BITS

FINANCIAL SERVICES ROUNDTABLE

BITS FRAMEWORK:
MANAGING TECHNOLOGY RISK FOR INFORMATION TECHNOLOGY (IT) SERVICE PROVIDER RELATIONSHIPS

SUBMITTED TO THE FINANCIAL SERVICES ROUNDTABLE AND BITS BOARDS OF DIRECTORS FOR ENDORSEMENT AT FALL CONFERENCE 2001

Version 3.2a
August 17, 2001

TABLE OF CONTENTS

INTRODUCTION

The financial services industry increasingly relies on information technology (IT) service providers ("Service Providers") to support the online delivery of financial services. This change 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 a financial services company's risk assessment and management of outsourced IT services.

In response to this business and technology environment, the BITS Information Technology (IT) Service Provider Working Group developed this document, the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships ("Framework")*. This **industry** approach to risk management strategies for IT service-provider outsourcing is based on the Working Group's interpretation of regulatory requirements and best practices. Overall, the *Framework* articulates the Working Group's recommendations for managing IT Service Provider relationships.

The *Framework* comprehensively covers most aspects of managing IT control, design and management practices where IT services are under consideration for outsourcing or have been outsourced. However, consistent with current regulatory guidance, the *Framework's* recommendations will likely be applied selectively based on a financial services company's risk assessment results. In this way, the *Framework* should be used as reference material, to stimulate firms to ask the right questions and to complement individual institution risk management policies.

The *Framework* is not an official government publication, nor does BITS suggest strict adherence to the defined *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 Council 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 the requirements established by the Office of the Comptroller of the Currency, the Federal Reserve Board, and other key regulators, consult Appendix 2 of this document for a matrix of the *Framework's* language in relation to the regulatory environment.

Outsourcing is defined as any circumstance where customer information or critical company data is outside the direct control of the financial services company. Examples of services that fall within the context of this *Framework* include:

- aggregation;
- development, enhancement and maintenance of an application in the context of an outsourced service (not a stand-alone purchase of software);
- authentication;
- core processing;
- online banking and other Internet-related services;
- security monitoring;
- storage or processing of customer information subject to the security and confidentiality provisions of the Gramm-Leach-Bliley Act of 1999; and
- storage or processing of critical company data.

The *Framework* closely parallels the FFIEC guidance, "Risk Management of Outsourced Technology Services," issued November 28, 2000. According to this guidance, " [the financial services company] board of directors and senior management are responsible for understanding the risks associated with [outsourced IT services] and ensuring that effective risk management practices are in place." In addition, the guidance notes that "as part of this responsibility, the board and management should assess how the outsourcing arrangement will support the [financial services company's] objectives and strategic plans and how the Service Provider's relationship will be managed."

The *Framework* also conforms to the requirements of the Federal Deposit Insurance Corporation's (FDIC) FIL-68-99 – "Risk Assessment Tools and Practices" issued in July 1999, and the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information," effective July 1, 2001 by issuance of OCC 2001-35 – Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information, released in July 2001. According to the Examination Procedures, financial services companies will be examined for their assessment of measures taken to oversee service providers. The examination will include a review of the financial services company's due diligence in selecting a service provider, monitoring of performance and security of both ongoing operations and cases of suspected or known malicious activity, and review of the financial condition of the Service Provider. The examination will include a review of all historical contracts with reference to compliance with the examination requirements by July 1, 2003.

Implementation of this industry-wide approach will more effectively provide a common understanding among IT Service Providers, address known control weaknesses in outsourced IT services, and result in more consistent and appropriate levels of management by financial services companies that outsource IT services.

For additional information about the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships*, contact:

Sharon O'Bryan, ABN AMRO, 773-714-3452, sharon.k.o'bryan@abnamro.com
Jim Dempster, Metavante Corporation, 414-357-2540, jim.dempster@metavante.com
Viveca Ware, ICBA, 202-659-8111, viveca_ware@icba.org
Faith Boettger, BITS, 202-289-4322, Faith@fsround.org
Peggy Lipps, BITS, 202-289-4322, Peggy@fsround.org
Ben Stafford, BITS, 202-289-4322, Ben@fsround.org

IT SERVICE PROVIDER WORKING GROUP

CO-CHAIRS: Sharon O'Bryan, ABN AMRO
Jim Dempster, Metavante Corporation
Viveca Ware, Independent Community Bankers of America

SECTION AUTHORS

Jim Dempster, Metavante Corporation
Robert Drozdowski, America's Community Bankers
Andrew Gault, PNC Bank
Ron Mitchell, State Farm Mutual Insurance
Sharon O'Bryan, ABN AMRO
Greg Stelly, Regions Financial Corporation
Lari Sue Taylor, FleetBoston Financial
George Vrabel, Bank of America Corporation
Martin Wake, Mercantile Bankshares Corp.
John Walsh, Allfirst Financial, Inc.
Viveca Ware, Independent Community Bankers of America

PARTICIPATING INSTITUTIONS

ABN AMRO North America, Inc.
Allfirst Financial, Inc.
America's Community Bankers
American Bankers Association
AmSouth Bancorporation
AMCORE Financial, Inc.
Associated Banc-Corp
Bank of America Corporation
BANK ONE CORPORATION
BB&T Corporation
Capital One Financial Corporation
Centura Banks, Inc.
Charles Schwab Corporation, The
Citigroup, Inc.
City National Corporation
Comerica, Incorporated
Compass Bancshares, Inc.
Cullen/Frost Bankers, Inc.
Credit Union National Association
Edward Jones Investments
Fidelity Investments
First National Nebraska, Inc.
First Tennessee National Corporation
First Union Corporation
First Virginia Banks, Inc.
FleetBoston Financial Corporation
Ford Financial Corporation
Fortis, Inc./ Assurant Group
Goldman Sachs Group, Inc.
Harris Bankcorp, Inc.
Hibernia Corporation
Home Street Bank
IBJ Whitehall Financial Group
Independent Community Bankers of America
KeyCorp
M&T Bank Corporation
Mellon Financial Corporation
Mercantile Bankshares Corporation
Metavante Corporation
Nationwide
Northern Trust Corporation
PNC Financial Services Group, Inc.
Regions Financial Corp.
State Farm Mutual Insurance Companies
SunTrust Banks, Inc.
Synovus Financial Corp.
The Chubb Corporation
Wachovia Corporation
Whitney National Bank
Zurich U.S.

PARTICIPATING ASSOCIATIONS

American Institute for Certified Public Accountants (AICPA)
Association for Financial Technology (AFT)
Bank Administration Institute (BAI)
International Security Trust & Privacy Alliance (ISTPA)
Information Technology Association of America (ITAA)
National Automated Clearing House Association (NACHA)
Securities Industry Association (SIA)

PARTICIPATING SERVICE PROVIDERS

Alltel
Arthur Andersen
AT&T
Axys Solution
Checkfree
Computer Sciences Corporation
Compuware
Counterpane
Digital Insight
DynCorp Information Systems
EDS
EMC Corporation
Ernst & Young
First Data
Fiserv
Gartner Group
Grant Thornton
IBM
Intel
Intrieve
ISS
Jordan & Jordan
LegalNetworks
McGriff
Metavante
Online Resources
PricewaterhouseCoopers
Smartpipes
Spherion
TPI Sourcing
Unisys Financial Services
Vigilinx
Wave Systems

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 document 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* will be performed continuously and should be integrated into the Receiver Company's business practices. Moreover, application of the *Framework* will vary depending on whether the Service Provider's environment is shared or dedicated.

1.1 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 must 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, using the end-to-end process flow (Section 3).
- Define backup, availability, and recovery requirements and responsibilities, using the end-to-end process flow (Section 3).
- Perform due diligence in selecting an IT Service Provider (Section 4).
- Validate evidence of general controls verification (Section 4).
- Validate evidence of control(s) verification and recovery capability of specific components according to end-to-end process flow (Section 4).
- Define contractual and service level agreements ("SLA") (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).

1.2 In the implementation of these steps, a variety of internal functions could be part of the due diligence and control validation process. Some organizations may have or may consider adding an IT Vendor Relations function to select and manage this process. Depending on a financial service company's size, the process could include representatives from:

- information security;
- information technology operations and support;
- incident response/CERT teams;
- business continuity;
- 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 It should be noted that each outsourced IT Service Provider relationship poses unique processing circumstances and the responsibilities of stakeholders may vary accordingly. Each financial services company on a case-by-case basis must determine participation in the risk assessment process and the allocation of responsibilities among stakeholders. In addition, each company should consider the application of this *Framework* based on the risk, complexity, nature, and scope of the outsourced IT services under consideration.

Furthermore, a financial services company should consider the following criteria when determining the extent to which this *Framework* should be used in managing the IT Service Provider relationship:

1.3.1 The system is part of the financial services company's strategic plan.

1.3.2 Customer and/or sensitive information is processed, stored, and/or transmitted.

1.3.3 Mitigating manual controls are not practical (e.g., high-volume systems).

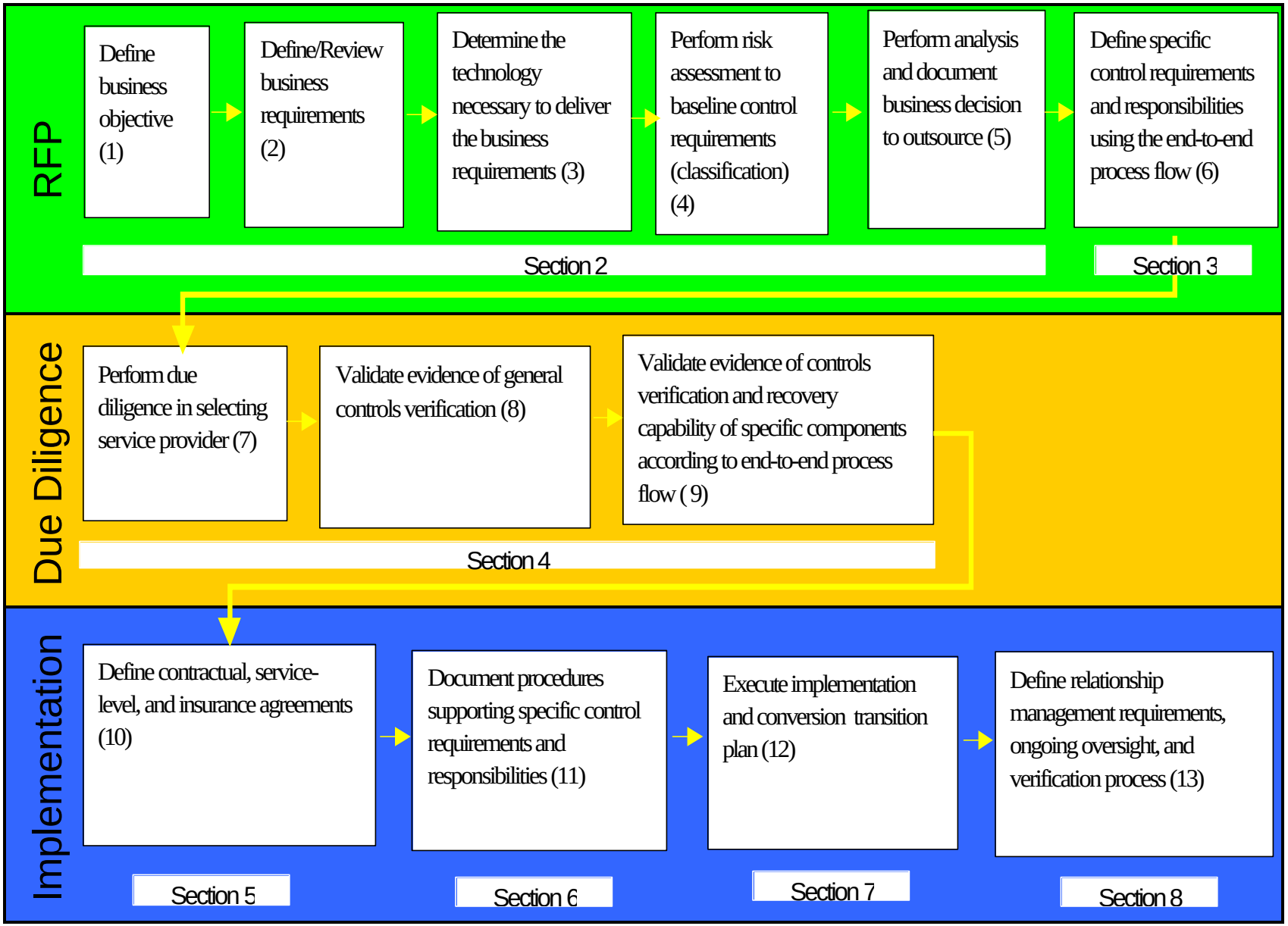
1.3.4 Adverse publication of unauthorized access could lead to loss of customer confidence in the financial services company's products and services.

1.3.5 Access control systems are managed by a third party.

1.3.6 The platform tools technology direction of the outsourcing service provider is a consideration.

1.4 The steps that a financial institution would take in evaluating an IT outsourcing decision are presented as a high-level flow diagram on the following page. The diagram shows the steps that are detailed throughout the *Framework* in relation to the Request for Proposal ("RFP") process, due diligence stage, and implementation phase of a decision to outsource IT services.

IT Framework Flow Diagram



SECTION 2: BUSINESS DECISION TO OUTSOURCE IT SERVICES

Section 2 provides guidance on which 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, 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 within 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 8 of this *Framework*; e.g., Section 4 addresses verification of how the Service Provider delivers the requirements specified in Section 3, and Section 5 provides detail about insurance that could be useful in documenting item 2.7 of this section. Considerations outlined in this section will be based upon the relationship with the Service Provider 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.

Deciding on Goals, Scope, and Risks

2.1 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. This definition is equally important in determining the levels of risk/reward that support business and strategic plans.

- 2.1.1 Define the business objectives to be achieved through the proposed technologies or services.
- 2.1.2 Define the criticality of this system or service to future business plans.
- 2.1.3 Define requirements regarding data accuracy, authentication, confidentiality or integrity.
- 2.1.4 Define regulatory and security standards to be met in safeguarding customer information.
- 2.1.5 Define the interaction this system will have with the Internet and with existing Service Provider relationships, if applicable.
- 2.1.6 Determine the interaction (written, electronic, verbal or face-to-face) the outsourced provider will have with the Receiver Company's customers.
- 2.1.7 Determine the business project sponsor to provide executive oversight.
- 2.1.8 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.

2.2.1 State the Receiver Company's requirements for handling the data, related security and privacy requirements, and classification of data.

2.2.2 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.

2.2.3 Define requirements for system and user administration.

2.2.4 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.

2.2.5 Define the system life cycle, expected timeline of the project, and ongoing support and services.

2.2.6 Determine volumes expected, both peak and average, during timeframes (e.g., end of month processing).

2.2.7 Determine hours of availability of system and allowable maintenance windows.

2.2.8 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.

2.3.1 Recommend the application types to be used by the Service Provider to perform the business function services for the Receiver Company.

2.3.2 Determine hardware environment(s) to be used to perform Receiver Company services.

2.3.3 Determine the database environment to be used to store Receiver Company data.

2.3.4 Determine network infrastructure requirements.

2.3.5 Determine technology requirements to implement the required level of security.

2.4 Perform a risk analysis 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) plus ongoing maintenance. The risk must include both direct hard-dollar loss and reputation impact.

The degree to which the *Framework* is used is dependent upon the degree to which the following criteria are met in the Service Provider relationship:

2.4.1 The system is part, or may become part, of the strategic plan for the financial institution.

2.4.2 Customer and/or sensitive information is processed, stored, and/or transmitted.

2.4.3 Manual controls are not practical (e.g., high volume-systems).

2.4.4 Publication of an unauthorized access could lead to loss of customer confidence in the financial institution's strategic products and services.

2.4.5 Access control systems are to be managed by a third party.

2.4.6 Platform tool technology direction is appropriately defined.

2.5 Define barriers to success in utilizing internal or external IT resources.

Determine what would limit success in achieving the business objectives if internal or 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.

Deciding on Costs

2.6 Perform internal versus external cost analysis.

In order to protect shareholder investment, decisions relative to cost management must be carefully thought through and the cost of performing IT processing must be assessed. Internal versus external sourcing costs, which will be 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:

2.6.1 Estimate costs for hardware, software, communications, staffing, facilities, and maintenance for IT services.

2.6.2 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, auditing, exception reporting, and the staffing required to support these functions.

2.6.3 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.

2.6.4 Estimate cost for insurance coverage associated with potential losses associated with proposed IT services.

2.6.5 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.

Deciding on Insurance

2.7 In a decision to outsource, the cost and type of insurance coverage should be considered. 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 (RFP)

Section 3 provides guidance and defines factors to consider, in developing the internal control, backup, and recovery requirements for a request for proposal (RFP). While not required in all outsourcing arrangements, the RFP process can be a valuable 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 vendors with the skills and experience to meet the procurement needs and objectives identified in Section 2. In addition to a clearly defined statement of work, the RFP should identify the specific procedures and processes, responsibilities, service level agreements and types of controls expected to be in place to ensure the integrity of information and transactions throughout the engagement.

The following list outlines some of the items that institutions should consider in developing an RFP. It is not intended to be all-inclusive; rather, it highlights elements that are discussed throughout the *Framework's* process flow to help a prospective vendor understand the requirements of the engagement. Factors included in the RFP will 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 its security policies and expect Service Providers to provide responses that outline cost-effective security architectures that adhere to these policies. It is important to fully understand the level of risk of the outsourced application or service when developing the RFP to ensure that the cost of the control processes does not exceed a reasonable risk/reward formula.

The Receiver Company should ensure that all terms are carefully and explicitly defined and reviewed with the RFP bidders at the time of issuance of the RFP to foster accurate understanding of the terminology (e.g., response time, system availability, etc.). In addition, if applications are to be developed by the Service Provider, the RFP requirements should include the use of a formal project management methodology.

RFP Definitions for Services, Tools, and Controls

3.1 Define service availability and performance requirements in a manner such that an effective comparison can be made between different service providers (e.g., do performance standards include a reference to the number of black-out periods per day?). Requirements could include:

- expectations for availability and operational redundancy;
- application availability and scalability;
- quality assurance and measurement;
- reporting requirements;
- minimum performance standards;
- service levels;
- responsiveness, hours of availability and communication tools available (e.g., written, verbal, electronic, face-to-face) of customer service; and
- acceptable capacity planning or other service delivery methodologies.

3.2 Define the types of security, auditing, and control tools required at each step in the process flow, keeping in mind that the tools that will be required will vary depending on the environment (shared vs. dedicated environment, single vs. multiple Service Providers) and 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). Typical control areas include:

- access controls,
- audit trails,
- authentication,
- authorization,
- availability,
- compliance,
- confidentiality,
- configuration management,
- data integrity,
- environmental systems (electricity, cooling, fire prevention and protection),
- identification,
- incident response,
- intellectual property ownership,
- intrusion detection,
- non-repudiation,
- penetration testing,
- physical and social security systems,
- privacy,
- procurement,
- reporting,
- security administration,
- source code maintenance and storage,
- system configuration,
- systems administration,
- training and awareness,
- transaction integrity, and
- vulnerability testing.

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

3.3.1 Access – Include all systems' access points for the Service Provider, the Receiver Company, existing service-provider relationships, and end users (including customers).

3.3.2 Transaction Points – Transaction points involve a change or modification of data immediately upon user request.

3.3.3 Batch Processing – Batch processing points involve modification of data at a scheduled time, based upon stored requests.

3.3.4 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.

3.3.5 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.

3.3.6 Hardware – Hardware platforms should include all components from workstation to hosts at the locations of the Service Provider, Receiver Company, and third parties.

3.3.7 Software – Software should include the operating system, utilities, tools, database, network and application software.

3.3.8 Network – Network points include network paths (circuits), routers, switches, hubs, and firewalls.

3.3.9 Internal Coordination – This includes automated and manual handoffs between departments and organizations such as purchasing, legal, print shop, etc.

RFP Definitions for Backup, Storage, and Recovery

3.4 Define data backup and offsite storage schedules and control requirements that are consistent with the Receiver Company's business continuity planning, such as:

- backup frequency and offsite rotation,
- offsite storage of system backup media,
- data restoration gap analysis,
- encryption standards including back-up, storage and recovery of encryption keys,
- security and climate-control of storage facility, and
- security and climate-control of media during transportation.

3.5 Define technology recovery requirements, which may include:

- operational recovery requirements for each application and/or system,
- cost/benefit analysis of recovery strategy compared to insurance programs,
- right to backup copy of application for recovery purposes,
- ongoing testing, and
- real-time recovery or continuous operation.

3.6 Define full disaster recovery plan and procedures, initial and period testing proposal and SLA for worst-case disaster recovery.

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 be dependent 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 plan and adequate resources and experience to ensure acceptable service, controls, systems backup, availability, and continuity of service to its clients.

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 strategy, reputation, experience, understanding and evaluation of required controls, and financial condition, as well as an understanding of any reliance by the Service Provider on additional third-party service providers to deliver the service. In addition, the Receiver Company should give some consideration to the cost of switching Service Provider if that Service Provider fails to meet contractual requirements, (e.g., consideration of whether the solution is a proprietary one). The Receiver Company should also identify any user groups associated with the service and the Service Provider's practice of communicating with customers through such groups. 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 of the control processes does not exceed a reasonable risk/reward formula.

Assessing Audits, Security, and Performance

4.1 Determine if the Service Provider has a current-year, independently conducted, third-party auditor 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.

It is recognized that a SAS 70 Type II, a SysTrust audit, an independent auditor's report, and/or a full penetration test are 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.

In a shared environment, these audits 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 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.

In the event that the third-party auditor report does not address the scope or location of the services being processed, 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, 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, the Service Provider should be given advance notice and details of the scope of the audit, 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.

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 auditor in accordance with the Statement on Auditing Standards of the AICPA (American Institute for 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 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.

If there are internal audits 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) efficiency and effectiveness in using resources to provide services for which the Receiver Company is charged, and (d) performance of the services according to performance standards.

A thorough Service Provider security review would include testing. The test areas should require written sign-off 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. Tests would include:

- security policies and procedures;
- physical security controls;
- external network penetration attempts;
- application penetration attempts;
- 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.

4.2 Determine the Service Provider's reliance on other third-party service providers.

4.2.1 Identify and review all Service Provider dependencies.

4.2.2 Verify the process the Service Provider has in place to review third parties' security policies and procedures.

4.2.3 Review the Service Provider's service record and experience with dependent providers.

4.2.4 Review the Service Provider's issue notification, communication, and contingency plans for dependent providers.

4.2.5 Evaluate interoperability security between Service Provider and dependent providers.

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

4.3.1 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.

4.3.2 Review network configurations to assess whether logical or physical separations are required between Service Provider connections and access points.

4.3.3 Review existing Service Provider contract terms to determine whether any are affected by the new Service Provider relationship.

4.3.4 Review existing insurance terms to determine whether any are affected by the new Service Provider relationship.

4.4 Determine service availability offerings and their link to requirements.

4.4.1 Determine if there are regularly scheduled time periods when the service is not available.

4.4.2 Determine if the Service Provider has historical statistics on system availability and response times.

4.4.3 Determine how additional transaction volume created by a new client affects system performance and availability.

4.4.4 Determine architecture for high availability and operational redundancy.

4.4.5 Determine the architecture's ability to provide and support additional capacity.

4.4.6 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).

Assessing the Recovery Plan

4.5 Request a copy of the Service Provider's recovery plan and consider possible integration of the plan into the Receiver Company's own business continuity plan.

4.5.1 Verify that emergency response procedures are in place to help ensure timely relocation of technical personnel.

4.5.2 Verify customer service relocation procedures support proper customer notification and status support.

4.6 Verify data backup, restoration validation and offsite storage schedules and control requirements.

4.6.1 Determine frequency of file backup and offsite rotation.

4.6.2 If transactions are posted in real time, determine if backups are performed frequently enough to prevent the Receiver Company from having to recreate an unreasonable amount of lost transactions.

4.6.3 Determine if backups are stored offsite and if they are stored in a secure, climate-controlled environment.

4.6.4 Determine if controls are in place to ensure that backup media is actually being received by the offsite storage facility and that transportation boxes have not been tampered with during transport.

4.6.5 Determine the storage media used and recovery compatibility with existing infrastructure.

4.6.6 Determine if acceptable data archiving requirements can be met.

4.6.7 Determine the level of data segregation on backup media.

4.6.8 Verify that media is replaced periodically prior to obsolescence.

4.7 Determine recovery time objective for customer access to restored systems and data.

4.7.1 Determine if recovery plans are application/system/service and/or customer specific.

4.7.2 Review the Service Provider's Business Impact Analysis (BIA) Report.

4.7.3 Determine prioritization of applications.

4.7.4 Determine if the Service Provider's recovery time objectives meet minimum recovery time objectives for dependent business units within the Receiver Company.

4.7.5 Determine what the **maximum** recovery time will be for the Service Provider to restore systems and, upon restoration, what the point-in-time recovery of data will be. Also determine if these criteria have been proven in testing.

4.8 Determine if the Service Provider has established "preferred priority restoration" with other customers of their services.

- 4.8.1 Determine if other clients have contracted for recovery priority.
- 4.8.2 Determine the true estimated restoration window for the system, as well as data to be used by the Receiver Company.
- 4.8.3 Determine the probability of other clients declaring a disaster simultaneously.
- 4.8.4 Determine the contingency plans in place to support multiple clients' recovery events.

4.9 Determine requirements for notification of a service outage.

- 4.9.1 Determine the Service Provider's procedures for notifying the Receiver Company in the event of planned and unplanned outages.
- 4.9.2 Determine reporting levels and links to tier ratings.
- 4.9.3 Determine procedures for problem reporting and escalation, both internal to the Service Provider and external to the Receiver Company and its customers.
- 4.9.4 Determine the Receiver Company's role in daily operational review processes.

4.10 Review the reliance of the Service Provider on other third parties to provide a recovery environment.

- 4.10.1 Determine if the other third parties are capable recovery service providers.
- 4.10.2 Determine if the Service Provider has had to declare a disaster requiring the activation of use of a third-party service provider's resources, and level of success.
- 4. 10.3 Determine certifications and capabilities of Service Provider's third-party providers.
- 4. 10.4 Determine if the Service Provider can leverage the Receiver Company's existing relationship(s) with other third-party providers.
- 4. 10.5 Determine the conditions under which a third-party site would be activated.
- 4. 10.6 Determine the level of access required for a third-party site.

Assessing Recovery Documentation and Testing

4.11 Review the Service Provider's status in documenting recovery procedures for **both** day-to-day processing platforms and the Service Provider's site outage.

- 4.11.1 Determine differences between operational recovery and disaster recovery.
- 4.11.2 Consider the Service Provider's disaster recovery site in the event of a local disaster.
- 4.11.3 Determine environmental differences for the operating system, database, application, and network environments.
- 4.11.4 Determine the use of formal service management processes to manage systems changes and operations.

4.12 Review technology recovery testing efforts recently performed by the Service Provider, including the scope and results of the test.

4.12.1 Determine if the applications used by the Receiver Company have been tested successfully.

4.12.2 Determine when the applications were last tested successfully.

4.12.3 Determine the frequency of tests.

4.12.4 Determine the scope of tests: (a) depth (e.g., O/S, database, application, network) and (b) breadth (e.g., operational, disaster).

4.12.5 Determine if testing is certified by an independent third party and obtain a copy of the certification.

4.12.6 Determine if there have been significant upgrades or other changes to these systems since the last time they were tested that would require retesting.

4.12.7 Define access control requirements under 'disaster response' mode involving a Service Provider site 'outage'.

4.12.8 Determine the differences, if any, in access controls between operational and disaster recovery scenarios.

4.12.9 Determine if the Receiver Company may participate in recovery tests and to what extent.

SECTION 5: CONTRACTUAL, SERVICE LEVEL, AND INSURANCE CONSIDERATIONS

Each contractual relationship between a Receiver Company and an IT Service Provider is unique. This section is intended to **supplement** the process of due diligence and ongoing maintenance associated with Service Provider relationships. The considerations that follow are written from the **Receiver Company** perspective and are intended to provide a checklist of suggestions for possible incorporation in contractual and service level agreements, as well as insurance provisions.

It is important to note that some service level requirements cannot be defined until after conversion and others must be improved over the term of the contract. Therefore, the contract between the Service Provider and the Receiver Company should specify when these benchmarks would be established and reviewed. Depending on the nature of the application, system or service to be outsourced, the Receiver Company and the Service Provider may choose to create a performance level plan which would determine milestones in the implementation process. Acceptance of milestones in the performance level plan may in turn be tied to payment terms.

The Receiver Company should give consideration to the relationship with the Service Provider and the service to be provided (e.g., dedicated vs. shared environment) and whether a contract is being entered into with one or multiple Service Providers when reviewing the considerations listed below. Where the Service Provider cannot, or will not, agree to critical considerations associated with controls, controls verification, insurance, and continuity planning, the Receiver Company should consider the need to put in place appropriate alternative controls and provisions 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.

Contractual and Service Level Considerations

The points below should be considered in determining the obligations of the Receiver Company and the Service Provider.

5.1 Scope of Services

5.1.1 Clearly articulate the services to be performed by the Service Provider on behalf of the Receiver Company 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);
- the information security role and responsibilities to be provided;
- the 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);
- the process and obligations required to add new services, modify current services or combine multiple services;

- terms for contract renewal and termination;
- the Receiver Company's rights to make changes to services;
- emerging technology considerations and provisions for replacing, reducing or adding services based upon technology changes;
- the timeframe for implementation of functionality of services; and
- a baseline for performance standards and each party's responsibilities.

5.1.2 Clearly document and understand the service levels and performance standards expected, the Receiver Company's responsibility in support of them, continuous improvement provisions, and the consequences and remedies of non-performance. Define performance-reporting requirements, hand-offs between the Receiver Company and the Service Provider, responsibilities for troubleshooting, and problem escalation. Document the requirements for:

- availability – percentage 'up-time', hours of operation (24x7x365), etc.;
- efficiencies – gained from improvements in technology;
- scalability – transaction growth, storage needs, seasonal or promotional spikes, etc.; and
- performance – precisely defined response time, transaction-processing time, time to resolution, etc.

5.1.3 For cross-border outsourcing arrangements, determine which country's laws and regulations are applicable.

5.2 Service Provider's Financial Soundness or Change in Business Strategy

Consider incorporating provisions for notification to the Receiver Company in the event of:

- financial difficulty that may result in an impact to 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; 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.

SLA Consideration: Support responsibility and hours associated with organizations subcontracted by the Service Provider should be specified.

5.3 Environment

The following should be considered based upon the relationship with the Service Provider and the service to be provided. These would help ensure that the Receiver Company has a solid understanding of the Service Provider's environment at the time of the agreement. This understanding is critical to establishing a baseline for control implementation.

5.3.1 Physical Processing and Data Storage – It may be important in a dedicated Service Provider environment to document the location(s), type and serial number(s) of equipment to be used in the processing and storage of Receiver Company programs and data. This will allow the Receiver Company 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 Receiver Company, additional verification and documentation will be required.

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

5.3.2 Logical Processing and Data Storage – 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.

5.3.3 Destruction of Intermediate Files – In instances where a shared storage or processing work area is authorized by the Receiver Company, proper due diligence should be followed to prevent the inadvertent disclosure of Receiver Company data. Either all work files created during the course of processing should reside on Receiver-dedicated physical media, or full appropriate procedures must ensure proper erasure prior to media reuse. This must occur prior to the storage being released for and/or by the Service Provider.

5.3.4 Software – Documenting 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 and patch revision history being used in the processing of Receiver Company programs and data, helps to ensure that bugs have been identified and corrective measures applied.

5.3.5 IT Service Providers/Vendors Contracted by the IT Service Provider – Depending on the application, system or service and the information to be processed at a third party, subcontracting by the Service Provider involving the Receiver Company's data, applications, and service may require the express written permission of the Receiver Company.

5.3.6 Intellectual Property – Ownership for the system, source code, processes, concepts, etc. should be clearly documented, with clear definitions of intellectual property rights. If the Service Provider retains ownership over source code, escrowing issues should be detailed.

5.3.7 System Controls – System controls associated with all platforms and the networks or network interfaces used to process Receiver Company applications and data should be managed and maintained in accordance with industry standards, including timely remediation of vulnerabilities and known bugs that could cause exposure to errors or malicious activity.

5.3.8 Storage and Processing – Depending on the service being provided, logical storage and processing of Receiver Company applications and data may be physically and/or logically separate from that of other companies processed by the Service Provider.

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

5.4 Confidentiality

The Service Provider and all its personnel supporting the processing relationship should be made aware of the Receiver Company's information classification and handling requirements as well as any personnel screening or confidentiality agreement requirements required by Receiver Company policy. These requirements will be dependent on the relationship with the Service Provider and the service to be outsourced and may include the following:

5.4.1 Information Classification – The information and materials processed or stored by the Service Provider on behalf of the Receiver Company should be handled in accordance with the classification (e.g., confidential, sensitive, public) of the information in accordance with applicable regulations as well as the Service Provider's standards and policies. This handling should meet or exceed the requirements of the Receiver Company's policies and standards as communicated to the Service Provider.

SLA Consideration: Media should be marked if necessary to identify highly confidential data and the capability of the Service Provider system to gain access to production data. Development and other support personnel should be identified and expectations documented.

5.4.2 Production Data Ownership – The agreements should clearly state that data are owned by the Receiver Company business management ("information owner").

5.4.3 Data Disposal: The agreement should clearly state the disposal requirements for data contained on all media (e.g., paper, microfiche, computer disks).

5.4.4 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 Receiver Company should not be allowed without the express written permission of the authorized Receiver Company information owner.

5.4.5 Release of User Information – The release of any user information, such as access rights, should be made only to the appropriately authorized Receiver Company personnel, and authorization will be verified prior to any disclosure.

5.4.6 Responsibilities – Responsibility for communication, authorization, and notification should be stated in the agreements and any supporting procedural guides.

5.4.7 Encryption – The requirements for the use of encryption, the maintenance of any keys and concomitant infrastructure requirements should be clearly stated and include consideration of the entire end-to-end transaction (e.g., origination, storage, network path, backups, recovery and legally mandated provisions).

5.4.8 Test Data – Production data must not be copied to the test environment unless appropriate masking is performed.

5.4.9 Programs and Intellectual Property – Programs, data and written materials of the Receiver Company and Service Provider must be protected from unauthorized copy, use, duplication, and storage.

5.5 Access Administration

The process associated with determining access requirements, request for access, and access should be clearly defined. These procedures should address both network access and physical access requirements should the access be through a telecommunications system or direct contact with the equipment, software, telecommunications wiring or other physical object involved with the processing or storage of data. Depending on the agreement, responsibilities will likely involve both the Service Provider and the Receiver Company and should consider the following:

5.5.1 File Access – Provisions for access to production data and programs for Receiver Company and Service Provider employees should be based on authorized job-related responsibilities with information access privileges consistent with Receiver Company requirements for employee screening. Individuals should be identified to provide the authorization of access. It is recommended that access requests be approved by the authorized Receiver Company information owner.

SLA Consideration: A guaranteed time of implementation of access from time of receipt of request should be established.

5.5.2 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 the access capability to the systems. These records should be retained in accordance with the Receiver Company record retention requirements.

SLA Consideration: The frequency of reports and response time for correcting access errors noted on report should be specified.

5.5.3 Authorization Verification – A reasonable process should be maintained to validate that the "signature" associated with granting access is an authentic "signature" of the Receiver Company owner or other person designated to grant access.

5.6 Security

The Receiver Company or Service Provider may be required to assume the costs of remediation for security issues where this is due to failure to fulfill obligations prior to the breach or other violation. The requirements and process for logging access and violations, for monitoring timely change or deletion of expired access authorizations, and for the prompt archiving and reporting of the recent activities of personnel responsible for the violations or subject to the revocation of access, and other information security requirements should include the following.

5.6.1 Violation Monitoring and Reporting – Actual or attempted logon violations and access violations should be logged. It is recommended that these logs be provided in a secure electronic format to an appropriately identified person within the Receiver Company for action. Include escalation, follow-up monitoring and a review procedure.

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 Receiver Company, and any requirement for redundant notification based upon the severity of the violation (e.g., telephone, email, fax, pager, etc.) should be specified.

5.6.2 Access History and Log Retention – Access history logs for critical application transactions will be generated, retained, and accessible by appropriate Receiver Company personnel. Requirements should include follow-up monitoring and review procedures.

SLA Consideration: The duration of log retention should be specified.

5.6.3 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 Receiver Company information.

SLA Consideration: The time lag between identification and notification to the Receiver Company should be specified.

5.6.4 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 the Receiver Company 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.

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

5.6.5 Proper Separation of Duties – The Service Provider should ensure the same level of separation of duties that the policy requirements of the Receiver Company direct.

SLA Consideration: Separation of duties should be stated for security administration, review of access, and violation reports when those responsibilities remain the responsibility of the Service Provider, and there should be separation between development personnel and operations, as well as other potentially conflicting roles as necessary.

5.6.6 Programs Written by Receiver Company and Processed by a Service Provider – Programs written by, or expressly for, the Receiver Company should be certified as free of any malicious code and appropriate for purpose by the Receiver Company and protected from unauthorized copy, use, duplication, and storage with asset management requirements specified.

5.6.7 Intrusion Detection Monitoring – The Service Provider will maintain intrusion detection in a manner consistent with risk and which will identify 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 Receiver Company with work flow diagrams, end-to-end sign-on and other process automation procedures, interfaces, etc. that will enable compliance monitoring and support audit and reporting standards. Receiver Company may request annual reviews of the Service Provider's access controls with focus on viability and appropriateness of security controls.

SLA Consideration: The Receiver Company should be notified in the event an exposure exists which impacts the Receiver Company's business. Expected hours of monitoring should also be considered. Additionally, the responsibility/liability issue should be allocated with respect to reasonable circumstance in which the service is shut down due to virus hit or other problem, as well as restoration time for information that is lost or damaged.

5.7 Vulnerability and Penetration Management – The Receiver Company 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 Receiver Company with any information that is required for the Receiver Company to understand and act upon any potential customer system and data compromise. According to regulatory guidelines and examination procedures, the Receiver Company is responsible for ensuring that Service Providers provide for 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.

5.7.1 Vulnerability Scanning – Service Providers should identify systems vulnerabilities in a timely manner. In a shared environment the Service Provider may establish the resolution time frame in order to avoid multiple competing requirements from Receiver Companies. Vulnerability scanning should be performed on a regular basis with corrective actions being taken within an appropriate time frame. Include follow-up monitoring and review procedure.

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.

5.7.2 Penetration Simulations – The Receiver Company should validate that the Service Provider periodically performs or contracts with an independent vendor to perform appropriate penetration simulations. If the Receiver Company contracts with the Service Provider to engage an independent vendor, testing should be coordinated with the Service Provider and it should not result in system availability issues, missed SLAs, downtime, customer dissatisfaction, etc.

SLA Consideration: Frequency, depth of testing, and response to close vulnerabilities should be considered.

5.8 Controls Verification

5.8.1 Independent Auditors Report – Based on the risk assessment of the services to be outsourced, an annual assessment by an independent auditor, including testing of controls, may be required. The scope of the independent auditor's report should include the environment used to process Receiver Company applications and data.

5.8.2 Right to Audit – The Receiver Company should retain the right to audit in order to ensure that controls verification is performed as deemed necessary by the results of the Receiver Company's risk assessment. Current independent auditor report(s) should be considered as a source of verification. Mutually acceptable personnel must conduct such audits, with advance notice and on a schedule that does not affect normal

operations of the Service Provider. In a shared environment, these audits may involve more than one Receiver Company and more than one process. The contract between the Receiver Company 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. Regulator-imposed audit requirements would be non-negotiable.

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.

5.8.3 Right to Audit in Subcontracting Situations – The Receiver Company 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 Receiver Company relationship, where such are not covered by relevant third-party review or other independent certification.

5.9 Change Control

5.9.1 Production Changes – All production changes that could affect the processing schedule or integrity of the Receiver Company's data should be communicated to the Receiver Company relationship manager or the backup. The Receiver Company should retain the right of approval on all production changes.

SLA Consideration: The SLA should specify the number of days, or weeks, of advance notification to the Receiver Company.

5.9.2 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 Receiver Company and the Service Provider and the risk involved with the changes, the Receiver Company may request the right to be involved with testing of the changes. The Receiver Company 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 Receiver Company.

SLA Consideration: The SLA should define "thoroughly" and specify the number of days, or weeks, of advance notification to the Receiver Company.

5.9.3 Change Notification – Advance notification should be provided to the Receiver Company of all version and release upgrades.

5.9.4 Depending on the type of service to be outsourced, the Receiver Company may want to consider additional production delivery elements, such as training and education, service delivery performance, capacity management, etc.

5.10 Records Retention

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

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

5.11 Backup, Emergency Notification, Technology Recovery, and Business Continuity

5.11.1 Backup – Data backup requirements and schedule should reflect the loss tolerance level of the Receiver Company, particularly with respect to critical data (e.g., some data may require simultaneous processing by physically separate centers and networks or real-time offsite data mirroring, while other data may only require a daily offsite rotation).

5.11.2 Contingency Testing – Periodic joint contingency and business continuity plan testing should include all impact scenarios that could potentially cause unacceptable interruption to production information processing.

5.11.3 Emergency Notification – In the event of a "disaster" or other emergency that affects the processing schedules, an Emergency Notification Schedule should be followed.

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 power, transport or environment.

5.11.4 Testing Schedules – The frequency of technology and business recovery testing, as well as expectations regarding the participation of the Receiver Company in those tests, should be specified.

5.11.5 Computer Forensics – In the event that it is necessary to conduct forensic tests to determine the cause of an application, system or service failure, the Service Provider should follow appropriate evidence handling procedures.

5.12 Compliance with Regulatory and Receiver Company Policies

5.12.1 Regulatory Compliance – The Service Provider must adhere to regulatory requirements, especially as they pertain to privacy and handling of customer information. These regulatory requirements should reflect any international environments that must be accommodated based upon processing locations. The Receiver Company may require the Service Provider to state and be audited for its privacy statement and policy.

The contract should reference the need to periodically review and update controls to comply with current and future regulatory guidelines. Implementation of the appropriate controls would be enabled through appropriate implementation of controls covered throughout the various sections of this document.

5.12.2 Receiver Company Policies – The Receiver Company should review the Service Provider's policies and standards to ensure that they are acceptable, appropriate and consistent with internal policies and standards. Implementation of the appropriate controls would be enabled through appropriate implementation of controls covered throughout the various sections of this document.

5.13 Penalties and Exit Clause

5.13.1 Failure to Perform – Measurable performance is critical to the assessment of 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 service level agreement. Failure to execute according to those requirements may be basis for negotiated restitution based on the contract.

5.13.2 Exit Clause – The contract may include a clause that allows for reasonable steps to terminate in the event that certain circumstances occur. The clause should include details on the related termination fees and responsibilities for the Service Provider and the Receiver Company in the event of early termination whether planned or unplanned. Circumstances may include events such as acquisition, merger, or other substantial changes not foreseen. The contract should clearly define the right of the Receiver Company to recover its data upon the expiration or termination of the contract and other considerations so that the transition of service or systems is orderly and transparent. In cases where the Service Provider retains ownership over source code for an application, the contract should include details for when the source code will be released to the Receiver Company (e.g., breach of contract or insolvency).

5.13.3 Service Provider Business Failure – Failure of a Service Provider can severely compromise the Receiver Company's ability to conduct its critical business. The Receiver Company must ensure that the contract includes specific statements relating to notification by the Service Provider of impending cessation of its business or that of a subcontractor and any contingency plans in the event of notice of such a failure. Depending on the nature of the outsourced application, service or system, the contract may also include provisions for the Receiver Company to work directly with any dependent Service Providers.

Insurance Considerations

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

5.14 When outsourcing IT activity, the Receiver Company should make sure that specific insurance protections are met according to the Receiver Company's requirements. The contract should define which party is responsible for each type of insurance coverage and the required amount of coverage. The Receiver Company 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. Where possible, the Receiver Company 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 must be compared, and state liabilities and restrictions of liability associated with insurance matters must 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 Receiver Company should request annual updates for coverages required in the agreement. In addition, the Service Provider should provide notice to the Receiver Company if any insurance which affects the applications, system or service maintained by the Service provider and provided to the Receiver Company is modified, canceled or not renewed, or if the insurance company providing the insurance rating changes.

Coverage should be in place whether or not the Service Provider's employees are on site at the Receiver Company's premises. In addition, the Receiver Company 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 Receiver Company.

The following insurance should be considered in addition to the Service Provider's property, casualty and fire insurance, based upon the Receiver Company's own business coverage and the potential impact of outsourcing.

5.14.1 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.

5.14.2 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.

5.14.3 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.

5.14.4 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 Receiver Company request evidence of such coverage for a period after the termination of the agreement.

5.14.5 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.

5.14.6 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, and/or the Internet.

5.14.7 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(s). 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.

5.14.8 Customer Information Privacy Liability – Coverage should be considered for protection in the event that the privacy of customer information is compromised in any way.

5.14.9 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 services.

5.14.10 Vicarious Liability and Supervision – Provision should be considered for vicarious liability and for supervision over the Service Provider.

5.14.11 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 Receiver Company's cash or customer information.

5.14.12 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.

5.14.13 Worker's Compensation – The Receiver Company 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.

5.14.14 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 and it is alleged that the driver is responsible for bodily injury or property damage.

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

Outsourcing IT services does not relieve the Receiver Company management of responsibility to ensure the design, management, implementation, and execution of appropriate controls. 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 will vary based on the specific vendor relationship, the service to be outsourced (e.g., dedicated vs. shared environment) and risk assessment results, and they should be clearly documented. 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 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 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. Controls should apply to both Provider and Receiver companies, 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;
- access request process flow;
- 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.

6.2 Document technology control procedures necessary to prevent and detect unauthorized use or alteration during data creation, transfer, and storage, such as the following:

- 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 Document exception report handling and follow-up procedures 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 Define technology control procedures 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";
- requirements for real-time monitoring such as intrusion detection; and response scenarios for network incidents.

Documenting the Controls for Systems

6.5 Define technology control procedures necessary to maintain confidentiality along the end-to-end transaction path, 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 Define or validate control procedures necessary 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 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 Define control procedures for maintaining system integrity and recovery, which should include:

- change control submission, approval, and reporting;
- backup, storage, and retention; and
- recovery responsibilities and notifications.

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 product 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, 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 will document milestones and deliverables, as well as assignment of responsibilities.

Implementation Phase

7.1 The implementation phase may include activities such as:

- planning and resource allocation;
- technical infrastructure procurement and installation;
- application system modifications;
- interface development;
- conversion of customer, account, and transaction data from a previous application system or service provider;
- documentation creation (see Section 6, above);
- training;
- system testing; and
- user acceptance testing.

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

- requirements definition (an updated version of the requirements listed in the RFP and in the due diligence process), management, and change control;
- 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;
- development of an appropriate contingency plan and exit strategy in the event the Service Provider fails to implement and/or provide service; and
- development of an appropriate communications plan for internal and external constituencies.

Post-Implementation Review

7.3 Finally, completion of the implementation should conclude with a post-implementation review between the Receiver Company and the Service Provider. This review will 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.

SECTION 8: ONGOING RELATIONSHIP MANAGEMENT AND CHANGES IN THE OUTSOURCED ENVIRONMENT

Section 8 highlights the obligation for ongoing management of an outsourcing relationship following initial implementation. While on some level, the Receiver Company will monitor the Service Provider daily, outsourcing relationships change over time, driven by both business changes (acquisitions, organizational responsibility shifts, volume growth or contraction, regulatory changes, etc.) and technology changes (application and operating system upgrades, hardware changes, network and other technology environment changes).

Ongoing Review and Change Management

8.1 Ongoing management review of the outsourcing relationship is required periodically (e.g., in conjunction with SLA timeframes), and in connection with significant changes and contract requirements (e.g., rate increases). The financial institution should ensure that proper resources are assigned to oversee the outsourced service with key departments represented (see Section 1.2) and with responsibilities 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.

Change management disciplines are needed for successful implementation of change in the outsourcing environment. The Receiver Company should verify that the Service Provider has a process in place to identify and assess new control exposures resulting from a change. Depending on the scope of the change, many of the same activities and assessments may be needed as occurred in the initial implementation (see Section 7, above), requiring close coordination between Service Provider and Receiver Companies.

It is critical that any changes associated with the delivery of the service be properly assessed to determine if the change presents new control exposures. For example, an upgrade to an operating system could present new vulnerabilities to hacker attacks, or a new release of an application could result in an inadvertent weakness in the application controls or logging.

Annual Review

8.2 In addition to change-driven activities, an overall review should be performed on an annual basis of all outsourced relationships. This annual review will serve both as additional insurance against undocumented changes and as an opportunity to evaluate the risk associated with the outsourced service to determine if additional due diligence or control processes are required. The Receiver Company should validate that the Service Provider has processes in place to ensure changes are documented, authorized and approved and that maintenance is performed on critical infrastructure components. In addition, the annual review should take into consideration the full process described in the *Framework* and should include, but is not limited to, the following elements:

- validation of the ongoing business objectives and the necessity for outsourcing;
- a high-level walk-through of all processes;
- an analysis of the financial condition of the Service Provider;

- review of a third-party audit report, e.g., a SAS 70;
- review of change control records;
- verification that supporting documentation (such as user requests) are in the appropriate files with the appropriate authorizations;
- verification that the service level agreement was met in all areas;
- verification of the Service Provider's technology recovery test objectives and conclusions;
- verification of maintenance to critical underlying infrastructure such as firewalls and independent vulnerability scans;
- verification of key contacts in the event of need for emergency contact or escalation of critical issues; and
- verification that appropriate controls validation has been performed and that results are consistent with expectations.

APPENDICES

Model Spreadsheet Detailing Generic Cost Categories

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
Labor													
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
Hardware													
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					
Write-Off 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
Software													
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					
Write-Off 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
Communications													
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
Maintenance													
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
Access Control													
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
Recovery													
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
Technical Expertise													
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
Facilities													
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
Ongoing Support													
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
Time to Market													
	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
TOTAL COST	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
COST SAVINGS	**Internal**							**External**					

Internal Human Resources (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
Sale of Equipment	$0.00							$0.00					
Reallocation of Building/Floor Space Vacated	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Sale or reallocation of Furniture/Equip/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
Mainframe Processing Hours Vacated (XX @ $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
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
TOTAL COST SAVINGS	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
TOTAL NET SAVINGS/(COST)	$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 IT Service Provider Framework with Federal Banking Agency Guidelines

Federal Banking Agency Guidelines	**BITS Framework**
I. Federal Financial Institutions Examination Council (FFIEC) **Risk Management of Outsourced Technology Services (Nov. 28, 2000)**	
I.a Risk Assessment	2.1, 2.4, 2.6, 2.7
I.b. Due Diligence in Selecting a Service Provider	Section 3, Section 4
I.b.1 Technical and Industry Expertise	4.1, 4.2
I.b.2 Operations and Controls	4.1, Section 6
I.b.3 Financial Condition	4.0, 5.2, 8.2
I.c. Contract Issues	Section 5
I.c.1 Scope of Service	2.1, 2.2, 5.1
I.c.2 Performance Standards	4.2, 4.2.2, 4.2.3, 5.1, 5.11
I.c.3 Security and Confidentiality	5.4, 5.5, 5.6, 5.12
I.c.4 Controls	4.1, 5.8, 5.9
I.c.5 Audit	4.1, 5.8
I.c.6 Reports	4.1, 5.5, 5.6.1, 5.6.2, 5.6.3, 5.6.7, 5.10
I.c.7 Business Resumption and Contingency Plans	4.2.1, 5.11
I.c.8 Sub-contracting and Multiple Service Providers Relationships	4.4
I.c.9 Cost	2.1, 2.2, 2.3, 2.6, 2.7
I.c.10 Ownership and License	5.4, 5.6.6
I.c.11 Duration	5.1, 5.13
I.c.12 Dispute Resolution	5.13
I.c.13 Indemnification	
I.c.14 Limitation of Liability	
I.c.15 Termination	5.1, 5.13, 5.14
I.c.16 Assignment	

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, Section 8
II. Federal Reserve Bank of New York	
Outsourcing Financial Services Activities: Industry Practices to Mitigate Risk	Entire Framework
II.a Managing and Monitoring the Outsourcing Arrangements	
II.a.1. *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.*	Section 2
II.a.2. *Create a management structure to establish, manage and monitor the outsourcing arrangement.*	
- Phase 1, Identify/Evaluate: Core Competencies	2.1, 2.6
Firm Wide Objectives	2.1
Activities to Outsource	2.2, 2.3, 2.4, 2.5
Cost Benefit Analysis	2.6, 2.7, Appendix 1
- Phase 2, Select Provider: Choose Type of Arrangement	Section 3
Perform Due Diligence	Section 4, Section 6
Negotiate the Contract	Section 5 (except 5.11)
Contingency Planning/Termination Conditions	5.11, 5.13, 7.2
- Phase 3, Manage Transition: Ensure Business Continuity	Institution's Program
Protect Employee Morale	Institution's Program
Communicate	7.2
- Phase 4, Long-Term Management: Monitor Contract	Section 8
Re-Evaluate Metrics	Entire Framework
Renegotiate Contract	Section 5, Section 8
Independent Validation	5.8

Federal Banking Agency Guidelines	**BITS Framework**
II.a.3. *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.*	Institution's Program
II.a.4. *Retain key individuals from the outsourced function to manage and monitor the outsourcing arrangement, and to provide future strategic direction.*	Institution's Program
II.a.5. *Monitor the relationship actively, respond to problems and issues aggressively, employ escalation procedures promptly, and engage in conflict resolution.*	8.1
II.a.6. *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.*	Section 3, Section 5
II.a.7. *Periodically review, renegotiate and renew the contract. Reset target service levels annually.*	Section 8
II.b. Selecting a Qualified Vendor	
II.b.1. *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.*	Section 4
II.c. Structuring the Outsourcing Arrangement	
II.c.1. *Negotiate a written contract that is operationally flexible and that clearly articulates the expectations and responsibilities of both sides.*	Section 5

Federal Banking Agency Guidelines	**BITS Framework**
II.d. Managing Human Resources	
II.d.1. *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.*	Institution's Program
II.e. Establishing Controls and Ensuring Independent Validation	
II.e.1. *Clearly define expected security controls in the outsourcing contract and develop appropriate performance measures to monitor consistent application of those controls.*	Section 3, Section 5, Section 6
II.e.2. *Involve internal and/or external audit in the entire outsourcing process.*	1.2, 5.8
II.f. Establishing a Viable Contingency Plan	
II.f.1. *Ensure that contingency plans are formulated and viable in the event of non-performance by the service provider.*	5.1, 5.2, 7.2
III. Comptroller of the Currency (OCC) Network Security Vulnerabilities – Alert 2001-4 (April 24, 2001)	
III.a. Response to Network Security Vulnerabilities	
III.a.1 Identify systems vulnerabilities and evaluate inherent risks. .	2.3, 2.4, 3.2, 3.3, 4.1, 4.2, 5.3
III.a.2 Eliminate unwarranted risks by applying vendor-provided software fixes.	5.3.4, 5.3.6
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.	5.9
III.a.5 Update vulnerability scanning and intrusion detection tools to identify known vulnerabilities and related unauthorized activities.	5.6.7, 5.7
III.a.6 Conduct subsequent penetration testing and vulnerability assessments, as warranted.	5.7
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.	5.1.1, 5.5, 5.6, 5.7, 6.4
III.a.8 Establish monitoring, reporting, and investigation controls.	5.5, 5.6, 5.8, 5.10, Section 6, Section 8

IV. Gramm-Leach-Bliley Act **Public Law 106-102, the Financial Modernization Act (November 12, 1999)**	
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 section505 (a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards- (1) to insure the security and confidentiality of customer records and information; (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.	Institution's Overall Program (1) and (3): 2.4, 3.2, 3.3, 3.4, 3.5, 4.1, 4.2, 4.4, 5.1–5.9, 5.12, 5.14, 6.1–6.7, 7.1–7.3, 8.1-8.2 (2): 3.2, 3.4, 3.5, 4.1–4.11, 5.7, 5.10, 5.11, 5.14, 8.1–8.2

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

Basel Committee on Banking Supervision			**BITS Framework**
	Risk Management Principles for Electronic Banking		
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.	
		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.	Section 4, Section 5, Section 6
	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.	
		The bank fully understands the risks associated with entering into an outsourcing or partnership arrangement for its e-banking systems or applications.	Application of Framework document based upon the level of risk associated with the outsourced application
		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.	Section 4
		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.	Section 5, Section 6
		All outsourced e-banking systems and operations are subject to risk management, security and privacy policies that meet the bank's own standards.	5.3, 5.4, 5.5, 5.6, 5.7, 5.9, 5.12, Section 6
		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.	4.1, 5.8, 8.2
		Appropriate contingency plans for outsourced e-banking activities exist.	7.2
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.	
		Transaction processes and systems should be designed to ensure that no single employee/outsourced service provider could enter, authorise and complete a transaction.	2.3, 5.6.5

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.	
		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.	5.3, 5.4, 5.5, 5.12, 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.	
		The bank's standards for customer data use must be met when third parties have access to customer data through outsourcing relationships.	5.4, 5.12, 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.	
		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.	5.1.2, 5.2, 5.5, 5.6, 5.7, 5.8, 5.9, 5.11
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.	
		Bank management should clearly identify the strategic purposes, benefits and costs associated with entering into outsourcing arrangements for e-banking with third parties.	Section 1, Section 2, Appendix 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.	Section 1 , Section 2
		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.	1.2

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.	
Banks should consider developing processes for soliciting proposals from several e-banking service providers and criteria for choosing among the various proposals.	Section 3, Section 4
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.	Section 4
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.	5.8 and Section 8
Banks need to ensure that adequate resources are committed to overseeing outsourcing arrangements supporting e-banking.	8.1
Responsibilities for overseeing e-banking outsourcing arrangements should be clearly assigned.	8.1
An appropriate exit strategy for the bank to manage risks should it need to terminate the outsourcing relationship.	5.13, 7.2
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:	
The contractual liabilities of the respective parties as well as responsibilities for making decisions, including any sub-contracting of material services are clearly defined.	Section 5
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.	Section 5
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.	5.3, 5.4, 5.5, 5.13, 5.14, 6.1
Performance expectations, under both normal and contingency circumstances, are defined.	5.1
Adequate means and guarantees, for instance through audit clauses, are defined to insure that the service provider complies with the bank's policies.	5.2, 5.8
Provisions are in place for timely and orderly intervention and rectification in the event of substandard performance by the service provider.	5.13, 7.2
For cross-border outsourcing arrangements, determining which country laws and regulations, including those relating to privacy and other customer protections, are applicable.	5.1.3

Basel Committee on Banking Supervision	**BITS Framework**
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.	5.8, 5.11
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.	
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.	5.11, 8.1, 8.2
5 Banks should develop appropriate contingency plans for outsourced e-banking activities.	
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.	5.11, 7.2
Contingency plans should address credible worst-case scenarios for providing continuity of e-banking services in the event of a disruption affecting outsourced operations.	7.2
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.	
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.	
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.	

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."

AICPA: The American Institute of Certified Public Accountants: the national, professional organization for all Certified Public Accountants (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.

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.

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.

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 breach in security protocol.

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 systems or information that have been damaged or lost.

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, third-party service providers obtain independent assurance on their control objectives and control processes. SAS 70 does not test or evaluate a pre-determined set of control objectives or control activities that service organizations must achieve.

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 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 Contents	**Type I Report**	**Type II Report**
1. Independent service auditor's report (i.e., 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	Optional	Included
4. Other information provided by the service organization (e.g., glossary of terms)	Optional	Optional

(SAS 70, continued) In a Type I report, the service auditor will express 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, and (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 in a Type I report, and (3) whether the controls that were 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 regarding the SAS 70 can be found at www.sas70.org. This website is not maintained by the AICPA and its contents have not been approved by the AICPA.

SysTrust: An assurance service that independently tests and verifies a system's reliability, providing an extension of the CPA's audit and information technology consulting functions. SysTrust defines a reliable system as one that is capable of operating without material error, fault or failure during a specified period in a specified environment. With SysTrust, a CPA tests whether a system is reliable as measured against four principles: availability, security, integrity and maintainability. The boundaries of the system are defined by the system owner and must include the following key components: infrastructure, software, people, procedures, and data. The SysTrust framework, applicable to any size and type of system, allows the licensed CPA to provide independent verification that a company has effective system controls and safeguards so that a system can function reliably upon completion of a SysTrust engagement. Upon achievement of the SysTrust principles, an assurance report is issued to company management. A SysTrust assurance report can be used by a company in its marketing materials or within outsourcing agreements and specific contracts with potential or existing clients.

SysTrust was jointly developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). SysTrust is provided by licensed CPAs and their Canadian counterparts. Discussions are underway to offer SysTrust in several other countries. Additional information on SysTrust can be found at www.aicpa.org/assurance/systrust/index.htm.

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 flow 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.

Sources

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

BITS Voluntary Guidelines for Aggregation Services, April 2001
Chubb CyberRisk Handbook – Guidelines for Risk Management, Chubb Group of Insurance Companies
Department of Defense Standard, *Department of Defense Trusted Computer System Evaluation Criteria*, 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
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
Rupp's Insurance & Risk Management Glossary, Richard V. Rupp, CPCU, Second Edition
Security Glossary, SET Solutions, Inc.
www.aicpa.org
www.SAS70.org