

BITS OUTSOURCING GLOSSARY OF TERMS

**A PUBLICATION OF THE
BITS THIRD PARTY SERVICE PROVIDER WORKING GROUP**

JANUARY 2007

**BITS
1001 PENNSYLVANIA AVENUE NW
SUITE 500 SOUTH
WASHINGTON DC 20004
(202) 289-4322
WWW.BITSINFO.ORG**

INTRODUCTION

The *BITS Outsourcing Glossary of Terms* was developed by the BITS Third Party Service Provider Working Group to assist member organizations and the financial industry in sharing a common set of definitions for third party service provider and outsourcing relationships.

This *Glossary* draws on the definitions included in the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships* and the sources used to compile that document. Additional resources include member companies' glossary of terms and Sourcingmag.com's online definition of terms. (www.sourcingmag.com/dictionary) Where provided by contributors or known, sources have been noted. If any attributions have been omitted, it is inadvertent. Please contact us at bits@fsround.org if additional attribution is needed.

Readers are encouraged to submit feedback to suggest additional terms to be defined, or terms that need additional clarification for future revisions of this Glossary.

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Z](#)
[Acronyms](#)

A

Acceptance	Process for approval by vendor of the transitioned assets/processes/technology, and formal termination of the transition process. Upon acceptance, the supplier takes responsibility for the transitioned process.
Acceptance Criteria	The testing measures that are mutually agreed upon for approval of the acceptance testing.
Acceptance Test	Testing and evaluation of the deliverable to determine if it conforms to specifications and performance standards and to ensure that the deliverable can be effectively utilized and is fully functional in the company's operating business environment.
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 (logical or physical), 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.
Action Plan	A distinct and defined task or series of tasks designed or intended to correct or remediate an identified exception; act on a process improvement opportunity; strengthen a control weakness; or, more fully understand an issue and enable the appropriate remedies or follow-up steps.

Additional Resource Charges (ARC)	Charges that increase the payment for volumes above the defined Base Case volumes.
Affected Employee	Institution employees working in jobs that currently have some or all of their functional job responsibilities considered for outsourcing.
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.
Agreed Upon Procedures (AUP)	<p>Agreed Upon Procedures are performed under the AICPA Attest Engagements (AT101) and Agreed Upon Procedures Engagements (AT201) standards. Under an Agreed Upon Procedures engagement, both the assessed organization and the recipient of the resulting report must agree to the procedures.</p> <p>Agreed Upon Procedures have been developed under the Financial Institution Shared Assessments Program (FISAP) described in this Glossary. The FISAP program has freely published AUPs which have been developed by the financial services industry as guidelines for service provider reporting on people, process and procedures. The Practitioner's Guide provides the details necessary for any acceptable assessment organization – CPA firm or consulting firm – to use to execute an assessment. A feedback and governance process has also been established to maintain and update the program to continue to raise the bar on security requirements.</p>
Agreement	An element of a legal contract. An agreement exists when an offer made by one party is accepted by the other party. Mutual understanding also must be present.
All-inclusive Pricing	A type of contract in which the buyer pays a set price that includes all costs and expenses associated with the deal including such things as taxes, permit fees and other external charges.
Application	Software used in connection with the delivery of the services that are either obtained from third parties, the financial institution or owned by the service provider.
Application Development and Maintenance	The development, management and upgrades of software by a third party provider.
Application Service Provider (ASP)	<p>A business that hosts an application program and data for one or more customers, and supports remote access to the application by the customer, usually over the Internet. The provider may manage the hardware, infrastructure, and basic maintenance, usually has expertise in the application and may provide enhancements to it. (Source: Electronic Commerce Dictionary)</p> <p>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, usually has expertise in the application and may provide enhancements to it.</p>

Assessment	Thorough review of potential areas for outsourcing, in order to create the most accurate and complete analysis of potential risks and benefits possible.
Assets	Equipment, software, goods and other resources; assets which are owned or used by the institution, service provider or their affiliates, agents or subcontractors, in connection with the provision or receipt of the services.
Audit Trail	In computer security systems, a chronological record of system resource usage. This includes user login, file access, other activities, along with a time and date stamp 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.

B

Base Case	A multi-year financial model that projects total expenses and benefits over a specified period of time for outsourcing a business process or function. It is a compilation of the financial institution's "all-inclusive" costs to support the specific functionality contemplated in the deal for the period of the proposed outsourcing.
Base Price	The annual price that includes fixed costs and variable costs for stated annual Base Case volumes.
Baseline	The process (and values of associated metrics) as it was operating in the client company.
Base-Year	A one-year set of data that becomes the foundation for the Base Case.
Benchmark	A standard by which something can be measured or judged. Benchmarking is the practice of identifying, from competitors or industry standards, qualitative and quantitative metrics as a point of reference against which the success of an organization can be measured. It can also be used to identify best practices or lessons learned. The practice of identifying qualitative and quantitative metrics against which the success of an organization can be measured, often in comparison to competitors and industry standards. Identifying best practices or lessons learned are common by-products of benchmarking. (Source: Gotcha! Berkeley.edu)

Best Practices	Techniques or methodologies of performing a process or sub-process that have been identified inside or outside of the organization as reliably leading to desired results. (Source: Gotcha! Berkeley.edu) Methods of performing a process or sub-process that have been identified inside or outside of the organization and which are validated, codified, diffused, and shared with others to encourage reciprocity and knowledge sharing.
Beta Agreement	An agreement between a software provider and an organization. It governs the use of a beta/test version of software.
Bidders Conference	A negotiation tool which brings together potential suppliers in one room, where an organization can explain procurement requirements to all of them, so they can hear the same message points.
BITS	BITS (www.bitsinfo.org) was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Advisory Board and BITS Advisory Council.
Bugs	Coding errors in software that cause such software to malfunction.
Build-Operate-Transfer (BOT)	A firm contracts with an offshore partner to build a shared services or offshore development center and operate it for a fixed interim period. Organizations try this with the expectation that the offshore partner can initiate operations and reach operating stability much faster than it can with an in-house effort.
Business Case	A document that presents all relevant facts concerning an outsourcing opportunity, including a quantitative summary of the institution's total cost of outsourcing, as well as qualitative considerations, such as risks, strategic alignment, organizational readiness and other issues.
Business Continuity	The ability to maintain operations and services, both technology and business, in the event of a disruption to normal operations and services. Assures that any impact or disruption of services is remedied within a documented and acceptable recovery time period and those systems or operations are resumed at a documented and acceptable point in the processing cycle.
Business Continuity Plan (BCP)	Documentation to assist with maintaining operations and services, both technology and business, in the event of a disruption to normal operations and services. Intent of the documentation is to document steps to remedy the impact or disruption of services within a defined and acceptable recovery time period.

Documentation also notes when systems or operations are resumed and at what point in the processing cycle.

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

Business Process Outsourcing (BPO)

A contractual arrangement transferring ongoing responsibility for a specific business function, such as payroll, to a third-party service provider. Often, companies implement business process outsourcing (BPO) to achieve cost reductions for work that is required but is not critical to maintaining a competitive advantage. Back office outsourcing includes internal business functions such as accounts receivable or purchasing; front office outsourcing includes customer-contact services such as help desk or marketing. (Source: WhatIs.com)

C

Capability Maturity Model (CMM or CMMI)

The Capability Maturity Model for Software (also known as the CMM and SW-CMM) has been a model used by many organizations to identify best practices useful in helping them increase the maturity of their processes. In 2000, the SW-CMM was upgraded to CMMI[®] (Capability Maturity Model Integration). (Source and further reference material can be found at: www.sei.cmu.edu)

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.

Captive Offshore

Employees of the institution perform work in an offshore facility that is owned by the institution either entirely or in a joint venture and is dedicated to serving the institution's needs.

Change Control Procedures

The procedures that will govern (i) the manner in which a party to an outsourcing contract may propose or request modifications, (ii) the process to be followed by the parties to an outsourcing contract in analyzing the effects of, and deciding whether to adopt, any such modifications, and (iii) the manner in which any agreed upon modifications are to be tested and documented.

Change Management (organizational)

The process of changing the client company's organizational culture and internal dynamics sufficiently to obtain the expected results. Not the same as project change management.

Change Request

Requested change to the scope of a project.

Checklist

A quality control tool consisting of a list of steps and deliverables required for successful completion of a process; includes signatures of parties responsible for reviewing the quality of each item.

Classification	Categorization (e.g., “confidential,” “sensitive,” “public”) of information.
Co-sourcing	The term used to describe organizations that execute a shared services center with an external vendor. Also known as joint venture.
Co-employment	A legal doctrine that applies when two organizations exert some control over an associate’s work or working conditions. Co-employment issues and liabilities are further defined by several federal and state laws and court decisions.
Company Data	Data, whether provided or produced before, on, or after the effective date: <ul style="list-style-type: none"> • All data that is provided by or on behalf of financial institution to service provider in order for service provider to provide the services, including keyed input and electronic capture of information by the services; • All data that is provided by or on behalf of service provider to financial institution by means of the services, including reports and all other output of the service provider software or services; • Consumer information of financial institution employees and clients; and • All data that is produced by means of the services as an intermediate step in using or producing any of the financial institution data, including databases and files containing financial institution data.
Complex Password	A password that is a combination of alphabetic and non-alphabetic characters such as special characters or numeric characters.
Compliance Risk	Outsourced activities that fail to comply with legal or regulatory requirements can subject the institution to legal sanctions. For example, inaccurate or untimely consumer compliance disclosures or unauthorized disclosure of confidential customer information could expose the institution to civil monetary penalties or litigation. (Source: FFIEC)
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	The protection of sensitive information from unauthorized disclosure and sensitive facilities from physical, technical or electronic penetration or exploitation.
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.
Connectivity	A general term for connecting devices to each other in order to transfer data among them. It often refers to network connections, such as, routers, switches, gateways and backbone networks. It may also refer to connecting a location to the Internet or connecting remote locations to one another. (Source: Answers.com) A generic term for connecting devices to each other in order to transfer data back and forth. It often refers to network connections, which

embraces bridges, routers, switches and gateways as well as backbone networks. It may also refer to connecting a location to the Internet or connecting remote locations to one another.

Constituent	A current active employee or contractor.
Consumer Information	All records, files, reports and other data relating to a financial institution's consumers and customers provided or accessible to the service provider by or on behalf of the institution, its affiliates or business partners, or otherwise collected or obtained by service provider, in connection with the services, including, but not limited to, personally identifiable information, regardless of form, pertaining to any person who obtains or seeks to obtain products or services of financial institution and/or its affiliates, such as a person's name, address, telephone number, social security number, driver's license number, account number, personal identification number, user name, password or other identifying information or reference, and any combination thereof, that may allow access to such person's account or potential account with financial institution, as well as any information derived from any of the foregoing.
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 recovery plan and emergency plan.
Contract	An agreement between parties or organizations. In order to be binding, a contract must include an offer, there must be acceptance, and there must be consideration.
Contract Date	The date an outsourcing contract is signed.
Controls	Internal controls are those processes implemented by management that help provide reasonable assurance objectives can be met. The internal control structure refers to all of the tools or controls implemented by management to mitigate risks to acceptable levels. Controls can generally be divided into two types: preventative or detective.
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.
Core Business	The primary product or service an organization offers that differentiates it from its peers.
Cost Plus	The cost of production plus a fixed rate of profit.
Country Risk	The risk to earnings or capital arising from exposures to economic, social and political conditions in a foreign country that would adversely affect a vendor's ability to meet its service level requirements.
Crisis Management	Overall coordination of an organization's response to a crisis to avoid or minimize damage to profitability, reputation or capability to operate.

Critical Incident	A significant issue with a vendor, often a result of a control weakness, which impacts the vendor risk profile. Examples of critical incidents include declaration of bankruptcy, declaration of a disaster due to a significant BCP event or an information security breach.
Cut-Over	Transfer of responsibility to the vendor; marks the division between transition and service delivery.

D

Data Integrity	The property that data has not been altered or destroyed in an unauthorized manner.
Data Privacy	Regulatory requirement and public expectation of privacy in the collection and sharing of data.
Dependent Provider	Company on which a service provider relies to provide some aspect of contracted service to a financial institution. Other terms used include downstream provider, subcontractor and secondary service provider.
Disaster Recovery	Plans for orderly restoration of computing, operational and telecommunications services.
Disaster Recovery Plan (DRP)	Documentation that includes procedures for orderly restoration of computing, operational and telecommunications services. Synonymous with contingency plan and emergency plan.
Displaced Employee	Employee who will not have the same job at the institution due to job changes.
Document of Understanding	A document that details the relationship between organizations and sets expectations of the roles of each other.
Domestic Outsourcing	<i>See</i> Onshore Outsourcing.
Downstream Provider	<i>See</i> Dependent Provider
Due Diligence	Technical, functional, and financial review by the financial institution 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.

E

Employee Leasing	<i>See</i> Staff Augmentation
Encryption	To scramble information so that only someone with the appropriate "key" can access the original information (through decryption).

End-To-End	Outsourcing initiatives from Assessment through Service Delivery; all phases need reporting and governance.
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.
Engagement	A specific, contractually defined, relationship between the institution and a supplier.
Equipment	All computing, networking, telecommunications and other equipment (hardware and firmware) procured, provided, operated, supported, or used by financial institution, service provider or authorized users in connection with the services.
Exception Reporting	Report that documents variances in established control requirements.
Executive Sponsor	Business unit leader who has ultimate responsibility for the performance and operations of the outsourcing agreement.
Exit Strategy	A plan to document the steps necessary to discontinue use of a service provider in a manner that limits the interruption to business and the cost resulting from terminating a contract, either prematurely or at the contract's expiry date. The absence of an exit strategy can result in negative consequences including monetary loss, employee and customer dissatisfaction, and business interruption. The exit strategy is put into operation according to the exit implementation plan.

F

Federal Financial Institutions Examination Council (FFIEC)	The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions. www.ffiec.gov
Financial Base Case	A multi-year financial model that projects total expenses over a specified period of time for operating a business process or function internally.
Financial Institution Shared Assessments Program (FISAP)	Developed by BITS to establish an effective and efficient method for evaluating service provider controls. Through a comprehensive questionnaire, the Supplemental Information Gathering(SIG), and objective and consistent assessment process, Agreed Upon Procedures (AUPs), the Program gathers detailed information on a service provider's controls (people, process and procedures) and tests those controls. Both documents are freely available to the industry to promote adoption and self assessment. www.bitsinfo.org/fisap .
Fixed Cost	A cost that does not vary depending on business volume, such as rent, property tax, insurance, or interest expense.

Fixed Price Contract	A model of pricing in which a project is undertaken by the service provider for a pre-agreed-upon price. A type of contract where the buyer agrees to pay the seller a set, predetermined amount regardless of actual costs. One advantage is that it is easy for the client to budget for the project. Two disadvantages are that the service provider may overestimate costs beforehand for possible unforeseen conditions or cut corners during the project to compensate for expenses that are higher than anticipated. The service provider will charge a premium for a fixed price relative to the risks involved. Appropriate for efficiency deals.
Foreign-Based Service Provider	Third parties whose servicing operations are located in a foreign country and subject to the laws and jurisdiction of that country. This includes U.S. service providers to the extent that their actual servicing operations are located in or outsourced (e.g., subcontracted) to entities domiciled in a foreign country and subject to the laws and jurisdiction of that country. It does not include a U.S.-based subsidiary of a foreign firm because its servicing operations are subject to U.S. laws.
FTE	Full time equivalent employee.

G

Global Outsourcing	Services of a company delivered by a third party vendor in another country.
Globalization	The tendency of businesses to move beyond domestic and national markets to other markets around the globe, thereby increasing the interconnectedness of different markets (Source: investopedia) and causing human beings to become more intertwined with each other around the world economically, politically, and culturally. It is brought about by modern communication, transportation and legal infrastructure as well as the political choice to consciously open cross-border links in international trade and finance. (Source: wikipedia) The Internet, more than any other phenomenon, has enabled the smallest company to have a global presence. (Source: techweb.com)
Governance	The oversight and management of all aspects of an outsourcing relationship. Areas of focus include change management, communications management, financial management, performance management, operational management, risk management, strategic management, and others.
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.”

H

I

Implementation Plan	A plan that details project management requirements and issues to be addressed during the period between the execution of an outsourcing agreement and the full production use of the outsourced services.
Incident Response	Plan that defines the action steps, involved resources, and communication strategy upon identification of a threatening or potentially threatening event such as a breach in security protocol, power or telecommunications outage, severe weather, or workplace violence.
Incumbent	Refers to a person who currently holds a specific role/position.
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 Security 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.
Information Technology Outsourcing (ITO)	The transfer of internal non-core IT processes, such as infrastructure, applications development and maintenance, end-user computing, help desk, network support and data center operations, to an external service provider that improves these processes and administers these functions to an agreed service standard and, typically, at a reduced cost.
Infrastructure	<p>The collection of platforms, networks, bridges, routers, switches and gateways, and the business rules regulating the flow of data and work among them, both internally and to external systems. (Source: Bitpipe) The collection of platforms, networks, bridges, routers, switches and gateways, and the business rules governing the flow of data and work among them, both internally and to external systems.</p> <p>Can also be used to discuss the stability and environmental structure of a city or country.</p>
Inherent Risk	The risk associated with a system, process, etc., if no mitigating controls were added. Inherent risk combines the value of information (data classification) with the likelihood of threats being realized if no controls were present.
Inherent Service	Services, functions or responsibilities not specifically described in an agreement or statement of work, but are reasonably required for proper performance and provision of service(s) required.

Initiative	The project to assess a business process and/or application for suitability for outsourcing, to identify a vendor partner, structure the deal, and transition the subject process/application to vendor control.
In-scope	Refers to a service, application, process, etc. that is being/has been considered for outsourcing. This does not mean the work will be outsourced, only that it is being studied for possible outsourcing.
Insourcing	A decision by an organization to retain functions internally rather than outsource. The decision is often made after the organization has performed independent benchmarking to determine that its costs and efficiencies are in line or better than those achieved by comparable organizations. The term is also used in cases where services are being brought back in house after a period of outsourcing them.
Integrity	Ensuring that information will not be accidentally or maliciously altered or destroyed (<i>See</i> Data Integrity).
Intellectual Property (IP)	Any intangible asset that derives from the work of the mind or intellect, specifically, an idea, invention, trade secret, process, program, data, formula, patent, copyright, or trademark or application, right, or registration. Terms and conditions protecting IP are to be included in every outsourcing contract.
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.

J

Joint Venture	A legal organization that takes the form of a short term partnership in which the parties jointly undertake a transaction for mutual profit. Generally each party contributes assets and shares risks.
----------------------	--

K

Key Performance Indicators (KPI)	Financial and non-financial metrics used to quantify various objectives in order to reflect the strategic performance of an organization.
Key Risk Indicators (KRI)	Metrics used to effectively monitor and track changes in risk levels and keep management apprised of shifts in established patterns.
Knowledge Process Outsourcing (KPO)	Involves outsourcing for high-end knowledge work. This includes research and work on intellectual property, equity and finance, analytics, market research and data management, etc. (Source: Cyber Futuristics)
Knowledge Repository	Collection of information on an application, system or environment.

Knowledge Transfer Actual movement of corporate information and understanding from one individual to another. Processes to capture technical and business knowledge needed to perform the outsourced service, organize it, standardize it and convey it to the new resources.

L

Line of Business (LOB) Individual business (es) within overall corporate entity.

Liquidated Damages A specific dollar amount (i.e., \$500,000) predetermined by the parties to the contract as the total compensation that a breaching party is liable to the non-breaching party. Such amount should typically be large enough to fully compensate the non-breaching party and should be a reasonable estimate of the actual damages that each party would suffer in the event the other party breached the contract.

M

Management Fee A reimbursement for the management and services provided.

Management Tools All software products and tools that are used by service provider to deliver and manage the services.

Master Services Agreement (MSA) Binding contract agreement which defines the terms, conditions, and responsibilities of each of the participants to the agreement. Follow-on work or ancillary service offerings may be described and agreed in Statements of Work (SOW) under the umbrella of the MSA. MSAs are usually comprised of the following elements:

- THE PURPOSE OF THIS AGREEMENT
- DEFINITIONS – Define key terms and objectives
- COMPENSATION – Defines the amount to be paid, over which time period or based on deliverables
- WARRANTY – Identifies the period of time and conditions that the service provider will fix or replace deficient deliverables
- TERM AND TERMINATION – Duration of agreement, condition under which the contract may be terminated
- AMENDMENTS AND MODIFICATIONS TO THIS AGREEMENT – identifies the rules for amending the agreement
- ASSIGNMENT, DELEGATION AND SUBCONTRACTING – Outlines the rights of both parties in the event the service provider must substitute or augment staff
- ENFORCEABILITY – If one part of the contract is found to be unenforceable, it does not cancel the obligations articulated in the remainder of the agreement
- SURVIVAL – The duration of time that the provisions and obligations of the MSA shall remain in effect
- NOTICES – How communications will be handled, usually in writing
- CONDITIONS PRECEDENT – Identifies critical path conditions, such as the services provider must show evidence of bonding,

- creditworthiness, or other vetting activities.
- EVENTS OF DEFAULT AND REMEDIES FOR DEFAULT – This section defines the conditions under which a participant would be considered in default of the Agreement and the actions that either party may or must take when a default occurs
- LIMITATION OF LIABILITY – This section would define the extent of liability of each party
- INDEMNIFICATION – This section typically provides that each party (the indemnifying party) shall hold harmless the other party (the indemnified party) from claims by a third party due to the negligence of the indemnifying party, subject to the limitations of liability
- FORCE MAJEURE – This section relieves the parties of liability due to events beyond their control or “Acts of God”
- AUDITS – Right to Audit Clause
- INSURANCE requirements
- GOVERNING LAW – Identifies the local jurisdiction whose laws apply to the execution of the MSA
- DISPUTE RESOLUTION
- NONDISCLOSURE/CONFIDENTIALITY – If not already covered in a separate NDA. The terms must align with Gramm-Leach-Bliley Act (Public Law 106-102, Title V)

Methodology

A collection of ways of performing tasks, definitions, roles, and standards that defines an integrated synthesis of approaches.

Multi-Regional Data Processing Servicers (MDPS)

The FFIEC agencies examine MDPS organizations because these entities pose a systemic risk to the banking system should one or more have operational or financial problems or fail. Since these companies service banks, thrifts, and credit unions, the FFIEC conducts interagency IT examinations of these large technology service providers. Interagency IT examinations provide a single examination report for the service provider management and the board of directors. A booklet detailing this program can be found at www.ffiec.gov

Multisourcing

Utilizing multiple vendors.

N

Near-Shore Outsourcing

Business decision to engage a third-party vendor in a country in close proximity to the parent company’s headquarters. In the case of the U.S., near-shore is considered to include Canada, Mexico and the Caribbean.

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-core Business

Activities that are critical to do correctly but do not differentiate an organization from its competitors.

**Non-disclosure
Agreements
(NDA)
Nonpublic Personal
Information
(NPPI)**

Documents indicating that the parties will not disclose information to any unauthorized persons.

According to the Gramm-Leach-Bliley Act, nonpublic personal information is defined as follows:

(A) The term "nonpublic personal information" means personally identifiable financial information -

- (i) provided by a consumer to a financial institution;
- (ii) resulting from any transaction with the consumer or any service performed for the consumer; or
- (iii) otherwise obtained by the financial institution.

(B) Such term does not include publicly available information, as such term is defined by the regulations prescribed under section 6804 of this title.

(C) Notwithstanding subparagraph (B), such term -

- (i) shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but
- (ii) shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information.

O

**Offshore Dedicated Center
(ODC)
Offshoring**

Can be wholly-owned or a captive facility providing services solely for the use of the financial institution.

A specific type of outsourcing to a service provider whose principal base of operation is outside the client company's own country.

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 restore data in case of accidental deletion, corruption or to be used only in an emergency.

Offsite Work

Work that is conducted at a location other than the company's primary location.

On-shore Outsourcing

Business decision to engage a third party vendor in the organization's home country. Also referred to as domestic outsourcing.

**Operational Procedures
Manual**

Guide or set of procedures that specifies, in detail, how the service provider will perform the contracted services. Includes the service provider's plan of operations; all processes and procedures related to the services, whether

standard or customized; and touch points with processes, procedures and service groups that remain with the client company. (Source: Technology & Business Integrators, Inc.) Specifies, in detail, how the vendor will perform the contracted services. This would include all of the vendor's operations plans; all standard and customized processes and procedures related to the services; and touch points with company-internal processes, procedures and service groups.

Organizational Change

Changes in processes, procedures, roles, or organizational structure, which require the workforce to perform work in a different way

Organizational Change Management

Provides a framework for supporting a systematic approach to planning, executing, and managing change within the organization. This may involve the total organization or smaller segments. If an organization is going to be effective (accomplish goals) it must adapt to change. OCM focuses on ways to help the organization to accept change.

Out-of-scope

Refers to a job, application, process, etc. that is not being considered for outsourcing at this time.

Outsourcing

Financial institution's contract with a third party to provide services, systems, or support. Outsourcing can be provided on or off premises, in the same country or in a separate country.

P

Pass-through

Costs that will be managed by the supplier but paid by the corporation at no additional mark-up.

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.

Performance Risk Assessment

Evaluates the risk associated with vendor's failure to meet performance standards. Assessment may involve the development and implementation of vendor "scorecards" or other metrics.

A vendor performance risk assessment evaluates the risk associated with vendor's failure to meet performance standards. A Performance Risk Assessment may involve the development and implementation of vendor "scorecards" or other metrics.

Pilot

A trial or test of a business process or service and at times a small scale solution to ensure its effectiveness and to test for the impact of the process or service. (Source: Six Sigma SPCA) Trial or test of a process, product, or service and sometimes a solution on a small scale to ensure it is effectiveness and to test for the impact of the process, product, or service.

Policy	Position statements that adhere to the institution's core values and guiding principles, and are intended to govern as well as determine decisions and actions. Policies provide the general framework for an operational structure around how governance requirements will be accomplished.
Portfolio Analysis	A study on the full scope of an application suite.
Privacy Policy	An official statement on the type of information collected, how the information will be used, how the individual can access this data and the steps for having the data removed. A privacy statement will also usually include information regarding systems that are in place to protect the information of website visitors, consumers or other persons whose data is being collected and used.
Production Data	Real customer or systems information used in support of the ongoing business of the financial institution.

Q

Quality Assurance	The actions, planned and performed, to provide confidence that all business processes, systems, equipment, software and components that influence the quality of the services are working as expected, both individually and collectively.
--------------------------	--

R

Readiness	A review of performance ability before cut-over. Evaluation and testing of operational preparedness for cutover to vendor support of people, processes, and platforms.
Recovery Capability	Ability to restore or replace systems, data, work areas, staff, utilities or information that have been damaged or lost.
Recovery Point Objective (RPO)	The point in time that data is recovered in order to resume production processing. It can be used to understand the maximum data loss resulting from a disaster event. The maximum data loss in hours, based on the frequency of offsite backups, resulting from a disaster event.
Recovery Service Levels	Collectively, terms that define the speed, quality and quantity of recovery capability in response to a disaster, including recovery time objective, recovery point objective, timely notification, percent of normal production SLAs that will be delivered during recovery mode, etc.
Recovery Time Objective (RTO)	The maximum time required to resume a business function or UIT function following a disaster event.
Reduced Resource Credits (RRC)	Charges that decrease the payment for volumes below the defined Base Case volumes. (Acronym: RRC)

Relationship Management	Administration processes and organizational structure that provide the framework for interaction between departments, individuals, functions and roles involved in planning/strategy, resourcing, standards/service levels, financial management, audit and reporting/forecasting, to ensure compliance with strategy, policy and contracts.
Remediation Plan	A plan of action to correct the deficiency or material weakness, includes: (1) details of actions to be taken by service provider and/or its subcontractors to correct the deficiency or material weakness, and (2) target dates for successful correction of the deficiency or material weakness.
Report Card	Evaluation of service providers, generally by an outside organization; may include such things as organizational focus, financial stability, strategic vision, recruiting, retention and hiring, project resourcing, and internal knowledge management.
Reputation Risk	Events such as eErrors, delays, or omissions in information technology or business processing that become public knowledge or directly affect customers that can significantly affect the reputation of the serviced financial institutions. (Source: FFIEC)
Request for Information (RFI)	A process to solicit information about a vendor's ability to meet an organization's requirements. An RFI is typically a less formal and comprehensive document than an RFP (Request for Proposal) and is often used to narrow down the field of vendors who will receive a formal RFP.
Request for Proposal (RFP)	A process to request specific information about a vendor's ability to meet an organization's requirements and the fees the vendor charges for the services. The RFP allows the organization to outline its business objectives, technical requirements and contract requirements, and to solicit responses from vendors that describe their ability to meet these needs and related prices.
Residual Risk	The risk remaining at the end of risk identification and mitigation planning; a decision must be made whether to accept residual risk.
Resource Base Cases	A forecast of resource unit consumption over the term of the agreement.
Resource Units	The basis for pricing a measurable unit of consumption.
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.
Results-based Contacts	A type of contract where the parties agree in advance on the desired end result expected from the seller. The seller is often given broad discretion on how to achieve the end result in the most cost effective manner. Also referred to as performance based contract.
Retained Costs	Costs that will remain within the corporation if the function in question is outsourced.

Retained Employee	Person who will be employed by the institution to either perform functions/processes kept in-house or fill a position on the new organizational structure.
Retained Organization	Functions and/or jobs kept in-house or new institution positions in the outsourcing governance structure.
Retention Requirements	Requirement established by a company or by regulation for the length of time and/or for the amount of information that should be retained.
Return on Investments (ROI)	Method for evaluating the value of an investment.
Rightsourcing	Utilizing the appropriate mix of customer and vendor(s) resources.
Risk Acceptance	The Process where an appropriate level of management chooses to accept a risk when the rRisk (regulatory risk at time) is deemed immaterial or tolerable based on RRisk AAppetite (Measurement Protocols); or an Action Plan is not possible or sufficient to mitigate a rRisk; or the cost to mitigate the rRisk may be so prohibitive that accepting that rRisk may be the more practical approach.
Risk Appetite	The amount of risk an organization is willing to accept in pursuit of value. The organization may often consider Risk Appetite qualitatively, with such categories as high, moderate, or low, or they may take a quantitative approach, reflecting and balancing goals for growth, return and risk.
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.
Root Cause Analysis	The formal process to be used by service provider to diagnose the underlying cause of problems at the lowest reasonable level so that corrective action can be taken that will eliminate repeat failures.
Run Rate	Financial performance of a company calculated by extrapolating current results out over a certain period of time. For example, if a company has revenues of \$10 million in its latest quarter, and if the company were to perform at the same level for the next year, it would have annual revenues of \$40 million, or a \$40 million run rate. (Source: investopedia) Financial performance of a company calculated by extrapolating current results out over a certain period of time. For example, if a company has revenues of \$100 million in its latest quarter, the CEO might say: "Our latest quarter puts us at a \$400 million run rate." That is, if the company were to perform at the same level for the next year, it would have annual revenues of \$400 million.

SAS 70 Type I and Type II Audits	An auditing standard developed by the American Institute of Certified Public Accountants (AICPA). In a SAS 70 Type 1 engagement, an independent auditor (service auditor) reports on: 1) a service organization's description of its internal controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements; 2) whether those controls were suitably designed to achieve specified control objectives; and 3) whether those controls had been placed in operation as of a specified date. In a Type II engagement, the service auditor reports on everything included in a Type I engagement, as well as whether the controls tested were operating with sufficient effectiveness to provide reasonable assurance that the related control objectives were achieved during a specified period. A Type II report includes the service organization's description of the controls, as well as the service auditor's description of the tests he or she performed and the results of those tests. Vendors obtain independent assurance of their control objectives and control processes. (See www.aicpa.org for additional information)
Score Card	A performance management report that tracks key metrics; a "balanced" scorecard usually contains four quadrants showing financial, business process, learning/growth, and customer perspectives.
Secondary Service Provider	<i>See</i> Dependent Provider.
Security	A condition that results from the establishment and maintenance of protective measures (automated systems and rules) intended to 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 Policy	A document or set of documents that an organization has published that defines requirements for one or more aspects of information security.
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 Delivery Management	Processes to oversee the active day-to-day provision of work, involving knowledge of the business process, and understanding of whether the services are being provided in a way that properly supports the business at the contracted service levels. (Source: TPI)

Processes to oversee the active day-to-day provision of work, involving knowledge of the business area in which the services are being provided, and understanding of whether the services are being provided in a way that correctly supports the business at the contracted performance levels.

Service Level Agreement (SLA)

Contractual service commitment. An SLA is a document that defines the minimum performance criteria for the provider delivering a specified service. (Source: looselycoupled.com)

The quality of service conditions being measured must be both within the service provider's influence or control and an valuable measure of the success of the deal (Source: Outsourcing Journal); they must clearly define service delivery expectations, provide an objective means of assessing whether performance meets those expectations, define who will measure it, how it will be measured, how often it will be reported, and clearly define incentives and penalties related to service delivery.

The service levels being measured must be both within the supplier's influence or control and an important measure of the success of the deal; they must clearly define service delivery expectations, provide an objective means of assessing whether performance meets those expectations, define who will measure it, how it will be measured and how often it will be reported, and clearly define incentives and penalties related to service delivery.

Service Level Objective

Elements of a Service Level Agreement (SLA). They are agreed to as a way to measure the performance of a service provider and are outlined as a way of avoiding disputes between the parties because of a misunderstanding.

Service Provider

A third party with whom a financial institution has contracted to provide services for the financial institution where there is a practical, financial, or strategic benefit to outsourcing the service or process. Service providers are generally classified as one of two types: technology service providers and business process service providers.

Shared Services

The consolidation of common business functions by different units within an organization in a highly skilled internal department or group, allowing the organization to focus on core business. These services may range from non-core activities such as purchasing and network hubs to higher end services like organizational development and business strategy, project management and marketing. (Source: AMCHAM)

Staff Augmentation

An arrangement in which the employee works for one company which lends the employee out to a third-party company for work. Daily oversight is provided by the third-party company and the staff augmentation company performs most administrative tasks such as payment of wages and benefits as well as tax withholding. Generally, staff augmentation employees will find themselves working primarily at the third-party company's worksite.

Also referred to as Employee Leasing. Contract workers brought in by an organization to supplement efforts of the internal staff in order to contain costs and handle overflow work.

Statement of Work (SOW)

Document used in the systems development life cycle. A software vendor or services company will send a SOW to notify a client of work about to be undertaken and agreed pricing. It is a brief summary of financial aspects of a contract; the technical details should have already been fleshed out by this stage.

Certain areas that need to be addressed are as follows:

- Scope of Work. Describes the work to be done in detail and specifies the hardware and software involved and the exact nature of the work to be done.
- Location of Work. Describes where the work is to be performed. Specifies location of hardware and software and where people will meet to perform the work.
- Period of Performance. This specifies the allowable time for projects, such as start and finish times, number of hours that can be billed per week or month, where work is to be performed and anything else that relates to scheduling.
- Deliverables Schedule. This part lists the specific deliverables, describing what and when it is due.
- Applicable Standards. Describes any industry specific standards that need to be adhered to in fulfilling the contract.
- Acceptance Criteria. This specifies how the buyer or receiver of goods will determine if the product or service is acceptable, what criteria will be used to state the work is acceptable.
- Special Requirements. This specifies any special hardware or software, specialized workforce requirements, such as degrees or certifications for personnel, travel requirements, and anything else not covered in the contract specifics.

Strategic Risk

Risk resulting from inadequate management experience and expertise leading to a lack of understanding causing financial institutions to make poor strategic decisions. (Source: FFIEC)

Inadequate management experience and expertise can lead to a lack of understanding and control of key risks. Additionally, inaccurate information from service providers can cause the management of serviced financial institutions to make poor strategic decisions.

Subcontracting

A contract that assigns some or all of the obligations of a prior contract to another party.

Subcontractor

See Dependent Provider.

Subject Matter Expert (SME)

An individual with deep knowledge in a certain domain. This individual may be seen as an authority and act as the gatekeeper of knowledge for their particular subject area. (Source: Gotcha! Berkeley.edu)

An individual with expertise in a certain topic area. This person may be seen as an authority and act as the gatekeeper of knowledge for their particular subject area.

Supplemental Information Gathering (SIG)	Part of the Financial Institution Shared Assessments Program. The Supplemental Information Gathering document is a uniform questionnaire used to obtain required documentation from a service provider and establish a profile on its operations and controls for each control area.
Supplier Assumed	Costs associated with the outsourced functions that are included in the supplier's bid.
Systems Development Life Cycle/Product Life Cycle	A conceptual model used in project management that defines the stages involved in the development of a project. The steps of the Systems Development Life Cycle are varied, but generally include the following phases... 1) planning and feasibility studies, 2) systems analysts and requirements gathering, 3) systems design, 4) development, 5) testing and integration, 6) acceptance, installation, and deployment, and 7) maintenance.

T

Termination Assistance Plan	A written plan covering all aspects of Termination Assistance Services to be rendered by vendor.
Termination Assistance Services	Assistance or services provided by service provider to allow the terminated or expired services to continue without interruption or adverse effect, to mitigate any disruption to business, and to facilitate the orderly transfer of responsibility for the terminated or expired services to financial institution or one or more successor service providers.
Termination Charges	Costs incurred to exit a contractual relationship.
Time and Materials Contract	A pricing model in which the client pays set rates and related expenses for each worker provided by the service provider. Paying this way, while allowing more flexibility, may lead to a less disciplined approach to the project. A type of contract where the buyer's payment obligations are calculated based on the actual amount of time spent performing the services plus the costs associated with any materials.
Transaction	This phase includes RFP, vendor selection, deal structuring, contract negotiation and signing.
Transactional Cost	Cost incurred in processing a business function.
Transition	The interval between the current state and the desired state in a planned change process. Outsourcing transition includes knowledge transfer, people/process/technology transfer. At the end of transition the vendor begins managing the outsourced process. Includes organizational change management and communications.
Transition Date	The date a functional workgroup is moved from the institution to the third party service provider.
Transition Price	Price for the transition / start-up activities that occur during the first 12-18 months of an outsourcing contract.

Transitioned/Rebadged Employee Employee whose employment relationship changes from the institution to third party service provider or vice versa; may also be referred to as rebadged employee.

U

User Any person who interacts directly with a computer system.

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

V

Value Leakage Lost opportunity cost due to missed benefits and or undiscovered business case obstacles. Mitigation requires identification of indicators of achievement of value and the tracking of the indicators over time.

Vendor Management Office Set up to efficiently negotiate the transactions between clients and vendors. Essentially, a vendor management office facilitates the procurement process away from the organization (such as away from CIOs or IT managers). A vendor management office also seeks higher levels of service and can track metrics and vendor performance. It also negotiates discounts for products, services, and consulting. In theory, a vendor management office should have better control over the technology buying process than other models.

Vendor Manager Person who works closely with vendors and is responsible for the quality and cost effectiveness of vendor services. Activities of vendor management may include vendor compliance, performance, communications, continuity planning, metrics, issue resolution, invoicing and budgeting.

Vendor/Supplier Any company or individual who provides goods or services to the institution regardless of location. Terms such as service provider and supplier are often interchangeable with vendor.

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 Computer instructions (i) that without functional purpose adversely affect the operation, security or integrity of a computing, telecommunications or other digital operating or processing system or environment including without limitation, other programs, data, computer libraries and computer and communications equipment, by altering, destroying, disrupting or inhibiting such operation, security or integrity; (ii) that without functional purpose, self-replicate without manual intervention; or (iii) that purport to perform a useful function but which actually perform either a destructive or harmful function, or perform no useful function and utilize substantial computer, telecommunications or memory resources.

Visa	An official authorization appended to a passport, permitting entry into and travel within a particular country or region. The Immigration and Nationality Act as amended over the years, provides the basic framework for regulating the flow of visitors, workers and immigrants to the United States. The last major overhaul of the immigration system was the Immigration Act of 1990. This Act provides most of the still-current immigrant and nonimmigrant classification and numerical ceilings (subsequent legislation has added new classifications and/or amended existing ones but the basic framework remains largely the same as in 1990). For information on US and foreign citizen visa requirements refer to http://www.uscis.gov/graphics/services/visas.htm .
Volume-based Pricing	Pricing that allows for cost variability as volumes vary during the contract term.
Vulnerability	Hardware, firmware, or software flaw that leaves an automated information system (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 automated information system (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 Assessment	A review that is used to determine the vulnerability of people, property, and the environment to risks by hazards. Items may include intrusion detection, intrusion prevention, firewall management, firewall monitoring, vulnerability management, email filtering, and physical security.
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.

W

Workgroup/ Workstream	The functional grouping of work within an organization. Examples of workgroups in Human Resources might include payroll, reporting, service center, etc. Terms such as tower and work domain are often used interchangeably with workgroups.
------------------------------	--

X

Y

Z

Acronyms

The following identifies some commonly used acronyms. Not all have been defined in this glossary.

24/7 Twenty-four hours a day, seven days per week

A

ADM Application Development and Maintenance
AICPA American Institute of Certified Public Accountants
ARC Additional Resource Charges
ASP Application Service Provider

B

BCP Business Continuity Plan
BOT Build Operate Transfer
BPO Business Process Outsourcing

C

CFO Chief Financial Officer
CIO Chief Information Officer
CISO Chief Information Security Officer
CMM Capabilities Maturity Model
CTQ Critical To Quality

D

DMAIC Define, Measure, Analyze, Improve, Control
DRP Disaster Recovery Plan

E

F

FFIEC Federal Financial Institutions Examination Council
FTE Full Time Equivalent

G

GLBA Gramm-Leach-Bliley Act

H

H1B Category designation by U.S. government regarding occupations and visas
HR Human Resources

I

IP Intellectual Property
ISO International Standards Operations
IT Information Technology
ITO Information Technology Outsourcing

J

K

KPI Key Performance Indicator
KRI Key Risk Indicator

KPO	Knowledge Process Outsourcing
L	
LOB	Line of Business
M	
MDPS	Multi-Regional Data Processing Services
MSA	Master Services Agreement
N	
NDA	Non-disclosure Agreement
NPPI	Nonpublic Personal Information
NVA	Non-Value Added
O	
ODC	Offshore Dedicated Center
OER	Operating Efficiency Ratio
OFAC	United States Department of the Treasury's Office of Foreign Assets Control
P	
PDQ	Product Data Quality
PMI	Project Management Institute
Q	
R	
RFI	Request For Information
RFP	Request For Proposal
ROI	Return on Investments
RPO	Recovery Point Objective
RRC	Reduced Resource Credit
RTO	Recovery Time Objective
RUP	Rational Unified Process
S	
SLA	Service Level Agreement
SME	Subject Matter Expert
SOW	Statement Of Work
T	
TQM	Total Quality Management
U	
V	
W	
X	
Y	
Z	

