

# BITS

FINANCIAL SERVICES  
R O U N D T A B L E

## **BITS FRAMEWORK FOR MANAGING TECHNOLOGY RISK FOR SERVICE PROVIDER RELATIONSHIPS**

**NOVEMBER 2003**

**REVISED IN PART  
MAY 2009**

BITS  
1001 Pennsylvania Avenue NW, Suite 500 South  
Washington, DC 20004  
(202) 289-4322 [WWW.BITS.ORG](http://WWW.BITS.ORG)

---

## TABLE OF CONTENTS

INTRODUCTION .....	2
<b>BITS VENDOR MANAGEMENT WORKING GROUP</b>	
<b>PARTICIPATING INSTITUTIONS AND ASSOCIATIONS.....</b>	<b>3</b>
<b>ABOUT BITS .....</b>	<b>4</b>
<b>SECTION 1: FRAMEWORK APPLICATION AND FLOW DIAGRAM.....</b>	<b>5</b>
<b>SECTION 2: BUSINESS DECISION TO OUTSOURCE IT SERVICES.....</b>	<b>9</b>
<b>SECTION 3: CONSIDERATIONS FOR THE REQUEST FOR PROPOSAL.....</b>	<b>14</b>
<b>SECTION 4: DUE DILIGENCE CONSIDERATIONS .....</b>	<b>19</b>
<b>SECTION 5: CONTRACTUAL, SERVICE-LEVEL, AND INSURANCE CONSIDERATIONS.....</b>	<b>30</b>
<b>SECTION 6: PROCEDURES FOR SUPPORTING SPECIFIC CONTROLS,     REQUIREMENTS, AND RESPONSIBILITIES .....</b>	<b>52</b>
<b>SECTION 7: IMPLEMENTATION AND CONVERSION PLAN .....</b>	<b>56</b>
<b>SECTION 8: RELATIONSHIP MANAGEMENT AND     CHANGES IN THE OUTSOURCED ENVIRONMENT.....</b>	<b>60</b>
<b>SECTION 9: CONSIDERATIONS FOR CROSS-BORDER OUTSOURCING.....</b>	<b>69</b>
<b>APPENDIX 1: MODEL SPREADSHEET FOR COST ANALYSIS.....</b>	<b>85</b>
<b>APPENDIX 2: FRAMEWORK MAP TO FEDERAL BANKING AGENCY GUIDELINES .....</b>	<b>87</b>
<b>APPENDIX 3: FRAMEWORK MAP TO BASEL COMMITTEE ON     BANKING SUPERVISION.....</b>	<b>95</b>
<b>APPENDIX 4: GLOSSARY OF TERMS.....</b>	<b>99</b>
<b>APPENDIX 5: DISASTER RECOVERY/BUSINESS CONTINUITY MATRIX.....</b>	<b>109</b>
<b>APPENDIX 6: SHARED ASSESSMENTS .....</b>	<b>124</b>
<b>APPENDIX 7: NON-U.S. NATIONALS WORKING IN THE U.S. –     SUMMARY OF VISA REQUIREMENTS .....</b>	<b>126</b>

## INTRODUCTION

The financial services industry increasingly relies on service providers to support the delivery of financial services. This shift in the delivery of financial services, coupled with the deployment of new and dynamic technologies, has resulted in heightened industry awareness and concern, accompanied by increased regulatory scrutiny of financial institution risk assessment and management of outsourced services.

In response, the BITS IT Service Providers Working Group developed the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships (Framework)* in 2001. While the original *Framework* provides an industry approach to outsourcing, additional regulatory and industry pressures and issues have since emerged. To address these changes, the Working Group updated the *Framework* in 2003 with further considerations for disaster recovery, security audits and assessments, vendor management, and cross-border considerations.

In 2008, the BITS Vendor Management Working Group, successor to the IT Service Providers Working Group, began a thorough refresh of the *Framework* to reflect the significant change in law and regulation and the maturation of practices since 2003. In addition, the broader scope of outsourcing today leads the group to expand the *Framework* beyond only IT service provider relationships.

Consistent with current regulatory guidance, the *Framework* recommendations should be applied selectively based on a financial services company's risk-assessment results. In this way, the *Framework* should be used as a reference, stimulating firms to ask the right questions and complementing individual institutions' risk-management policies.

**The *Framework* is not an official government publication, nor does BITS suggest strict adherence to the *Framework*.** BITS offers this *Framework* in the full spirit of the Federal Financial Institutions Examination Council (FFIEC) Guidance on Technology Outsourcing, which is characterized by the FFIEC as, rather than prescriptive, being intended for consideration in conjunction with an organization's overall risk-management program. To review the specific ways in which the *Framework* responds to Office of the Comptroller of the Currency, Federal Reserve Board, and other key regulatory requirements, consult the matrix in Appendix 2, which compares *Framework* language with the regulatory environment.

Broad implementation of the *Framework* will help create a common understanding of the financial services industry's needs among Service Providers and help to address known control weaknesses in outsourced services, resulting in more consistent and appropriate levels of management by financial services companies that outsource services. For additional information about the *BITS Framework for Managing Technology Risk for Service Provider Relationships*, please contact:

John Ingold, BITS, 202-589-2438, [johni@fsround.org](mailto:johni@fsround.org)

The original *Framework* was developed under the leadership of Sharon O'Bryan and Viveca Ware, ICBA, and Jim Dempster, Metavante, and with the dedication of many individuals authoring sections and providing comments. We thank all of those who have been involved in creating this document.

---

**REVISION STATUS**

<b>Section</b>	<b>Last Revised</b>
Section 1: Framework Application and Flow Diagram	November 2003
Section 2: Business Decision to Outsource IT Services	November 2003
Section 3: Considerations for the Request for Proposal	November 2003
Section 4: Due Diligence Considerations	November 2003
Section 5: Contractual, Service-Level, and Insurance Considerations	May 2009
Section 6: Procedures for Supporting Specific Controls, Requirements, and Responsibilities	November 2003
Section 7: Implementation and Conversion Plan	November 2003
Section 8: Relationship Management and Changes in the Outsourced Environment	November 2003
Section 9: Considerations for Cross-Border Outsourcing	November 2003
Appendix 1: Model Spreadsheet for Cost Analysis	November 2003
Appendix 2: Framework Map to Federal Banking Agency Guidelines	November 2003
Appendix 3: Framework Map to Basel Committee on Banking Supervision	November 2003
Appendix 4: Glossary of Terms	November 2003
Appendix 5: Disaster Recovery/Business Continuity Matrix	November 2003
Appendix 6: Shared Assessments	May 2009
Appendix 7: Non-U.S. Nationals Working in the U.S. – Summary of Visa Requirements	November 2003

---

## ABOUT BITS

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A division of The Financial Services Roundtable, BITS works to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS provides intellectual capital and addresses emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS's efforts involve representatives from throughout our member institutions, including CEOs, CIOs, CISOs, and fraud, compliance and vendor management specialists. For more information, please visit [www.bits.org](http://www.bits.org).

BITS  
1001 Pennsylvania Avenue, NW  
Suite 500 South  
Washington, DC 20004  
202-289-4322  
[www.bits.org](http://www.bits.org)

---

## SECTION 1: FRAMEWORK APPLICATION AND FLOW DIAGRAM

Section 1 provides an overview of the *Framework* and the steps a financial institution would take in evaluating a decision to outsource IT services. Although the *Framework* follows the sequential flow of making the business decision to outsource, selecting a Service Provider and implementing and managing the relationship, many of the steps outlined in the *Framework* should be performed continuously and be integrated into the Receiver Company's business practices. For example, Vendor Management requirements are outlined in Section 8, however many of the processes that provide information required for ongoing relationship management are detailed in Sections 2 through 7 of the *Framework*.

Application of the *Framework* may vary depending on risk, the environment (shared vs. dedicated, single vs. multiple Service Providers), the application, system or service being outsourced, and the use of any dependent Service Providers.

1.1 Framework Flow: The *Framework* is intended to be used as part of, and in supplement to, the financial services company's ("Receiver Company's") due diligence process associated with defining, assessing, establishing, supporting, and managing a business relationship for outsourced IT services. The *Framework* covers the steps listed below, while acknowledging that the cost of the control processes should not exceed a reasonable risk/reward formula.

- Define the business objectives (Section 2).
- Define and review the business requirements for the technology (Section 2).
- Determine the technology necessary to deliver the business requirements (Section 2).
- Perform a risk assessment to baseline the control requirements (classification) (Section 2).
- Perform analysis and document the business decision to outsource (Section 2).
- Define specific control requirements and responsibilities (Section 3).
- Define backup, availability, and recovery requirements and responsibilities (Section 3).
- Perform due diligence in selecting an IT Service Provider (Section 4).
- Evaluate privacy, confidentiality, legal, regulatory and compliance considerations (Section 4).
- Validate evidence of general controls verification (Section 4).
- Validate evidence of control(s) verification and recovery capability of specific components (Section 4).
- Define contractual and service level agreements ("SLAs") (Section 5).
- Document termination terms, conditions and responsibilities (Section 5).
- Document procedures supporting specific control requirements and responsibilities (Section 6).
- Execute an implementation and conversion transition plan (Section 7).
- Define relationship management requirements, ongoing oversight, and verification process (Section 8).
- Evaluate considerations for cross-border relationships (Section 9).

---

The steps a financial institution should take in evaluating an IT outsourcing decision are presented as a high-level flow diagram on page 4. The diagram shows the steps detailed throughout this document in the request for proposal (“RFP”) process and due diligence, implementation, and control procedures development stages, as well as contractual and ongoing relationship management considerations.

1.2 **Functional Involvement:** In the implementation of these steps, a variety of internal functions could be part of the selection and management process. Some organizations may have or may consider developing an executive committee and/or IT vendor relations function to oversee, select and manage this process. Depending on a financial service company’s size, the process could include representatives from the following areas, and/or may include consultants involved at various stages in the process:

- information security;
- privacy officer;
- information technology operations and support;
- incident response/CERT teams;
- business continuity/disaster recovery;
- finance;
- technology recovery planning;
- legal;
- internal compliance and monitoring groups;
- risk management;
- applications development;
- database management;
- network design, engineering, and operations;
- audit;
- facilities;
- asset management;
- accounting and tax;
- business operations (e.g., system, application and service delivery management);
- purchasing/sourcing organizations; and
- human resources.

1.3 **Risk Management:** Each outsourced IT Service Provider relationship poses unique processing circumstances, and the responsibilities of stakeholders may vary accordingly. Each financial services company should, on a case-by-case basis, determine who will participate in the risk assessment process and how responsibilities will be allocated among stakeholders. In addition, each company should decide the extent to which this document is applicable, based on the risk, complexity, nature, and scope of the services being considered.

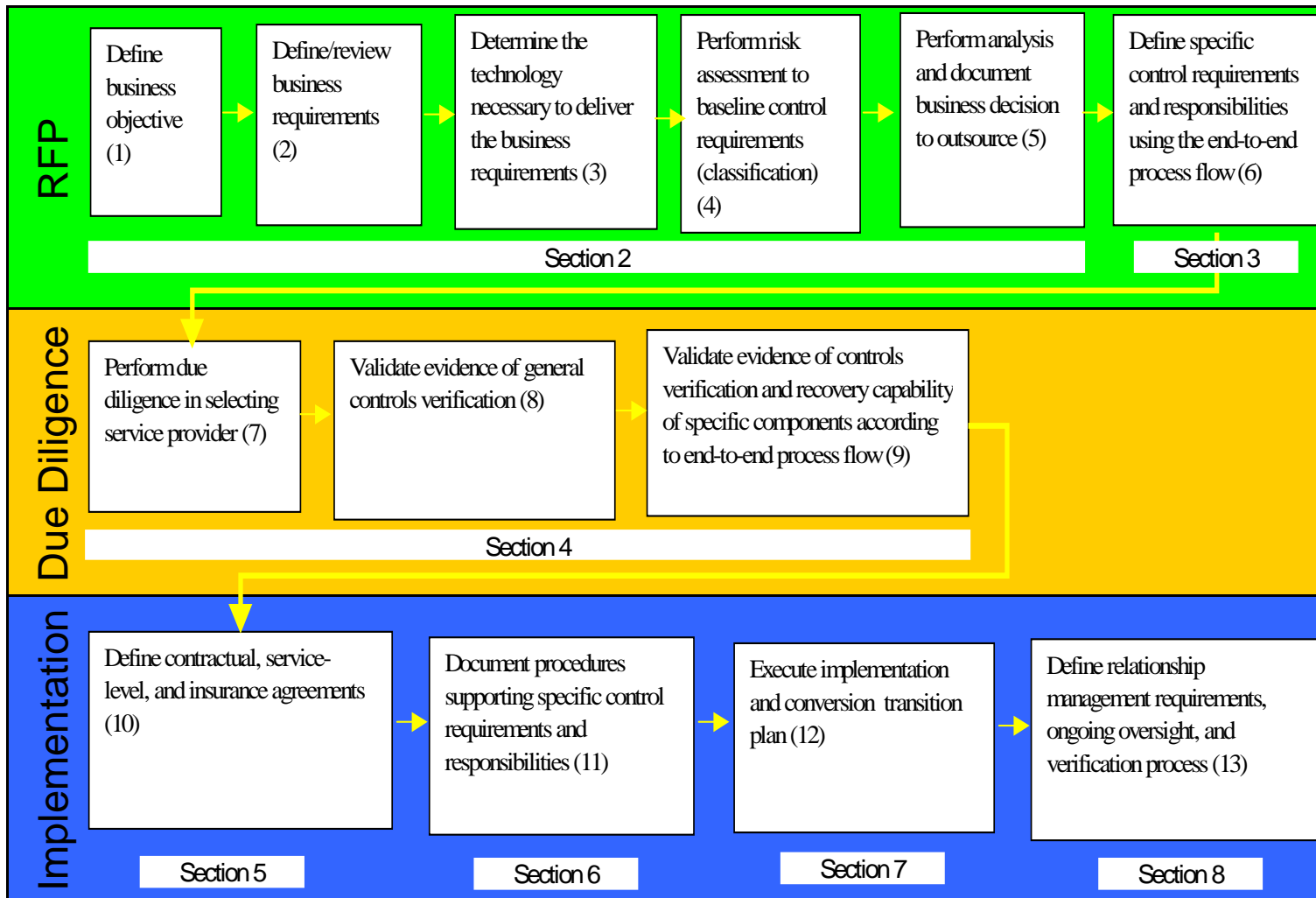
1.4 **Disaster Recovery/Business Continuity Planning:** Throughout the *Framework* and summarized in Appendix 5 are disaster recovery/business continuity considerations. At each stage of the selection and management process, Receiver Companies and Service Providers should establish

---

requirements for risk analysis, recovery objectives, planning, testing, event management, governance and insurance.

- 1.5 Security: Considerations for security and control that should be incorporated into the RFP, due diligence and management processes are incorporated throughout the *Framework*. The IT Service Providers Working Group has developed an Expectations Matrix to give service providers an outline with which to document their practices, processes and controls in relation to industry and regulatory requirements. High-level expectations for each control area from the Expectations Matrix appear in Appendix 6.
  
- 1.6 Cross-Border Outsourcing: While Sections 1 through 8 apply to all Service Provider relationships, including relationships involving Service Providers providing services to an institution outside of the US, Section 9 provides additional considerations for outsourced applications, systems and services based outside of the US. Issues include: strategy, legal and structural considerations, country risk, due diligence considerations, disaster recovery/business continuity planning, implementation issues, vendor management, communications requirements and exit strategy.

# BITS Framework Flow Diagram



---

## SECTION 2: BUSINESS DECISION TO OUTSOURCE IT SERVICES

Section 2 provides guidance on factors to consider in making a decision to outsource IT services. This section is also key to defining the services to be provided and is therefore a basis for determining the associated level of risk. Defining the IT services to be outsourced requires clear documentation of the scope, strategic importance, and acceptable levels of risk, and whether there are any regulatory issues with outsourcing the service. These definitions are necessary for successful use of the *Framework*.

Section 2 should be completed early in the project, when alternative solutions and associated vendors (internal and external) are being considered, to ensure that all management levels in the organization have access to sufficient information to proceed. In documenting goals, scope, and risks, it may be beneficial to refer to Sections 3 through 9. For example, Section 4 addresses verification of the Service Provider's delivery of the requirements specified in Section 3; Section 5 provides detail about insurance that could be useful in documenting item 2.8; and Section 9 provides a summary of additional considerations for Service Providers performing work outside of the US that should be considered early in the project. Considerations outlined in this section should be based upon the relationship being established and the service to be provided. It is also important to ensure that the cost of the control processes does not exceed a reasonable risk/reward formula.

### 2.1 Deciding on Goals, Scope, and Risks

Define business objectives.

A clear definition of the business objectives and system requirements is essential in deciding whether to outsource or to process in-house. For those processes currently handled in-house, the Receiver Company may consider documenting requirements to optimize the service. This definition is equally important in determining the levels of risk/reward that support business and strategic plans.

- Review existing corporate policies governing outsourcing. (See Section 8 for more information about outsourcing policies.)
- Define the business objectives to be achieved through the proposed technologies or services.
- Define the criticality of this system or service to future business plans.
- Define requirements regarding data accuracy, authentication, confidentiality or integrity.
- Define regulatory and security standards to be met in safeguarding customer information.
- Define the interaction this system will have with the Internet and with existing Service Provider relationships, if applicable.
- Determine the interaction (written, electronic, verbal or face-to-face) the outsourced provider will have with the Receiver Company's customers.
- Determine the business project sponsor (s) to provide executive oversight.
- Define the critical success criteria in order to determine if goals have been met.

### 2.2 Define the business requirements for the technology to be outsourced, specifying the desired results and industry standards, but not the technology to be employed.

---

In order to achieve business objectives, ensure integrity and organizational branding requirements, and maintain or improve service levels, it is important to clearly document the scope of the systems and/or services to be outsourced.

- State the Receiver Company's requirements for handling the data, related security and privacy requirements, and classification of data.
- Define requirements for support, maintenance, bug fixes, problem management, and change management for support and equipment. This may apply to any asset that is used by the Service Provider to supply the service to the Receiver Company.
- Identify existing third-party relationships, partnerships or agreements that might be affected by the proposed outsourced system, application or service.
- Define requirements for system and user administration.
- Define requirements for monitoring and reporting on service levels and security incidents and policies for the Receiver Company to initiate incident handling procedures upon notification from the Service Provider of a security incident.
- Define the system lifecycle, expected timeline of the project, and ongoing support and services.
- Determine volumes expected, both peak and average, during timeframes (e.g., end of month processing).
- Determine hours of availability of system and allowable maintenance windows.
- Determine location and facilities to be used for services.

### **2.3 Recommend the technology requirement necessary to deliver the business requirements.**

Document the end-to-end transaction flow of the processes, considering automated and manual control points, hardware, software, databases, network protocols, security recovery and real-time versus periodic processing characteristics. Obtain flow diagram of the transaction process, the Service Provider's internal and external network connectivity and any dependent or existing Service Provider relationships the Receiver Company may have. Review the flow diagram to ensure that only required resources use or access the transactions and that no single employee can enter, authorize, divert and/or complete a transaction and determine gaps that may exist in the product service delivery.

- Recommend the application types to be used by the Service Provider to perform the business function services for the Receiver Company.
- Determine hardware environment(s) to be used to perform Receiver Company services.
- Determine the database environment to be used to store Receiver Company data.
- Determine network infrastructure requirements.
- Determine technology requirements to implement the required level of security.

### **2.4 Perform a risk assessment to baseline the control requirements.**

Cost-effective information protection and technology risk management are achieved when the cost of the potential exposure is mitigated by security measures that do not exceed the value of the control investment. This investment includes implementation costs (e.g., personnel, hardware, software, and network impact), contract requirements, and ongoing maintenance. In order to evaluate risk and the corresponding degree to which the *Framework* is used, the risk of the application, system or service

---

should be assessed. The risk assessment should include both direct hard-dollar loss and reputation impact, and be based on a review of the following:

- The system is part, or may become part, of the strategic plan for the financial institution.
- The degree of difficulty in implementing the application, system or service.
- The level of expertise required to evaluate and manage the Service Provider.
- Customer privacy and/or sensitive information is processed, stored, transmitted and/or handled.
- The degree of interaction with financial institution customers.
- Manual controls are or are not available. (e.g., high-volume systems).
- The volume of transactions or dollars to be processed by the application, system or service, which may impact possible loss resulting from system errors, failures, or exposures.
- The degree to which publication of an unauthorized access would lead to loss of customer confidence in the financial institution's strategic products and services.
- The degree to which Receiver Company logo is used or referenced (e.g., hosts website).
- Access control systems are to be managed by a third party.
- Platform technology direction is appropriately defined.
- Required conformance with laws, rules, regulations, policies, procedures or ethical standards.
- The degree to which the Receiver Company will be dependent on the Service Provider:
- The system, application or service is a new or existing business.
- The level of difficulty and knowledge transfer required to switch vendors, if necessary.
- The ability to develop an effective exit strategy based upon the evaluation of alternative service providers (e.g., the outsourced application, system or service is provided by few service providers, which could impact the ability to switch vendors) or the ability to move the business in house.

## **2.5 Meet disaster recovery/business continuity planning requirements.**

In a post-9/11 world, financial institutions, regulators and Service Providers are taking a closer look at their ability—along with their partners' and the industry's ability—to recover from a disaster.

Financial institutions should incorporate requirements for disaster recovery into every aspect of the outsourcing decision, through the termination of the relationship. As part of this process, institutions should consider not only the Service Provider's own disaster recovery/business continuity plans, but also the impact the relationship may have on internal plans and existing Service Provider relationships. In this process, the following components should be considered:

2.5.1 Risk Analysis: The Receiver Company should conduct a risk assessment and business impact analysis to determine the events and environments that could adversely affect the company. The risk analysis should consider the criticality of the outsourced services or products to the Receiver Company. In most cases the risk assessment and impact analysis should be conducted collaboratively with the affected Receiver Company business units.

- 
- 2.5.2 Recovery Objective: A definition of the required recovery time objective(s) (RTO) and recovery point objective(s) (RPO) for each service or product the Receiver Company is considering outsourcing should be defined during this phase in the outsourcing process. This helps the Receiver Company determine if regulatory or risk issues will impact its ability to maintain required availability expectations and/or requirements.
  - 2.5.3 Plans: As part of the business decision to outsource, the Receiver Company should consider how the relationship will affect its disaster recovery/business continuity plans and/or any related products or services.
  - 2.5.4 Testing: In evaluating the ability to outsource an application, system or service, the Receiver Company should consider how the relationship will affect the institution's testing requirements and/or any related products or services.
  - 2.5.5 Event Management: The Receiver Company should consider its ability to test and execute internal event management plans and assess the impact of assigning responsibilities to the outsourced provider for components of the plan, such as emergency response notification, escalation, and communications.
  - 2.5.6 Governance: The Receiver Company should evaluate its governance structure to determine the effect of coordinating with and overseeing a Service Provider, including identifying any relevant regulatory requirements.
  - 2.5.7 Insurance: The Receiver Company should determine whether outsourcing will affect existing insurance coverages.

## **2.6 Define barriers to success in utilizing internal or external IT resources.**

Determine whether the business objectives could be met successfully if internal versus outsourced IT resources were used. Barriers to success may include staffing levels, staffing morale, experience, technology investment, technical expertise, time-to-market, ongoing support, and market reaction.

## **2.7 Perform internal versus external cost analysis.**

In order to protect shareholder investment, decisions relative to cost management should be carefully thought through and the cost of performing IT processing should be assessed. Internal versus external sourcing costs, which are identified in this section and the RFP and due diligence processes outlined in Sections 3 and 4, should be analyzed to ensure that outsourcing is reflective of the business plan. Costs of internal versus external sourcing should be measured in relation to estimated benefits such as time-to-market, efficiency, reliability, staff expertise, total cost of ownership and corporate focus on core competencies. A model spreadsheet detailing generic cost categories, found in Appendix 1 of the *Framework*, is suitable for estimating costs as described below:

- 2.7.1 Estimate costs for hardware, software, communications, staffing, facilities, and maintenance for IT services.
- 2.7.2 Estimate costs to establish appropriate level of access control and monitoring. These costs may include infrastructure and software for performing user access authentication and

---

administration, security monitoring, remote access requirements, auditing, exception reporting, and the staffing required to support these functions.

- 2.7.3 Based on the factors outlined in 2.5, estimate costs to establish recovery capability commensurate with the availability and data loss tolerance constraints. These costs may include hardware and software technologies such as disk mirroring, full and incremental backups, automated fail-over systems, recovery facilities (contract or owned), recovery plans, and the staffing required to support these functions.
- 2.7.4 Estimate cost for insurance coverage associated with potential losses associated with proposed IT services.
- 2.7.5 In addition to these initial costs, estimate cost of terminating an outsourced service and establishing an alternate resource for the service, whether in-house or another Service Provider.

## **2.8 Decide on insurance coverage.**

In a decision to outsource, the cost and type of insurance coverage should be considered, including an evaluation of how outsourcing will affect current insurance coverages. Section 5 of the *Framework* provides details on the types of coverage and the contractual considerations involved.

---

## SECTION 3: CONSIDERATIONS FOR THE REQUEST FOR PROPOSAL

Section 3 provides guidance and defines factors to consider in developing a request for proposal (RFP). Factors included in an RFP should be based upon the objectives outlined in Section 2, the relationship with the Service Provider and the service to be provided. The Receiver Company should design the RFP to reflect the service level requirement, performance measurement criteria, availability and other support requirements. In addition to a clearly defined statement of work, the RFP should identify the specific procedures and processes, responsibilities, SLAs, and types of controls expected to be in place to ensure the integrity of information and transactions throughout the engagement. While not required in all outsourcing arrangements, the RFP process can be an essential part of the selection process for complex projects involving significant investment and may be performed in-house or by an outside consultant. The RFP can help identify a set of qualified Service Providers with the skills and experience to meet the Receiver Company objectives.

Receiver Companies should fully understand the level of risk of the outsourced application or service when developing the RFP to ensure the cost of the control processes does not exceed a reasonable risk/reward formula. While the RFP primarily deals with expected production service levels and measurement requirements, the Receiver Company should require that control measures be in place for information protection, business continuity and change management. The Receiver Company should also state clearly its own information-protection, business-continuity and change-control policies, and expect Service Provider responses that outline a cost-effective program that adheres to these policies. To assist Receiver Companies and Service Providers in identifying control areas to evaluate, the BITS IT Service Providers Working Group has created a high-level set of industry expectations for Service Provider operations in Appendix 6. These high-level expectations have been further defined in an Expectations Matrix that defines processes and controls in the context of the industry and regulators' requirements, which should be included in financial institution assessments or independent audits of Service Provider operations.

The Receiver Company should ensure that all terms are carefully and explicitly defined and reviewed with the RFP bidders to foster accurate understanding of the terminology (e.g., system availability, response time, information security controls, recovery objectives, notification etc.). The following list outlines some of the items that institutions should consider in developing an RFP. The list is not intended to be all-inclusive; rather, it highlights elements that are discussed throughout the *Framework* process flow to help a prospective Service Provider understand the requirements of the engagement.

### RFP Definitions for Services, Tools, and Controls

- 3.1 Define service availability and performance requirements so that an effective comparison can be made between different Service Providers. (For example, do performance standards include a reference to the number of blackout periods per day?) Requirements may include:
  - application availability and scalability;
  - minimum performance standards and service levels;
  - expectations for availability and operational redundancy;
  - quality assurance and measurement;
  - acceptable capacity planning or other service-delivery methodologies;
  - recovery objectives;
  - incident and outage communication procedures;

- 
- physical access controls;
  - responsiveness, hours of availability and communication tools available (e.g., written, verbal, electronic, face-to-face) of customer service, and
  - reporting requirements.

3.2 Define the types of security, recovery, auditing, and control tools required at each step in the process flow, keeping in mind that the tools required may vary depending on the environment (shared vs. dedicated environment, single vs. multiple Service Providers), criticality of the application, system or service being outsourced (e.g., an application will require an evaluation of architectural design elements specifically as they relate to the Receiver Company's infrastructure), and the use of any dependent Service Providers. For each of the control areas outlined below, the Receiver Company should consider including the following provisions for security in the RFP:

- frequency and format of reports;
- procedures for identification of information security incidents;
- incident notification procedures between parties;
- associated software to identify penetration attempts;
- security administration procedures;
- intrusion detection monitoring;
- facilities and customer equipment monitoring;
- security and climate control of storage facility; and
- security and climate control of media during transportation.

Typical control areas include:

- access controls;
- audit trails;
- authentication;
- authorization;
- availability;
- change control;
- compliance;
- confidentiality;
- configuration management;
- data integrity;
- disaster declaration criteria/controls;
- disposal of data and equipment;
- environmental systems (electricity, cooling, fire prevention and protection);
- encryption;
- escalation and notification;
- incident response;
- intellectual property ownership;
- intrusion detection;

- 
- non-repudiation;
  - penetration and vulnerability testing;
  - physical and administrative security systems;
  - privacy;
  - procurement;
  - recovery plan maintenance and testing;
  - reporting;
  - security architecture and administration;
  - source-code maintenance and storage;
  - system configuration and administration;
  - training and awareness;
  - transaction integrity; and
  - virus protection and patch-management processes.

3.3 Based upon the risk associated with the application, system or service, identify which of the above controls should be considered at the following discrete points in the process flow.

- Access – Include all system access points for the Service Provider’s processing locations (including offsite storage and recovery facilities), the Receiver Company, existing service-provider relationships, and end users (including customers). Procedures include specific provisions to address access to data or processing of data physically, or via network, telecommunications, or any other means. Evaluation should include:
  - requirements for specific access to production data;
  - access capability to stored data (security measures in place);
  - access for maintenance of owned equipment;
  - physical access to production and recovery facility;
  - identification of all individuals and maintenance personnel;
  - identification of remote access requirements (e.g., teleworkers, remote access support, security requirements);
  - retention of access procedures and personnel lists (access logs, etc.); and
  - verification procedures for access.
- Transaction Points – Transaction points involve a change or modification of data immediately upon user request.
- Batch Processing – Batch processing points involve modification of data at a scheduled time, based upon stored requests.
- Data Storage – Data storage points should include all locations where data is stored by the Service Provider, Receiver Company, and any third parties that may be involved in the process.
- Data Processing – This includes any points where operations are performed on data such as handling, merging, sorting, and computing where the content of the original data is not changed. The content of the processed data may be changed. Depending on the outsourced application, system or service, consideration should be given to the production data that is required.

- 
- Hardware – Hardware platforms should include all components from workstation to hosts at the locations of the Service Provider, Receiver Company, and third parties.
  - Software – Software should include the operating system, utilities, tools, database, and network and application software.
  - Network – Network points include network paths (circuits), routers, switches, hubs, and firewalls.
  - Internal Coordination – This includes automated and manual handoffs between departments and organizations such as purchasing, legal, print shop, etc.

3.4 Define provisions for change control to address scalability, changes in technology or processes, financial changes to the Service Provider that would affect the Receiver Company, and other customer changes that would affect the Service Provider's environment and in turn affect service to its customers. The provisions for change control should address:

- advance notification procedures for production equipment/software/hardware changes/changes to the business;
- delivery performance specifications;
- acceptance testing procedures for new changes to production environment;
- right of involvement in acceptance testing that affects the production environment;
- certification of completed acceptance testing prior to re-implementation of changes to production environment;
- training, capacity management, and delivery performance specifications provided by Service Providers (depending on the extent of changes); and
- updated recovery plan reviews.

3.5 Based on the risk of the application, system and service, the Receiver Company should consider defining the following elements of business continuity/disaster recovery in the RFP:

3.5.1 Risk Analysis: The RFP should require evidence that a risk assessment has been conducted to determine the events and environment that could adversely affect the Service Provider. Corresponding risk reduction or mitigation steps should be documented. The RFP response should include a review of the Service Provider's risk profile, considering the criticality of the service or products to the Receiver Company.

3.5.2 Recovery Objective: The RFP should specify the required RTO(s) and RPO(s) for each service or product the client is receiving. RTOs establish the length of time for which a process can be unavailable. RPOs establish the amount of data that can be lost or how old the data can be, e.g., 24 hours since the last backup. The Service Provider should have contingency plans in place to support multiple clients' recovery events.

3.5.3 Plans: The RFP should require documented continuity plans and supporting recovery strategies. The plans should consider recovery of activities supported by dependent Service Providers. A periodic maintenance cycle is required, not to exceed 12 months.

- 
- 3.5.4 Test: The RFP should require minimum testing standards, including a strategy for testing plans (frequency not to exceed 12 months), test schedule, and client involvement goals. Testing requirements should also include type of tests conducted (e.g., tabletop, live test, simulation, end-to-end), test results documentation (including follow-up responsibilities and an ongoing update process for existing plans), Receiver Company observation/participation in Service Provider tests, and regulatory compliance as it relates to testing.
- 3.5.5 Event Management: The RFP should require evidence of a formal event-management plan that includes emergency response, escalation and communications at the corporate level. The Service Provider should notify a designated point of contact at the Receiver Company if a disaster or service interruption occurs. Event management should address regular status reporting procedures for use during outages and testing of the event-management plan.
- 3.5.6 Governance: The RFP should require that a process be in place at the Service Provider to ensure accountability and compliance with the goals and objectives of the Receiver Company's continuity planning program. The Service Provider's governance program should be audited regularly and the results monitored and signed off on by its senior executives. Also, the Service Provider should ensure that federal and state regulations are met and managed as they apply to their customers.
- 3.5.7 Insurance: The RFP should define any requirements for business interruption insurance sufficient to mitigate any business interruption. The cost and type of insurance coverage should be considered, including an evaluation of the impact outsourcing will have on current insurance coverages. Section 5 provides details on the types of coverage and corresponding contractual considerations.

---

## **SECTION 4: DUE DILIGENCE CONSIDERATIONS**

Section 4 addresses verification of how the Service Provider delivers the requirements specified in Section 3 to meet the business objectives outlined in Section 2. Use of the due-diligence process to verify the RFP responses will depend on the Receiver Company's analysis of the RFP responses and may be undertaken for some or all of the respondent companies. In addition, the Receiver Company may choose to perform due diligence in-house or hire an outside organization to perform this and the RFP function. The intent is to verify that the Service Provider has a well-developed process and adequate resources and experience to ensure acceptable service, controls, systems backup, availability, and continuity of service to its clients.

Below are considerations for assessing the overall risk of outsourcing to a particular third-party provider. The possible risks are diverse, ranging from financial to operational risks. Because each outsourcing relationship is unique and the appropriate level of scrutiny may vary widely, following all of the guidelines below may not be warranted in every case. It is important to fully understand the level of risk of the outsourced application, systems or service when performing due diligence in order to ensure that the cost to review the control processes does not exceed a reasonable risk/reward formula. Receiver Companies may consider applying different levels of due diligence based on criteria established by their risk management process (e.g., all new Service Provider relationships, risk-assessment rating, criticality of the outsourced service, Service Providers who process, store or transmit customer information).

In addition to a review of the components outlined in this section, the due-diligence review should include a thorough understanding of the Service Provider's reliance on additional third-party Service Providers to deliver the service. The Receiver Company should also give some consideration to the components of an exit strategy and cost of switching Service Providers if the Service Provider fails to meet contractual requirements (e.g., consideration of whether the solution is a proprietary one).

### **Corporate Due Diligence**

During the due diligence phase, the Receiver Company should evaluate qualitative and quantitative resources specific to the industry, company and business practices for the type of application, system or service to be performed by the Service Provider.

#### **4.1 Corporate Structure**

Receiver Company should:

- confirm the Service Provider's legal name and address;
- determine how long the Service Provider has been in business and offering the relevant services;
- obtain the latest corporate organizational chart, including affiliates, subsidiaries and board members to determine whether the Receiver Company currently has relationship(s) with any of the Service Provider's operations, principals or subsidiaries, as well as to identify potential conflicts of interest;
- check the Office of Foreign Assets Control regulations and "Specially Designated Nationals and Blocked Persons List" for Service Provider employee names; and

- 
- evaluate the Service Provider's governance structure to ensure that the company is able to effectively manage the relationship. While the contract and SLA may identify accountability and responsibilities, during the due diligence process the Receiver Company should ensure necessary processes and personnel are in place. Review of the Service Provider's governance program should include a review of its plan to monitor federal and state regulations applicable to the relationship.

#### 4.2 **Business Strategy and Reputation**

The Receiver Company's due diligence should include a thorough evaluation of available information related to the Service Provider. Due diligence should include the Receiver Company:

- researching management backgrounds/experience, overall staffing levels and turnover rates;
- performing background checks, including criminal checks, on company principals;
- finding out how many clients the company has, what kind of business reputation it has, what its presence is in the marketplace, and its market share;
- researching any complaints, litigation or liens against it;
- determining the percentage of the Service Provider's total business the Receiver Company would represent and/or if the Service Provider relies significantly on one or two existing clients;
- checking references from current and past clients;
- reading any available analyst reports and user-group information;
- conducting at least one site visit;
- obtaining a product marketing package that may include a product description, pro forma financial analysis, telemarketing script, direct mail pieces, buyer profiles, tracking reports and references to financial services companies offering the product;
- reviewing the proposed marketing strategy for the service offering;
- determining days and hours of operation, including availability of toll-free customer service lines and after hours and holiday contacts;
- if any user groups are associated with the service, determining how well the Service Provider communicates with customers through those groups; and
- for products delivered through a provider network, identifying the number of providers by state.

#### 4.3 **Financial Analysis**

The level of financial review should be consistent with the complexity of the Service Provider's business activities.

- 4.3.1 The Receiver Company should consider performing a financial analysis on the Service Provider's three most recent fiscal and quarterly audits. Financial statements should be prepared in accordance with Generally Accepted Accounting Principles.

---

Statements should be audited in a timely fashion by reputable and independent accounting firms.

4.3.2 Obtain and examine:

- available SEC filings (for public companies);
- available financial ratings from external and internal sources such as Standard & Poor's, Dun & Bradstreet, Moody's, and Bloomberg; and
- credit reports.

4.3.3 Understand the Service Provider's sources of capital and project its future financial condition.

## Risk Analysis

### 4.4 Assessing Audits and Assessments

4.4.1 Right to Audit: The Receiver Company should retain the right to audit the facility, the general controls environment, implementation of certain policies, adherence to customer-specific processing policies, adherence to security and customer-information requirements and adherence to procedures associated with the relationships with the Receiver Company. The third-party auditors should be mutually acceptable personnel and may not disclose any of the proprietary information of the Service Provider or Receiver Company. For the audit or assessment, the Service Provider should be given advance notice and details of the scope, in order to prevent impact to availability, SLAs, customer satisfaction, etc. Internal or external audit results should be shared with the Service Provider, within a specific time frame after an audit is issued by the Receiver Company or its external provider, to discuss and mutually determine audit items that may need resolution and/or mutually develop plans and procedures to address any changes suggested by the audit.

A Service Provider might ask a Receiver Company to rely on an audit by a third party as a substitute for an audit by Receiver Company. When considering such a request, the Receiver Company should take into consideration the level of risk, its comfort with the third-party auditor, and the scope of the audit. If a decision is made to grant such a request, the Receiver Company should have access to the audit results and plan for resolution of any findings. Additionally, the Receiver Company should not surrender its right to audit.

4.4.2 Availability of Audits: Determine if the Service Provider has a current-year, independently conducted, third-party audit or assessment report that includes testing of general and technology-based controls for the specific scope of work at the site where work is to be performed. Review of this report should include an analysis of the cover letter to determine the scope of what is, and is not, covered by the engagement and by the User Control Consideration section that represents the control points the user organization is responsible for addressing. Based upon the level of risk associated with the services to be performed, the Receiver Company may require a review of the hardware, software, and processes.

---

A SAS 70 Type II, a SysTrust audit, a WebTrust audit, an independent auditor's report, a security assessment, and/or a full penetration test are some of the available tools but, depending on the application, system or service to be outsourced, may be cost prohibitive. It is important to fully understand the level of risk of the outsourced application or service and whether it is a shared or dedicated processing environment. For a business-critical application containing sensitive data, a thorough test should be conducted. As the level of risk decreases, alternative assessments may be considered. They may include any subset of the components in the list below, as well as system or server scans, news group and other research, and references from other customers.

- 4.4.3 Audits of Shared Environments: In a shared environment, these audits or assessments may involve more than one Receiver Company and more than one process. Consideration should be given to the practicality of individual financial institutions participating in audit or assessment engagements. In cases where more than one Receiver Company engages in the audit, participating in scheduled audits can reduce cost, minimize service disruption, and increase participation of key workgroups.
- 4.4.4 Review of Audits or Assessment: If there is a third-party review, the Receiver Company should validate that the report was prepared, and detailed controls testing was performed, by an independent third party (e.g., an independent auditor conducting an evaluation in accordance with the Statement on Auditing Standards of the AICPA (American Institute of Certified Public Accountants)). The Receiver Company should further validate whether controls related to services for the Receiver Company are functioning as intended based on testing. The Receiver Company should determine if the report is for the current year. It is important to determine whether there have been any material changes to the infrastructure or configuration of the systems since the last review or test and whether the location and technology environment associated with the services are materially the same. If so, those components should undergo a further review to ensure that integrity has been maintained. It is also critical to ensure that the systems and infrastructure reviewed are the same components that will be hosting the application, systems or services to be outsourced.
- 4.4.5 Control Testing: A thorough Service Provider security review would include testing. The test areas should require written signoff by the Receiver Company and the Service Providers because of the potential for service disruption, financial loss, and the triggering of certain automatic security responses. While further detailed in Appendix 6, tests would include:
- a review of the Information Security Policy documents;
  - security policies and procedures;
  - physical security controls;
  - external network penetration attempts;
  - application penetration attempts;
  - vulnerability assessment;
  - internal penetration attempts;

- 
- attempts to gain access through social engineering techniques;
  - a complete report of attacks and tools used, findings, and recommendations;
  - a follow-up review to confirm that recommendations were implemented; and
  - a determination of whether controls testing was performed on each technology control to be relied upon in production processing—including physical access, operating system, network, application, and database controls.

4.4.6 Internal Audits: If internal audits have been performed by the Service Provider on the applications, system or service performed for the Receiver Company, during the due diligence process the Receiver Company may also want to evaluate this information and the process used to conduct the audits. The Receiver Company may also request any audits that relate to verification of the Service Provider's compliance with contractual obligations, e.g., (i) accuracy of charges and invoices, (ii) the Service Provider's performance related to its (a) internal practices and procedures, (b) disaster recovery and backup, (c) data and network security, (d) efficiency and effectiveness in using resources to provide services for which the Receiver Company is charged, and (e) performance of the services according to performance standards.

#### 4.5 Service Provider Maturity

To determine the Service Provider's level of maturity in process control, the Receiver Company should:

- evaluate its employee development and training programs, including security-awareness training;
- evaluate the customer problem tracking and resolution process;
- understand customer service organization, including outsourced functions;
- review service standards, tracking reports and corrective action processes;
- review MIS capabilities and reports;
- understand process controls and work validations to ensure contract compliance;
- acquire a copy of any outstanding software bugs and patches needed and find out the timeframe planned for fixing bugs and installing patches;
- evaluate the production change-management process, including change logging, management approval, backout plans required, and enforcement; and
- understand the quality control program and workflow. If the Service Provider is certified to ensure quality and security in its operations, find out who performed the evaluations (including whether it was a self-assessment), where it was performed (including whether it was at the location where the Receiver Company's work will be performed), when one was last performed, and whether certifications are performed regularly. Finally, in assessing the quality control program and workflow, the Receiver Company should evaluate the impact the certification may have on its own operations and processes.

#### 4.6 Privacy and Confidentiality Considerations

The Receiver Company should evaluate the procedures in place at the Service Provider to protect information (such as customer or employee data), including:

- finding out if there is a privacy policy and determining whether its provisions are adequate;

- 
- understanding how the privacy policy was/is implemented and how it was/is communicated;
  - reviewing the privacy policy employee training program and tracking;
  - reviewing privacy policy employee fraud-detection training and management reporting;
  - examining the employee confidentiality policy and signed confidentiality agreements;
  - examining the contractor/subcontractor confidentiality policy and signed confidentiality agreements;
  - examining employee disciplinary policies/actions for privacy policy violations;
  - understanding the adequacy of privacy procedures for temporary/contract staff;
  - examining employee background-check procedures, including process for screening current, prospective, contract and temporary employees;
  - reviewing procedures to protect, retain and destroy nonpublic personal information;
  - reviewing procedures to advise Receiver Company of, and comply with, “Do not call”, “Do not mail” and “Do not email” requests;
  - obtaining privacy policy script used by customer service employees; and
  - comparing the Service Provider’s privacy policy to Receiver Company’s policy and identifying any gaps.

#### **4.7 Assess the Service Provider’s diligence in legal, regulatory and compliance areas.**

- Determine the existence and adequacy of the Service Provider’s compliance program and objectives.
- Determine how the Service Provider’s legal department is used, including staffing levels and functions, and the use of outside counsel.
- Determine the adequacy of procedures to ensure compliance with state and federal legal and regulatory requirements.
- Determine the adequacy of procedures used to ensure compliance with any Receiver Company-specific privacy standards or guidelines (i.e., privacy rules unique to the Receiver Company that are not necessarily federal or state regulatory requirements).
- Determine the adequacy of processes used to stay abreast of statutory, regulatory and administrative changes affecting its business. This includes monitoring for any business patents that could affect the Service Provider's business.
- Determine whether the Service Provider keeps abreast of case law affecting its business.
- Review any current or recent (within 3 years) governmental, regulatory or administrative investigations, proceedings, complaints or lawsuits against it or any of its officers or employees.
- Review any recent (within 3 years) complaints about the Service Provider by customers to any regulatory authority or consumer complaint agency.
- Determine whether there is a process for disseminating compliance updates and similar relevant information to its financial services customers.
- Review any processes used to track pending legislation. Find out if the Service Provider would consider the Receiver Company’s position on issues.

- 
- Review any process used to amend client contracts based on changes in business practice due to law or regulation.
  - Review procedures for remaining current on banking/insurance/direct mail/telemarketing regulations.
  - Review procedures for complying with state licensing requirements.
  - Examine procedures for complying with state advertising requirements.
  - Review approval procedures for advertising and promotional materials.
  - Review procedures to maintain the confidentiality and privacy of client records.

#### **4.8 Determine the Service Provider's technology and systems architecture.**

- Review the high-level systems architectural design to determine its relationship to industry and Receiver Company standards for scalability, capacity, performance and code structure.
- Understand the availability of source code for extension, co-development or escrow purposes.
- Determine if Service Provider products conform, have been evaluated or tested against security criteria (e.g., BITS Product Certification Program, Common Criteria).
- Review the risks and controls of systems connectivity between Service Provider and Receiver Company.
- Understand whether the application could be brought in-house or to another Service Provider.
- Understand third-party products and licenses.

#### **4.9 Determine the Service Provider's reliance on other third-party service providers.**

- Identify and review all Service Provider dependencies.
- Verify the process the Service Provider has in place to review third parties' security policies and procedures.
- Review the Service Provider's service record and experience with dependent providers.
- Review the Service Provider's issue notification, communication, and contingency plans for dependent providers.
- Evaluate interoperability security between Service Provider and dependent providers.
- Determine if the other third parties have disaster recovery Service Providers.
- Determine if the Service Provider has had to declare a disaster requiring the activation of its recovery process, and the level of success.
- Determine certifications and capabilities of Service Provider's third-party providers.
- Determine if the Service Provider can leverage the Receiver Company's existing relationship(s) with other third-party providers.
- Determine the conditions under which a third-party backup or recovery site would be activated.
- Determine the level of access required for a third-party site.
- Determine the Service Provider's access rights per their contract with a recovery Service Provider, i.e., is it first come, first served or dedicated capacity, or is access determined by the recovery Service Provider based on other clients' simultaneous requests?

- 
- If recovery resources are not dedicated, determine the recovery Service Provider's ability to recover simultaneously all clients within a reasonable area and timeframes. Consider a risk-based approach to establishing separation of operations or facilities.
  - Determine what, if any, time limit exists on operating from the recovery site.

#### **4.10 Determine what impact the Service Provider will have on other Service Provider relationships that already exist in your network.**

- Review access control, security and privacy requirements from previously established Service Provider relationships to determine whether any of them are affected by the new relationship.
- Review network configurations to assess whether logical or physical separations are required between Service Provider connections and access points.
- Review existing Service Provider contract terms to determine whether any are affected by the new Service Provider relationship.
- Review existing insurance terms to determine whether any are affected by the new Service Provider relationship.

#### **4.11 Determine service availability offerings and their link to requirements.**

- Determine if there are regularly scheduled time periods when the service is not available.
- Determine if the Service Provider has historical statistics on system availability and response times.
- Determine how additional transaction volume created by a new client affects system performance and availability.
- Determine architecture for high availability and operational redundancy.
- Determine the architecture's ability to provide and support additional capacity.
- Determine if the Service Provider supports a dual, high-availability environment in case of interruptions in local/regional utility service (e.g., communications, gas, electric, sewer, water).

#### **4.12 Exit Strategy Considerations**

To help identify possible risks, define potential losses, and ensure the continuity of services, the Receiver Company should begin developing an exit strategy during the selection process. The Receiver Company should not only plan for the transition of services to the selected Service Provider, but also evaluate possible transition of services from the selected Service Provider to another third party or in-house, in the event that the Service Provider is unable to continue to provide contracted services.

#### **4.13 Disaster Recovery/Business Continuity Requirements**

##### **4.13.1 Risk Analysis**

- Examine the list of threats from possible internal and external sources identified by the Service Provider, along with the assessment of impact and probability.
- Verify that the Service Provider has introduced controls to mitigate the effects of identified threats.

- 
- Review the types of business functions the Service Provider has identified as critical to ensure that Receiver Company requirements will be met.

#### 4.13.2 Recovery Objective

- Determine whether offsite backup checks are performed frequently enough to meet the Receiver Company's RPOs. Backup checks should include examination of:
  - controls on offsite storage site environment and access;
  - encryption standards including backup, storage and recovery of encryption keys; and
  - location of secondary storage facility relative to the primary facility.
- Verify the integrity of the backup either through planned or random sampling (particularly in open systems environments).
- Determine whether the Service Provider's recovery time is sufficient to meet the Receiver Company's RTO.
- Based on continuity strategies defined in the Service Provider's plans, determine what the **maximum** recovery time will be for the Service Provider to restore systems and, upon restoration, what the worst-case data recovery time will be.
- Determine whether these criteria have been validated through testing.
- Determine whether the Service Provider has established "preferred priority restoration" with other clients.
- Determine the probability of other clients declaring a disaster simultaneously and the impact this could have on the Receiver Company.
- Examine the contingency plans in place to support multiple clients' recovery events should resources be required simultaneously.

#### 4.13.3 Plans

- Review the written recovery plan. Verify that it is updated annually and that copies are stored at the recovery site and other secure offsite locations.
- Examine the plan for coverage of:
  - remote command center;
  - recovery site;
  - staff relocation plans;
  - recovery teams with defined tasks;
  - critical third parties (recovery vendors, equipment vendors, transportation, utilities, and public safety);
  - activation/notification method;
  - communications to customers;
  - communications with the media;

- 
- communications with public safety services; and
  - acquisition of critical IT resources.
  - Verify that adequate geographic separation exists between the Service Provider's primary facility and its recovery site(s) and storage facility(ies).
  - Verify that network documentation is maintained for production and recovery configurations, including connections to external data sources not controlled by the Service Provider.
  - Determine if processing can be accomplished from the recovery site using normal production processes. If not, determine whether the recovery plan contains documentation of special processes.

#### 4.13.4 Testing

- Review recovery testing efforts performed by the Service Provider, including the scope and results of the test(s). Determine when the continuity plans for the Receiver Company were last tested successfully. Determine the frequency, scope and type of testing (e.g., walkthrough, simulation, etc.).
- Determine whether test documentation contains scope, objectives, timeline and results.
- Determine whether testing is certified by an independent third party and obtain a copy of the certification.
- Determine whether the Receiver Company may participate in recovery tests and to what extent (e.g., observation, planning, testing, data entry, observation of results, validation against production results).
- Determine whether the test results demonstrate recoverability within the recovery service levels (e.g., recovery time and data loss) required by the Receiver Company.
- Determine whether the test results are reviewed and signed off on by the Service Provider's senior management, and whether the results are available to the Receiver Company.
- Determine whether testing anomalies are documented, and whether root-cause analysis was applied and used to modify the recovery plan and subsequent test objectives.

#### 4.13.5 Event Management

- Examine the Service Provider's documented event-management plan for clearly defined emergency response, escalation and communications procedures, including notification of designated Receiver Company contacts.
- The Service Provider should include representation from:
  - corporate communications (internal to employees and external to customers, government agencies, regulators and the media);
  - building security;
  - building management;

- 
- information systems management (including data security and disaster recovery);
  - human resources;
  - dependent Service Providers;
  - essential business units;
  - public safety agencies; and
  - executive management.

#### 4.13.6 Governance

- Verify that the Service Provider has a documented process in place to ensure accountability and compliance with the goals and objectives of the Receiver Company's continuity planning program. The Service Provider's governance program should be audited regularly and the results should be monitored and signed off on by its senior executives. Also, the Service Provider should ensure that federal and state regulations are met and managed as they apply to its customers.
- Verify that a specific group or individual at the Service Provider is responsible for monitoring the company's compliance with Receiver Company business continuity goals and objectives and with all applicable federal and state regulations.
- Ensure that testing of continuity plans validates regulatory compliance and that test results are reported to the Receiver Company's compliance group or other appropriate individual(s).
- Review follow-up procedures for non-compliance issues and ensure that responsibility is assigned, remedies are identified, and reasonable target dates are established. Results should be used to update continuity plans.

#### 4.13.7 Insurance

- Ensure minimum liability insurance coverage is in place, consistent with the Receiver Company's standards.
- Obtain copies of any insurance policies, including liability, errors and omissions and business continuity/disaster recovery policies.
- The Receiver Company should review its own existing insurance terms to determine whether any policies are affected by the new Service Provider relationship.

---

## **SECTION 5: CONTRACTUAL, SERVICE-LEVEL, AND INSURANCE CONSIDERATIONS**

The considerations that follow are written from the financial institution perspective and are intended to provide a checklist of suggestions for possible incorporation in contracts. However, each contractual relationship between a financial institution and a service provider is unique and institutions should develop contracts consistent with their risk appetites and in the context of the business environment in which they operate.

Some high-level considerations that may affect an institution's contracting practices are the relationship with the service provider, the services to be provided (e.g., dedicated vs. shared environment), and whether a contract is being entered into with one or multiple service providers (i.e., single sourcing or multi-sourcing). Contract requirements may also vary depending on the type of application, system, or service being outsourced.

Where the service provider cannot, or will not, agree to critical considerations associated with controls, controls verification, insurance, and continuity planning, the financial institution should consider the need to implement appropriate alternative provisions and controls to manage the associated risk. It is important to fully understand the level of risk of the outsourced application or service when evaluating contractual, service level, and insurance considerations to ensure that the cost of the control processes does not exceed a reasonable risk/reward formula.

### **Service Level and Risk Review**

#### **5.1 Contractual and Service Level Considerations**

##### **5.1.1 Scope of Services**

5.1.1.1 Clearly articulate the services to be performed by the service provider on behalf of the financial institution, including:

- situations requiring recovery, recovery time objectives (how long to recover), recovery point objectives (how far back—to what point in processing—to recover, considering what information or transactions may have been lost), and the percentage of normal production volume that should be met while operating in recovery mode;
- the information-security role and responsibilities to be provided;
- the network, software, and hardware support services to be provided;
- the customer service support to be provided (including SLA considerations of hours of service, use of automated customer service, problem resolution times, guaranteed time for call-back, crisis communications plan);
- costs and compensation related to the provision of services and fees associated with the outsourced activity;
- the process and obligations required to add new services, modify current services, or combine multiple services;
- terms for contract renewal and termination;
- the financial institution's rights to make changes to services;

- 
- emerging technology considerations and provisions for replacing, reducing or adding services based on technology changes;
  - the timeframe for implementation of functionality of services; and
  - a baseline for performance standards and each party's responsibilities.
- 5.1.1.2 Clearly identify required service levels and performance standards as well as the consequences of and remedies for nonperformance. Consider including monetary penalties for failure to meet individual and aggregate service level agreements on a periodic basis (e.g., monthly, quarterly). Also consider establishing continued failures of service level requirements (both individual service failures and in the aggregate) as separate triggers for default (distinct from the general default for "breach of a material term of the agreement"), giving the financial institution the right to terminate the agreement immediately upon notice. As appropriate, also identify any of the financial institution's obligations related to meeting the service level agreements and any continuous improvement expectations. Define performance reporting requirements, required handoffs between the financial institution and the service provider, responsibilities for troubleshooting, and problem escalation. Document the requirements for:
- quality/customer service, such as:
    - accuracy,
    - customer satisfaction, and
    - acceptance of deliverables;
  - timeliness/responsiveness, such as:
    - on time delivery,
    - response time,
    - turnaround time,
    - implementation timeframes/time to market, and
    - problem resolution;
  - availability – percentage "up-time", hours of operation;
  - efficiencies – gained from improvements in technology;
  - scalability – transaction growth, storage needs, seasonal or promotional spikes; and
  - continuity – pre-event recovery strategy which includes the minimal threshold of performance for backup or alternate site processing.
- 5.1.1.3 It is important to note that some service level requirements cannot be fully defined until after contract implementation/conversion. Others should be improved over the term of the contract. Therefore, the contract should specify when these benchmarks would be established and reviewed. However, negotiation leverage is substantially decreased after the initial contract is signed, so every effort should be made to establish service level requirements prior to contract execution. Depending on the nature of the application, system, or service, the financial institution and the service provider may choose to create a performance-level plan

---

that defines milestones in the implementation process. Acceptance of milestones in the performance-level plan may in turn be tied to payment terms.

### 5.1.2 Change in Service Provider's Financial Soundness or Business Strategy

Failure of a service provider can compromise the financial institution's ability to conduct its business. The financial institution should include language relating to notification by the service provider of impending material changes to the service provider's operations or strategy. Consider incorporating provisions requiring notification to the financial institution in the event of:

- financial difficulty that may affect service, including loss of any significant customers or relevant complaints, litigation, liens, fines, or judgments;
- material change in tactical or strategic decisions regarding the provision of services or purchase and support of hardware or software related to processing performed on behalf of the financial institution;
- significant staffing reductions or changes in key staff that may affect the service provider's ability to provide the agreed-upon support and service;
- changes in staff licensing, gain or loss of regulatory certification, and participation in or withdrawal from alliances or other business partner arrangements;
- decisions to materially reduce core expertise in the area in which the services are being provided;
- changes in support responsibility and hours associated with the service provider's subcontractors; and
- service provider decisions to outsource, acquire, sell, or otherwise transfer operations or support associated with the services, applications, data, network, or other critical component of the environment used to provide services to the financial institution.

### 5.1.3 Environment

The financial institution should obtain a sound understanding of the service provider's environment at the time of the agreement. This understanding is critical to establishing a baseline for control implementation.

5.1.3.1 Physical Processing and Data Storage – It may be important in a dedicated service provider environment to document the locations, type, and serial numbers of equipment to be used in the processing and storage of financial institution programs and data. This allows the financial institution to determine whether controls tested on their processing are accurate. Notification of changes in equipment used may be required in some instances. If a separate processing and storage environment has been established for the financial institution, additional verification and documentation should be required.

*SLA Consideration:* Frequency or timing of notification when changes are made should be specified.

---

5.1.3.2 Logical Processing and Data Storage – Depending on the service being provided, logical storage and processing of financial institution applications and data may be physically or logically separate from that of other companies processed by the service provider. Where logical controls are used to separate processing and storage, minimum guidelines should be established to support an appropriate assurance that inadvertent access will be avoided.

*SLA Consideration:* Offsite storage hours of access and access capability, historical retention, and isolation of backup media from other customers' media should be specified.

5.1.3.3 Destruction of Intermediate Files – In instances where a shared storage or processing work area is authorized by the financial institution, proper due diligence should be followed to prevent the inadvertent disclosure of financial institution data. All work files created during the course of processing should reside on dedicated physical media, or full appropriate procedures should ensure proper erasure prior to media reuse. This should occur prior to the storage being released for or by the service provider.

5.1.3.4 Hardware – Equipment owned by the financial institution but located at the service provider's facility should be covered in contracts addressing equipment. Procedures for responsibilities during a disaster, including salvage and replacement responsibilities, should also be documented.

5.1.3.5 Software – To ensure that bugs have been identified and corrective measures applied for software and systems used in work performed for the financial institution, document the validity of all licenses for operating system and application software, as well as the database and storage systems, product names, version and release numbers. This information also is essential for restoring service in the event of a disaster and should be stored with recovery plans.

5.1.3.6 Internet Domain Names created by the service provider on behalf of the financial institution should be properly registered to protect the financial institution's reputation and brand identity. The agreement between the service provider and the financial institution should document ownership of the domain names.

5.1.3.7 Subcontracting by the service provider involving the financial institution's data, applications, and service or any reciprocal agreements with recovery providers may require the express permission of the financial institution.

The financial institution should be able to review and accept recovery plans for each subcontractor. The ultimate responsibility for the quality of all controls, including recovery, should rest with the contracted service provider.

5.1.3.8 Intellectual Property – Ownership of the system, its components, source code, processes, concepts, documentation, enhancements to the system, and related concepts should be clearly documented. Intellectual property rights should be explicitly delineated. If the service provider retains ownership over source code, escrow rights should be detailed and recovery procedures outlined.

5.1.3.9 System Controls – Financial institutions should require service providers to maintain according to industry standards all system controls associated with all platforms,

---

networks, or network interfaces used to process financial institution applications and data. Factors to consider include restoration, timely remediation of vulnerabilities and known bugs, and system recovery objectives that would limit exposure to errors or malicious activity.

#### 5.1.4 Confidentiality

The service provider should educate its personnel who support the processing relationship of the financial institution's confidentiality standards. The financial institution's information classification and handling requirements, as well as any personnel screening or confidentiality agreements required by financial institution policy should be clearly communicated to the service provider. Specific requirements may include the following:

5.1.4.1 Information Classification – The information and materials processed or stored by the service provider on behalf of the financial institution should be handled in accordance with both applicable laws and regulations (e.g., the Gramm-Leach Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), Fair and Accurate Credit Transactions Act (FACTA), Regulation P) and the service provider's standards and policies. This handling should meet or exceed the requirements of the financial institution's policies and standards as communicated to the service provider.

Media should be marked, if necessary, to identify highly confidential data and the capability of the service provider system to access production data. Development and other support personnel should be identified and expectations documented.

5.1.4.2 Limitations on Access and Use – The agreement should require the service provider to limit access to information to employees, officers, financial institution-approved subcontractors, and agents on a "need to know" basis and for the exclusive purpose of providing the services that the service provider has contracted to provide. Consider including provisions that require that the service provider permit their personnel access to confidential information only after both informing those personnel of the nature of the information and after obtaining from them a written agreement to protect the information.

5.1.4.3 Production Data Ownership – The agreements should clearly state that data are owned by the financial institution, including both data provided by or on behalf of the financial institution and that created as a result of service provider processing or other services.

5.1.4.4 Data Storage and Disposal – The agreement should clearly state the storage periods and disposal requirements for each type of data and each type of media on which the data may be stored.

5.1.4.5 Other Uses of Data – Use of data by the service provider for data mining or for any purpose other than the processing directly contracted by the financial institution should not be allowed without the express written permission of the authorized financial institution information owner.

5.1.4.6 Release of Service Provider User Information – Unless otherwise required or prohibited by law or regulation, the release of any service provider user information, such as access rights, should be made only to the appropriately authorized financial institution personnel, and authorization should be verified prior to any disclosure.

- 
- 5.1.4.7 Responsibilities – Responsibility for communication, authorization, and notification should be stated in the agreements and any supporting procedural guides.
  - 5.1.4.8 Encryption – The requirements for the use of encryption, the maintenance of any keys and concomitant infrastructure requirements should be clearly stated. and the requirements should include consideration of the entire end-to-end transaction and lifecycle (e.g., data/file origination, storage, retention, network path, backups, and recovery; key/certificate escrow and storage, exchange, revocation, supercession and replacement, and post-supercession retention; and security and audits of encryption or encrypted assets, processes, flows, and recovery). The requirements also should include provisions mandated by law and regulation, including state laws.

*SLA Considerations:* a.) Keys/certificates and their management; b.) data/files and their management; and c.) meeting security and audit requirements, e.g., protection, monitoring, and compromise.

- 5.1.4.9 Test Data – Production data should not be copied to the test environment unless appropriate masking is performed or appropriate controls are in place to prevent compromise of sensitive data.
- 5.1.4.10 Programs and Intellectual Property – Programs, data and written materials of the financial institution and service provider should be protected from unauthorized copy, use, duplication, and storage.
- 5.1.4.11 Injunctive Relief - Consider adding a provision that permits the financial institution to seek to enforce confidentiality provisions, in addition to all other remedies.
- 5.1.4.12 Publicity – Consider provisions prohibiting press releases or general use of the financial institution’s identity, including marks and domain names, without prior consent. Such provisions can help prevent brand dilution and avoid the impression that the financial institution supports, guarantees, or recommends the service provider.
- 5.1.4.13 Disclosure to Regulators – Regulated entities should add provisions permitting disclosure of any information in its possession, including confidential information of the service provider, in response to a request from any federal or state bank examiner, or other regulatory official having regulatory authority over the regulated entity.
- 5.1.4.14 Customer Preferences – If the service provider will have contact with customers of the financial institution, require the service provider to promptly notify the financial institution of any expressed customer preference regarding the financial institution’s marketing contact with the customer.

## 5.1.5 Access Administration

The financial institution should clearly define the processes for determining access requirements, requesting access, and granting access. These procedures should address access, whether physical or remote, to the financial institution’s network, data, or physical facilities.

- 5.1.5.1 File Access – Provisions for access to production data and programs for financial institution and service provider employees should be based on authorized job-related responsibilities. Information access privileges should be consistent with financial institution requirements for employee screening. Both the financial institution and

---

service provider are responsible to establish procedures to communicate changes in new or existing personnel that require adding, amending, or terminating access privileges. Individuals responsible for access authorization should be identified by the financial institution.

*SLA Consideration:* Establish guaranteed access implementation times from receipt of access request. Those times should be established for both standard operating conditions and for the mass changes required in a recovery scenario.

- 5.1.5.2 Record of Access – A record of all access requests and authorization should be maintained and used by authorized parties only to verify the work of the personnel implementing system access rights. These records should be retained in accordance with the financial institution record retention requirements.

*SLA Consideration:* The frequency of access reports and the response time for correcting access errors noted on access reports should be specified. Critical reporting elements associated with recovery efforts (e.g., temporary permissions, time and date of access, activity performed) should also be delineated prior to implementation.

- 5.1.5.3 Authorization Verification – A reasonable process should be maintained to validate that the “signature” associated with granting access is an authentic “signature” of the person designated by the financial institution to grant access.

Processes for emergency authorization and verification of signatures should be defined and incorporated into recovery plans.

- 5.1.5.4 Remote Access – Policies and controls for remote access to financial institution information and systems should be clearly defined, including:

- requirements for permissible mobile and telecommuting equipment (service provider, financial institution, or personally owned);
- minimum security requirement standards for permissible equipment (e.g., personal firewall software or hardware, virus protection software), their configurations, and patch levels;
- requirements for authentication mechanisms, including two-factor authentication where possible, to be used in conjunction with the permissible equipment; and
- isolation requirement for remote access equipment, in particular, requirements for copying software/data onto portable media and prohibition or control of “bridging” the permissible equipment with the financial institution network.

- 5.1.5.4 Maintenance Access – Financial institutions should implement policies, processes, and controls for allowing service provider to remotely conduct maintenance activities. Include the process of registering maintenance access procedures, identify who has this access, and audit the process to track access.

## 5.1.6 Security

The financial institution or service provider may be responsible for remediation costs where they fail to fulfill security obligations prior to the breach or other violation. In addition to relevant customer notice laws and regulations, consider the following when developing your requirements and processes for logging access and violations, monitoring timely changes to or deletion of expired access authorizations, and promptly archiving and reporting recent activities of personnel responsible for the violations or subject to the revocation of access.

---

5.1.6.1 Violation Monitoring and Reporting – Actual or attempted logon violations and access violations should be logged. These logs should be provided in a secure electronic format to an appropriately identified person within the financial institution for review and action. Include escalation, follow-up monitoring, and review procedures.

*SLA Consideration:* The SLA should include the frequency and format of reports being generated. The process for identifying serious violations, the time lag between violation and verbal notification to the financial institution, and any requirement for redundant notification (e.g., telephone, email, fax) based upon the severity of the violation should be specified.

5.1.6.2 Access History and Log Retention – Access history logs for critical application transactions should be generated, retained, and made accessible to appropriate financial institution personnel. A risk and cost analysis should determine the type of information detailed access records and audit logs retained, the duration of log retention, and follow-up monitoring and review procedures.

5.1.6.3 Penetration Attempts – The service provider should maintain the proper software, hardware, personnel, and other resources necessary to ascertain that a penetration attempt is being made against any part of the network or server facilities used by the service provider to process or transport financial institution information.

*SLA Consideration:* The time lag between identification and notification to the financial institution should be specified and tracked.

5.1.6.4 Access ID and Password Format – Where possible, the access ID, password format, or other access device (e.g., smartcard) should be consistent with the criteria set forth in financial institution policies. Considerations may include ID and password minimum characters, logging, suspension, and reset. All default access IDs should be removed or, at a minimum, have the passwords changed. Provisions for restoring access devices, suspending privileges, and resetting passwords in a business continuity setting should also be defined.

*SLA Consideration:* Response time to create, change, or delete ID and password requests should be specified.

5.1.6.5 Proper Separation of Duties – The service provider should ensure the same level of separation of duties as required by financial institution policies.

Separation of duties should be stated for security administration, access review, and violation reports when those responsibilities remain the responsibility of the service provider. There also should be separation between development and operations personnel, as well as other potentially conflicting roles.

5.1.6.6 Programs Written by the Financial Institution and Processed by a Service Provider – Programs written by, or expressly for, the financial institution should be certified as free of any malicious code and appropriate for the financial institution's intended purpose. They should also be protected from unauthorized copy, use, duplication, and storage. Asset management requirements should be specified.

5.1.6.7 Intrusion Detection Monitoring – The service provider should maintain intrusion detection in a manner consistent with risk analysis and which will identify both internal and external risks that could result in unauthorized disclosure, misuse, alteration, or

---

destruction of customer information or customer information systems. The service provider maintains operations and reports on its operation of system security software. This may include providing the financial institution with work flow diagrams, end-to-end sign-on and other process automation procedures and interfaces that enable compliance monitoring and support audit and reporting standards. The financial institution may request periodic reviews of the service provider's access controls with a focus on viability and appropriateness of security controls for both normal and recovery procedures.

*SLA Consideration:* The financial institution should be notified in the event an exposure exists which impacts the financial institution's business. Expected hours of monitoring should be identified, as well as restoration time for information that is lost or damaged. Additionally, responsibility and liability allocation considerations should encompass situations in which service is shut down due to a virus or other problem.

### 5.1.7 Vulnerability and Penetration Management

The financial institution should ensure that service providers have appropriate monitoring and response processes to identify vulnerabilities in the IT environment and are performing penetration testing at reasonable intervals. The service provider should provide the financial institution with any information that is required for the financial institution to understand and act upon any potential customer system or data compromise. Regulatory guidelines and examination procedures hold the financial institution responsible for ensuring that service providers provide sufficient reporting to allow the institution to appropriately evaluate the service provider's performance and security, both in ongoing operations and when malicious activity is suspected or known. Penetration simulations should be planned in advance and should occur during non-production time periods to avoid service level disruptions.

5.1.7.1 Vulnerability Scanning – service providers should identify known system vulnerabilities in a timely manner and as agreed upon at the outset of the engagement. In a shared environment the service provider may establish the resolution time frame in order to avoid multiple competing requirements from their clients. Vulnerability scanning should be performed on a regular basis and corrective action taken within an appropriate time frame. Financial institutions should also include follow-up monitoring and review procedures in their agreements.

The contract may require the service provider to monitor industry standard information channels (e.g., bugtraq, CERT, OEMs) for newly identified system vulnerabilities with respect to the technologies and services (e.g., application software, databases, servers, firewalls, routers and switches, hubs) provided to the financial institutions.

*SLA Consideration:* Responsibility, frequency, and timely notification of identified vulnerabilities should be specified. Also, based on risk level, an agreed-upon resolution time frame should be established.

5.1.7.2 Penetration Simulations – The financial institution should validate that the service provider periodically performs or contracts with an independent party to perform appropriate penetration simulations. The contract might specify annual penetration tests, testing when the service undergoes a major revision, or both. The specific

---

language may depend on the sensitivity of the relationship and the cyber posture of the service (e.g., web-facing vs. internal hosting). If the financial institution contracts with the service provider to engage an independent party, testing should be coordinated with the service provider and it should not result in system availability issues, missed SLAs, downtime, or customer dissatisfaction.

Should the financial institution make arrangements with the service provider to perform its own penetration tests, a separate contractual agreement should be signed between the parties that may specify the scope of the test, backup requirements, emergency communication channels, test windows, test participants, notified parties, restricted report distribution, tester account ID deletion, and executive sign-off (for both parties). Since the NDA between parties may not provide sufficient impetus to drive these discussion items, the financial institution should consider being prepared with its own standard language in the form of an addendum, statement-of-work, or other binding method. If the service provider does not directly manage the penetration simulation targets, then the standard language should require the service provider to own the communications with and obtain the approval of its own third party hosting provider, if applicable.

*SLA Consideration:* Frequency, depth of testing, and responsiveness of the service provider's mitigation efforts should be considered.

#### 5.1.8 Controls Verification

- 5.1.8.1 Independent Auditors or Shared Assessments Report – Based on the risk assessment of the services to be outsourced, an annual audit or assessment by an independent organization, including testing of controls, may be required. The scope of the report should include the environment used to process financial institution applications and data. Each of the control areas are defined in detail in the Shared Assessments documents (see Appendix 6 for more details on the Shared Assessment program).
- 5.1.8.2 Right to Audit – The financial institution should retain the right to audit in order to ensure that controls verification is performed as deemed necessary by the results of the financial institution's risk assessment. Current independent auditor or assessment reports should be considered as a source of verification. Mutually acceptable personnel or an independent third party should conduct such assessments, with advance notice and on a schedule that does not affect normal operations of the service provider. In a shared environment, these assessments may involve more than one financial institution and more than one process. The contract between the financial institution and the service provider should define what events or circumstances would trigger the audit as well as who will incur the cost of the audit. Contract terms should not preclude or limit rights of regulators, for regulatory examination purposes, to access records and information of a service provider or its subcontractors related to the services provided. The contract should state that the service provider will provide all assistance required for the financial institution to comply with regulator-imposed examination or audit requirements. Satisfying regulator requirements are non-negotiable provisions for financial institutions.

Internal or external audit results should be shared with the service provider, within a specific time frame after an audit is issued by the financial institution or its external

---

provider, to discuss and mutually determine audit items that may need resolution or to mutually develop plans and procedures to address any changes suggested by the audit.

5.1.8.3 Right to Audit in Subcontracting Situations – The financial institution may require the right to audit relative to contracts of the service provider with another service provider to support, store, recover, or otherwise handle the systems or data associated with the financial institution relationship, where such are not covered by relevant third-party review or other independent certification. Contract terms should not preclude or limit rights of regulators, for regulatory examination purposes, to access records and information of a service provider’s subcontractors related to the services provided. The contract should state that the service provider will provide all assistance required for the financial institution to comply with regulator-imposed examination or audit requirements, including examination or audit of services subcontracted by the service provider. Satisfying regulator requirements are non-negotiable provisions for financial institutions.

#### 5.1.9 Change Control

5.1.9.1 Production Changes – All production changes that could affect the processing schedule or integrity of the financial institution’s data should be communicated to the financial institution relationship manager or that individual’s backup. The financial institution should retain the right of approval on all production changes. The contract should specify the required number of days, or weeks, of advance notification to the financial institution.

5.1.9.2 Change Testing – All changes should be thoroughly tested in a test environment prior to implementation in a production environment. Testing should include user acceptance testing, especially in the event of changes to functionality such as calculations, automated notifications involving customers, control processes, and database structures. Depending on the agreements between the financial institution and the service provider and the risk involved with the changes, the financial institution may request the right to be involved in the testing. The financial institution should have the right to witness or accept certification that the testing has been performed. In a shared service provider environment, sufficient user acceptance testing should be performed to serve as a proxy for each affected financial institution.

5.1.9.3 Other Considerations – Depending on the type of service to be outsourced, the financial institution may want to consider additional production delivery elements (e.g., training and education, service delivery performance, capacity management).

#### 5.1.10 Records Retention

Records retention requirements vary among business operations. Communication of those requirements should be clearly documented to help ensure the appropriate offsite storage and recall capability of historical data. The financial institution may have the following types of retention needs:

- violation and transaction logs;
- access authorization and implementation;
- notification of control compromise; and

- 
- return or disposal requirements, subject to any requirements imposed on the service provider by law or regulation.

## 5.2 Disaster Recovery/Business Continuity Planning Requirements

The contracts governing the products or services delivered to the financial institution should include terms describing the recovery service levels to be delivered. Exclusion for continuity plans in *force majeure* clauses is advised. Contracts may also include provisions for financial institution participation in testing, delivery of continuity plans to the financial institution, service levels (as a percentage of normal production volume) while operating in recovery mode, and notification of the financial institution in the event of continuity plan activation. Financial institutions need to fully understand and document in an agreement with the service provider what specific services and response times will be required from the service provider in case of a disaster by the financial institution as well what services and response times a service provider needs to meet if they have a disaster. In any circumstance the financial institution should ensure only minimally disrupted services. By ensuring plans are fully documented and tested as needed, financial institutions can minimize their risks in this area.

In addition to the considerations listed under each subsection in this section, both parties should consider including the following in contracts and discussions:

- Establishing and maintaining policies and procedures relevant to contingency plans, recovery solutions and appropriate risk controls to ensure continued performance under the contract.
- Ensuring that recovery strategies and documented recovery plans (e.g., vital records protection, testing plans, testing frequency) cover all areas of operations necessary to deliver the contracted products or services.
- Obtaining from the service provider off-site backup plans for critical data, software, documentation, forms, and supplies.
- Addressing both short and long-term disruptions in facilities, environmental support and data-processing equipment. The possibility of total destruction of business operations should be considered.
- Continuing to provide service to the financial institution while the financial institution activates its contingency plan or moves to an interim site to conduct its business, including during tests of the financial institution's contingency operations plans.
- Providing to the financial institution, on a regular basis, copies of all contingency exercise final reports. The service provider should allow the financial institution to observe contingency testing.

Business continuity plans should also consider dependent service providers that are critical in delivering the products and services to the financial institution. The service provider must be responsible for ensuring the validity of its downstream providers' recovery solutions.

### 5.2.1 Risk Analysis

- The contract should include a provision requiring a documented risk analysis.
- The financial institution and service provider should review the risk analysis regularly and evaluate requirements based on changes in the outsourced service.

---

### 5.2.2 Recovery Objectives

- The recovery objectives should reflect the considerations and service level metrics outlined in the RFP.
- Backup – The data backup schedule and requirements should reflect the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) of the financial institution, particularly with respect to critical data. Some data may require simultaneous processing by geographically separated centers and networks or real-time offsite data mirroring, while other data may require only a daily offsite rotation.
- Offsite Storage – Backup storage media should be sent to an offsite location on a scheduled rotation and with a defined retention period. Transmittal records of this movement should be stored at both onsite and alternate locations. Backup media should be secured before being transported and remain secured until they are returned to the primary site. Reasonable distance between the primary and offsite location should exist to mitigate the risk of one event disabling both facilities.
- Equipment Recovery – Detailed information on recovering installed equipment for salvage operations at the service provider site should be stored with recovery plans in an accessible, but secure, location.
- Recovery Prioritization – The order in which the service provider will recover processes and systems should be based on the recovery objectives defined by the financial institution. This information should be available to the financial institution and the financial institution should be notified of any changes to this prioritization before the service provider makes the change. Often contracts will state that in the case of a large regional or national disaster, recovery services are based on a first come, first served basis. If this is the case, the financial institution's disaster recovery team needs to be aware of this and place a call to the disaster recovery service provider as soon as possible, once it has been determined that disaster recovery services will be needed.

### 5.2.3 Plans

The contract should require evidence of a written plan and include requirements for updating the plan. Requirements may be driven by time, service, or environmental considerations.

The service provider should provide the financial institution with proof of business continuity plans that address any outage that would affect the service provider's ability to provide the contracted service to the financial institution. The plans should include defined strategies for standby and work-around procedures, and for addressing production failures, facility shutdowns, personnel shortages or reduced staff, supply-chain issues, affects on customers and work backlog. Procedures for returning to normal operations should also be included.

### 5.2.4 Testing

- Joint disaster recovery and business continuity plan testing should be conducted periodically. Testing should include all scenarios that could potentially cause an unacceptable interruption to production information processing. Within thirty days of testing, the financial institution should receive a report with all test and exercise documentation, including results of testing the financial institution's processes and technologies.

- 
- The frequency of technology and business recovery testing, as well as expectations regarding financial institution participation in those tests, should be specified and made available prior to the test.
  - The financial institution should identify requirements for accessing the recovery location.

#### 5.2.5 Event Management

The service provider should have a process for managing both minor and major disruptions to delivery of the contracted services or products. The service provider should regularly report activity related to disruption-management testing, activation, and issue resolution to the financial institution. Additionally, a documented process should exist to ensure that notification and escalation lists and procedures remain current. Procedures for contacting the financial institution during holidays and outside of normal business hours should also be documented.

- Emergency Notification – In the event of a disaster or other emergency that affects the processing schedules, an emergency notification schedule should follow.
  - *SLA Consideration:* The minimum and maximum recovery time frames associated with a service provider’s environment, minimum and maximum time to data integrity validation, and minimum and maximum time that the receiver company would be unable to perform production tasks should all be stated. Such schedules should consider the federal, state, and local requirements pertinent to emergencies such as those related to power, transportation or environment.
- Computer Forensics – If forensic tests must be conducted to determine the cause of an application, system, or service failure, the service provider should follow appropriate evidence-handling procedures.

#### 5.2.6 Governance

- Statements documenting compliance with applicable government regulations are required.
- No provision in the contract, in particular any *force majeure* terms, should remove the service provider’s obligation to provide recovery services at the required service levels.
- Failure to comply with any of the recovery terms in the contract should be referred to adequate remedies or termination terms of the contract.

#### 5.2.7 Insurance

The contract should include a requirement for proof of insurance (Insurance Certificate). (See Section 5.5.)

#### 5.2.8 Regulatory Resources

For further details and a comprehensive discussion on each subject area addressed in this Section (5.2), review the Federal Financial Institution’s Examination Council (FFIEC) Information Technology (IT) Handbook on Business Continuity planning, issued in March 2008.

### 5.3 Compliance with Regulatory and Financial Institution Policies

---

### 5.3.1 Financial Institution Policies

The financial institution should provide the service provider copies of all relevant policies impacting the service that will be provided. This can be done as an attachment to the contract or as part of the ongoing vendor governance process.

### 5.3.2 Service Provider Policies

The service provider must provide copies of their security and other policies and standards that support the financial institution's relevant policies and procedures and in addition support all relevant statutory and regulatory requirements.

### 5.3.3 Financial Institution Review

The financial institution should review the service provider's policies and standards to ensure they are acceptable, appropriate, and consistent with internal policies and standards.

### 5.3.4 Service Provider Compliance

The service provider should provide written evidence to ensure that relevant statutory, regulatory, and contractual requirements are documented and kept up to date for each information system within their organization that relates to or affects the products or services being provided under the agreement.

### 5.3.5 Regulatory Compliance

The service provider should adhere to applicable legal and regulatory requirements, especially as they pertain to security, privacy, and handling of customer information, including applicable state laws. This includes requirements that apply in all processing locations. Further, contracts should require the service provider to comply with laws and regulations, and to assist the financial institution in doing so. Assistance may include providing the financial institution with the information necessary to be audited for its privacy statement and policy, as well as providing information for regulatory reports or IT examinations. Contracts should require service providers to periodically review and update controls to comply with current and future regulatory guidelines. Regulators expect that a financial institution will not share any nonpublic information of the regulators, such as an examination report or the existence of an examination, with a service provider except with express approval of the regulators. Accordingly, if applicable, the contract should provide that no such information will be shared with a service provider without the regulator's express prior approval (See Federal Reserve Board Supervisory Letter SR 07-19.).

### 5.3.6 Regulatory Resources

- OTS – Thrift Bulletin 82a: Third Party Arrangements
- SEC - 17 CFR Part 248: Privacy of Consumer Financial Information and Safeguarding Personal Information
- FDIC - FIL-81-2000: Risk Management of Technology Outsourcing
- FDIC - FIL-9968a: Risk Assessment Tools and Practices for Information System Security
- GLBA - Title V: Privacy SEC 501(b)

- 
- FFIEC - Publication: Risk Management of Outsourced Technology Services

## 5.4 Termination Fees and Strategies

Contracts are terminated for a variety of reasons, both planned and unplanned. Common termination reasons include contract expiration, change in strategic objectives, or failure to perform. A strategy upon termination, or an “exit strategy” helps identify possible risks, defines potential losses, and ensures continuity of services. With an exit strategy in hand at the outset of a service provider relationship, the financial institution’s needs are incorporated into the contract, ensuring minimum business and customer disruption in the event that the relationship is terminated.

Termination clauses should include details on any related termination fees and responsibilities of the service provider and the financial institution in the event of early termination, whether planned or unplanned.

5.4.1 Termination terms and conditions need to be clearly defined and should provide flexibility. A contract should include four forms of termination:

- Normal termination – A specified expiration of contract at the end of the term or non-renewal (usually with prior notice) at the end of the term.
- Termination for cause – Permits the financial institution to exit from the contract when identified problems are not resolved in the required time frame, including failure to perform or failure to meet SLAs, quality standards or other contract requirements. In failure to perform, performance measures are critical to assessing the service provider’s record of performance. Performance measure reports should be provided on an agreed-upon basis and reviewed against the minimum requirements as described in the SLA. Failure to meet those requirements may be the basis for negotiated restitution based on the contract.
- Termination for convenience – Permits cancellation at will, though there may be financial liability on the part of the party terminating the agreement. The contract should specify termination fees as well as the service provider and financial institution responsibilities in the event the termination for convenience clause is executed.
- Termination for regulatory/supervisory requirements - Permits cancellation or modification of a contract if required by regulators or changes in regulations, guidelines, or law. Examples include but are not limited to:
  - The OCC 2001-47 requirement that “the contract should include a provision that enables the bank to terminate the contract, upon reasonable notice and without penalty, in the event that the OCC formally objects to the particular third-party arrangement.”
  - USA PATRIOT Act Termination, which requires termination if a service provider/supplier shows up on the OFAC list. This reason for terminating a contract was enacted by Congress to stop the flow of money going to organizations that are a threat to US security or are involved with money laundering with known terrorist organizations.

---

#### 5.4.2 Ongoing Service Requirements

An exit strategy should set forth the financial institution's service requirements for the period during which the parties are transitioning out of the relationship (the "transition" or "wind-down period"). These requirements may include:

- An obligation by the service provider to continue performing the services at the same level for the transition period and to continue to comply with all contractual obligations.
- A provision that the service provider give all work product and code to the financial institution at regular intervals during the transition period.
- Specifications for consulting at a reduced hourly rate, upon request.
- Requirements for the provision of parallel services for a certain period, with the right to extend the term as necessary to resolve issues before the final cutover.
- An obligation by the service provider to keep the same service provider team performing services during the transition period.
- Confidentiality on any communications regarding the termination of the relationship.

#### 5.4.3 Data Security and Privacy

Data security and privacy are critical. The exit strategy should consider these issues carefully, including:

- Providing for the immediate transfer of all data that belongs to the financial institution, including customer information.
- Determining an acceptable method by which the service provider will destroy and remove the financial institution's proprietary information, including information about the system, operations, and business. The exit strategy should identify how the service provider will destroy and remove this sensitive information from all media, ensuring it is not disclosed to other individuals or organizations.
- Recovering and terminating any sublicenses to third-party software and technology, and all financial institution technology licensed to the service provider.
- Taking custody of any tangible property (e.g., PCs, servers, network equipment) provided to the service provider.
- Determining responsibility for compliance with import/export regulations when making final transfers of data and technology.
- Documenting any issues related to intellectual property transfers or protection assistance.

#### 5.4.4 Documentation and Knowledge Transfer

Rigorous documentation and knowledge transfer requirements in the contract will pay dividends when the relationship ends. Be sure to:

- Secure the right to buy the assets, license the software, and assume the subcontracts used by the service provider to perform the services.
- Require the service provider to give you access to everything your company will need to maintain service.

- 
- Clearly delineate which party owns the work performed by the service provider and which party is responsible for solidifying the transfer of ownership.
  - Fully document the service description for any additional services of the service provider during the transition period (e.g., training your employees or training new service provider personnel).
  - Require the service provider to supply a full inventory, architecture, and configuration of servers, routers, and other hardware and software involved in service delivery, along with supporting documentation.
  - Require the service provider to supply your company with copies of data, procedures, access logs, error logs, documentation, and other information that the service provider generates as a part of providing the services. The service provider should also grant your company the right to provide this information to potential successor service providers.

#### 5.4.5 Costs

Transition, termination, and timing are a key part of the financial aspects of an exit strategy. Be sure the contract:

- Will not penalize your institution for an early exit, especially if the termination is due to the service provider's failure to perform adequately.
- Specifies when compensation should be paid and how much, including compensation for any continuing base services and transition activities. For example, payment for transition services may be made at different milestones of the transition or when the transition has been completed successfully. In either case, there may be a monetary bonus to the service provider when the transition services are completed successfully.
- Specifies the return of any pre-paid fees for which services have not been rendered.
- Tailors the compensation arrangement for the transition period in such a way to motivate the service provider to perform.

#### 5.4.6 Personnel

An exit strategy should cover personnel issues, such as:

- The institution's right to hire service provider employees who perform services for you. This may take the form of a waiver of a contract's non-solicitation clause in certain circumstances, such as termination for cause or bankruptcy.
- Ensuring that service provider personnel and key resources with relevant knowledge and expertise remain on the project and committed during the transition.
- Define the exit-strategy team and its roles, including identifying any situations that should be rehearsed.

Of course, some issues are unforeseeable, so it is a good idea to include an all-encompassing clause. For example, "Service provider shall provide such transition assistance as reasonably requested by Customer." Being both strict and generous in the exit strategy ensures your service provider is motivated to perform. As with all components of managing an outsourcing relationship, review your exit strategy periodically to ensure it meets your needs and the needs of the evolving business relationship.

---

## 5.5 Insurance Considerations

Insurance coverage should include the following considerations as factors in evidence and maintenance of proper insurance.

5.5.1 When outsourcing IT activities, the financial institution should make sure that specific insurance protections are met according to the financial institution's requirements. The contract should define which party is responsible for each type of insurance coverage and the required amount of coverage. The financial institution should give consideration to the relationship with the service provider and the service to be provided (e.g., dedicated vs. shared environment) when reviewing the considerations listed below. Whenever possible, the financial institution should be named as an additional insured on applicable service provider policies that address loss, damage, and liability for the outsourced activity, data, and transactions. Insurance provisions vary from company to company and state to state.

Policies should be compared, and state liabilities and restrictions of liability associated with insurance matters should be confirmed, to support the agreement reached in the contract.

The service provider should maintain a level of insurance in accordance with all insurance categories agreed upon, and specifically noted, within the contract. As most insurance policies are renewed annually, the financial institution should request annual updates for coverages required in the agreement. The contract should request a Certificate of Insurance. In addition, the service provider should provide notice to the financial institution of any insurance changes, including if any insurance that affects the applications, system, or service maintained by the service provider and provided to the financial institution is modified, canceled or not renewed, or if the rating of the insurance company providing the insurance changes.

Coverage should be in place whether or not the service provider's employees are on site at the financial institution's premises. In addition, the financial institution should consider how it will address the review and acceptance of insurance coverages carried by dependent providers, independent contractors, subconsultants, and subcontractors of the service providers for work done by or on behalf of the financial institution.

A financial institution's insurance coverage should also be reviewed and understood to make sure that a financial institution's insurance policy is adequate for the types and levels of service being provided by service providers.

To better understand insurance coverage, it is advisable to list all types of possible losses that could occur based on the services the service provider has contracted to provide. It is also suggested to ask the service provider to address how they would handle insurance for the possible losses the financial institution could sustain during the course of the contract/agreement.

5.5.2 The following insurance should be considered in addition to the service provider's property, casualty, and fire insurance, based upon the financial institution's own business coverage and the potential impact of outsourcing. Not all coverages will be needed in every contract, and many of the coverages mentioned can be incorporated within one policy.

5.5.2.1 Media Replacement/Reconstruction – Coverage should be considered for protection in the event that physical media containing the application or data is lost, corrupted, or damaged in some manner.

- 
- 5.5.2.2 Extra Expense (reimbursement coverage) – Coverage should be considered for protection in the event that recovery expenditures in relation to the contract exceed agreed-upon levels.
  - 5.5.2.3 Business Interruption – Coverage should be considered for protection in the event that normal business operations are disrupted due to system or application failure. Service level requirements for availability should be defined, and financial losses due to disruption of services should be estimated.
  - 5.5.2.4 Errors and Omissions (E&O) – Coverage should be considered for protection in the event that the technology or services provided contain errors or omissions that would lead to missed deadlines, improper functioning of the system, or other errors that would affect the success of the defined strategic business objectives. It is also advisable when E&O coverage is required, that the financial institution request evidence of such coverage for a period after the termination of the agreement.
  - 5.5.2.5 Media Transit – Coverage should be considered for protection in the event that loss, theft, or damage occurs during the physical shipment of media. Resulting losses could include service disruption, compromise of data integrity, or compromise of privacy data.
  - 5.5.2.6 Electronic Transmission – Coverage should be considered for protection in the event that loss, theft, or damage occurs during the electronic transmission of data. This includes transmission over internal networks, extranets, dedicated links, or the Internet.
  - 5.5.2.7 Computer Crime – Coverage should be considered for protection against losses due to the malfunction, disablement, or impairment of a service or system, where forensic evidence demonstrates these losses are due to illegal computer-based activities by third parties or unauthorized insiders. Such losses indicate victimization by computer crime, even without the identification and conviction of a perpetrator. Such crimes often induce or exploit service disruption and involve the compromise of data integrity, defacement of web pages, or abuse of systems as “zombie” launching pads for attacks against other sites.
  - 5.5.2.8 Customer Information Privacy Liability – Coverage should be considered for protection in the event that the privacy of customer information is compromised in any way.
  - 5.5.2.9 Reputational Risk – Coverage should be considered for protection against loss incurred due to publicity in relation to a computer security attack or other technology-related interruption of service.
  - 5.5.2.10 Vicarious Liability and Supervision – Provision should be considered for vicarious liability and for supervision over the service provider.
  - 5.5.2.11 Blanket Fidelity – Consideration should be given to a bond to insure against dishonest acts of employees if the service provider’s employees come into contact with the financial institution’s cash or customer information. In order for the fidelity bond to insure against the service provider’s employees stealing from the financial institution, there has to be an endorsement to cover “client’s property” (financial institution’s property).

- 
- 5.5.2.12 General and Umbrella Liability – Consideration should be given to coverage against third-party liability, contractual accepted liability, or product liability in a situation that resulted in bodily injury or property damage or personal injury allegedly by a third party as a result of their involvement on the service provider’s premises or in relationship to its business. Umbrella liability is in excess of general liability, thereby providing for higher limits than under general and other insurance coverages.
  - 5.5.2.13 Worker’s Compensation – The financial institution should seek evidence that the service provider, its affiliates, agents and assigns maintain through the term of the agreement valid workers compensation coverage in accordance with the laws in the states in which the service provider, its affiliates, agents, and assigns have operations.
  - 5.5.2.14 Automobile Liability – Coverage should be considered for auto-related situations when a vehicle or driver is involved in an incident in the performance of job responsibilities, including driving onto the premises of the financial institution, and it is alleged that the driver is responsible for bodily injury or property damage.

## 5.6 Offshore Services

In general, if services are being provided by a service provider from a location outside of the United States, the laws and regulations of that foreign country will be applicable to such services. It is critical to understand the foreign laws and regulations that are applicable to the offshore services arrangement and apply them to the drafting and negotiation of the particular offshore services contract. Legal counsel by an expert in the laws of the applicable foreign jurisdiction should be obtained to advise the financial institution regarding legal and regulatory issues related to the offshore services and service provider, contract provisions necessary to comply with foreign laws and regulations, and enforceability of the contract.

In addition, consider the following issues specific to offshore services contracts:

- 5.6.1 Prohibition on Providing Offshore Services Outside of the Authorized Foreign Country: In order to avoid issues from further foreign offshoring of services, the contract should prohibit the service provider from providing services from anywhere other than at the specific physical location outside of the United States where offshore services, or portions of offshore services, are to be performed. Similarly, the service provider should be prohibited from subcontracting any portion of the offshore services without the express prior written consent of the financial institution. Consider requiring the cost of any site visits to the subcontractor’s location outside the United States that are required by the financial institution to be funded by the service provider.
- 5.6.2 Audit Rights: Consider specifying the financial institution’s right to audit the service provider’s location in the applicable foreign locations, and the obligation of the service provider to comply with regulator requests for all information related to the offshore services to be made available promptly upon request and in English. Consider provisions allocating the costs of such audits, e.g., at service provider expense if the audit is required due to a failure of the service provider to materially comply with the terms of the service agreement or applicable law or regulation.
- 5.6.3 Compliance with Laws and Treaties: Consider adding a representation and warranty that the service provider personnel will comply with all applicable laws and treaties in connection with its performance under the services agreement, including without limitation, applicable permits

---

and licenses related to export, re-export, or transfer, whether direct or indirect, in any jurisdiction as may be required in connection with providing the offshore services.

- 5.6.4 Mandated Changes Pursuant to Laws and Treaties: Consider adding a provision which requires that, if any provision of law or treaty requires the financial institution to adopt specific standards with respect to its service providers which relate to the offshore services or the service provider's methods of doing business, the service provider will modify the offshore services, or the service provider's methods of doing business, as required to enable the financial institution to comply with such laws or treaties.
- 5.6.5 Language; Official Version of the Contract: In order to satisfy regulatory audit requirements, consider adding provisions which require the offshore services provider to agree that the contract and all documents related to the offshore services be maintained in English. In some countries, such as China, official versions of the contract are maintained in the language of both countries. The versions may not match, so to avoid the risk of any ambiguity, the parties should specify that the English language version of the contract will control.
- 5.6.6 Governing Law and Venue: Consider adding a provision whereby the service provider waives the application of the laws of the foreign jurisdiction to any dispute and consents to the laws and venue of the jurisdiction designated in the contract (as selected by the financial institution with advice of foreign law legal counsel).
- 5.6.7 Dispute Resolution: Despite selection of governing law and venue, some foreign courts may assert jurisdiction in the courts of foreign country. Seek advice from foreign law legal counsel and consider adding alternative dispute resolution provisions, including arbitration. The dispute may be resolved more expeditiously via arbitration than via the court system, and may be more easily enforced in the foreign country.
- 5.6.8 Foreign Corrupt Practices Act: If the offshore services involve a foreign government official or employee, political party or official, or candidate, or an enterprise in which there is significant foreign government ownership or control, consider adding a representation and warranty that service provider personnel are in compliance with the Foreign Corrupt Practices Act ("FCPA"). Note that the Department of Justice takes an expansive view of what constitutes government ownership or control of a legal entity for FCPA purposes. Each country's laws and customs may vary as to what constitutes ownership of or control over a legal entity. Consult with foreign law legal counsel to determine whether the FCPA is applicable to the specific offshore services and to draft appropriate contract provisions.
- 5.6.9 Other Issues: Consult with foreign law legal counsel to identify and address other issues which may apply to the specific offshore services, such as intellectual property rights, data protection requirements, and employee background checks.

---

## **SECTION 6: PROCEDURES FOR SUPPORTING SPECIFIC CONTROLS, REQUIREMENTS, AND RESPONSIBILITIES**

Outsourcing IT services does not relieve Receiver Company management of responsibility to ensure the design, management, implementation, and execution of appropriate controls, including security and recovery of the outsourced processes and procedures. Therefore, it is not appropriate to entrust these activities solely to the Service Provider. Section 6 provides guidance in the design, development, and implementation of control processes in an outsourced environment. The controls may vary based on the specific Service Provider relationship, the service to be outsourced (e.g., dedicated versus shared environment) and, risk/business impact assessment results, and they should be clearly documented in the Services Provider's information-security/recovery strategy. The specific roles of the Service Provider and the Receiver Company should be defined and included in the outsourcing agreement. Such documentation is required to ensure the sufficiency of controls in protecting the privacy, and integrity security and recoverability of the systems and data covered under the outsourcing agreement. It is important to fully understand the level of risk of the outsourced application or service when documenting this information to ensure that the cost of the control processes does not exceed a reasonable risk/reward formula.

### **Documenting the Controls for Processes**

6.1 **Access Control** – Document the control procedures to help ensure that only personnel associated with authorized use and/or support of the system have access to the operating system, application, and databases to be used in the services provided, during both normal and recovery operations. Controls should apply to both Service Provider and Receiver Company, should specify which uses of the system are authorized and which are prohibited (e.g., unacceptable hardware and software installations), should establish an access request process and an access review process, and should be consistent with control processes in the Receiver Company's own information security program, as follows:

6.1.1 The access request process should include:

- access levels for users of the system or services;
- access level control schema defining the protection requirements of each information service, system, subsystem, and resource;
- access levels for development and support of system or services including specific access controls where appropriate;
- method of access and authorization process for maintenance access;
- access request process flow;
- access levels for recovery/resumption;
- physical access during recovery scenarios;
- format of the mechanism to be used to request the addition of an access ID;
- approval authority for access ID requests (approval may be required from the Receiver Company and/or the Service Provider);
- responsibility (Receiver Company or Service Provider) for implementation and maintenance of access IDs; and

- 
- validation of the “authorized signature”.

6.1.2 The access review validation should describe:

- responsibility for creation and maintenance of the access authorization list;
- responsibility for review and approval of the access authorization list;
- frequency review of the access authorization list;
- control processes to ensure timely change or deletion of access upon employee transfer and/or termination;
- record-keeping requirements for access requests, including retention of access request forms for IDs, as well as transaction and data access requests; and
- a process for performing timely validation of access request changes through review of changes made in comparison to changes requested.

Note: All review validation points should be considered for both normal daily operations as well as during recovery/resumption efforts.

6.1.3 User Access Logging. Outsourced systems should provide some form of user access logging that records files accessed, parameter changes, transactions processed, user ID, time, and date. Logs should be maintained in a secure library and kept for a reasonable period of time. The Service Provider agreement should indicate how these logs are stored and who has access to them.

6.2 **Technology Detection Control** – Document technology control procedures for daily operations and recovery/resumption efforts. The procedures are necessary to prevent and detect unauthorized use or alteration during data creation, transfer, and storage. The following are examples of key procedures which should be considered:

- encryption requirements for both data transfer and storage;
- use of hash totals or other automated application-level control;
- requirements for initial and ongoing verification that data stored on Service Provider equipment is appropriately segregated from data of other companies;
- activities to be logged, considering performance impact;
- audit trail preservation and protection from tampering;
- reports necessary for violation monitoring;
- responsibility for monitoring reports;
- retention requirements for audit trail files, reports, and follow-up activity; and
- the overall process for violation monitoring, follow-up, and record keeping.

6.3 **Exception Reporting** – Document exception report handling and follow-up procedures to include daily operations and recovery/resumption efforts for incidents and/or suspicious activities, such as the following:

- exception-reporting requirements such as changes in average file size, transaction amounts, and the number of transactions;

- 
- notification requirements for exceptions or incidents (whom to notify, how to notify, at what point notification should occur);
  - frequency of reports;
  - formulated response scenarios for defined exceptions and/or incidents;
  - composition of incident response teams, including Receiver Company and Service Provider representatives;
  - post-mortem documentation requirements;
  - responsibility for validation that the exception or incident has been corrected; and
  - responsibility for filing of suspicious-activity reports to regulators.

6.4 **Technology Control Procedures** – Define technology control procedures for daily operations and recovery/resumption efforts necessary to ensure adequate network control, incident identification, and incident response, including the following:

- tools required to protect systems from attacks both internally and externally (firewalls, physical segregation from unrelated internal LANs, intrusion detection systems, etc.);
- requirements for regular, independent vulnerability testing against the network;
- responsibility for identification of vulnerabilities and application of “fixes”; and
- requirements for real-time monitoring, such as intrusion detection; and response scenarios for network incidents.

### **Documenting the Controls for Systems**

6.5 **Network Control Procedures** – Define technology control procedures necessary to maintain confidentiality along the end-to-end transaction path, both for daily operations and recovery/resumption efforts such as the following:

- identification and ongoing inventory maintenance of all systems, servers, and network path components that will house or process confidential or sensitive data;
- encryption requirements of data stored and moved along the network including the link between the Receiver Company and the Service Provider and any other business partners;
- encryption and data-protection requirements for data stored on various devices, backup tapes, and other media;
- identification and authentication requirements for login process; and
- access control and authentication requirements (e.g., password length, password expiration, number of invalid login attempts allowed, password strength, and additional authentication requirements such as certificates).

6.6 **Physical Access Control** – Define or validate control procedures necessary for daily operations and recovery/resumption efforts to restrict physical access to sensitive devices to be implemented at Service Provider locations, for example:

- identification and authentication of individuals at the Service Provider who have access to the physical resources;
- definition of processes for requesting and approving physical access;
- definition of security and maintenance requirements for transaction and user access logs;

- 
- definition of physical control requirements (lock and key, cameras, electronic access badge, biometric controls, etc.);
  - determination of whether the physical resources are dedicated to the Receiver Company or shared by multiple receiver companies;
  - determination of how resources are physically and securely segregated from the Service Provider resources or other Receiver Company resources; and
  - definition of control requirements for remote administration capabilities of physical resources.

## 6.7 Disaster Recovery/Business Continuity Requirements

- 6.7.1 Risk Analysis: Verify that mitigation efforts are maintained for the risks identified in the risk analysis reports.
- 6.7.2 Recovery Objectives: Verify that risk analysis information (BIA reports, RTO/RPO listings) is used to update disaster recovery and business continuity plans.
- 6.7.3 Plans: Verify that controls are in place for the storage and handling plans, including records management and offsite storage.
- 6.7.4 Tests: Validate security procedures are in place for handling receiver company data and telecommunications during test exercises.
- 6.7.5 Event Management: Validate disaster declaration authority and notification lists.
- 6.7.6 Governance:
  - Validate control procedures for maintaining system integrity and recovery.
  - Validate control procedures for data retention.
  - Validate control procedures for data backup and offsite storage.
- 6.7.7 Insurance: Verify that insurance coverage is maintained as systems, services, locations and other aspects of the business change.

---

## SECTION 7: IMPLEMENTATION AND CONVERSION PLAN

Section 7 highlights transition-planning issues in the period between the execution of an outsourcing agreement and the full production use of the outsourced services. This interim phase can be referred to as the implementation phase. In the case of a new product, there may be no conversion, but for moving an existing application, system or service to a Service Provider, conversion is often the primary activity in the implementation.

The implementation phase can be the most challenging and highest-risk period in the lifecycle of an outsourcing relationship. An implementation that is not well planned and managed may result in overall failure, customer inconvenience and dissatisfaction, a strained relationship or unexpected operational support costs. The risks of an unsuccessful implementation are best mitigated by definition and execution of a detailed, agreed-upon implementation project plan involving resources of both Receiver Company and Service Provider, a performance level plan which will define milestone dates and resources required to fully implement the application, system or service, and a transition plan in the event that the contract is not fully implemented. Each party should have a designated representative or “project executive” with overall responsibility for that party’s activities during the implementation. The implementation project plan should document milestones and deliverables, as well as a clear assignment of responsibilities. The implementation project plan may include an estimate or a cap on the cost for the services of the Service Provider to the Receiver Company during the implementation period.

Implementation requirements may vary depending on the degree of difficulty of implementation, the level of risk in the outsourced application, system or service, the degree of customer interface, and the impact on existing products or services.

### 7.1 Pre-Implementation

Before implementation begins, the Service Provider and Receiver Company should:

- document and validate roles, responsibilities, and persons assigned to the Receiver Company, Service Provider and any dependent or third parties involved;
- create an interface development plan, including scope and definitions;
- develop a technical infrastructure design, procurement, and implementation plan;
- define application system modifications;
- identify and define vendor or third parties’ roles;
- develop and test the rollout strategy and create a timeline;
- inform relevant organizations of the timeline and milestones;
- identify parties responsible for operational functions associated with implementation, and confirm that the Service Provider can perform the operational functions associated with implementation;
- confirm that responsible parties will be able to supply the support needed during the pre-implementation and post-implementation phases and be sure the Service Provider has and understands hardcopy and electronic records (customer files, work in progress, contract files, etc.) for future research purposes;
- have signed acceptance from both parties on documentation (both paper and electronic) for all phases of the project;

- 
- define metrics, such as a dashboard, scorecard or financial metrics, for measuring performance during implantation and its success;
  - verify or audit assets being transferred to Service Provider (e.g., software, hardware, copiers, PCs, etc.) and signed records for tracking (may also include documentation, records and proprietary information);
  - identify critical issues and a mock or pilot plan to resolve them prior to “live” implementation;
  - review capacity planning, including evaluation of tolerance limits on processing, storage, network transport, etc. and operational/staffing capacity;
  - develop a communication strategy and plan for notifying associated vendors, subcontractors and third parties to confirm requirements, contracts, terminations, etc; and
  - agree to a cap on implementation cost for the Service Provider’s services to the Receiver Company; and
  - develop appropriate contingency plan(s) and an exit strategy in the event the Service Provider fails to implement and/or provide service.

## 7.2 Implementation Phase

7.2.1 Depending on the components of the pre-implementation phase, the implementation phase may include activities such as:

- planning and resource allocation. Resources should be identified prior to any implementation for software or hardware projects;
- technical infrastructure procurement and installation;
- application system modifications;
- interface development;
- conversion of data (e.g., customer, account, transaction) from a previous application system or Service Provider;
- documentation creation (see Section 6, above);
- training; and
- user acceptance testing.

7.2.2 Elements of the implementation, which are important from a risk management perspective, include:

- verification of control procedures;
- verification of security infrastructure and controls;
- verification of functionality through user acceptance testing;
- verification of the accuracy of customer data being converted;
- verification of the accuracy of systems interfaces;
- verification of the backup and recovery procedures;
- verification of adequate training of user personnel;
- verification of the implementation of all contracted terms;

- 
- verification of any software development activity (customization, enhancements) related to the implementation; and
  - requirements definition (an updated version of the requirements listed in the RFP and in the due diligence process), management, and change control. This should be monitored in the control plan, but this should be done prior to implementation.

### **7.3 Disaster Recovery/Business Continuity Requirements**

#### **7.3.1 Risk Analysis**

The Receiver Company should expect to maintain its existing disaster recovery and business continuity plans and resources until after verification that the Service Provider is fully operational. The risk analysis should include:

- verification of backup and recovery procedures;
- development of an appropriate contingency plan and exit strategy in the event the Service Provider fails to implement;
- verification of an appropriate emergency communications plan;
- verification of control procedures;
- verification of contingency plan and exit procedures for conversions; and
- verification of proper planning and testing of all implementations or conversions prior to implementation date.

#### **7.3.2 Plans**

The Receiver Company should verify that the Service Provider is documenting appropriate disaster recovery and business continuity plans.

#### **7.3.3 Testing**

The Service Provider/The Receiver Company/both parties should:

- conduct recovery testing prior to or soon after production conversion, sufficient to verify that recovery objectives can be met;
- conduct a post-mortem review and document lessons learned from every test; and
- ensure business continuity/disaster recovery plans are updated following each test exercise.

#### **7.3.3 Event Management**

Following any major event, the Receiver Company and Service Provider should conduct a post-mortem review. During the review, open issues should be identified and responsibility assigned for resolving those issues. High-level communications or post-implementation controls, processes and management responsibilities should be documented.

### **7.4 Post-Implementation Review**

Completion of the implementation should conclude with a post-implementation review between the Receiver Company and the Service Provider. This review should incorporate an overall evaluation of the implementation process and documentation of any significant exceptions to the implementation plan and objectives. Open issues should be identified, including assignment of responsibility for resolution, with high-level communications or post-implementation controls, processes and management responsibilities documented with the Receiver Company and Service Provider. This

---

should include an acceptance-test scenario with Receiver Company and Service Provider signoff prior to completion of project.

---

## **SECTION 8: RELATIONSHIP MANAGEMENT AND CHANGES IN THE OUTSOURCED ENVIRONMENT**

While the term “relationship management” implies that the management process will commence when the contract and SLA have been signed, successful vendor-management practices should be incorporated at every stage of the selection process. Effective management requires defining governance structures at both the Receiver Company and Service Provider organizations. A formal program should be established to ensure there is a consistent approach throughout the organization through the implementation of corporate policies, procedures, tools and training.

As has been outlined throughout this document, practices and processes employed by each financial institution should be commensurate with the risk associated with the outsourced system, service, or application.

### **8.1 Vendor Management**

Management of vendor relationships is required at the initiation of the relationship and on an ongoing basis. The need for managing these relationships is driven by business requirements and expectations expressed by the regulators of financial institutions. Regulatory guidance stresses the importance of a risk management function for Service Provider relationships that includes processes for due diligence, contract negotiation and performance monitoring. Businesses need to ensure they continue to evaluate the impact corporate strategy will have on the use and management of third-party providers.

This section provides an outline for the considerations an institution should review when developing a vendor management process.

#### **8.1.1 Policy**

The purpose of a vendor management policy statement is to define organizational and regulatory expectations and requirements for establishing and maintaining the Receiver Company’s outsourcing relationships. The policy, or series of policies, should define the Service Providers covered by the policy as well as any functions or services that cannot be outsourced by the Receiver Company. In order to be effective, policies should be enforceable and accountability for carrying out, overseeing, maintaining and enforcing the directive should be assigned.

The policy should be supported by procedures that identify requirements for establishing a business case, defining risk, conducting risk assessments and feasibility studies, performing vendor selection and due diligence, assigning organizational responsibilities (e.g., approval and additional signoff requirements), contract development and management, and ongoing oversight of the outsourced activity. Procedures should identify who, what, when, why and how the processes or activities should be accomplished. Furthermore, policy and procedures should identify the impact the risk assessment process should have on the selection, contractual and management processes.

As with other corporate policies, the Receiver Company should communicate the policy and procedures throughout the organization and implement controls in order to ensure adherence.

---

### 8.1.2 Program Structure

Those responsible for oversight and management of the outsourcing arrangements and vendor relationship should be identified as early in the process as possible, and should be part of the selection process.

The Receiver Company should ensure that proper resources are assigned to oversee the outsourced service with key departments represented (see Section 1.2) and with responsibility for oversight clearly defined between business units. The Receiver Company should determine if there is a need to establish a steering committee that would meet regularly to review any open issues and report to senior management at both the Receiver Company and Service Provider.

Both centralized and decentralized models for managing vendor relationships can be effective. In fact, some organizations have developed hybrid models in which some functions are centralized and others are decentralized. Regardless of the model, those programs that are successful:

- identify accountability and process throughout the Receiver Company;
- train all involved on the holistic view as well as their individual roles and responsibilities;
- identify a senior management sponsor and associated responsibilities;
- communicate the process throughout the Receiver Company (line of business, information technology, information security, compliance, audit, etc.);
- develop tools that allow the organization to track relevant information, such as financial analysis, contracts, annual review process, SLAs, trigger events such as contract renewal and termination dates, and enterprise-wide annual spending;
- define responsibility for enterprise Service Provider relationships;
- define the process for communicating the risks of mission-critical outsourced arrangements to senior management and the board of directors; and
- determine whether or not the success of the program will be qualitatively or quantitatively measured by such factors as:
  - cost savings;
  - better risk management;
  - better relationship management;
  - increased capacity for IT projects; and
  - increased corporate influence (legal, IT, compliance, procurement).

### 8.1.3 Contract File Structure

The Receiver Company should establish a process for properly maintaining contract files. (Contract files may be electronic or paper, or a combination.) The repository may be a contract file or other form of centralized repository. The files should be made available to other governance groups (e.g., line of business, risk management or privacy office) for use in their review processes.

---

The Receiver Company should consider including the following in the Service Provider files:

- completed due diligence checklist;
- current financial statement and historical financial review of the Service Provider;
- third-party, Service Provider or Receiver Company audit or assessment reports (e.g., SAS 70 report from an independent auditor, WebTrust, SysTrust and other external reports);
- copy of current contract and any amendments;
- performance review documentation, such as SLAs;
- business continuity plans, test results, and audits (if available);
- information security assessment;
- documentation of Service Provider business reviews, to include minutes, scorecards and documentation of follow-up items, accountability, resolutions and escalation requirements;
- current privacy review (if required);
- risk classification for review purposes and copy of Service Provider risk assessment reports;
- contact information for both the Receiver Company and Service Provider; and
- reports to any Receiver Company oversight committee or board of directors.

#### 8.1.4 Contract-Management Process

The contract-management process should include functionality to notify management of the following events:

- scheduled risk assessments;
- scheduled performance reviews;
- scheduled financial reviews;
- contract reviews;
- contracts due for renewal; and
- contracts about to expire.

Additional contract-management services include archiving contract files and maintaining an audit trail for contract activity.

## 8.2 Ongoing Vendor Management

The Service Provider relationship should continue to be monitored and managed to ensure requirements are being met and service and performance issues are identified and addressed. Periodic formal management reviews should be conducted to review processes and controls.

### 8.2.1 Oversight Planning

The oversight planning process should begin before a new Service Provider contract is executed. Oversight planning includes all activities involved in identifying, defining and negotiating the levels of service expected in a vendor relationship prior to signing a contract or agreement. Oversight planning also encompasses the activities involved in monitoring,

---

measuring and reporting the level of service delivered by the Service Provider once a contract is in effect.

Key contract requirements and Receiver Company expectations should be reviewed with the Service Provider account representative. Consideration should be given to the following requirements:

- Review of SLAs and reporting expectations
- Review of change control requirements, including:
  - changes in the transmission of data and policy requirements for risk management;
  - advance notification procedures for production equipment/software/hardware changes/changes to the business;
  - delivery performance specifications;
  - acceptance testing procedures for new changes to production environment;
  - right of involvement in acceptance testing that affects the production environment;
  - certification of completed acceptance testing prior to re-implementation of changes to production environment;
  - training, capacity management, and delivery performance specifications provided by Service Provider (depending on the extent of changes); and
  - updated recovery plan reviews.
- Review of notification requirements, including:
  - security breaches, including requirements for monitoring and notification;
  - customer complaints;
  - pending press releases on any subject that might affect the Receiver Company;
  - financial difficulty that may affect service;
  - material change in tactical or strategic decisions regarding the purchase and support of hardware or software related to processing performed on behalf of the Receiver Company;
  - significant staffing reductions or changes in key staff that may affect the Service Provider's ability to provide the agreed-upon support and service;
  - changes in staff licensing, gain or loss of regulatory certification, and participation in or withdrawal from alliances or other business-partner arrangements; and
  - a decision by the Service Provider to outsource, sell, or acquire significant operations or support associated with the applications, data, network, or other critical component of the environment used to provide services to the Receiver Company.

### 8.2.2 Ongoing Performance Monitoring and Operational Oversight

The ongoing, day-to-day oversight of a Service Provider should consider the following:

- review and verification of SLA reports to ensure the Service Provider is meeting established SLAs;
- review and verification of Service Provider notifications concerning the Service Provider's organization and/or operational effects on the Receiver Company;

- 
- involvement and/or communication with Service Provider user groups; and
  - review of press releases, financial statements and other information concerning the Service Provider's operations.

Other reviews might be conducted on an ongoing basis if warranted by the risk and materiality of the relationship.

### 8.2.3 Event-Triggered Relationship Reviews

Significant events at the Service Provider or Receiver Company may affect the outsourcing relationship. Significant events can include business changes, such as acquisitions, organizational shifts, volume growth or contractions, regulatory changes, or technology changes, such as application and operating system upgrades, hardware changes and network and other changes in the technology environment.

Contract termination is a key trigger event. The contract-management system or process should trigger a notification within a predetermined number of days (120 days, 90 days, 60 days, etc.) prior to contract termination. At that time, it is appropriate to begin a comprehensive due diligence review of the Service Provider relationship, including a thorough review of contract terms and a full assessment of the items identified in Section 8.2.4. It may also be appropriate to review alternative vendors or options for moving the service in house. (Section 8.2.5 provides additional information concerning exit strategies.)

Section 5 provides a comprehensive review of the language that should be negotiated into a Service Provider contract. If current standards are not incorporated in the existing Service Provider contract, the renewal period provides an opportunity to update it. Key areas for review include:

- improvements in negotiated SLAs;
- appropriate remedies for non-performance;
- appropriate notifications and change control requirements, as outlined in section 8.2.1;
- appropriate insurance requirements;
- appropriate termination language; and
- any changes in legal or regulatory requirements.

### 8.2.4 Scheduled Reviews and Assessments

Reviews should be conducted regularly. The frequency may depend on contractual, legal and regulatory requirements as well as the overall Service Provider risk profile—including consideration of any financial, operational, or performance issues. Scheduling reviews at least once a year is generally appropriate. Formal reviews should encompass the following as appropriate:

- A high-level overall relationship assessment (including services received, costs/benefits versus expectations, and other factors) to ensure initial expectations are being met and to validate that the relationship continues to make good business sense.

- 
- Service Provider’s business-continuity plans and information-security programs to ensure the plans meet current business-recovery requirements and are adequately maintained and tested. (Test results should be reviewed.)
  - A current, third-party SAS-70 report from an independent auditor or other audit or assessment report should be reviewed to determine if required control areas have been included in the scope of the report.
  - If the Service Provider is reviewed under the FFIEC’s Technology Service Provider examination program, review recent Report of Examination’s Open Section, which is available to serviced financial institutions.
  - Service Provider’s financial condition
  - Service Provider performance and quality, to include compliance with SLAs and other business and contractual requirements.
  - Walk-through of key business processes with the Service Provider, ensuring compliance with business and contractual requirements—particularly those that are driven by legal or regulatory requirements.
  - Service Provider’s change-control processes, ensuring the Service Provider has processes in place to identify and assess new control exposures resulting from a change.
  - Service Provider’s training programs, quality initiatives, etc., as deemed appropriate.
  - Service Provider’s policies and procedures documents to ensure no significant changes have been made and that they still meet contractual and business requirements. It may also be appropriate to verify that policies and procedures are being followed by reviewing file documentation. (Documentation review confirms that appropriate supporting documentation, such as requests with authorized approvals, exist for any requests/changes.)
  - Service Provider’s third-party’s relationship with dependent service providers.
  - Current contact information, including key personnel assignments, emergency contacts and escalation points.

The scheduled review period is also an appropriate time to review key contract terms to ensure they continue to meet business requirements and current contract standards. Section 8.2.3 outlines a number of key terms that should be reviewed as part of the contract-renewal process. Inclusion of appropriate SLAs and termination language with defined termination support requirements are important considerations.

A corrective action plan should be developed for any Service Provider performance issues, with appropriate monitoring and follow-through. Significant issues should be escalated, as appropriate, to senior management. Depending upon the risk associated with the Service Provider relationship, it may be appropriate to consider exit strategies.

Receiver Companies may also wish to develop a scorecard process, providing a formal evaluation or rating of key performance and service indicators and/or requirements, to include SLA performance, other quality metrics, business continuity/disaster recovery planning, security assessments, etc.

---

## 8.2.5 Escalation and Exit Strategies

Receiver Companies should consider requirements for developing exit strategies and implementation plans. Such plans might be implemented due to vendor performance issues or a management decision to move to an alternative Service Provider, or to move the service in house.

Depending on the risk associated with the outsourced application, system or service or the Service Provider's financial viability, business strategy, or performance, the Receiver Company may determine that it is appropriate to require an annual review of alternative vendors. The assessment should include:

- identifying trigger events, or circumstances in which the exit strategy would be implemented;
- identifying all or significant elements of cost and time involved in transitioning the business, including required testing and any possible impact on other existing projects should resources and funds need to be reallocated to exit the relationship;
- assessing risks associated with implementation of the exit strategy, including its effect on customers; and
- exploring transition strategies, including roles and responsibilities and the effect on customers.

Look to recent RFPs, vendors currently used by the Receiver Company, consultancies and industry trade magazines for guidance in finding another Service Provider.

The business continuity plan should be updated to include manual workarounds should termination of service be required.

When Service Providers fail to meet SLAs, expectations or requirements, or when other serious issues arise—such as Service Provider financial viability, security breaches, and recurring service issues that are not addressed—the Receiver Company should ensure that appropriate management escalation takes place. An escalation process should be in place for mission-critical Service Providers with a heightened level of risk due to financial condition or deterioration of performance.

## 8.3 Disaster Recovery/Business Continuity Requirements

### 8.3.1 Risk Analysis

- Determine how the risk matrix for the application, system or service is maintained and updated for each Service Provider.
- Review the risk analysis and Service Provider's business continuity/disaster recovery program annually.
- Review the Service Provider's change-management processes and controls annually

### 8.3.2 Recovery Objectives

- 
- Verify that established recovery service levels are being met and exceptions are being documented, with actions taken accordingly.
  - Verify that the Service Provider's recovery time capability meets or exceeds the established recovery.
  - Review recovery service levels annually, including business requirements and technology changes and enhancements time objective.

#### 8.3.3 Plans

Verify that business continuity/disaster recovery plans are maintained annually and/or updated following major system enhancements.

#### 8.3.4 Testing

Verify through participation or direct observation that business continuity/disaster recovery plans are being tested annually and/or according to the expectations set forth in the contract.

#### 8.3.5 Event Management

- Verify key emergency contacts to use in the event of escalation of critical issues.
- Conduct a post-mortem following any activation of the Service Provider's recovery plan and identify and address any issues that affect the ability to deliver the recovery objectives.

#### 8.3.6 Governance

- Verify that the Service Provider has a process in place to identify and assess new control exposures resulting from a change.
- Verify the Service Provider's technology recovery test objectives and conclusions.
- Review change-control records.
- Review third-party audits of business continuity/disaster recovery plans and testing results.

#### 8.3.7 Insurance

The Receiver Company should ensure that insurance requirements are being met and required certificates of insurance are received in a timely manner.

---

## SECTION 9: CONSIDERATIONS FOR CROSS-BORDER OUTSOURCING

The use of cross-border outsourcing as a tool for increasing productivity and providing enhanced services to customers of financial institutions has been growing in recent years. Increasingly, companies need guidance on the issues they should consider when contemplating a cross-border relationship.

While most of the considerations required in approaching and managing cross-border relationships are covered in Sections 1 through 8, several areas require further consideration. Section 9 provides recommendations for those areas that should be addressed as part of a financial institution's evaluation, implementation, and ongoing relationship management when embarking on an offshore relationship.

Consistent with prior sections of this *Framework*, these recommendations should be applied selectively, based on the financial institution's risk-assessment results and the type of system, application or service being outsourced.

### **Cross-Border Outsourcing Defined**

A financial services firm can enter into a cross-border relationship in one of two ways. The company may establish its own offshore operations (either solely owned or through joint ventures/partnerships), or it may contract with a Service Provider that conducts all or a part of its work outside of the US.

Today, as with domestic outsourcers, companies are using cross-border Service Providers for a wide range of services. The level of risk associated with cross-border outsourcing should be measured by the same institutional definitions of risk as that of domestic Service Provider relationships (intellectual property considerations, access to customer information, mission criticality, etc.), with some nuances based upon the relevance of the following factors:

- more pronounced corporate and culture differences;
- potential language barriers;
- extreme time-zone differences;
- geographic distance;
- compliance requirements to ensure continued adherence with US laws and regulations;
- legal jurisdiction and governing law for the contract (e.g., identifying the most appropriate structure for a transaction, recognizing the significant differences in local laws and regulation);
- consideration of political and economic instability;
- infrastructure issues (e.g., telecommunications, utilities);
- availability of disaster recovery/business continuity resources and options;
- knowledge transfer;
- impact on performance risk (e.g., potential difficulty maintaining different business operations and systems in different countries);
- challenges of quantifying total costs; and
- reputational risks.

The following guidelines are intended to assist financial institutions as they develop strategies to mitigate these risks. These considerations are applicable to both application-development and business-process outsourcing.

---

## 9.1 Cross-Border Outsourcing Strategy

### 9.1.1 Policy

Before developing a cross-border strategy, the Receiver Company should review corporate policies to determine whether existing policies prohibit cross-border outsourcing, or if new policies should be developed to effectively identify, communicate and manage risk. The policy, or series of policies, should provide a definition for Service Providers covered by the policy and reflect the considerations outlined in Section 9.1. In order to be effective, policies should be established that are enforceable, and accountability for carrying out, overseeing, maintaining and enforcing the directive should be assigned.

### 9.1.2 Strategy Team and Sponsorship

The Receiver Company should obtain senior management support for a cross-border strategy. Depending on the level of outsourcing being considered, a chief sourcing officer could be appointed to manage the strategy, as well as the selection, implementation and relationship-management process. As is the case with domestic outsourcing, roles and responsibilities for the cross-border outsourcing strategy and relationship management should be defined at the institution regardless of the structure of the organization. Strategy formalization should include establishing a risk advisory council with appropriate representation from operations risk, legal, human resources, corporate real estate, corporate communications, international, corporate information security, and other business areas.

In addition to the guidelines in Section 1.2, the cross-border outsourcing evaluation team may include:

- Attorneys knowledgeable about the unique provisions required for cross-border outsourcing transactions (may be part of the in-house legal team). Such unique provisions include corporate tax, regulatory compliance, software import/export, governing law, employment considerations, immigration, and other considerations. Companies may also consider using outside counsel with geographic reach in the countries where the outsourcing service provider is headquartered or where the services will be provided. Attorneys should be involved as early as possible in the transaction, preferably at the RFP stage, to understand the level and scope of the arrangement in drafting an appropriate contract, to prevent delay and to ensure both business and legal terms are considered.
- Individuals at the financial institution who are knowledgeable about country-risk issues (e.g., those in correspondent banking may have lines of credit in place based on country risk).
- Security, risk-management and audit personnel knowledgeable about the Receiver Company's policies and processes, as well as cross-border implications.
- Those knowledgeable about accounting practices in the country where the Service Provider is located (e.g., Service Provider may have different rules for expensing versus amortizing, etc.).
- Those with dedicated cross-cultural integration expertise.
- Independent consultants experienced in cross-border outsourcing.

- 
- Individuals with technical expertise who understand communication options with the Service Provider.

#### 9.1.3 Strategic Considerations:

- Consider how the cross-border relationship would reflect the overall corporate strategy.
- Consider the types of projects to be outsourced—short term versus long term, application development, production support or business-process outsourcing, systems or applications that process customer information. Each will carry a different degree and type of risk.
- Possible development of growth strategy:
  - Management-set goals (e.g., percentage of development budget sourced from cross-border resources)
  - Bottom-up or organic growth (e.g., line of business to determine use of cross-border resources)
- The strategy should also evaluate the different types of cross-border resources that may be used:
  - Near-shore or offshore locations
  - Cross-border vendors with a US presence
  - Vendors with more than one cross-border location
  - US vendors using overseas resources or locations and offering a global delivery package
- Sole or multiple (redundant) supplier strategy.
- Reputation considerations.

#### 9.1.3 Communications Considerations

When developing the initial strategy, consider the future need to, at a high level, communicate internally and externally the company's business needs. Define and communicate the potential effects on the organization, such as layoffs, increased revenue, and retooling of resources. A communication strategy should identify and proactively address impact to employee morale at the enterprise and project levels, as well as national and local market reaction to the cross-border activity.

#### 9.1.4 Cost Analysis

In addition to the elements outlined in Appendix I, total cost of ownership considerations should include costs incurred in a cross-border outsourcing arrangement. These include, but are not limited to the following:

- audits (internal and external);
- tax implications;
- currency risk;
- increased travel;
- telecommunications;
- redundancy;

- 
- ongoing due diligence;
  - infrastructure and technology requirements;
  - transition costs; and
  - program management.

## 9.2 Legal and Structural Considerations

A cross-border outsourcing arrangement may be affected by structural, legal and regulatory requirements, enforceability of choice of law, and other factors.

### 9.2.1 Structural Considerations

A cross-border outsourcing arrangement should be structured to address the needs of both parties, taking into account the impact of local laws and regulations on the arrangement. Possible structures to consider include:

- Directly contracting with a Service Provider in its non-US location.
- Directly contracting with domestic affiliate of a non-US Service Provider. If a non-US Service Provider does not have sufficient assets to back up performance of its obligations, consider entering into an agreement with the parent company or obtaining a parent-company guarantee.
- Setting up a legal entity outside of the US to contract directly with the Service Provider.
- Setting up a joint venture with the Service Provider. This can provide more control and share in profits and equity, but can cause problems in the event a party seeks to exit the relationship.
- Acquiring the non-US Service Provider outright.

### 9.2.2 Legal Considerations:

In order to evaluate legal considerations for a cross-border outsourcing arrangement, the Receiver Company should consider engaging either outside counsel with offices in the local country or local counsel experienced in cross-border outsourcing to provide input on the structure of the arrangement and the impact of local legal requirements, as well as to review contracts and ensure enforceability. A person familiar with local accounting practices should also be consulted.

In addition, the Receiver Company should determine whether or not it already has a presence in the country being considered—either with a physical location or via correspondent banking. If there is a presence, consider whether establishing the outsourced business in any way changes the charter of that presence. If there is not a presence, consider what activities or actions would create a presence in the country and the impact on the Receiver Company.

A review of US, local and international laws and regulations will help to outline due diligence, contract and relationship-management requirements. Particular attention should be paid to:

- Tax laws.
- US regulatory and legal requirements, including, but not limited to, national sanctions and embargo programs, GLBA, FFIEC, Basel and OCC 2001-47 and 2002-16, and OTS 82

---

requirements. The due-diligence process should also consider the parties' responsibilities if there are regulatory changes in the US or the relevant country that may impact performance of the agreement.

- Privacy, data-protection and security breach laws.
- Mandatory local laws, for example, laws concerning transfer of assets and data-protection and privacy laws, as well as limitation of liability issues.
- US and local technology import/export, asset transfer and depreciation differences.
- Limitation on liability laws.
- International and local telecommunications rules and regulations.
- Intellectual property rights. (These rights are territorial in nature; to protect these rights in the local territories, local laws should be considered.)
- Federal laws, e.g., what would happen if its FBI equivalent stepped in and seized its operations?
- Reporting requirements, e.g., is there a local equivalent to the SAR?
- Employment/hiring/firing laws, such as Europe's Acquired Rights Directive and the impact of transferring employees to the Service Provider.
- Labor requirements, e.g., is there an OSHA equivalent?
- Immigration laws.
- Insurance availability and limitations.
- Currency restrictions, e.g., what currency can be used for payables and receivables?
- Internet liability policies and Internet use regulations.
- Legal validity of electronic communications and signatures.
- Exit strategies and local laws on termination, transfer of employees and assets back to the Receiver Company.

### 9.2.3 Contract Issues:

An outsourcing contract should be flexible to reflect the developing relationship between the parties. It should be drafted to match the internal structures and processes of the parties rather than rely on the Service Provider's standard contracts. When asking for protections, it is advisable to only ask for those protections that the Receiver Company may realistically need. (Protections are likely to come at a price, so consider if the increased costs outweigh the benefits.)

Ensure contracts are not prescriptive and include changing mechanisms to manage variations in volumes of business and service, and provide an effective mechanism to cover the cost of change. Consider the consequences of possible regulatory changes, different approval procedures for different types of change, and the impact and consequences of a change in control or ownership at the Service Provider (e.g., changes that could occur through buyout or acquisition).

Contracts between the Receiver Company and a non-US-based Service Provider should:

- 
- Take into account business requirements and key factors identified during the Receiver Company's risk-assessment and due-diligence processes. In particular, there should be provisions protecting the privacy and confidentiality of consumers' records.
  - Include a provision indicating that the Service Provider agrees that the services it performs for the Receiver Company are subject to US regulatory requirements and examination.
  - Provide procedures to ensure that English-language copies are maintained of all contracts, results of due-diligence efforts, regular risk-management oversight, performance and audit reports, and relationship with the Service Provider.
  - Include choice-of-law and jurisdictional covenants that provide for resolution of all disputes between the parties under the laws of a specific jurisdiction. (Note, however, that certain local laws are mandatory and will apply to the contract regardless of the choice of law clause in the contract, such as data-protection laws and limitation of liability laws.) Local or outside counsel with offices in the country should review this as part of the due-diligence or RFP process.
  - The Service Provider should be prohibited from disclosing or using financial institution data other than to carry out the contracted services; this information should remain the property of the financial institution. Any disclosures of nonpublic customer information should be conducted in accordance with applicable privacy regulations. Security measures should also be in place to safeguard customer information.
  - The parties should evaluate and discuss what hardware/third-party software and/or third-party tools will be needed by the Service Provider. The contract should specify who will pay for the procurement and licensing of these tools and how export issues will be addressed. Any additional third-party services required by the parties should also be set forth along with an understanding of any subcontracting relationships held by the Service Provider.

#### 9.2.4 Service Levels

As with domestic outsourcing arrangements, financial institutions should structure contracts and SLAs that include metrics showing productivity improvements and provisions for changes in laws and regulations applicable to the outsourcing arrangement (e.g., taxes and import/export laws).

### 9.3 Country Risk

Country risk is dynamic. Even a strong Service Provider can be hurt by a country's economic, social and political environment.

- 9.3.1 A company's country-risk rating is composed of key political and economic factors, as well as historical economic and business indicators that should be evaluated and graded to provide individual and overall assessments. Understanding that obtaining good objective information is sometimes difficult, financial institutions should query their correspondent banking group to obtain any internal country rating information and credit-risk intelligence. Consider using rating criteria from a third party, like Fitch Risk, Moody's, or Standard & Poor's, and conducting additional research to determine sovereign rating, or overall country-risk rating.

---

Review of country-risk issues should evaluate the entire country, as there may be sections that are more prone to disturbances than others. The financial institution should put into place a monitoring system by which more frequent updates can be generated from auditors regarding the country's situation, with alerts when the situation reaches predefined conditions.

9.3.1.1 Political factors include:

- government process, ranging from a broad-based democracy to anarchy;
- general level of support for party in power, ranging from broad to none;
- opposition parties, ranging from no major opposition to imminent revolution;
- disenfranchised political subgroups, ranging from no meaningful activity to civil war;
- general socioeconomic conditions, ranging from homogenous population with reasonable wealth to abject poverty;
- political vulnerability due to economic factors, ranging from economic factors a major plus to economic factors leading to a revolution;
- attitude toward nationalization and repudiation of foreign debt, ranging from free and open economy with clean record to action against businesses underway;
- influence on/interaction with neighboring states, ranging from positive and supportive to hostile with active opposition;
- attitude toward foreign investment, ranging from positive and very attractive to hostile with across-the-board restrictions on foreign investments; and
- attitude toward and alliance with US, ranging from full support of active pacts and treaties to hostile.

9.3.1.2 Economic factors include:

- GDP per capita;
- real GDP growth;
- percent change in exports;
- inflation;
- growth in M1;
- reserves/monthly imports;
- net debt/exports;
- current account balances/export \$;
- debt service ratio;
- change in currency;
- government budget balance/GDP;
- current account/GDP;
- relationship between government and business;
- sustainability of economics; and
- labor projections.

---

### 9.3.1.3 Economic and business indicators include:

- basic structure of economy (population and GDP);
- internal performance (GDP growth and government revenues);
- external performance (balance of payments, level of foreign trade, international liquidity, foreign debt structure, exchange rate);
- exports – goods and partners; and
- software industry growth rates.

### 9.3.2 Financial institutions should evaluate additional resources that could be used to gather information specific to the industry, company and business practices in the country/countries being evaluated. To understand the source and objective for providing the information, Receiver Companies should:

- Determine the maturity of the Service Provider community. How long has it been operating, to what extent, and in which industries?
- Understand any impact to the financial institutions' ability to comply with applicable US laws and regulations by consulting with in-house counsel, engaging outside counsel with experience in similar transactions and a presence in the country, and/or engaging local counsel to advise on local law. Based upon the Service Provider's corporate structure, the financial institution may choose to evaluate the benefits of entering into a contract with a US-based company owned by the third party.
- Understand the infrastructure limitations of each country being explored. Is this a country prone to rolling black outs? Are local means of backup power generation available? Are telecommunications systems reliable in all regions of the country? Receiver Companies should also be aware of the impact infrastructure limitations may have on SLA requirements.
- Understand the travel risks for receiver staff. Review any unsafe transportation methods. For example, is taxi transportation acceptable when traveling alone? What possible health or vaccinations are required for travel? Travel times inter-city and intra-city may vary considerably.
- Understand the business practices and ethics of each country.
- Know encryption limitations and requirements.

Additionally, the generally accepted auditing principles and practices of each relevant country should be well understood and agreed to by both parties.

## 9.4 Due Diligence Considerations

### 9.4.1 Vendor Overview and Strategy

Where are the Service Provider's operations located (including not only operational locations but also sales, marketing, technical support, customer service)? Does the Service Provider have a presence in the US and, if so, what is its purpose? Is the Service Provider already doing work for other US companies, and if so, in which industries? Can the companies be contacted for references? What is the Service Provider's strategy for staffing projects?

---

Considerations for staff selection may include whether the company ensures that staff have worked on onsite projects before being deployed to the US, and whether the staff assigned to the project have worked on similar projects in the past for financial services or other industries.

#### 9.4.2 Cultural Fit

Depending on the function(s) to be outsourced, it may be important to determine whether the Service Provider's culture fits with the financial institution's. This may require sending senior managers to the foreign site to meet with Service Provider senior management. To ensure effective discussions, Receiver Companies should learn about cultural nuances related to communications and behaviors appropriate for the Service Provider and the country. Some organizations use cultural analysis models for this purpose.

#### 9.4.3 Financial Viability

Receiver Companies should develop a thorough understanding of accounting standards, audits, currency risk, auditing, etc. Sources of information will vary by country and for public versus private companies. As with US-based Service Providers, the Receiver Company should then execute based on its perceived risk. The financial standing of the Service Provider may affect the legal structure selected to implement the transaction.

#### 9.4.4 Onsite Visits

Evaluating where the financial institution's work will be performed with a cross-border Service Provider is similar to the process for evaluating an onshore provider. However, there are additional considerations for an overseas visit. Financial institutions should consider developing a "script" for the onsite review, including interviews with a wide range of employees working at different functions and levels within the organization in order to identify any inconsistencies in information provided. Consider requesting references while visiting the site. In addition, onsite visits should be scheduled so that the financial institution can observe the Service Provider's operations during US business hours. Depending on the risk, the Receiver Company may engage an independent audit or assessment organization to review the Service Provider's operations to assist in the review. Site visits should also include meeting government officials to verify the country analysis, including attitudes about US outsourcing and the general business climate.

The evaluation should include:

- an overall evaluation of technology and operations to determine whether requirements can be met and sustained, including evaluation of appropriate data-storage facilities;
- depth of management and project management within the company;
- review of infrastructure requirements and status;
- an overall evaluation of technology and operations to determine whether requirements can be met and sustained, including evaluation of appropriate data-storage facilities;
- depth of management and project management within the company;
- review of infrastructure requirements and status;
- review of information security practices and access controls; and
- overall staff awareness of Receiver Company policies and procedures.

---

#### 9.4.5 Human Resources

The financial institution should gain an understanding of employment/hiring/training/firing policies and criteria. It should also evaluate local employment guidelines and rules that may impact the availability of required talent or any humanitarian issues that may increase reputational risk. In evaluating these issues, the Receiver Company should include considerations for employees going to the cross-border location or coming to the Receiver Company's site. The Receiver Company should understand any visa issues that might impact the Service Provider's ability to utilize resources where needed. (See Appendix 7 for background on US visas.) Furthermore, depending upon the outsourced service, application or system, the Receiver Company should also know what kind of information is available on employees' backgrounds, including credit or criminal checks, as well as what documentation the Service Provider keeps and whether this satisfies regulatory requirements. Local or outside counsel with offices in the foreign territory should advise on local employment laws applying to the transfer of employees to the Service Provider or back to the financial institution when the relationship terminates.

#### 9.4.5 Security

The same due diligence and oversight followed for onshore Service Provider relationships should be applied to cross-border relationships. The preceding sections provide specific guidance in these areas and should be referenced in more detail, as well as the high-level industry expectations outlined in Appendix 6.

Cross-border outsourcing due diligence should evaluate the status of the Service Provider's policies, practices and procedures for its operations and those of any dependent service providers. The Receiver Company should ensure that the review evaluates change-management and patch-management considerations, as well as requirements should the Service Provider need systems access in an emergency. The financial institution should obtain a copy of and review any audits or assessments available on the overseas operations. The Service Providers should maintain and adhere to policy, standards, procedures, and controls for governing the security of information and systems accessed from outside company facilities as well as the security of information stored on mobile and telecommuting equipment. The parties should determine whose policies take precedence if there are any discrepancies between the Service Provider's and Receiver Company's policies.

#### 9.4.7 Infrastructure

Consistent with domestic outsourcing arrangements, an evaluation of the infrastructure to support the application, system or service should be evaluated. In cross-border situations, however, the financial institution should understand both the macro and micro implications of the company's and country's infrastructure. For example, the financial institution should thoroughly review the telecommunications system and its reliability in the specific area of the country where operations or backup sites are being considered and evaluate the time it takes to get infrastructure requirements and building permits.

#### 9.4.8 Business Practices

The Receiver Company should consider evaluating differences in cross-border outsourcing that may impact the operations of the application, system or service, and, where necessary build in contractual provisions to ensure continuity of service. Considerations include:

- 
- What are the typical hours of operation, holidays, overtime, etc. that will impact the company's ability to provide service as required?
  - Will Service Provider's staff be available for consultation during receiver's normal business hours?
  - What presence does the vendor have in the foreign country? Is the company based outside of the country in which it is operating?

#### 9.4.9 Existing Technology and Service Provider Relationships

The new Service Provider relationship may need to connect to the financial services technology infrastructure and/or with other technology and Service Providers.

Considerations include:

- If network connectivity to existing technology and Service Providers is required for the outsourcing function, does the contract with that vendor provide for connectivity to a third party? If yes, what cable or satellite system will be used for transporting voice or data? Is redundancy built in to the systems?
- Is connectivity required to the financial institution? If so, how will that be achieved? What type of monitoring will need to be in place?
- Are there licensing issues relevant to this new outsourcing arrangement? (For example, do any existing contracts require a notice or waiver for transferring to a third party, in or outside the US? Or will this result in a change to the contract with the existing technology or Service Provider that may require the Service Provider's consent? Do any of the financial institution's licenses require the product to be used exclusively in the US? Will the cross-border relationship require changes to that license that may then require regulatory approval or increase costs?)

### 9.5 Disaster Recovery/Business Continuity Planning

Consistent with the rest of the *Framework*, the Service Provider's business-continuity strategy should be reviewed throughout the selection and management process. The Service Provider should be required to test the strategies regularly. In addition to the elements listed elsewhere and incorporated into Appendix 5, a review of the Service Provider's plans should include evaluating risks associated with country, political, and currency risk factors, change in government or tariffs, trade issues, export controls, and monetary policy. The evaluation of these risks, once identified, will likely affect the financial institution's own disaster recovery/business continuity plan. The Receiver Company should consider developing a matrix of subject-matter experts and requirements for bringing them to the site to execute or manage the disaster-recovery plan. The evaluation should include an understanding of any visa or passport issues that might affect the ability to transfer these key personnel to a backup location.

#### 9.5.1 Risk Analysis

- What local conditions should be evaluated (e.g., likelihood of earthquakes or volcanoes) and what threat scenarios are included in the Service Provider's evaluation?
- Has the Service Provider established a system for monitoring and assessing political, economic, and country-risk issues that might affect its ability to conduct business with the Receiver Company? Does this monitoring process include US government legal or

---

regulatory changes to the Receiver Company's ability to transact business or travel to the Service Provider's location?

- In countries where there are few or no third-party providers of disaster-recovery services, what contingency plans are in place? Receiver Companies should evaluate risks and may consider establishing a local entity to which assets and employees can be transferred if necessary. If practicable, consider asking for "step-in rights," which allow the financial institution to provide the services, possibly remotely, until the Service Provider issues are resolved.
- Are satellite or microwave communications available?

#### 9.5.2 Recovery Objectives

- Are there levels of service degradation that might invoke disaster-recovery plans?

#### 9.5.3 Plans

- How often can and should data be transferred/copied to the Receiver Company for storage in order to comply with regulatory and business requirements? What capabilities exist for safely transporting data to offsite storage locations?
- Can the Receiver Company back up the Service Provider at its location?
- At the backup site, is there a standard development or processing environment to aid in the event of a rapid transition?
- How often does the Service Provider test its disaster recovery/business continuity plans?
- How often does the Service Provider audit third-party providers of disaster recovery/business continuity plans?
- Is diverse path routing (local and global circuits) available from the Service Provider?

#### 9.5.4 Testing

- How will Receiver Company's disaster-recovery tests be conducted to include the cross-border location?

#### 9.5.5 Event Management

- In an emergency, how will essential personnel (Receiver Company or Service Provider) be evacuated from the country? (Considerations include identifying and notifying personnel, determining whether they hold current visas and passports, and designating housing and backup sites.)

#### 9.5.6 Governance

- The Receiver Company should evaluate its governance structure to determine the effect of coordinating with and overseeing a Service Provider located outside of the US, including identifying any relevant regulatory requirements.

---

### 9.5.7 Insurance

- The Receiver Company should determine whether outsourcing outside of the US will affect existing insurance coverages.

## 9.6 Implementation Issues

Implementation issues with a cross-border outsourcing arrangement are the same as those with a domestic outsourcing, except that the cross-border arrangement has the potential for greater cultural, language, and geographic challenges.

How the outsourcing arrangement is implemented will depend greatly on the quality of the contract, the business values both parties bring to the table, and the quality of the project management. Implementation of the agreement may, like onshore implementations, require a great deal of back-and-forth communications between the Receiver Company and the Service Provider. Steps should be taken to ensure there is a smooth transfer from the contract negotiation team to the delivery team implementing the project, including:

- scope management;
- issues management;
- knowledge transfer;
- arbitration procedures (such as use of international arbitration); and
- criteria for creation or modification of SLAs.

The implementation's project managers should establish well-defined procedures for:

- ensuring that infrastructure is in place well ahead of any deliverable dates—installation times for new equipment, LANs, etc. can be much longer than US installation times;
- provision of hardware and software used by the Service Provider, as well as determination of whether these will be owned/provided by the Service Provider or the financial institution, and how upgrades, patches and servicing will be conducted;
- knowledge transfer;
- training for both the suppliers and users of the outsourced service;
- parameters around systems access and security;
- a regular return of work completed to date to the US;
- communications management, to provide a clear and regular means of communication between the two parties' implementation teams, keeping in mind time-zone differences;
- creating and distributing accurate project status information should be established;
- quality control and UAT;
- managing possible language and cultural differences among team members;
- key personnel involved in implementation to have knowledgeable, fully trained backup in the event that they are unable to travel because of visa issues; and
- a process of operational maintenance and/or scheduled downtime. Operational maintenance should not disrupt cross-border operations and access to systems due to time-zone differences. Timing for conference calls and operations should be established.

---

Having buyer and supplier staff at each other's sites during the implementation may help facilitate communications, training, and issues resolution. Considerations for employees who are to be located at the Service Provider or financial institution site should be considered. Each party's employees will likely be working in a locale and environment to which they are not accustomed. Staffing requirements should be planned for in advance when staffing the project and arranging for accommodations at the various project sites.

## **9.7 Vendor Management and Communication Requirements**

Implementation of a cross-border relationship, regardless of whether it is providing an information-technology or business-process service, will need an effective oversight program to monitor the Service Provider's ongoing financial condition, performance and controls. How the vendor is managed should depend on the degree of management oversight required for the outsourced application, system or service.

Consideration should be given to the following when developing a vendor-management program:

- **Monitoring:** Evaluation should include ongoing assessment of country risk and legal and regulatory issues.
- **Operational issues:** How cross-border issues affect operations and performance requirements such as time-zone differences, technology availability and staff travel should be continually evaluated.
- **Knowledge transfer:** While similar to domestic Service Provider relationship issues, training becomes more critical when the development or processing experts are located overseas and may have contact with the Service Provider's customers. Documentation in English is a critical component.
- **Monitoring of physical assets:** A process should be established for monitoring any physical assets provided to or used by the Service Provider, including not only customer information but also computers and other equipment.
- **Issue escalation:** Contractual and operational definitions for escalation of issues should be documented, agreed to and monitored.
- **Cross-culture integration.**

### **9.7.1 Receiver Company Staff**

Receiver Companies should prepare their staff for working with the Service Provider by:

- defining the potential impacts to the organization and notifying staff of changes, such as layoffs, increased revenue or retooling of resources;
- reviewing the overall cross-border strategy;
- creating tools to ensure compliance with contracts and corporate strategies;
- establishing protocol for communicating with the Service Provider;
- creating staff training programs on cultural differences, including differences in lifestyle, language and culture;
- considering establishing an intranet or other source of current information on the outsourcing relationship, strategy and policies;

- 
- identifying requirements for Service Provider personnel located in the US and/or financial institution personnel located overseas; and
  - reviewing required changes to procedures, such as CMM processes, to ensure methodology consistency.

#### 9.7.2 Internal and External Communications

The Receiver Company should establish a communications plan for internal and external audiences, including:

- engaging the Receiver Company public affairs and human resources personnel to communicate its cross-border strategy;
- developing a formal employee opportunity program that supports employees shifting to other jobs inside or outside of the organization, should layoffs be required;
- developing a program that allows employees to shift from a job with the Receiver Company to one with the Service Provider; and
- communicating the cross-border strategy to employees, shareholders, and the press. The strategy should include goals for staff development, increased quality and other objectives.

### 9.8 Exit Strategy

Terminating a cross-border relationship is more complex than terminating with a domestic Service Provider. And, while termination is often a right of last resort, effective governance mechanisms can ensure that the service or service levels do not deteriorate.

In addition to the recommendations outlined elsewhere in the *Framework*, the Receiver Company should ensure that there is a detailed exit plan. The exit plan should consider:

- Service Provider employees working at the Receiver Company. Can the Receiver Company hire or transfer key staff? Do onsite personnel carry transferable visas? (See Appendix 7.)
- The strategy for recapture and disposal of any technology equipment owned by the Receiver Company but operated by the Service Provider. For example, the equipment might be sold or shipped back to the institution. Is it cheaper to sell it locally than to bring it to the US? Also, is the Service Provider using these assets to provide services to other customers?
- Software license considerations for application-development and business-process outsourcing arrangements.
- A strategy for shifting services provided by the Service Provider to the Receiver Company or to alternate Service Providers so that the underlying business or reputation is not affected.
- Establishing a local entity to employ staff. Upon termination, those employees would return to the Receiver Company.
- Licensing back from Service Provider to the Receiver Company all intellectual property necessary to provide the services that the Receiver Company does not already provide.
- Plans for documenting any disposal of Service Provider data, code, and documentation and verification.
- Plans for ensuring adequate knowledge transfer from the Service Provider to the Receiver Company.

- 
- Defining the exit-strategy team and its roles, including identifying if there are any situations that should be rehearsed.

## **APPENDICES**

Model Spreadsheet Detailing Generic Cost Categories

See Section 9.1.4 for additional cost considerations for cross-border outsourcing.

Costs	Internal						External					
	Yr 1	Yr 2	Yr 3	Yr 4	Yr 5	Total	Yr 1	Yr 2	Yr 3	Yr 4	Yr 5	Total
<b>Labor</b>												
Salaries/Wages	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Overtime	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Benefits	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Payroll Taxes	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Travel	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Other Employee Expenses	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Contract Employee Expenses	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>Hardware</b>												
Purchase	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Sales Taxes @ XX% of Purchase	\$0.00						\$0.00					
Shipping	\$0.00						\$0.00					
Installation	\$0.00						\$0.00					
Writeoff of BV of Old Hardware	\$0.00						\$0.00					
Removal and Disposal of Old HW	\$0.00						\$0.00					
Other:	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>Software</b>												
Recurring License Fees	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Purchase	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Taxes @ XX% of Purchase	\$0.00						\$0.00					
Installation	\$0.00						\$0.00					
Writeoff of BV of Old Software	\$0.00						\$0.00					
Other:	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>Communications</b>												
Circuits	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Other:	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>Maintenance</b>												
Hardware	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Software	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Other:	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>Access Control</b>												
Infrastructure	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Administration	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Monitoring	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>Recovery</b>												
Staffing	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Hardware	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Software	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Vendor Services	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>Technical Expertise</b>												
Contract Programming	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Use of Internal Resources (XX hrs @ XX/ hr.)	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Perm Addition to Staff (XX FTEs @ XX salary)	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Training	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Travel	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Other:	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>Facilities</b>												
Building/Floor Space	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Property Taxes												
Utilities												
Furniture/Equipment/Fixtures	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>Ongoing Support</b>												
Audit	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Legal	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Insurance	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>Time to Market</b>												
	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>TOTAL COST</b>	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>COST SAVINGS</b>												

*Appendix 1: Model Spreadsheet for Cost Analysis*

<i>Internal Human Resources (XX FTEs @ XX salary)</i>	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<i>Sale of Equipment</i>	\$0.00						\$0.00					
<i>Reallocation of Building/Floor Space Vacated</i>	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<i>Sale or reallocation of Furniture/Equip/Fixtures</i>	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<i>Mainframe Processing Hours Vacated (XX @ \$XX/hr)</i>	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<i>Other: _____</i>	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>TOTAL COST SAVINGS</b>	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>TOTAL NET SAVINGS/(COST)</b>	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00

**COMPARISON OF BITS FRAMEWORK WITH FEDERAL BANKING AGENCY GUIDELINES**

Federal Banking Agency Guidelines	BITS Framework
<b>I. Federal Financial Institutions Examination Council (FFIEC) Risk Management of Outsourced Technology Services (Nov. 28, 2000)</b>	
I.a. Risk Assessment	2.1, 2.4, 2.7, 9.1
I.b. Due Diligence in Selecting a Service Provider	Section 3, Section 4, 9.4
I.b.1 Technical and Industry Expertise	4.4, 4.9, 9.3.2, 9.4
I.b.2 Operations and Controls	3.2, 3.3, 3.4, 4.4, 4.5, 5.1.8, Section 6, 9.4
I.b.3 Financial Condition	4.3, 5.1.2, 5.1.3, 8.2, 9.4.3
I.c. Contract Issues	Section 5
I.c.1 Scope of Service	2.1, 2.2, , 5.1.1
I.c.2 Performance Standards	2.1, 3.1, 4.11, 5.1.1
I.c.3 Security and Confidentiality	2.2, 4.6, 5.1.4, 5.1.5, 5.1.6, 5.1.7, 5.1.9, 5.3, 9.4.5
I.c.4 Controls	5.1, 5.3, 5.5, Section 6
I.c.5 Audit	4.4, 5.1.7
I.c.6 Reports	2.2, 4.4, 5.1.5, 5.1.6, 5.1.7, 5.1.8, 5.1.9
I.c.7 Business Resumption and Contingency Plans	2.5, 3.5, 4.13, 5.2, 6.7, 7.3, 8.3, 9.5
I.c.8 Subcontracting and Multiple Service Providers Relationships	4.9, 4.10
I.c.9 Cost	2.1, 2.2, 2.3, 2.6, 2.7, 9.1.4
I.c.10 Ownership and License	5.1.4, 5.1.6.6, 9.4.9
I.c.11 Duration	5.1, 5.4, 8.2.3
I.c.12 Dispute Resolution	5.4, 8.2.4, 9.2
I.c.13 Indemnification	
I.c.14 Limitation of Liability	
I.c.15 Termination	4.12, 5.4, 8.2.5, 9.8
I.c.16 Assignment	4.9, 5.1.3.7

Appendix 2: Framework Map to Federal Banking Agency Guidelines

Federal Banking Agency Guidelines	BITS Framework
I.d. Oversight of Service Provider	
I.d.1 Monitor Financial Condition and Operations	Section 7, Section 8
I.d.2 Assess Quality of Service and Support	Section 7, Section 8
I.d.3 Monitor Contract Compliance and Revision Needs	Section 7, Section 8
I.d.4 Maintain Business Resumption Contingency Plans	Section 7, Appendix 5
<b>II. Federal Reserve Bank of New York</b>	
<b>Outsourcing Financial Services Activities: Industry Practices to Mitigate Risk</b>	Entire Framework
II.a. Managing and Monitoring the Outsourcing Arrangements	
II.a.1. <i>The board of directors and senior management must retain accountability for any outsourced activity. They determine the strategic role and objective for the outsourcing arrangement, and provide necessary approvals.</i>	Section 2, 8.1
II.a.2. <i>Create a management structure to establish, manage and monitor the outsourcing arrangement.</i>	
- Phase 1, Identify/Evaluate:	2.1, 2.7
<i>Core Competencies</i>	2.1, 8.1, 9.1
<i>Firm-Wide Objectives</i>	2.2, 2.3, 2.4, 2.6, 2.7
<i>Activities to Outsource</i>	2.7, 2.8, Appendix 1, 9.1.4
<i>Cost Benefit Analysis</i>	Section 3, 9.2
- Phase 2, Select Provider:	Section 4, Section 6, 9.4
<i>Choose Type of Arrangement</i>	Section 5, 9.2
<i>Perform Due Diligence</i>	2.5, 3.5, 4.12, 4.13, 5.2, 5.4, 6.7, 7.3, 8.2.5, 8.3, 9.5, 9.8
<i>Negotiate the Contract</i>	Summarized in Appendix 5
<i>Contingency Planning/Termination Conditions</i>	Institution's Program
- Phase 3, Manage Transition:	Section 7, Section 8, 9, 9.1.3, 9.7
<i>Ensure Business Continuity</i>	Section 8
<i>Protect Employee Morale</i>	Entire Framework
<i>Communicate</i>	Section 5, Section 8
- Phase 4, Long-Term Management:	4.4, 5.1.8, 8.2
<i>Monitor Contract</i>	
<i>Re-Evaluate Metrics</i>	
<i>Renegotiate Contract</i>	
<i>Independent Validation</i>	

Appendix 2: Framework Map to Federal Banking Agency Guidelines

Federal Banking Agency Guidelines	BITS Framework
II.a.3. <i>Create cross-functional teams, including internal audit, information security, human resources, legal, and the business units, to ensure broad representation of viewpoints and to enhance institution-wide support.</i>	1.2, 9.1.2
II.a.4. <i>Retain key individuals from the outsourced function to manage and monitor the outsourcing arrangement, and to provide future strategic direction.</i>	Institution's Program
II.a.5. <i>Monitor the relationship actively, respond to problems and issues aggressively, employ escalation procedures promptly, and engage in conflict resolution.</i>	Section 8, 9.7
II.a.6. <i>Identify objective and quantifiable performance measures that are well specified, relevant for the supported business units, mutually agreed to, and are readily comparable with established criteria.</i>	2.1, Section 3, 4.11, Section 5
II.a.7. <i>Periodically review, renegotiate and renew the contract. Reset target service levels annually.</i>	Section 8
<b>II.b. Selecting a Qualified Vendor</b>	
II.b.1. <i>Perform due diligence on the service provider to ensure technical capabilities, managerial skills, financial viability, familiarity with the financial services industry, and a demonstrated capacity to keep pace with innovation in the marketplace.</i>	Section 4, 9.4
<b>II.c. Structuring the Outsourcing Arrangement</b>	
II.c.1. <i>Negotiate a written contract that is operationally flexible and that clearly articulates the expectations and responsibilities of both sides.</i>	Section 5, 9.2

Appendix 2: Framework Map to Federal Banking Agency Guidelines

Federal Banking Agency Guidelines	BITS Framework
<b>II.d. Managing Human Resources</b>	
II.d.1. <i>Involve the human resources department early in the process when staff is to be released or transferred to the service provider. Incorporate these issues into the contract and proactively communicate with the staff.</i>	Institution's Program
<b>II.e. Establishing Controls and Ensuring Independent Validation</b>	
II.e.1. <i>Clearly define expected security controls in the outsourcing contract and develop appropriate performance measures to monitor consistent application of those controls.</i>	Section 3, Section 5, Section 6, 9.4.5
II.e.2. <i>Involve internal and/or external audit in the entire outsourcing process.</i>	1.2, 5.1.8
<b>II.f. Establishing a Viable Contingency Plan</b>	
II.f.1. <i>Ensure that contingency plans are formulated and viable in the event of non-performance by the service provider.</i>	Summarized in Appendix 5
<b>III. Comptroller of the Currency (OCC)</b>	
<b>Network Security Vulnerabilities – Alert 2001-4 (April 24, 2001)</b>	
<b>III.a. Response to Network Security Vulnerabilities</b>	
III.a.1. Identify systems vulnerabilities and evaluate inherent risks.	2.3, 2.4, 3.2, 3.3, 4.4, 4.8, 4.9, 5.1.3
III.a.2. Eliminate unwarranted risks by applying vendor-provided software fixes.	5.1.3
III.a.3. Ensure that exploitable files and services are assessed and removed or disabled.	
III.a.4. Ensure that changes to security configurations are documented, approved, and tested.	5.1.9
III.a.5. Update vulnerability scanning and intrusion detection tools to identify known vulnerabilities and related unauthorized activities.	5.1.6, 5.1.7
III.a.6. Conduct subsequent penetration testing and vulnerability assessments, as warranted.	5.1.7
III.a.7. Ensure that security maintenance and reporting responsibilities (including notification of systems security breaches that may affect the bank) are clearly described in service provider contract.	Section 5
III.a.8. Establish monitoring, reporting, and investigation controls.	Section 5, Section 6, Section 8
<b>IV. Comptroller of the Currency (OCC)</b>	
<b>Third Party Relationships: Risk Management Principles OCC 2001-47 (November 1, 2001)</b>	
Risk Management Process	
Risk Assessment and Strategic Planning	1.3, 2.4
Integration with overall strategic objectives	Section 2, 9.1

*Appendix 2: Framework Map to Federal Banking Agency Guidelines*

Expertise to oversee and manage the activity	2.4, Section 8
Cost/benefit relationship	2.7, 9.1.4
Customer expectations	2.4
Selecting a Third Party and Due Diligence	Section 4, 9.4
Contract Issues	Section 5
Scope of arrangement	5.1
Performance measures or benchmarks	5.1
Responsibilities for providing and receiving information	Section 5
The right to audit	4.4, 5.1.8
Cost and compensation	5.1.1
Ownership and license	5.1.3, 9.4.9
Confidentiality and security	5.1, 4.6
Business resumption and contingency plans	Summarized in Appendix 5
Indemnification	
Insurance	5.5
Dispute resolution	5.4, 8.2.4, 9.2
Limits on liability	
Default and termination	4.1.2, 5.4, 8.2.5, 9.8
Customer complaints	
Foreign-based service providers	Section 9
OCC supervision	5.3
Oversight of Third Party Relationships	Section 8
Monitor financial condition	8.2.4
Monitor controls	Section 8
Assess quality of service and support	Section 8
Documentation	8.1.3
<b>V. Comptroller of the Currency</b>	
<b>Bank Use of Foreign-Based Third-Party Service Providers – OCC 2002-16 (May 15, 2002)</b>	
Policy on National Bank Use of Foreign-Based Third Party Service Providers	
Country risk	Section 9.3
Compliance risk	9.2.2
Due diligence	Section 9.4

Appendix 2: Framework Map to Federal Banking Agency Guidelines

Contracts	9.2.3, 9.2.4
Choice of law	9.2.2, 9.2.3
Confidentiality of information	9.2.3
Monitoring and oversight	9.4.6, 9.7
Access to information	9.5
OCC access to information	9.2.2
<b>VI. Office of Thrift Supervision Bulletin Third Party Arrangements TB 82 (March 18, 2003)</b>	
VII.a Third Party Arrangements	
VII.a.1 OTS Requirements for all Associations	
Notice	
Recordkeeping	
Troubled associations	
Affiliates and subsidiaries	
Foreign third-party relationships	Section 9
VII.a.2 Management responsibilities	2.1, 2.2
Risk assessment	2.4, 2.5.1
The importance and criticality of the function	2.5.1, 4.13.1
The nature of the activities that the third party will perform	2.1
Availability of other parties to provide any particular function, and the costs if it becomes necessary to change the party that provides the service	2.5, 2.7, 4.13, 8.3
An assessment of contractual obligations and requirements for both you and the third party	Section 5
Your ability to perform assessments of the third-party activities to evaluate consistency and third-party performance on an ongoing basis	4.4, Section 8
Due diligence in selecting a third party	Section 4
Experience in implementing and supporting the proposed activity	4.1, 4.5, 4.8, 4.9, 4.10
Financial condition	4.3, 4.3.1, 4.3.2, 5.1.2
Business reputation, complaints, and litigation past and pending	4.2
Staff competence, qualification, and training	4.5
Internal control environment	4.4, 5.1.3
Information and reporting systems	5.1.3
Contingency and recovery plans	4.13

Appendix 2: Framework Map to Federal Banking Agency Guidelines

Subcontractor reliance	4.9, 5.1.2, 5.1.8.3, 8.2.1
Insurance coverage	2.8, 3.5.7, 4.13.7, 5.5
Contact issues	Section 5
Policies, procedures, and internal control	4.4, 5.1.3
Ongoing oversight of Third Parties	Section 8
VII.a.3 OTS supervision	
<b>VII. National Credit Union Administration Letter to Credit Unions Regarding Due Diligence Over Third Party Service Providers (Letter No. 01-CU-20)</b>	
1. Due Diligence	
<i>Credit union officials are responsible for planning, directing, and controlling the credit union's affairs. To fulfill these duties, the officials should require a due diligence review prior to entering into any arrangement with a third party.</i>	Section 4, Section 5, Section 6
I.A. Planning	
<i>The officials should determine whether the proposed activities are consistent with the credit union's overall business strategy and risk tolerances. Those risks include the potential loss of capital invested if the venture fails, the loss of member confidence if the program does not meet their expectations, and the costs associated with attracting and retaining qualified personnel and investing in the required infrastructure (e.g., technology, space, communications). If the officials do not believe the activities would complement their strategic vision for the credit union, the third-party relationship should not be pursued.</i>	Section 1, Section 2, Appendix I
I.B. Background Check	
<i>It is always important to understand how the third party has performed in other relationships. Contacting credit unions or other clients of the third-party is essential. Inquire how satisfied these credit unions or third parties are with the prospective partner, and what pitfalls they may have encountered. Sources such as the Better Business Bureau and Federal Trade Commission also maintain complaint histories on businesses.</i>	4.1, 4.2
I.C. Legal Review	
<i>The credit union's attorneys should review all contracts to ensure that the officials clearly understand the rights and responsibilities of each party. For example, the review should indicate which party bears the costs of collateral disposition, and whether or not there are recourse arrangements. The credit union should exercise its right to modify contracts to make them fair and equitable. Further, a credit union should understand what actions it may take if the contract is breached or services are not performed as expected.</i>	Section 5, Section 6
I.D. Financial Review	
<i>Financial statements of the company should be reviewed to determine the strength of the institution. Weakly capitalized companies or those exhibiting weak earnings may not be able to continue as ongoing concerns. This could lead to disruptions in member service, uncollected payments on loans and leases, and potential losses if the third party fails to remit funds due to the credit union. Preferably, a licensed CPA will have audited the financial statements to attest to their accuracy.</i>	4.3, 5.1.2, 8.2
I.E. Return on Investment	
<i>The credit union should project its expected revenue, expenses and net income on its investment, and recognize how each of these factors may change under different economic conditions. For example, expected losses, collection costs, or the volume of activity would fluctuate depending upon the economy or the members' employment stability. Profit projections generated by the prospective third-party should be</i>	2.7, Appendix I

Appendix 2: Framework Map to Federal Banking Agency Guidelines

<i>scrutinized and the underlying assumptions fully understood by the credit union.</i>	
I.F. Insurance Requirements	
<i>Third-party relationships can result in increased liabilities. Therefore, they necessitate a thorough review of the credit union's insurance coverage, including the fidelity bond and policies covering such matters as errors and omissions, property and casualty losses, and fraud and dishonesty.</i>	2.7, Section 5.5, and Summarized in Appendix 5
II. Controls	
<i>The credit union should develop detailed policy guidance that set forth responsibilities, authorities, and reporting requirements. Limits should be established so that the program grows at a controlled pace and reflects the risk tolerance of the officials. For example, a credit union may limit the number of leases initially granted so it can assess performance or identify problems before the leasing volume becomes significant.</i>	Section 6
II.A. Staff Oversight	
<i>A credit union staff member should be responsible for monitoring the performance of the program. Actual results should be compared to projections and the third party's performance should be reviewed to determine compliance with expectations and contracts.</i>	1.2, , 5.1.1.2, Section 6, Section 8
II.B. Reporting	
<i>Reports should be submitted to the credit union's senior officials and the credit union's directors to keep them abreast of significant findings, especially areas of non-compliance. The officials should be informed when targets are met or exceeded, or limits breached. Reports should also consist of appropriate information so that the officials can make informed decisions and take timely corrective action.</i>	5.3
<b>VIII. Gramm-Leach-Bliley Act</b>	
<b>Public Law 106-102, the Financial Modernization Act (November 12, 1999)</b>	
Subtitle A – Disclosure of Nonpublic Personal Information	
IV. Title V: Privacy	
(b) Financial Institutions Safeguards – In furtherance of the policy in subsection (a), each agency or authority described in section 505 (a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards	Entire Framework
(1) to insure the security and confidentiality of customer records and information;	4.6, 4.7
(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and	
(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to a customer.	

**Other Regulatory Resources:**

In 2001, the FDIC published three informational documents on outsourcing. The documents were provided as a source of practical information to community banks on how to select service providers, draft contract terms, and oversee multiple service providers when outsourcing for technology products and services. The documents are intended not as examination procedures or official guidance, but as informational tools for community bankers, and are available at [www.fdic.gov/news/news/financial/2001/fil0150.html](http://www.fdic.gov/news/news/financial/2001/fil0150.html).

**Comparison of BITS IT Service Provider Framework with Basel Committee on Banking Supervision: Risk Management Principles**

Basel Committee on Banking Supervision	BITS Framework
<b>Risk Management Principles for Electronic Banking</b>	
II.A. Principle 1 The Board of Directors and senior management should establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks.	
<i>Addressing any unique risk factors associated with ensuring the security, integrity and availability of e-banking products and services, and requiring that third parties to whom the bank has outsourced key systems or applications take similar measures.</i>	Section 4, Section 5, Section 6, Section 9
Principle 3 The Board of Directors and senior management should establish a comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking.	
<i>The bank fully understands the risks associated with entering into an outsourcing or partnership arrangement for its e-banking systems or applications.</i>	Application of Framework document based upon the level of risk associated with the outsourced application
<i>An appropriate due diligence review of the competency and financial viability of any third-party service provider or partner is conducted prior to entering into any contract for e-banking services.</i>	Section 4, 9.3, 9.4
<i>The contractual accountability of all parties to the outsourcing or partnership relationship is clearly defined. For instance, responsibilities for providing information to and receiving information from the service provider should be clearly defined.</i>	Section 5, Section 6, 9.2
<i>All outsourced e-banking systems and operations are subject to risk management, security and privacy policies that meet the bank's own standards.</i>	Section 5, Section 6, 9.4
<i>Periodic independent internal and/or external audits are conducted of outsourced operations to at least the same scope required if such operations were conducted in-house.</i>	4.4, 5.1.7
<i>Appropriate contingency plans for outsourced e-banking activities exist.</i>	Summarized in Appendix 5
II.B Principle 6 Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.	
<i>Transaction processes and systems should be designed to ensure that no single employee/ outsourced service provider could enter, authorise and complete a transaction.</i>	2.3, 5.1.3, 6.1

Appendix 3: Framework Map to the Basel Committee on Banking Supervision

Basel Committee on Banking Supervision		BITS Framework
Principle 10	Banks should take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and/or stored in databases.	
	<i>The bank's standards and controls for data use and protection must be met when third parties have access to the data through outsourcing relationships.</i>	4.6, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.3, 6.5
II.C Principle 12	Banks should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services.	
	<i>The bank's standards for customer data use must be met when third parties have access to customer data through outsourcing relationships.</i>	5.1.4, 5.3, 6.5
Principle 14	Banks should develop appropriate incident response plans to manage, contain and minimise problems arising from unexpected events, including internal and external attacks, that may hamper the provision of e-banking systems and services.	
	<i>To ensure effective response to unforeseen incidents, banks should develop a clear chain of command, encompassing both internal as well as outsourced operations, to ensure that prompt action is taken appropriate for the significance of the incident. In addition, escalation and internal communication procedures should be developed and include notification of the Board where appropriate.</i>	5.1.1.2, 5.1.2, 5.1.5, 5.1.6, 5.1.7, 5.1.8, 5.1.9, 5.2
Appendix II (Basel Committee): Sound Practices for Managing Outsourced E-Banking Systems and Services		
1	Banks should adopt appropriate processes for evaluating decisions to outsource e-banking systems or services.	
	<i>Bank management should clearly identify the strategic purposes, benefits and costs associated with entering into outsourcing arrangements for e-banking with third parties.</i>	Section 1, Section 2, Appendix I, 9.1, 9.4
	<i>The decision to outsource a key e-banking function or service should be consistent with the bank's business strategies, be based on a clearly defined business need, and recognise the specific risks that outsourcing entails.</i>	Section 1, Section 2, 8.1, 9.1
	<i>All affected areas of the bank need to understand how the service provider(s) will support the bank's e-banking strategy and fit into its operating structure.</i>	1.2, 9.1

Appendix 3: Framework Map to the Basel Committee on Banking Supervision

Basel Committee on Banking Supervision	BITS Framework
2 Banks should conduct appropriate risk analysis and due diligence prior to selecting an e-banking service provider and at appropriate intervals thereafter.	
<i>Banks should consider developing processes for soliciting proposals from several e-banking service providers and criteria for choosing among the various proposals.</i>	Section 3, Section 4
<i>Once a potential service provider has been identified, the bank should conduct an appropriate due diligence review, including a risk analysis of the service provider's financial strength, reputation, risk management policies and controls, and ability to fulfil its obligations.</i>	Section 4, 9.4
<i>Thereafter, banks should regularly monitor and, as appropriate, conduct due diligence reviews of the ability of the service provider to fulfil its service and associated risk management obligations throughout the duration of the contract.</i>	5.1.8, Section 8, 9.7
<i>Banks need to ensure that adequate resources are committed to overseeing outsourcing arrangements supporting e-banking.</i>	8.1, 9.7
<i>Responsibilities for overseeing e-banking outsourcing arrangements should be clearly assigned.</i>	8.1, 9.7
<i>An appropriate exit strategy for the bank to manage risks should it need to terminate the outsourcing relationship.</i>	4.12, 5.4, 8.2.5, 9.8
3 Banks should adopt appropriate procedures for ensuring the adequacy of contracts governing e-banking. Contracts governing outsourced e-banking activities should address, for example, the following:	
<i>The contractual liabilities of the respective parties as well as responsibilities for making decisions, including any sub-contracting of material services are clearly defined.</i>	4.9, Section 5
<i>Responsibilities for providing information to and receiving information from the service provider are clearly defined. Information from the service provider should be timely and comprehensive enough to allow the bank to adequately assess service levels and risks. Materiality thresholds and procedures to be used to notify the bank of service disruptions, security breaches and other events that pose a material risk to the bank should be spelled out.</i>	Section 5, 6.8
<i>Provisions that specifically address insurance coverage, the ownership of the data stored on the service provider's servers or databases, and the right of the bank to recover its data upon expiration or termination of the contract should be clearly defined.</i>	5.1.3, 5.1.4, 5.1.5, 5.4, 8.2.5, 9.8
<i>Performance expectations, under both normal and contingency circumstances, are defined.</i>	2.5, 3.5, 4.1.3, 5.2, 6.7, 7.3, 8.3, 9.5
<i>Adequate means and guarantees, for instance through audit clauses, are defined to insure that the service provider complies with the bank's policies.</i>	4.4, 5.1.2, 5.1.8
<i>Provisions are in place for timely and orderly intervention and rectification in the event of substandard performance by the service provider.</i>	5.4, 7.2.2
<i>For cross-border outsourcing arrangements, determining which country laws and regulations, including those relating to privacy and other customer protections, are applicable.</i>	9.2

Appendix 3: Framework Map to the Basel Committee on Banking Supervision

Basel Committee on Banking Supervision	BITS Framework
<i>The right of the bank to conduct independent reviews and/or audits of security, internal controls and business continuity and contingency plans is explicitly defined.</i>	5.1.8, 6.7
4 Banks should ensure that periodic independent internal and/or external audits are conducted of outsourced operations to at least the same scope required if such operations were conducted in-house.	
<i>For outsourced relationships involving critical or technologically complex e-banking services/applications, banks may need to arrange for other periodic reviews to be performed by independent third parties with sufficient technical expertise.</i>	4.4, 5.1.7, 5.1.8
5 Banks should develop appropriate contingency plans for outsourced e-banking activities.	
<i>Banks need to develop and periodically test their contingency plans for all critical e-banking systems and services that have been outsourced to third parties.</i>	Summarized in Appendix 5
<i>Contingency plans should address credible worst-case scenarios for providing continuity of e-banking services in the event of a disruption affecting outsourced operations.</i>	Summarized in Appendix 5
<i>Banks should have an identified team that is responsible for managing recovery and assessing the financial impact of a disruption in outsourced e-banking services.</i>	Summarized in Appendix 5
6 Banks that provide e-banking services to third parties should ensure that their operations, responsibilities, and liabilities are sufficiently clear so that serviced institutions can adequately carry out their own effective due diligence reviews and ongoing oversight of the relationship.	
<i>Banks have a responsibility to provide serviced institutions with information necessary to identify, control and monitor any risks associated with the e-banking service arrangement.</i>	

## GLOSSARY OF TERMS

**Access:** The ability to physically or logically enter or make use of a system or area (secured or unsecured); the process of interacting with a system.

**Access Control:** A mechanism to allow, deny, or limit access to a resource, whether to individuals or remote machines; typically based on the authenticated identity of the individual or remote machine requesting access. Access controls prevent unauthorized access to a resource, including prevention of the use of a resource in an unauthorized manner.

**Agency:** A legal relationship between two parties who agree that one (the agent) is to act on behalf of another (the principal), subject to the latter's general control. The principal is held liable for the agent's actions.

**Aggregation:** Consolidation (aggregation) of digital information from multiple sources. Automated tools allow aggregators to access and consolidate a customer's online accounts (financial and non-financial) through the Internet, using customer-provided account numbers, user IDs, and PINs. The method of obtaining a customer's account information from multiple websites is called "screen scraping."

**American Institute of Certified Public Accountants (AICPA):** The national professional organization for all certified public accountants ([www.aicpa.org](http://www.aicpa.org)).

**AIS:** Automated information system.

**Application Service Provider:** A company that hosts an application and data for one or more customers, providing the hardware, software, infrastructure, and basic maintenance. The provider supports remote access to the application by the customer, usually over the Internet, and usually has expertise in the application and may provide enhancements to it.

**Audit Trail:** In computer security systems, a chronological record of system resource usage. This includes user login, file access, other activities, and indications of whether any actual or attempted security violations occurred, either legitimate or unauthorized.

**Authenticate:** To establish the validity of a claimed user or object.

**Authentication:** To positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

**Authorization:** The granting of rights. Authorization mechanisms are used to allow, deny, or limit access to a resource, whether to individuals or remote machines, and are typically based on the authenticated identity of the individual or remote machines requesting access.

**Availability:** Whether or how often a system is available for use by its intended users. Since downtime is usually costly, availability is an integral component of security.

**Business Continuity:** The ability to maintain operations and services, both technology and business, in the event of a disruption to normal operations and services. Assures that any impact or disruption of services is within a documented and acceptable recovery time period and that systems or operations are resumed at a documented and acceptable point in the processing cycle.

**Capacity Planning Methodology:** The process used to determine if a service, application, or process is sufficient to handle volumes at peak times and/or to meet growth projections for a specific period of time. Analysis should consider hardware (including networks, servers, routers, etc.), software (including operating system and application), and personnel.

**Classification:** Categorization (e.g., “confidential,” “sensitive,” “public”) of the information processed by the Service Provider on behalf of the Receiver Company.

**Computer Security:** Technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of information managed by the computer system.

**Confidentiality:** Assuring information will be kept secret, with access limited to appropriate persons.

**Configuration Management:** The management of security features and assurances through control of changes made to a system’s hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the development and operational life of the system.

**Contingency Plan:** A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Synonymous with disaster plan and emergency plan.

**Control Requirements:** Process used to document and/or track internal processes to determine that those established procedures and/or physical security policies are being followed.

**Conversion Plan:** A plan that details transition planning and implementation issues in the period between the execution of an outsourcing agreement and the full production use of the outsourced services.

**Crisis Management:** Overall coordination of an organization’s response to a crisis to avoid or minimize damage to profitability, reputation or capability to operate.

**Data Integrity:** The property that data has not been altered or destroyed in an unauthorized manner.

**Dependent Provider:** Company on which a Service Provider relies to provide some aspect of contracted service to a Receiver Company.

**Disaster Recovery:** Plans for orderly restoration of computing and telecommunications services.

**Due Diligence:** Technical, functional, and financial review to verify the Service Provider’s ability to deliver the requirements specified in its proposal. The intent is to verify that the Service Provider has a well-developed plan and adequate resources and experience to ensure acceptable service, controls, systems backup, availability, and continuity of service to its clients.

**Encryption:** To scramble information so that only someone with the appropriate “key” can access the original information (through decryption). The following chart details public and widely-used or financial industry standards:

Symmetric encryption algorithms	3DES, IDEA, RC4, RC5, AES Candidate Finalists
Asymmetric algorithms	RSA, D-H, ECDH
Digital signature algorithms	DSA, SHA-1, MD5, ECDSA
Key management standards and protocols	ANSI X9.17, CMP, PKCS standard, IETF PKIX standards

**End-to-End Process Flow:** Document that details the flow of the processes, considering automated and manual control points, hardware, databases, network protocols, and real-time versus periodic processing characteristics.

**Exception Reporting:** Report that documents variances in established control requirements.

**Firewall:** A link in a network that relays only data packets clearly intended and authorized to reach the other side. Firewalls help keep computers safe from intentional hacker attacks and from hardware failures occurring elsewhere.

**Gramm-Leach-Bliley Act (GLBA):** The Financial Services Modernization Act. GLBA includes security guidelines containing a range of risk management obligations focused on implementing the congressional policy of protecting customer data. A significant component of the GLBA legislation is the affirmative and continuing obligation for a financial institution to “respect the privacy of its customers.” As part of this privacy-related obligation, GLBA explicitly includes a responsibility to protect certain data—namely the “security and confidentiality of customers’ nonpublic personal information.”

**Hardware:** The physical elements of a computer system; the computer equipment as opposed to the programs or information stored in the machine.

**Implementation Plan:** A plan that details project management requirements and issues to be addressed during the period between the execution of an outsourcing agreement and the full production use of the outsourced services.

**Incident Response:** Plan that defines the action steps, involved resources, and communication strategy upon identification of a threatening or potentially threatening event such as a breach in security protocol, power or telecommunications outage, severe weather, or workplace violence.

**Information Assurance (IA):** Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-

repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

**Information Security:** The result of any system of policies and/or procedures for identifying, controlling, and protecting from unauthorized disclosure, information for which protection is authorized by executive order or statute.

**Information Systems Technology:** The protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that information.

**Information Technology:** Systems technologies, including operations such as central computer processing, distributed processing, end-user computing, local area networking, and nationwide telecommunications. These operations often represent critical services to financial institutions and their customers.

**Integrity:** Ensuring that information will not be accidentally or maliciously altered or destroyed (see Data Integrity).

**Intrusion Detection:** Techniques that attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data; detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.

**Network Security:** Protection of computer networks and their services from unauthorized entry, modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and that there are no harmful side effects. Network security includes providing for data integrity.

**Non-Repudiation:** Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

**Offsite Rotation:** Used for backup and/or disaster recovery; moving a copy of the most current database, information, file, or tape to an offsite storage facility to be used only in an emergency.

**Outsourcing:** In the context of this document, the financial institution's contract with a third party to provide services, systems, or support.

**Password:** A secret sequence of typed characters that is required to use a computer system or software program, thus preventing unauthorized persons from gaining access to the computer or program.

**Penetration:** The successful unauthorized entry to an automated system or access to data (except during authorized testing; see "Penetration Testing" below).

**Penetration Testing:** The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and

implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users.

**Policy:** Organization-level rules governing acceptable use of computing resources, security practices, and operational procedures.

**Production Data:** Real customer or systems information.

**Receiver Company:** The financial institution that has contracted with a Service Provider to perform a specific service.

**Recovery Capability:** Ability to restore or replace systems, data, workareas, staff, utilities or information that have been damaged or lost.

**Recovery Time Objective (RTO):** The maximum time required to resume a business function or IT function following a disaster event.

**Recovery Point Objective (RPO):** The maximum data loss in hours, based on the frequency of offsite backups, resulting from a disaster event.

**Recovery Service Levels:** Collectively, terms that define the speed, quality and quantity of recovery capability in response to a disaster, including recovery time objective, recovery point objective, timely notification, percent of normal production SLAs that will be delivered during recovery mode, etc.

**Request for Proposal (RFP):** A process to obtain specific information about a Service Provider's ability to meet a Receiver Company's requirements and the fees the Service Provider charges for the service. The RFP allows the Receiver Company to outline its business objectives and technical requirements and to solicit responses from Service Providers that describe their ability to meet these needs and related prices.

**Response Time:** The amount of time it takes to complete a process, from the time the data is received until the operation is complete and the results are made available.

**Retention Requirement:** Requirement established by a company or by regulation for the length of time and/or for the amount of information that should be retained.

**Risk Analysis:** The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards; synonymous with risk assessment. Risk analysis is an integral part of risk management.

**Risk Assessment:** A study of vulnerabilities, threats, likelihood, loss, or impact, and theoretical effectiveness of security measures; the process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

**Risk Management:** The total process required to identify, control, and minimize the impact of uncertain events. The objective of a risk management program is to reduce risk and obtain and maintain appropriate management approval.

**Security:** A condition that results from the establishment and maintenance of protective measures (automated systems and rules) that ensure a state of inviolability from hostile acts or influences.

**Security Architecture:** A detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements.

**Security Audit:** An independent review and examination of system records and activities to test for adequacy of system controls, ensure compliance with established policy and operational procedures, and recommend any indicated changes in control, policy, and procedures.

**Security Violation:** An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources.

**Separation of Duties:** The establishment of responsibilities for personnel handling information or systems in order to ensure that there are no conflicting roles and that no transaction can be entered, processed, and approved by the same individual.

**Service Level Agreement (SLA):** Contractually binding clauses documenting the performance standard and service quality agreed to by the Receiver Company and Service Provider. The SLA's primary purpose is to specify and clarify performance expectations, establish accountability, and detail remedies or consequences if performance or service quality standards are not met.

**Service Provider:** Technology service provider, among a broad range of entities including but not limited to affiliated entities, nonaffiliated entities, and alliances of companies providing products and services. This may include but is not limited to: core processing; information and transaction processing, and settlement activities that support banking functions such as lending, deposit-taking, funds transfer, fiduciary or trading activities; Internet-related services; security monitoring; systems development and maintenance; aggregation services; digital certification services, and call centers. Other terms used to describe Service Providers include vendors, subcontractors, external service provider, application service providers, and outsourcers.

**Statement on Auditing Standards No. 70 (SAS 70):** An auditing standard developed by the American Institute of Certified Public Accountants (AICPA). In a SAS 70 engagement, an independent auditor (service auditor) reports on: (1) a service organization's description of its controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements; (2) whether those controls were suitably designed to achieve specified control objectives; and (3) whether those controls had been placed in operation as of a specified date, for example, as of June 30, 2003. This is called a "Type I engagement."

In a Type II engagement, the service auditor reports on everything included in a Type I engagement, as well as whether the controls tested were operating with sufficient effectiveness to provide

reasonable assurance that the related control objectives were achieved during a specified period. A Type II presentation includes the service organization’s description of the controls, as well as the service auditor’s description of the tests he or she performed and the results of those tests. Third-party Service Providers obtain independent assurance on their control objectives and control processes. The period of time covered by a Type II report is at the discretion of the service organization; however, SAS 70 indicates that the report ordinarily should cover a minimum reporting period of six months.

SAS 70 does not test or evaluate a predetermined set of control objectives or control activities that service organizations must achieve. The control activities and objectives should be tailored to the financial statements prepared by the user organizations.

A SAS 70 independent audit report (“service auditor’s report”) is issued to the service organization at the conclusion of a SAS 70 audit engagement. There are two types of service auditor’s reports: Type I and Type II. A Type I report describes the service organization’s description of controls at a specific point in time (e.g., June 30, 2000). A Type II report not only includes the service organization’s description of controls, but also includes detailed testing of the service organization’s controls. The period of time covered by a Type II audit is at the discretion of the auditor or the Service Provider, and is defined in terms of how much evidence needs to be gathered or over what period of time it is necessary to test in order to form an opinion as to the effectiveness of the controls. The contents of each type of report are described in the following table:

Report Sections and Contents of Type I and Type II Reports	Type I Report	Type II Report
1. Independent service auditor’s report (opinion)	Included	Included
2. Service organization’s description of controls	Included	Included
3. Information provided by the independent service auditor, including a description of the service auditor’s tests of operating effectiveness and the results of those tests	Tests and results of tests are not included Optional	Included
4. Other information provided by the service organization (e.g., glossary of terms)	Optional	Optional

In a Type I report, the service auditor will provide an opinion on:

1. Whether the service organization’s description of its controls presents fairly, in all material respects, the relevant aspects of the service organization’s controls that had been placed in operation as of a specific date.
2. Whether the controls were suitably designed to achieve specified control objectives. (In a Type II report, the service auditor will express an opinion on the same items noted above for the Type I report.)
3. Whether the controls tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified. Additional information about the SAS 70 can be found at [www.sas70.org](http://www.sas70.org).<sup>1</sup>

<sup>1</sup> This website is not sponsored maintained by the AICPA, nor have its contents been approved by the AICPA.

**SysTrust:** An assurance service that independently tests and verifies system reliability against a framework of standards, providing an extension of the CPA’s audit and information technology consulting functions. The SysTrust service is made up of a “family” of assurance services designed for a wide variety of systems as may be defined by the entity and, upon attainment of an unqualified assurance report, would entitle the entity to display a SysTrust Seal and accompanying auditor’s report. The principles of SysTrust consist of security, processing integrity, availability and confidentiality. SysTrust branded assurance services include the following, applied in the context of an entity’s defined system:

- **SysTrust – Systems Reliability.** The scope of the assurance engagement includes the security, availability, and processing integrity principles and criteria.
- **SysTrust.** The scope of the assurance engagement includes one or more combinations of the principles and criteria not anticipated with the SysTrust – Systems Reliability engagement.

A SysTrust engagement can be performed on any type of system. A SysTrust engagement cannot be used to provide a practitioner’s opinion on privacy, which is reserved solely for WebTrust. A SysTrust report is required to cover operating effectiveness of the controls and compliance with criteria; compliance with commitments is an optional reporting requirement. A SysTrust system description is normally a detailed description of five system components (infrastructure, software, data, people and processes). The principles and criteria can be used by CPAs to deliver attestation as well as advisory services.

SysTrust was jointly developed by the AICPA and the Canadian Institute of Chartered Accountants (CICA). SysTrust is provided by licensed CPAs and their Canadian counterparts. SysTrust is offered in several other countries as well. Additional information on SysTrust can be found at [www.aicpa.org/trustservices](http://www.aicpa.org/trustservices).

**User:** Any person who interacts directly with a computer system.

**User Identification:** The process, control, or information by which a user identifies himself to the system as a valid user (as opposed to authentication).

**Vicarious Liability:** Liability attributed to a person who has control over or responsibility for another who negligently causes an injury or otherwise would be liable. Whenever an agency relationship exists, the principal is responsible for the agent’s action. The negligence of an employee acting within the scope of employment is attributed to the employer.

**Virus:** A program that can “infect” other programs by modifying them, including a possibly evolved copy of itself.

**Vulnerability:** Hardware, firmware, or software flaw that leaves an AIS open for potential exploitation; a weakness in automated system security procedures, administrative controls, physical layout, internal controls, etc., that could be exploited by a threat to gain unauthorized access to information or to disrupt critical processing.

**Vulnerability Analysis:** Systematic examination of an AIS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

**Vulnerability Scanning:** Systematic examination of systems in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.

**WebTrust:** An assurance service made up of a “family” of assurance services designed for e-commerce-based systems that provides an extension of the CPA’s audit and IT consulting functions. Upon attainment of an unqualified assurance report, an entity is entitled to display a WebTrust Seal and accompanying practitioner’s report on its website. WebTrust’s principles are security, privacy, processing integrity, availability and confidentiality. WebTrust branded assurance services include the following for e-commerce systems:

- **WebTrust Online Privacy.** The scope of the assurance engagement includes the privacy principle and criteria.
- **WebTrust Consumer Protection.** The scope of the assurance engagement includes both the processing integrity and privacy principles and criteria.
- **WebTrust.** The scope of the assurance engagement includes one or more combinations of the principles and criteria not anticipated above.
- **WebTrust for Certification Authorities.** The scope of the assurance engagement includes the principles and related criteria unique to certification authorities (see Section 6).

As mentioned above, WebTrust is performed only on e-commerce systems. WebTrust engagements can be used to provide a practitioner’s opinion on any of the five Trust Services Principles. WebTrust reports cover operating effectiveness of controls, compliance with the criteria, and compliance with commitments supporting the applicable Trust Services principle. A WebTrust system description is normally accomplished by discussing certain information on the entity’s website so as to clearly delineate the boundaries (as well as to communicate certain required disclosures to users).

The principles and criteria can also be used by CPAs to deliver attestation as well as advisory services. WebTrust was jointly developed by the AICPA and the Canadian Institute of Chartered Accountants (CICA). WebTrust is provided by licensed CPAs and their Canadian counterparts. WebTrust is offered in several other countries as well. Additional information on WebTrust can be found at [www.aicpa.org/trustservices](http://www.aicpa.org/trustservices).

### **Sources**

The following sources were used to develop the definitions in the preceding glossary:

The American Institute of Certified Public Accountants website, [www.aicpa.org](http://www.aicpa.org)  
*BITS Voluntary Guidelines for Aggregation Services*, BITS, April 2001  
*Chubb CyberRisk Handbook – Guidelines for Risk Management*, Chubb Group of Insurance Companies  
*Department of Defense Trusted Computer System Evaluation Criteria*, Department of Defense Standard, DOD 5200.28-STD, GPO 1986-623-963, 643 0, December 26, 1985  
FDIC Technology Outsourcing Series, Paper #1 – Selecting a Service Provider  
FDIC Technology Outsourcing Series, Paper #2 – Service Level Agreements  
FDIC Technology Outsourcing Series, Paper #3 – Multiple Service Providers  
*FFIEC IS Examination Handbook*, Federal Financial Institutions Examination Council

*FleetBoston Acronyms and Glossary*, FleetBoston Financial Corp.

M. Abrams, S. Jajodia, and H. Podell, Eds., *Information Security: An Integrated Collection of Essays*,  
IEEE Computer Society Press, January 1995

NSA Glossary of Terms Used in Security and Intrusion Detection

Richard V. Rupp, *Rupp's Insurance & Risk Management Glossary*, CPCU, Second Edition  
*Security Glossary*, SET Solutions, Inc.

SAS 70 Solutions website, [www.SAS70.org](http://www.SAS70.org)

Appendix 5: Disaster Recovery/Business Continuity Matrix

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
<b>Section 2: Business Decision to Outsource IT</b>	The Receiver Company should conduct a risk assessment and business impact analysis to determine the events and environmental surroundings that could adversely affect the Receiver Company. The risk analysis should consider the criticality of the outsourced services or products to the Receiver Company. In most cases the risk assessment and impact analysis should be conducted collaboratively with the affected Receiver Company business units.	A definition of the required recovery time objective(s) (RTO) and recovery point objective(s) (RPO) for each service or product the receiver company is considering outsourcing should be defined during this phase in the outsourcing process. This helps the Receiver Company to determine if regulatory or risk issues will impact its ability to maintain required availability expectations and/or requirements.	As part of the business decision to outsource, the Receiver Company should consider how the relationship will affect its disaster recovery/business continuity plans or any related products or services.	In evaluating the ability to outsource an application, system or service, the Receiver Company should consider how the relationship will affect the institution's testing requirements and/or any related products or services.	The Receiver Company should consider its ability to test and execute internal event management plans and assess the impact of assigning responsibilities to the outsourced provider for components of the plan, such as emergency response notification, escalation, and communications.	The Receiver Company should evaluate its governance structure to determine the effect of coordinating with and overseeing a Service Provider, including identifying any relevant regulatory requirements.	The Receiver Company should determine whether outsourcing will affect existing insurance coverages.

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
<b>Section 3: Considerations for the RFP</b>	<p>The RFP should require evidence that a risk assessment has been conducted to determine the events and environment that could adversely affect the Service Provider. Corresponding risk reduction or mitigation steps should be documented. The RFP response should include a review of the Service Provider's risk profile, considering the criticality of the service or products to the Receiver Company.</p>	<p>Recovery Objective: The RFP should specify the required RTO(s) and RPO(s) for each service or product the client is receiving. RTOs establish the length of time for which a process can be unavailable. RPOs establish the amount of data that can be lost or how old the data can be, e.g., 24 hours since the last backup. The Service Provider should have contingency plans in place to support multiple clients' recovery events.</p>	<p>The RFP should require documented continuity plans and supporting recovery strategies. The plans should consider recovery of activities supported by dependent Service Providers. A periodic maintenance cycle is required, not to exceed 12 months.</p>	<p>The RFP should require minimum testing standards, including a strategy for testing plans (frequency not to exceed 12 months), test schedule, and client involvement goals. Testing requirements should also include type of tests conducted (e.g., tabletop, live test, simulation, end-to-end), test results documentation (including follow-up responsibilities and an ongoing update process for existing plans), Receiver Company observation/participation in Service Provider tests, and regulatory compliance as it relates to testing.</p>	<p>The RFP should require evidence of a formal event-management plan that includes emergency response, escalation and communications at the corporate level. The Service Provider should notify a designated point of contact at the Receiver Company if a disaster or service interruption occurs. Event management should address regular status reporting procedures for use during outages and testing of the event-management plan.</p>	<p>The RFP should require that a process be in place at the Service Provider to ensure accountability and compliance with the goals and objectives of the Receiver Company's continuity planning program. The Service Provider's governance program should be audited regularly and the results monitored and signed off on by its senior executives. Also, the Service Provider should ensure that federal and state regulations are met and managed as they apply to their customers.</p>	<p>The RFP should define any requirements for business interruption insurance sufficient to mitigate any business interruption. The cost and type of insurance coverage should be considered, including an evaluation of the impact outsourcing will have on current insurance coverages. Section 5 provides details on the types of coverage and corresponding contractual considerations.</p>

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
<b>Section 4: Due Diligence Considerations</b>	<ul style="list-style-type: none"> <li>Examine the list of threats from possible internal and external sources identified by the Service Provider, along with the assessment of impact and probability. Verify that the Service Provider has introduced controls to mitigate the effects of identified threats. Review the types of business functions that the Service Provider has identified as critical to ensure that Receiver Company requirements will be met.</li> </ul>	<ul style="list-style-type: none"> <li>Determine if offsite backup checks are performed frequently enough to meet the Receiver Company's RPOs. Backup checks should include examination of:                             <ul style="list-style-type: none"> <li>controls on offsite storage site environment and access;</li> <li>encryption standards including backup, storage and recovery of encryption keys; and</li> <li>location of secondary storage facility relative to the primary facility.</li> </ul> </li> <li>Verify the integrity of the backup either through planned or random sampling (particularly in</li> </ul>	<ul style="list-style-type: none"> <li>Review the written recovery plan. Verify that it is updated annually and that copies are stored at the recovery site and other secure offsite locations.</li> <li>Examine the plan for coverage of:                             <ul style="list-style-type: none"> <li>remote command center;</li> <li>recovery site;</li> <li>staff relocation plans;</li> <li>recovery teams with defined tasks;</li> <li>critical third parties (recovery vendors, equipment vendors, transportation, utilities, and public safety);</li> <li>activation/notification method;</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Review recovery testing efforts performed by the Service Provider, including the scope and results of the test(s). Determine when the continuity plans for the Receiver Company were last tested successfully. Determine the frequency, scope and type of testing (e.g., walkthrough, simulation, etc.).</li> <li>Determine whether test documentation contains scope, objectives, timeline and results.</li> <li>Determine whether testing is certified by an independent third party and obtain a copy of the certification.</li> <li>Determine if the</li> </ul>	<ul style="list-style-type: none"> <li>Examine the Service Provider's documented event-management plan for clearly defined emergency response, escalation and communication s procedures, including notification of designated Receiver Company contacts.</li> <li>The Service Provider should include representation from:                             <ul style="list-style-type: none"> <li>corporate communications (internal to employees and external to customers, government agencies, regulators and the media);</li> <li>building security;</li> <li>building</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Verify that the Service Provider has a documented process in place to ensure accountability and compliance with the goals and objectives of the Receiver Company's continuity program. The Service Provider's governance program should be audited regularly and the results should be monitored and signed off on by its senior executives. Also, the Service Provider should ensure that federal and state regulations are met and managed as they apply to their customers.</li> </ul>	<ul style="list-style-type: none"> <li>Ensure minimum liability insurance coverage is in place, consistent with the Receiver Company's standards.</li> <li>Obtain copies of any insurance policies, including liability, errors and omissions and business continuity/disaster recovery policies.</li> <li>The Receiver Company should review its own existing insurance terms to determine whether any policies are affected by the new Service Provider relationship.</li> </ul>

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
Section 4: Due Diligence (cont.)		<p>open systems environments).</p> <ul style="list-style-type: none"> <li>• Determine whether the Service Provider's recovery time is sufficient to meet the receiver company's RTO.</li> <li>• Based on continuity strategies defined in the Service Provider's plans, determine what the <b>maximum</b> recovery time will be for the Service Provider to restore systems and, upon restoration, what the worst-case data recovery time will be.</li> <li>• Determine whether these criteria have been validated through testing.</li> </ul>	<ul style="list-style-type: none"> <li>- communications to customers;</li> <li>- communications with the media;</li> <li>- communications with public safety services; and</li> <li>- acquisition of critical IT resources.</li> <li>• Verify that adequate geographic separation exists between the Service Provider's primary facility and their recovery site(s) and storage facility(ies).</li> <li>• Verify that network documentation is maintained for production and recovery configurations, including connections to external data sources not controlled by</li> </ul>	<p>Receiver</p> <p>Company may participate in recovery tests and to what extent (e.g., observation, planning, testing, data entry, observation of results, validation against production results).</p> <ul style="list-style-type: none"> <li>• Determine if the test results demonstrate recoverability within the recovery service levels (e.g., recovery time and data loss) required by the receiver company.</li> <li>• Determine if test results are reviewed and signed off on by the Service Provider's senior management, and whether the</li> </ul>	<p>management;</p> <ul style="list-style-type: none"> <li>- information systems management (including data security and disaster recovery);</li> <li>- human resources;</li> <li>- dependent Service Providers;</li> <li>- essential business units;</li> <li>- public safety agencies; and</li> <li>- executive management.</li> </ul>	<ul style="list-style-type: none"> <li>• Verify that a specific group or individual at the Service Provider is responsible for monitoring the company's compliance with Receiver Company business continuity goals and objectives and with all applicable federal and state regulations. Ensure that testing of continuity plans validates regulatory compliance and that test results are reported to the Receiver Company's compliance group or appropriate individual.</li> <li>• Review follow-up procedures for non-compliance</li> </ul>	

Appendix 5: Disaster Recovery/Business Continuity Matrix

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
		<ul style="list-style-type: none"> <li>• Determine if the Service Provider has established “preferred priority restoration” with other clients.</li> <li>• Determine the probability of other clients declaring a disaster simultaneously and the impact this could have on the Receiver Company.</li> <li>• Examine the contingency plans in place to support multiple clients’ recovery events should resources be required simultaneously.</li> </ul>	<p>the Service Provider.</p> <ul style="list-style-type: none"> <li>• Determine if processing can be accomplished from the recovery site using normal production processes. If not, determine whether the recovery plan contains documentation of special processes.</li> </ul>	<p>results are available to the Receiver Company.</p> <ul style="list-style-type: none"> <li>• Determine if testing anomalies are documented, and whether root-cause analysis was applied and used to modify the recovery plan and subsequent test objectives.</li> </ul>		<p>issues and ensure that responsibility is assigned, remedies are identified, and reasonable target dates are established. Results should be used to update continuity plans.</p>	
<b>Section 5: Contractual, Service Level and Insurance</b>	<ul style="list-style-type: none"> <li>• The contract should include a provision requiring a documented</li> </ul>	<ul style="list-style-type: none"> <li>• The recovery objectives should reflect the considerations and service level</li> </ul>	The contract should require evidence of a written plan and include requirements for	<ul style="list-style-type: none"> <li>• Joint disaster recovery and business continuity plan testing should be conducted</li> </ul>	The Service Provider should have a process for managing both minor and major disruptions to	<ul style="list-style-type: none"> <li>• Statements documenting compliance with applicable government regulations are</li> </ul>	The contract should include a requirement for proof of insurance. See section 5.5.

Appendix 5: Disaster Recovery/Business Continuity Matrix

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
Section 5: Contractual, Service	<p>risk analysis.</p> <ul style="list-style-type: none"> <li>The Receiver Company and Service Provider should review the risk analysis regularly and evaluate requirements based on changes in the outsourced service.</li> </ul>	<p>metrics outlined in the RFP.</p> <ul style="list-style-type: none"> <li>Backup – Data backup requirements and schedule should reflect the RTOs and RPOs of the Receiver Company, particularly with respect to critical data. (Some data may require simultaneous processing by geographically separated centers and networks or real-time offsite data mirroring, while other data may only require a daily offsite rotation.)</li> <li>Offsite Storage – Backup storage media should be sent to an offsite location on a scheduled rotation and</li> </ul>	<p>updating the plan. Requirements may be driven by time, service, or environmental considerations.</p> <p>The Service Provider should provide the Receiver Company with proof of business continuity plans that addresses any outage that would affect the Service Provider’s ability to provide service to the Receiver Company. The plans should include defined strategies for standby and work-around procedures, and for addressing production failures, facility shutdowns, personnel shortages or reduced staff, supply-chain issues, affects on customers and</p>	<p>periodically. Testing should include all scenarios that could potentially cause an unacceptable interruption to production information processing. Within 30 days of testing, the Receiver Company should be given a report with all test and exercise documentation, including results of testing the Receiver Company’s processes and technologies.</p> <ul style="list-style-type: none"> <li>The frequency of technology and business recovery testing, as well as expectations regarding Receiver Company participation in those tests,</li> </ul>	<p>delivery of the contracted services or products. The Service Provider should regularly report activity related to disruption-management testing, activation and issue resolution to the Receiver Company. Additionally, a documented process should exist to ensure notification and escalation lists and procedures remain current. Procedures for contacting the Receiver Company during holidays and outside of normal business hours should also be documented.</p> <ul style="list-style-type: none"> <li>Emergency Notification – In the event of a disaster or</li> </ul>	<p>required.</p> <ul style="list-style-type: none"> <li>No provision in the contract, in particular any <i>force majeure</i> terms, should remove the Service Provider’s obligation to provide recovery services at the required service levels.</li> <li>Failure to comply with any of the recovery terms in the contract should be referred to adequate remedies and/or termination terms of the contract.</li> </ul>	

Appendix 5: Disaster Recovery/Business Continuity Matrix

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
Level and Insurance (cont.)		<p>retention period. Transmittal records of this movement should be stored at both onsite and alternate locations. Backup media should be secured before being transported and remain secured until they are returned to the primary site. Reasonable distance between the primary and offsite location should exist to mitigate the risk of one event disabling both facilities.</p> <ul style="list-style-type: none"> <li>Equipment Recovery – Detailed information on recovering installed equipment for</li> </ul>	<p>work backlog. Procedures for returning to normalization should also be included.</p>	<p>should be specified and made available prior to the test.</p> <ul style="list-style-type: none"> <li>The Receiver Company should identify requirements for accessing the recovery location.</li> </ul>	<p>other emergency that affects the processing schedules, an emergency notification schedule should follow.</p> <p><i>SLA Consideration:</i> The minimum and maximum recovery time frames associated with a Service Provider’s environment, minimum and maximum time to data integrity validation, and minimum and maximum time that the receiver company would be unable to perform production tasks should all be stated. Such schedules should consider the federal, state and local</p>		
Section 5: Contractual,							

Appendix 5: Disaster Recovery/Business Continuity Matrix

Service Level and Insurance	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
		<p>salvage operations at the Service Provider site should be stored in a secure location with recovery plans.</p> <ul style="list-style-type: none"> <li>Recovery Prioritization – The order in which the Service Provider will recover processes and systems should be available to the Receiver Company based on the recovery objectives defined by the Receiver Company. The Receiver Company should be notified of any changes to this prioritization prior to the Service Provider making the change.</li> </ul>			<p>requirements pertinent to emergencies such as those related to power, transportation or environment.</p> <ul style="list-style-type: none"> <li>Computer Forensics – If forensic tests must be conducted to determine the cause of an application, system, or service failure, the Service Provider should follow appropriate evidence-handling procedures.</li> </ul>		

Appendix 5: Disaster Recovery/Business Continuity Matrix

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
<b>Section 6: Procedures for Supporting Specific Controls, Requirements and Responsibilities</b>	Verify that mitigation efforts are maintained for the risks identified in the risk analysis reports.	Verify that risk analysis information (BIA reports, RTO/RPO listings) is used to update disaster recovery and business continuity plans.	Verify that controls are in place for the storage and handling plans, including records management and offsite storage.	Validate security procedures are in place for handling receiver company data during test exercises.	Validate disaster declaration authority and notification lists.	<ul style="list-style-type: none"> <li>• Validate control procedures for maintaining system integrity and recovery.</li> <li>• Validate control procedures for data retention.</li> <li>• Validate control procedures for data backup and offsite storage.</li> </ul>	Verify that insurance coverage is maintained as systems, services, locations and other aspects of the business change.

Appendix 5: Disaster Recovery/Business Continuity Matrix

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
<b>Section 7: Implementation and Conversion</b>	<p>The Receiver Company should expect to maintain its existing disaster recovery and business continuity plans and resources until after verification that the Service Provider is fully operational. The risk analysis should include:</p> <ul style="list-style-type: none"> <li>• verification of backup and recovery procedures;</li> <li>• development of an appropriate contingency plan and exit strategy in the event the Service Provider fails to implement;</li> <li>• verification of an appropriate emergency communications plan;</li> </ul>		<p>The Receiver Company should verify that the Service Provider is documenting appropriate disaster recovery and business continuity plans.</p>	<p>The Service Provider/The Receiver Company/Both parties should:</p> <ul style="list-style-type: none"> <li>• conduct recovery testing prior to or soon after production conversion, sufficient to verify that recovery objectives can be met;</li> <li>• conduct a post-mortem review and document lessons learned from every test; and ensure business continuity/disaster recovery plans are updated following each test exercise.</li> </ul>	<p>Following any major event, the Receiver Company and Service Provider should conduct a post-mortem review. During the review, open issues should be identified and responsibility assigned for resolving those issues. High-level communications or post-implementation controls, processes and management responsibilities should be documented.</p>		

*Appendix 5: Disaster Recovery/Business Continuity Matrix*

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
	<ul style="list-style-type: none"> <li>• verification of control procedures;</li> <li>• verification of contingency plan and exit procedures for conversions; and</li> <li>• verification of proper planning and testing of all implementations or conversions prior to implementation date.</li> </ul>						

Appendix 5: Disaster Recovery/Business Continuity Matrix

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
<b>Section 8 Ongoing Relationship Management</b>	<ul style="list-style-type: none"> <li>Determine how the risk matrix for the application, system or service is maintained and updated for each Service Provider.</li> <li>Review the risk analysis and Service Provider's business continuity/disaster recovery program annually.</li> <li>Review the Service Provider's change-management processes and controls annually</li> </ul>	<ul style="list-style-type: none"> <li>Verify that established recovery service levels are being met and exceptions are being documented, with actions taken accordingly.</li> <li>Verify that the Service Provider's recovery time capability meets or exceeds the established recovery.</li> <li>Review recovery service levels annually, including business requirements and technology changes and enhancements time objective.</li> </ul>	Verify that business continuity/disaster recovery plans are maintained annually and/or updated following major system enhancements.	Verify through participation or direct observation that business continuity/disaster recovery plans are being tested annually and/or according to the expectations in the contract.	<ul style="list-style-type: none"> <li>Verify key, emergency contacts to use in the event of escalation of critical issues.</li> <li>Conduct a post mortem following any activation of the Service Provider's recovery plan and identify and address any issues that affect the ability to deliver the recovery objectives.</li> </ul>	<ul style="list-style-type: none"> <li>Verify that the Service Provider has a process in place to identify and assess new control exposures resulting from a change.</li> <li>Verify the Service Provider's technology recovery test objectives and conclusions.</li> <li>Review change-control records.</li> <li>Review third-party audits of business continuity/disaster recovery plans and testing results.</li> </ul>	The Receiver Company should ensure that insurance requirements are being met and required certificates of insurance are received in a timely manner.
<b>Section 9</b>	In addition to the elements listed elsewhere, in Cross-Border Relationships, the Receiver Company should review the following:						
<b>Cross Border Outsourcing</b>	<ul style="list-style-type: none"> <li>What local conditions should be evaluated</li> </ul>	Are there levels of service degradation that might invoke	<ul style="list-style-type: none"> <li>How often can and should data be transferred/copied to the</li> </ul>	<ul style="list-style-type: none"> <li>How will Receiver Company's disaster-</li> </ul>	<ul style="list-style-type: none"> <li>In an emergency, how will essential personnel</li> </ul>	<ul style="list-style-type: none"> <li>The Receiver Company should evaluate its governance</li> </ul>	<ul style="list-style-type: none"> <li>The Receiver Company should determine</li> </ul>

Appendix 5: Disaster Recovery/Business Continuity Matrix

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
	(e.g., likelihood of earthquakes or volcanoes) and what threat scenarios are included in the Service Provider's evaluation? Has the Service Provider established a system for monitoring and assessing political, economic, and country risk issues that might affect its ability to conduct business with the Receiver Company? Does this monitoring process include US government legal or regulatory changes to the	disaster recovery plans?	Receiver Company for storage in order to comply with regulatory and business requirements? What capabilities exist for safely transporting data to offsite storage locations? <ul style="list-style-type: none"> <li>• Can the Receiver Company back up the Service Provider at its location?</li> <li>• At the backup site, is there a standard development or processing environment to aid in the event of a rapid transition?</li> <li>• How often does the Service Provider test its disaster recovery/business continuity plans?</li> </ul>	recovery tests be conducted to include the cross-border location?	(Receiver Company or Service Provider) be evacuated from the country? (Considerations include identifying and notifying personnel, determining whether they hold current visas and passports, and designating housing and backup sites.)	structure to determine the effect of coordinating with and overseeing a Service Provider located outside of the United States, including identifying any relevant regulatory requirements.	whether outsourcing outside of the United States will affect existing insurance coverages.

Appendix 5: Disaster Recovery/Business Continuity Matrix

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
	<p>Receiver Company's ability to transact business or travel to the Service Provider's location?</p> <ul style="list-style-type: none"> <li>In countries where there are few or no third-party providers of disaster-recovery services, what contingency plans are in place?</li> </ul> <p>Receiver Companies should evaluate risks and may consider establishing a local entity to which assets and employees can be transferred if necessary. If practicable, consider asking for</p>		<ul style="list-style-type: none"> <li>How often does the Service Provider audit third-party providers of disaster recovery/business continuity plans?</li> <li>Is diverse path routing (local and global circuits) available from the Service Provider?</li> </ul>				

Appendix 5: Disaster Recovery/Business Continuity Matrix

	Risk Analysis	Recovery Objective	Plans	Test	Event Management	Governance	Insurance
	<p>“step-in rights,” which allow the financial institution to provide the services, possibly remotely, until the Service Provider issues are resolved.</p> <ul style="list-style-type: none"> <li>• Are satellite or microwave communications available?</li> <li>• Are there levels of service degradation that might invoke disaster recovery plans?</li> </ul>						

## **SHARED ASSESSMENTS**

The Shared Assessments Program provides both organizations that outsource services and service providers an efficient, cost effective means of meeting internal and external compliance and audit requirements. By focusing on principal information services control areas, the program is an excellent risk management tool for organizations that incorporate program results into an enterprise risk monitoring plan.

The economic value for Shared Assessments is based on the fundamental concept that replacing a repetitive, labor-intensive process with a non-repetitive, labor-saving approach makes business sense because it reduces operational expense and in many cases allows for a redeployment of staff.

### **The Program Tools**

The Shared Assessments Program documents are aligned with ISO 27002:2005, PCI DSS, and COBIT, as well as FFIEC Guidance.

As part of the Shared Assessments Program and consistent with ISO 27002:2005, twelve areas of information security management provide the foundation for two complementary program tools. These tools, described below, are designed to document the service provider's management of information security controls. Both tools and much more information about the Shared Assessments program is available at the program's website, [sharedassessments.org](http://sharedassessments.org).

### **Agreed Upon Procedures (AUP)**

This on-site assessment tool was developed by Shared Assessments program members including the largest financial institutions and service providers in the U.S. The AUP was reviewed by the Big 4 accounting firms acting as technical advisers. It provides objective and consistent procedures that can be performed under each control area during the onsite assessment. Procedures address control objectives in:

- risk management;
- information security policy;
- organization of information security;
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access control;
- information systems acquisition;
- development and maintenance;
- information security incident management;
- business continuity management; and
- compliance.

The procedures allow client organizations to view results in the context of industry risk management. The AUP is completed by either an assessment firm or an audit firm and the results are provided to the service provider. The service provider can then share the reports with clients.

### **Standardized Information Gathering (SIG) Questionnaire**

The SIG was developed by BITS members to address the twelve control areas covered in ISO 27002:2005. The questionnaire can be used to obtain required documentation, establish a profile for each control area, and obtain verifiable information for each. As a standalone document, the SIG is used by institutions and service providers to assist in evaluating information security controls.

When the SIG and AUP are completed, recipients have evidence that the controls outlined in each either exist or do not exist. Institutions are then better able to identify risks, comply with regulatory requirements, and reduce inconsistencies in evaluating the information they receive from their service providers.

### **The Santa Fe Group's Role**

The Santa Fe Group is a preferred service provider to BITS and is dedicated to supporting the development of the Shared Assessments Program. For more information, please go to [santa-fe-group.com](http://santa-fe-group.com).



**FOLEY HOAG** LLP  
ATTORNEYS AT LAW

**NON-US NATIONALS WORKING IN THE US – SUMMARY OF VISA REQUIREMENTS**

Several pieces of legislation have been introduced in the US Congress which, if enacted, would significantly change the L-1 program, making it look much more like the H-1B program.

	<b>B-1</b> <b>(“Business visitor”)</b>	<b>L-1</b> <b>(“Intracompany transferee status”)</b>	<b>H-1B</b> <b>(“Temporary worker”)</b>
<b>1. Who is eligible?</b>	Direct employees of foreign company.	Employees of U.S. affiliate of foreign company who have worked abroad for the company or an affiliate for more than 1 year and are managers or have specialized company knowledge.	Professional foreign nationals possessing special skills. Payment of prevailing U.S. wages and working conditions required.
<b>2. Duration</b>	Typically 1-3 months, but at discretion of INS at port of entry.	Normally an initial period of 3 years, with subsequent extensions of 4 more years for managers and 2 more years for specialized knowledge employees. Subject of recent critical focus by INS in outsourcing context.	Up to 6 years.
<b>3. Procedures and time to obtain</b>	Depends on country of origin. For some countries (e.g., India), application must be made at U.S. Consulate; for other “designated” countries, foreign nationals may apply at port of entry.	Petition filed by the U.S. employer with the INS to establish individual qualifies for L-1 classification, (2-3 months) and then an application by the individual at the U.S. Consulate for the actual L-1 visa (1-2 weeks).	Standard processing, 4 months. Expedited processing (\$1000 additional fee), 2 weeks.

	<b>B-1</b> <b>(“Business visitor”)</b>	<b>L-1</b> <b>(“Intracompany transferee status”)</b>	<b>H-1B</b> <b>(“Temporary worker”)</b>
<b>4. Transferability to a new employer in U.S.</b>	If a foreign national is in U.S. on a B-1 visa, new employer must file petition for H-1B. Foreign national can stay in U.S. while petition pending, but cannot commence work with new employer until petition is approved.	There is some flexibility to move around the qualifying company group; it is not transferable to another company outside the company group. If outside company group, new employer must file petition for H-1B. Foreign national can stay in U.S. while petition pending, but cannot commence work with new employer until petition is approved.	Employee is eligible to work for new employer as soon as transfer petition is filed. Note, however, that the 6 year maximum is a cumulative total, including all prior employment with H-1B status.
<b>5. Effect of cessation of employment (e.g., due to bankruptcy, disaster recovery circumstances)</b>	Foreign national loses nonimmigrant status and must promptly leave U.S., unless transfers to new employer as noted in 4.	Foreign national loses nonimmigrant status and must promptly leave U.S., unless transfers to new employer as noted in 4.	Current employer must notify INS of termination of employment and pay foreign national’s reasonable return costs home, unless transfers to new employer as noted in 4.

**Other Visa Categories**

TN-1 status: available to Canadian citizens under NAFTA who are entering to work in specific designated fields and who typically have at least a Bachelor’s degree in that field.

E-1/E-2 status: this is a very complicated category. In summary, it is available to employees of foreign companies which are owned by nationals of a country with which U.S. has a treaty of trade or commerce who are coming to U.S. to facilitate that international trade or to oversee an investment in U.S.

This table was last reviewed by Foley Hoag on July 31, 2003