enterprise architecture, from storage to user interface. Degrees of multi-tenancy. The degrees of multi-tenancy are based on how much of the core application , SaaS layer is designed to be shared across tenants and include the following:

- Highest degree: the database schema is shared and supports customization of the business logic, workflow and user-interface layers
- Middle degree: clusters of homogenous tenants that share database schemae and other application layers. Each cluster of users has its own version of database schema and the application itself
- Lowest degree: limited to IaaS and PaaS layers, with dedicated SaaS layers for each tenant – safest

- 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.

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
- The Information Security Policy
- The Security Incident or Customer Notification Policy
- The Business Continuity Plan