

VENDOR SELECTION AND MANAGEMENT POLICY AND STANDARDS

OWNER:

CITIGROUP OPERATIONS AND TECHNOLOGY:
CITIGROUP BUSINESS SERVICES

CONTACT(s):

MICHAEL VALENTINI (212) 615-8714
PAUL PITRE (813) 604-0202

ISSUE DATE:

MAY 2006

Table of Contents

1 OVERVIEW	1
2 POLICY STATEMENTS	2
3 POLICY STANDARDS	3
DEFINITIONS	16
APPENDIX A – ITEMS TO CONSIDER WHEN EVALUATING A VENDOR’S FINANCIAL CONDITION	23
APPENDIX B – SOME TERMS AND CONDITIONS TO CONSIDER FOR OSP CONTRACTS	27
APPENDIX C – ITEMS TO CONSIDER WHEN DETERMINING APPROPRIATE ONGOING VENDOR MANAGEMENT	29
APPENDIX D – ONGOING VENDOR MANAGEMENT FOR OSPs	30

1 OVERVIEW

1.1 OBJECTIVE

Vendor relationships must be managed in order to ensure appropriate controls are in place to protect Citigroup assets and interests as well as our customers' assets and privacy, especially when the vendor provides critical products or services, or when the vendor is an Outsource Service Provider (OSP).

These Citigroup Vendor Selection and Management Policy and Standards ("Standards") were developed to facilitate the following objectives:

- Vendor consolidation to maximize Citigroup's economic leverage
- Common standards and procedures for the selection and management of vendors, especially in the case of OSPs, Critical Vendors, and Major Vendors
- Accurate and relevant vendor information that can be shared across the enterprise
- Documentation of the requirements of the Citigroup Approved Supplier Program (CASP)
- Standard and consistent Contract provisions
- Compliance with applicable Citigroup policies (and regulatory requirements)

1.2 SCOPE

This policy applies to Citigroup, Inc., and its consolidated subsidiaries.

1.3 TARGET AUDIENCE

The target audience for these Standards is those employees responsible for the selection of vendors and ongoing management of vendor relationships.

1.4 OWNER

This policy is sponsored by the Citigroup Head of Operations and Technology. This policy, and any changes to this policy, must be approved by the Head of Citigroup Business Services (CBS). The Head of CBS is responsible for ensuring the ongoing applicability of this policy, and maintaining it appropriately.

1.5 EFFECTIVE DATE / TRANSITION PERIOD

This policy is effective June 1st, 2006, with a 7-month grace period to fully implement the requirements of this policy, or request a policy exception.

1.6 RETIRED POLICIES / RELATED POLICIES

This is a new Citigroup-level Policy. It updates and replaces the Citigroup Technology Vendor Selection and Management Standards (dated March 2003) and the Citigroup Approved Supplier Policy (dated December 2002).

A copy of this document can be found on the CBS website at http://www.citigroup.net/citigroupbusinessservices/wizard_policy_standard.shtml

2 POLICY STATEMENTS

- Each business or country must ensure Approved Vendors, where available, are used to the extent possible when obtaining products or services on behalf of Citigroup.
- Each business or country must identify and classify its Approved Vendors in the Citigroup Approved Supplier Program website.
- In countries and regions where appropriate, Citigroup encourages the utilization of Diverse Suppliers.
- To the extent possible, competitive bids must be obtained and documented as part of the vendor selection process for all applicable vendors.
- Based on the nature of the vendor work performed, the vendor may be required to comply with certain Citigroup policies or applicable regulatory requirements.
- Each business must utilize current Citigroup Enterprise-Wide License Agreements (ELAs) and Master Agreements to the extent possible.
- Products or services must be purchased through the Procure-to-Pay (P2P) or other approved electronic ordering tools, where available.
- Dependent on vendor classification and type of vendor relationship, each business must ensure appropriate due diligence is performed prior to Contract award, as applicable.
- Contracts must be in writing and include terms and conditions approved by appropriate Citigroup legal counsel.
- Based on the nature of the vendor relationship, work performed, and other risk characteristics, the business must perform appropriate ongoing vendor management.
- Each business or country must have processes and procedures that meet the requirements of these Standards.

3 POLICY STANDARDS

Citigroup businesses benefit from maintaining strong relationships with vendors. Benefits include cost savings; improved cycle times for product and services delivery, improved service levels for internal and external customers, expedited time to market for product launches, and improved productivity of internal resources.

Effective vendor management is essential for Citigroup to mitigate key risks, including compliance risk, transaction risk, credit risk, and reputation risk.

3.1 CITIGROUP APPROVED SUPPLIER PROGRAM, ELAs, AND MASTER AGREEMENTS

- 3.1.1. Each business or country must ensure Approved Vendors, where available, are used to the extent possible when obtaining products or services on behalf of Citigroup. A listing of Citigroup Approved Vendors for each business and/or country may be found on the [Citigroup Approved Supplier Program \(CASP\) website](#).
- 3.1.2. Current ELAs and Master Agreements must be reviewed prior to vendor selection to determine whether the product and/or services can be obtained under an existing arrangement. For information on current ELAs and Master Agreements, contact the appropriate member of CBS Procurement. Contact information can be found on the [CBS Procurement website](#).
- 3.1.3. Each business or country must identify and classify its Approved Vendors in the CASP website as follows:
 - Critical Vendor
 - Major Vendor
 - Active Vendor
- 3.1.4. Regardless of Approved Vendor classification or annual expenditure, vendors must be added to the CASP website if the vendor has any one of the following characteristics:
 - Connectivity to Citigroup's networks;
 - Access to Citigroup's [Electronic Transportable Media](#);
 - Access to information classified as Confidential or Restricted per the [Citigroup Information Security Standard \(CISS\)](#); or
 - Is an Outsource Service Provider

Countries or businesses with an approved exclusion on file from CASP are not exempted from complying with this requirement.

- 3.1.5. Annually at minimum, each business or country must review and update the corporate-wide Approved Vendor List posted on the CASP website to ensure their business or country information is accurately reflected. To add or modify vendors on the list, each business or country should contact the appropriate CASP Coordinator. A listing of CASP Coordinators can be found on the [CASP website](#).
- 3.1.6. Where available, each business must review Compliance Reports summarizing the utilization of Approved Vendors and Non-Approved Vendors and take appropriate action to improve the utilization of Approved Vendors.
- 3.1.7. In countries and regions where appropriate, Citigroup encourages the utilization of Diverse Suppliers. When contracting with suppliers that do not meet Citigroup's criteria for Diverse Suppliers, it is Citigroup's preference for the supplier to subcontract a share of the Contract to a Diverse Supplier(s). Additional information about Citigroup's Supplier Diversity Program can be found on the [Citigroup Supplier Diversity website](#).

3.2 PROSPECTIVE VENDOR IDENTIFICATION

- 3.2.1. A Non-Disclosure Agreement (NDA) must be executed with each potential vendor prior to discussions about, or the exchange of, any Citigroup Confidential or Restricted information, as defined in the [CISS](#). A listing of active current Citigroup NDAs can be found on the [Operations and Technology website](#).
- 3.2.2. If a business has a need for a product or service that is not covered by an existing ELA or Master Agreement, the business must contact CBS Procurement or individuals who have been authorized by the respective business to identify potential vendors prior to vendor selection.
 - a. Technology Products and Technology Services: If the Technology Product and/or Technology Service required by a business is not available pursuant to an existing ELA or Master Agreement, the Business Unit Chief Information Officer (CIO) and CBS Procurement representative should collaborate to identify potential Technology Vendors, in consultation with other subject matter experts as needed, prior to the outset of any discussion regarding terms and conditions with any prospective Technology Vendor.

- b. The [ITLC Contracts Committee](#) must be notified prior to execution of a Contract with any prospective Technology Vendor when a proposed Contract meets one or more of the following:
 - Enterprise-wide applicability is anticipated
 - Results in significant spend to the business
 - Involves essential Technology Products and/or Technology Services without which the business could not operate effectively, even for a very limited period of time.
- c. Emerging Technology and Key Technology Application: If the request for a new vendor is for Emerging Technology and/or a Key Technology Application, the appropriate technology organization or business must consult with the [Enterprise Technology Office \(ETO\)](#).

3.3 VENDOR SELECTION AND DUE DILIGENCE PRIOR TO CONTRACT AWARD

- 3.3.1. To the extent possible, competitive bids must be obtained and documented as part of the vendor selection process for all vendors. In general, a competitive bid will include when applicable: a description of required products or services, pricing, performance/quality levels, timing and any other important documentation deemed appropriate under the circumstances. Electronic auction tools (eAuction) should be utilized to the extent possible, where available.
 - a. In general, a competitive bid process is not required for:
 - Orders against or amendment to an existing Contract
 - Sole or single source requirement (i.e. where there are no viable alternate suppliers that can be considered)
 - Emergency requirement where time is of the essence to maintain customer service or continuity of business
 - Contractual commitment less than 25,000 USD, unless an alternative threshold has been established by the business or for a specific commodity. If the alternative threshold is greater than 25,000 USD, the threshold must be approved by Citigroup's Chief Procurement Officer (CPO).
 - b. Bid exceptions must be documented using a bid exception form, unless the contractual commitment is less than 25,000 USD or the alternative threshold established by the business or for a specific commodity. A suggested template is located on the [CASP website](#).

- 3.3.2. Vendors must be checked against the list of Specially Designated Nationals (SDN) published by the Office of Foreign Assets Control and any other applicable U.S. and domestic lists of sanctions. Additionally, countries other than the U.S. must check any local lists and consult with their local Compliance office for specific requirements. If a vendor is found on the SDN list or another sanctions list, the business must contact Citigroup Global Compliance for guidance. The SDN list and other sanctions lists can be found on the [Citigroup Global Compliance Website](#).
- 3.3.3. When required, a vendor's financial stability must be evaluated and understood prior to entering into a new Contract or vendor relationship. Items to consider when performing a financial evaluation are included in [Appendix A](#).
- 3.3.4. Access to Confidential Information, Restricted Information, or Network Connectivity: If the vendor will have access to information classified as Confidential or Restricted or have network connectivity according to the [CISS](#), the business must ensure that the vendor complies with the applicable requirements of the [CISS](#). These requirements include:
- If the vendor has Internet Protocol connectivity to the Citigroup network, the connectivity must be protected by a Citigroup Technology Infrastructure managed firewall per [CISS](#) section 10.8.
 - If a third party is provided access to a software application over private connectivity or the Internet it must have a vulnerability assessment performed using the [Information Security Technology Group approved process](#).
 - If the vendor stores, processes, manages, or accesses Citigroup information, the vendor must sign a Citigroup legal counsel approved NDA or other provision that limits the disclosure of that information only to authorized parties, unless an existing Master Agreement contains appropriate language to address this requirement.
 - If the vendor stores Citigroup Confidential or Restricted information, a Third Party Information Security Assessment (TPISA) must be performed in accordance with the [TPISA process](#).
- In addition, the business must submit an Outsourcing and Access to Information Questionnaire (OAIQ) to CASP within 90 days of Contract execution
- 3.3.5. Major Vendor: In addition to the requirements outlined in Section 3.3.1, through 3.3.4, requirements for a vendor classified as a Major Vendor include:
- Assessment of the vendor's financial stability performed prior to contract execution or renewal unless a financial review of the vendor has been performed within the last twenty-four months

- 3.3.6. Critical Vendor: In addition to the requirements outlined in Sections 3.3.1 through 3.3.4, requirements for a new Critical Vendor or new products or services with an existing Critical Vendor include:
- a. Performance of an assessment of the vendor's financial stability within the last twelve months (if the last financial risk rating assigned was Medium or High) or (if the last financial risk rating assigned was Low) twenty-four months
 - b. Determination of the vendor's use of third parties to provide the requested products or services
 - c. Mitigation of any high-risk issues found while performing due diligence and applicable assessments
 - d. Submission of a business Contingency Plan (CP) to CASP for Critical Vendors with high financial risk rating within 90 days of Contract execution, unless a current CP is already on file in CASP that addresses the same business and the same process
 - e. Submission of a Critical Supplier Questionnaire (CSQ) to CASP within 90 days of Contract execution, unless a CSQ is already on file in CASP for the same business or country
 - f. Other requirements deemed appropriate under the circumstances
- 3.3.7. Outsource Service Provider (OSP): Due to risk that may be associated with Outsourcing relationships, additional due diligence must be performed for vendors designated as OSPs, regardless of Approved Vendor classification, as follows. A suggested form to utilize in performing due diligence can be found on the [CASP website](#):
- a. For OSPs involving a Non-Core Business Process:
 1. Assessment of the OSP's financial stability performed prior to Contract execution or renewal unless a financial review of the OSP has been performed within the last twenty-four months
 2. Evaluation of the OSP's experience in implementing and supporting the proposed activity, including management experience and ability to maintain the service level over time
 3. Assessment of the OSP's business reputation, including publicly-reported complaints and litigation
 4. Identification of OSP's principals and their relationship to the vendor's operation
 5. Assessment of OSP's ability to comply with applicable Citigroup Policies and Standards
 6. Cost/benefit analysis, including transition requirements, when applicable

7. Review of OSP's reliance on subcontractors to provide the requested services and, if applicable, assessment of subcontractors' ability to perform such services
 8. Review of OSP's insurance coverage
 9. References from other companies using the OSP for similar services
 10. Review of Citigroup-Specific Continuity of Business (CoB) Plan from OSP within 90 days of Contract execution
 11. Submission of an Outsourcing and Access to Information Questionnaire (OAIQ) to CASP within 90 days of Contract execution
- b. For OSPs involving a Core Business Process or Information Technology Outsourcing (ITO), in addition to the requirements in 3.3.7.a, the following due diligence and actions must be performed:
1. Review of OSP's internal and/or external audit reports pertaining to the business process or service provided, when available. A SAS-70 type II review or equivalent report conducted by an independent third party that covers the business process or service may satisfy this requirement.
 2. A risk assessment must be performed on the OSP. A suggested Vendor Risk Assessment Model can be found on the [CASP website](#).
 3. Submission of a business Contingency Plan (CP) to CASP within 90 days of Contract execution, unless a current CP is already on file in CASP that addresses the same business and the same process.
 4. As required under current applicable regulations at the time of Contract execution, notice of Contract award to regulatory entity(ies) relevant to the Citigroup business. Regulatory entities that may require notice include: the Office of Thrift Supervision (OTS) for relevant Citigroup businesses, which include all federally chartered banks, all state chartered banks (e.g. Citibank), and thrift institutions (e.g. savings banks and savings and loan associations); and the Office of the Comptroller of the Currency (OCC).

- c. For Offshore Outsourcing, in addition to the applicable requirements listed in 3.3.7.a and 3.3.7.b, the following must be considered:
 - 1. Country Risk: geographical, political, legal, economic, and regulatory changes that may impact the Outsourcing arrangement
 - 2. Choice of law and forum provisions
 - 3. OSP's local jurisdiction laws, regulatory requirements, local business practices, accounting standards, and legal environment
 - 4. Responsibilities of each party in the event of U.S. or local regulatory changes
 - 5. Ability of OSP to comply with applicable U.S. and domestic (if Citigroup business is outside of the U.S.) legal obligations, including U.S. and domestic data protection requirements
- d. When an Affiliate is selected as an OSP, when required by applicable law, the business must show that terms are comparable to those of an external vendor.
 - 1. For ICAs where the process is considered by the business sector to be related to a Sarbanes Oxley (SOX) 404 transaction (e.g. the service provider's process impacts financial reporting), the business must perform a review as set forth in the "Rules of the Road" guidance for "Process Hand-Off Documentation" found on the [Citigroup Finance website](#).

3.4 CONTRACTING

- 3.4.1. Products or services should be purchased through the Procure-to-Pay (P2P) tool, where available. When P2P is not applicable or available, other available electronic ordering tools approved for the business or country must be used.
- 3.4.2. A business must not permit a vendor to commence performance unless a Contract has been fully negotiated and executed or a purchase order (PO) has been issued. If there are extenuating circumstances, a business may permit a vendor to commence performance only (a) with the authorization of the Business Head and appropriate Citigroup legal counsel, and (b) if documentation satisfactory to the Citigroup legal counsel for the business is executed by the parties.

- A Contract or a purchase order must be in writing and include as appropriate:
- a. Clear and enforceable expectations and obligations of each party
 - b. Citigroup and business policies and standards applicable to the Contract
 - c. Safeguards and controls to protect Citigroup's assets, interests and customer information
 - d. Terms and conditions as recommended by the appropriate Citigroup legal counsel
- 3.4.3. Contracts may require additional terms and conditions to comply with regulatory requirements or corporate policies. Examples of Contracts that may require additional terms and conditions are those with vendors that:
- a. Access or process Citigroup Confidential or Restricted Information
 - b. Provide critical technology applications
 - c. Provide outsource services
 - d. Transmit, store and/or dispose of business records
 - e. Dispose of hazardous materials or waste products
 - f. Provide business continuity services to Citigroup
 - g. Are privately held or do not make financial statements available to the general public
- 3.4.4. Every Contract with a vendor must (a) be reviewed and approved by the appropriate Citigroup legal counsel, (b) have all proper internal approvals in place, including financial commitment as appropriate per the business' delegation of authority and the requirements in the [Citigroup Expense Management Policy](#), and (c) be properly executed. Citigroup legal counsel may approve an alternative process for legal review of a Contract within the business s/he supports.
- 3.4.5. The business must comply with any applicable maximum Contract length as well as standard payment terms detailed in the [Citigroup Expense Management Policy](#).
- 3.4.6. Each business should document all active Citigroup vendor-related Contracts in the Contract Management System (CMS), where available, unless a related expenditure is listed as an exclusion to the CASP requirements in Section 3.6. More information on CMS can be found on the [CBS Procurement website](#).
- 3.4.7. Major Vendor: A Major Vendor must have a purchase order or Contract with terms and conditions that have been approved by Citigroup legal counsel.
- 3.4.8. Critical Vendor: A Critical Vendor must have a fully executed Contract with terms and conditions that have been approved by Citigroup legal counsel.

- 3.4.9. Outsource Service Provider (OSP): For OSP Contracts, in addition to the requirements in 3.4.1 through 3.4.8, the following are required, when applicable:
- a. For all OSPs, including OSPs involving a Non-Core Business Process, Core Business Process, or ITO, where appropriate, additional terms and conditions must be included in the Contract. A listing of some terms and conditions to consider are included in [Appendix B](#).
 - b. Offshore Outsourcing: For Offshore Outsourcing, the Contract must be reviewed by Citigroup legal counsel familiar with local laws and regulations.
 - c. ICAs: In certain situations, under applicable laws in certain jurisdictions, ICAs (also commonly referred to as Inter-Affiliate Agreements) should reflect an arm's length transaction and payments terms based on market rates.
 - d. If the business is subject to New York Stock Exchange (NYSE) and National Association of Securities Dealers (NASD) regulation, ensure the NYSE and NASD have access to the OSP's products or services provided, as would be the case if the activities had been directly performed by the business.
 - e. For OSP's performing a service for Citigroup that is a significant process affecting internal controls as related to financial reporting under Sarbanes-Oxley section 404:
 - Any OSP that performs a service affecting internal controls related to Citigroup's financial reporting must also be evaluated by management and verified by Citigroup's independent auditors. Per the Public Company Accounting Oversight Board (PCAOB), OSPs are considered to be a part of financial reporting if the OSP affects any of the following: 1) operational transactions that are significant to financial statements; 2) procedures by which transactions are initiated, authorized, recorded, processed, and reported from incurrence to inclusion in financial statements; 3) accounting records specific to company's transactions; 4) how the company's information system captures events and conditions significant to Citigroup financial statements; or 5) the financial reporting process used to prepare Citigroup's financial statements, including significant accounting estimates and disclosures. For guidance on management's evaluation of OSPs, refer to the ["Rules of the Road"](#) guidance for "Relying on the Work of Others – Use of SAS 70" found on the [Citigroup Finance website](#).
 - A SAS 70 type II report with an unqualified opinion may provide significant proof of compliance to SOX 404.

3.5 ONGOING VENDOR MANAGEMENT

- 3.5.1. Based upon the criticality and other risk characteristics of the vendor, each business must determine what ongoing vendor management is appropriate and, if such ongoing management is required, ensure that it is performed. Items to consider when determining appropriate vendor management are included in [Appendix C](#).
- 3.5.2. A vendor already providing services pursuant to an ELA or Master Agreement may already have ongoing vendor management by a Citigroup entity. In such cases, and after consultation with that Citigroup entity, a business may conclude that additional ongoing management is not necessary.
- 3.5.3. Access to Confidential Information, Restricted Information, or Network Connectivity: If the vendor will have access to information classified as Confidential or Restricted or have network connectivity according to the [CISS](#), the business must ensure that the vendor complies with the applicable requirements of the [CISS](#). These ongoing requirements include:
- a. If the vendor has Internet Protocol connectivity to the Citigroup network, the connectivity must be protected by a Citigroup Technology Infrastructure managed firewall per [CISS](#) section 10.8.
 - b. If a third party is provided access to a software application over private connectivity or the Internet, it must have a vulnerability assessment performed using the [Information Security Technology Group approved process](#).
 - c. If the vendor stores Citigroup Confidential or Restricted information, a TPISA must be performed in accordance with the [TPISA process](#).
- 3.5.4. Major Vendor: In addition to requirements in 3.5.1 through 3.5.3, the business must ensure:
- a. Performance of a financial review every twenty-four months from the last date of review, at minimum.
 - b. The vendor's operational performance is monitored on an ongoing basis as needed.
- 3.5.5. Critical Vendor: In addition to the requirements in 3.5.1 through 3.5.3, the business must ensure:
- a. Performance of a financial review every twelve months or (if the last financial risk rating assigned was Low) twenty-four months. If the vendor's financial condition is considered to be at risk, a more frequent review cycle may be appropriate.
 - b. The vendor's operational performance is monitored on an ongoing basis as needed. Such monitoring must be documented annually, at minimum.

- c. The Contingency Plan is updated on an annual basis for Critical Vendors with a High financial risk rating. If during the course of the Contract, the Critical Vendor's financial risk rating is changed to "High," the business must submit a CP within 90 days of notification of the High Financial Risk Rating.
 - d. Completion of a CSQ if the Vendor's critical classification is modified.
 - e. Review of vendor's CoB Plan on an annual basis, where available.
- 3.5.6 Most Critical Vendor (MCV): Requirements for a vendor designated as an MCV include:
- a. A Lead Vendor Manager must be assigned by the Vendor Risk Management Committee (VRMC) or Citigroup's CPO to monitor the overall vendor management activities associated with the MCV. A Lead Technology Contact(s) must be assigned by the VRMC or the Global Technology Council to assist the Lead Vendor Manager and Vendor Risk Management Unit in assessing the risk and determining the risk management activities required for each MCV. In addition to the requirements in 3.5.5, the Lead Vendor Manager, with the assistance of the Lead Technology Contact(s), must ensure completion and documentation of the following requirements:
 - Documentation of an annual risk assessment. A suggested Vendor Risk Assessment Model can be found on the [CASP website](#).
 - Periodic meetings held with the Vendor Managers utilizing critical products or services from the MCV
 - Periodic briefings to Citigroup senior management summarizing issues, if any, and activities associated with the MCV
 - If the MCV has been designated as a Strategic Vendor Partner by the ETO, the Lead Vendor Manager must review Emerging Technology risks identified by the ETO annually, at minimum
 - Annual submission of a Most Critical Supplier Questionnaire (MCSQ)
 - b. An overall assessment of the MCV's performance within Citigroup must be reviewed annually, at a minimum, with the VRMC.
 - c. Performance of a financial review every twelve months, regardless of financial risk rating. If the vendor's financial condition is considered to be at risk, a more frequent review cycle may be appropriate.
 - d. Annual submission of a Contingency Plan for each business or country that has classified the vendor as a Critical Vendor, regardless of financial risk rating.
- 3.5.7 Outsource Service Provider (OSP): In addition to requirements 3.5.1 through 3.5.3, requirements for an OSP include:

- a. Each business must perform ongoing monitoring and due diligence for each of its OSP relationships. The monitoring activities and frequency of such activities vary according to the OSP agreement: Non-Core Business Process, Core Business Process, ITO, and Offshore Outsourcing. [Appendix D](#) contains a chart outlining the requirements and frequency the business must follow for each type of Outsourcing agreement.
- b. Core Business Process and ITO: If the OSP has an impact on Citigroup's financial reporting as applicable to Sarbanes Oxley (SOX) 404, the business must test the controls over end-to-end process flows and any outsourced functions as outlined in the ["Rules of the Road"](#) guidance for "Relying on the Work of Others – Use of SAS 70" found on the [Citigroup Finance website](#).
- c. ICAs: For ICAs where the process is considered by the business sector to be related to a Sarbanes Oxley (SOX) 404 transaction (e.g. the service provider's process impacts financial reporting), the business must perform a review as set forth in the ["Rules of the Road"](#) guidance for "Process Hand-Off Documentation" found on the [Citigroup Finance website](#).
- d. Additional monitoring and due diligence may be recommended depending on the risk and criticality of the OSP relationship.

3.6 EXCLUSIONS

Exclusions from the CASP requirements in 3.1 are provided for:

- A country or business that has an annual spend with vendors determined to be immaterial within their region may be excluded from CASP if an exclusion is approved by the Head of Citigroup Business Services. Such exclusions must be reviewed by the country or business on an annual basis.
- Expenditures associated with entertainment, hotels utilized for business travel, government agencies, inter-company transactions, philanthropy, taxing authorities, utility companies that operate as a monopoly, premises/rent charges, legal settlements, wage garnishments, employee reimbursements, commissions for sales agents and/or marketing companies, or vendors used for a one-time purchase.
- Vendors with which a business' or country's annual expenditures is less than 25,000 USD. A business or country may establish a lower value if deemed necessary.
- Emergencies, time constraints, or geographic location that prohibit the utilization of an Approved Vendor. Such exclusions must be documented and retained by the business and/or country.

The engagement of outside legal counsel services is excluded from requirements in 3.1 through 3.5, except requirement 3.1.3, which requires that vendors be identified and classified on the CASP website. If a business has a need to engage outside legal counsel, the business must ensure adherence to applicable Policies and Guidelines posted on the [Legal Information and Resources website](#).

[Value Transfer Networks \(VTNs\)](#) are excluded from the requirements in these Standards. Businesses utilizing VTNs should ensure adherence to the [Citigroup Payment Systems Risk Policy](#).

Inter-Company Agreements (ICAs) are excluded from the requirements in 3.1 through 3.5, except where otherwise noted.

3.7 EXCEPTION PROCESS

If a business cannot comply with one or more of the requirements in these Standards, an exception from the Standards must be obtained using an exception form, which can be downloaded from the [CASP Website](#).

Exceptions from these Standards must be approved by the applicable Business Head and Citigroup's CPO. In the case of a Technology Vendor, exceptions must be approved by the applicable Business Head, Citigroup's CPO, and the appropriate Business Unit Chief Information Officer. An exception is valid for one year from the date the exception is approved.

Copies of approved exceptions must be provided to the Head of Citigroup Business Services.

DEFINITIONS

Affiliate is an entity that controls, is controlled by, or is under common control with another entity. Control in this case consists of managing either directly or indirectly through ownership of voting equity interests, by contract, or through other forms of management.

Approved Vendor is a vendor that is authorized by the business and/or by CBS Procurement to provide products and/or services to Citigroup and that is listed on the CASP website. There are three classifications of Approved Vendors: Critical Vendor, Major Vendor, and Active Vendor:

Critical Vendor is an Approved Vendor that directly or indirectly provides essential products and/or services without which the business could not operate effectively, even for a very limited period of time. Some examples may include vendors providing operating system software, application software, or sole source outsource operations that are critical or strategic to the business. Critical Vendors may also include those vendors with which Citigroup has established a strategic alliance or partnership. Factors in determining Critical Vendors include: complexity of exit/transition strategy, internal and external impact of loss of vendor, and availability of alternate vendors.

Most Critical Vendor (MCV) is a Critical Vendor that has been designated as a Most Critical Vendor by the Vendor Risk Management Committee (VRMC) or Citigroup's CPO because: (1) its failure or failure of its products or services would result in significant loss of reputation to Citigroup or the world's financial markets; and (2) its products or services are significantly embedded into the support of critical customer deliveries or regulatory reporting and there are no readily available alternatives; and (3) its products or services have enterprise-wide applicability such that failure of the vendor or its products or services would impact more than one business within Citigroup and its failure has the potential to affect the entire enterprise.

Major Vendor is an Approved Vendor that provides products and/or services to Citigroup that are not critical to business operations, yet Citigroup's actual or anticipated annual expenditure with the vendor is greater than 5,000,000 USD. A business or country may establish a lower value if deemed necessary.

Active Vendor is an Approved Vendor not classified as Critical or Major that provides products and/or services to Citigroup and an ongoing business relationship exists.

Business Process Outsourcing (BPO) is Outsourcing a Citigroup Core Business Process to a vendor.

CBS Procurement is a division of Citigroup Business Services (CBS) that provides procurement through strategic sourcing, vendor management partnerships, and advanced technology based solutions.

Citigroup Approved Supplier Program (CASP) is a global program that encourages vendor consolidation to maximize Citigroup's economic leverage and supports due diligence processes to mitigate Citigroup's operational and financial risk. The CASP website at [CASP Website](#) hosts the corporate-wide Approved Vendor List, enables Citigroup businesses to more effectively manage Approved Vendors, and provides a

central location for businesses to: identify and maintain Approved Vendor information; view internal Citigroup points of contact; review vendor accreditation information and access reports.

Compliance Reports are quarterly reports produced by Citigroup Business Services that give detail as to approved and non-approved spend with vendors for countries and businesses where spend information is available.

Confidential Information is used in these Standards as defined in the [CISS](#).

Contingency Plan (CP) is a document utilized to identify Citigroup's plan to ensure continuity of services in the event a current vendor is unable to continue to provide products or services in an acceptable manner. This may include a transition plan and/or exit strategy, but it is not the vendor's Continuity of Business Plan.

Continuity of Business (CoB) Plan is the vendor's plan describing how it will manage to recover its operations supporting Citigroup business(es) during potential disasters that impede the continuation of normal functions.

Contract is a written legal document signed by two or more parties that includes an offer, acceptance, consideration, obligations of the parties, and legality of purpose. Examples of Contracts may include Master Agreement, Enterprise Wide Agreement, Service Agreement, Statement of Work, and/or amendment, schedule, or order thereto, or any other written document signed by a Citigroup entity and a vendor. A Non-Disclosure Agreement (NDA) is also considered a Contract for the purpose of these Standards.

Contract Management System (CMS) is a web-based system to provide the enterprise with the visibility and control required to successfully manage the Contract lifecycle. CMS is integrated with the Citigroup Approved Supplier Program (CASP) website at [CASP Website](#). In addition, the system provides Contract Managers automatic email alerts of key contractual requirements and associated dates. CMS also provides optical imaging capabilities to scan vendor Contracts.

Diverse Supplier is a Citigroup supplier that can be categorized as one of the following:

Minority Business Enterprise (MBE): A for profit enterprise presently located in the United States or its trust territories, and is at least 51% owned by African Americans, Hispanic Americans, Native Americans, Asian-Indian Americans and Asian-Pacific Americans. Individual(s) must be involved in the day-to-day management of the business.

Woman Business Enterprise (WBE): A for profit enterprise presently located in the United States or its trust territories, and is at least 51% owned, controlled, and operated by a woman or women of U.S. citizenship. Individual(s) must be involved in the day-to-day management of the business.

Disabled Business Enterprise (DBE): A for profit enterprise presently located in the United States or its trust territories, and is at least 51% owned by an individual(s) of U.S. citizenship with a permanent physical or mental impairment which substantially limits one or more of such persons' major life activities. Individual(s) must be involved in the day-to-day management of the business.

Disabled Veteran Business Enterprise (DVE): A for profit enterprise presently located in the United States or its trust territories, and is at least 51% owned by an individual(s) who have performed active service in one of the United States

armed services and is disabled as defined above in DBE. Individual(s) must be involved in the day-to-day management of the business.

Veteran-Owned Small Business (VOSB): A small business (as defined pursuant to Section 3 of the Small Business Act) presently located in the United States or its trust territories, and is at least 51% owned by an individual(s) who have performed active service in one of the United States armed services.

ELA is an Enterprise-Wide License Agreement negotiated by a Citigroup entity under the terms of which Citigroup may acquire Technology Products and allows, but does not obligate, other Citigroup entities to license such Technology Products under the same terms.

Emerging Technology involves new Technology Products and/or Technology Services that are often still evolving and are at an early stage of adoption. A subset of those technologies that are likely to have high impact across the enterprise are classified as "Watch List" technologies. Examples include, but are not limited to SOA (Service Oriented Architecture), VoIP (Voice over Internet Protocol), Thin Client Computing, Grid Computing, speech recognition, and biometric technologies.

Enterprise Technology Office (ETO) is the organization within Citigroup Operations and Technology that is chartered to (1) sponsor the Architecture Council, which will be responsible for establishing a governance structure for managing IT Architecture; (2) partner with the business sectors in the implementation of engineering solutions; (3) lead in the introduction/adoption of new architectures, technologies, and techniques; (4) implement the emerging technology process to objectively evaluate and prioritize new technologies; and (5) leverage the strategic vendor partnership program; and 6) assure the viability of processes, business critical technical standards and solutions by deploying them in select projects that result in real business solutions.

ITLC is the Information Technology Leadership Council. The ITLC ensures that technology investments, strategies and best practices are leveraged across Citigroup. Its members include senior IT managers from throughout Citigroup. A current list of the ITLC members can be found at http://www.citigroup.net/operationsandtechnology/docs/ITLC_Members.xls

ITLC Contracts Committee is a group that coordinates the development of all significant Citigroup technology Contracts that meet the criteria set forth in these Standards. The ITLC Contracts Committee includes global representation from various CBS Procurement Services, technology, business and legal organizations.

Key Technology Application is a type of application used throughout the enterprise to perform key support services for businesses. Examples would include, but are not limited to: Customer Relationship Management (CRM), Interactive Voice Response (IVR), desktop computing, and middleware. Key technology applications are also found in call centers, data centers, and in the core network infrastructure.

Lead Technology Contact is the focal point within the business responsible for interfacing with the Lead Vendor Manager and the Vendor Risk Management Unit in assessing the risk and determining the risk management activities required for each Most Critical Vendor. Other responsibilities include: (1) Monitor operational or performance assessment data, (2) Participate in the development of Citigroup's strategy with Most Critical Vendor, (3) Validate and assist with the implementation of risk mitigation activities, as necessary, (4) Provide input for annual vendor assessments. If

the relationship or most of the spend is specific to a particular business or technology organization, a Lead Technology Contact is selected from the appropriate organization.

Lead Vendor Manager is responsible for ensuring the completion of the initial and ongoing vendor management activities for each Most Critical Vendor as follows: (1) Required due diligence is performed before vendor engagement, (2) Contracts include appropriate provisions and are approved by Citigroup legal counsel, (3) Vendor's financial stability is monitored, (4) Vendor's adherence to contractual obligations is monitored, excluding operational performance (5) Additional assessments required for Outsource Service Providers are completed, (6) Provide input for annual Vendor assessments. The Vendor Risk Management Committee or Citigroup's CPO assigns a Lead Vendor Manager to each Most Critical Vendor. A Lead Vendor Manager is selected from CBS Procurement if the vendor contractual relationships cross multiple businesses or technology organizations. If the relationship or most of the spend is specific to a particular business or technology organization, a Lead Vendor Manager is selected from the appropriate organization.

Master Agreement is a Contract negotiated by a Citigroup entity that establishes consistent terms and conditions and allows, but does not obligate, Citigroup entities to participate in the Master Agreement when acquiring the products and/or services. The Master Agreement may reflect a negotiated pricing schedule or pricing may need to be separately negotiated at the time a business is ready to participate under the Master Agreement.

Non-Disclosure Agreement (NDA) is an agreement between Citigroup and a vendor whereby the exchange and disclosure of information is governed by the terms of the agreement.

Non-Approved Vendor is a vendor that is not authorized to provide products and/or services to Citigroup or has performance that poses unacceptable risk to Citigroup.

Outsource Service Provider (OSP) is an external or Affiliate service provider that has an arrangement with a Citigroup business to operate, perform, or manage all or part of a business function, role, service, or system operation that was at one time performed internally by the Citigroup business or would ordinarily be performed internally by a similar business. This does not include services where the Citigroup business retains management control of the service received, such as third party maintenance Contracts or temporary staff working under Citigroup direction. A relationship with an OSP involves a Core Business Process, Information Technology Outsourcing, or a Non-Core Business Process:

Core Business Process is a function, operation, or service that is so essential to a Citigroup business that a weakness or failure of the function, operation, or service would seriously impact the business' ability to operate effectively, to deliver its products and services, and / or to comply with applicable legal and regulatory requirements. Core Business Processes include, but are not limited to, loan processing, deposit processing, fiduciary and trading activities, and customer call centers. For the purpose of these Standards, internal audit and compliance functions are also considered Core Business Processes. If an OSP performs a Core Business Process that also could be considered Information Technology Outsourcing, the OSP process will be designated as a Core Business Process.

Information Technology Outsourcing (ITO) is Outsourcing to a vendor all or part of a Citigroup business' information technology (IT) function, operation, role,

or service (e.g. system development and maintenance, production support, security monitoring and testing, network operations, and help desk operations supporting systems). If an OSP performs a Core Business Process that also could be considered Information Technology Outsourcing, the OSP process will be designated as a Core Business Process.

Non-Core Business Process is a function, operation or service that is not a Core Business Process. Non-Core Business Processes may include, but are not limited to, mailroom operations, physical security, property management, and photocopy centers.

Outsourcing is an arrangement for an external or Affiliate service provider to operate, perform, or manage all or part of a Citigroup business function, role, service, or system operation that was at one time performed internally by the business or would ordinarily be performed internally by a similar business. This does not include services where Citigroup retains management control, such as third party maintenance Contracts or temporary staff working under Citigroup direction. Outsourcing may include three types of business agreements:

(1) Agreements between a business unit and an Outsource Service Provider (OSP) located in the same country (i.e. Domestic Outsourcing / Onshore Outsourcing)

(2) Agreements between a business unit and an OSP located in different countries, including arrangements with vendors within close geographical proximity to the business (i.e. Nearshore Outsourcing) and arrangements with vendors in a different geographical region than the business (i.e. Offshore Outsourcing). For the purpose of these Standards “Offshore” refers to both “Offshore” and “Nearshore” Outsourcing arrangements.

(3) Inter-Company Agreements (ICAs), which are legal agreements between two or more Citigroup Affiliates. In certain situations, under applicable laws in certain jurisdictions, ICAs must reflect an arm’s length transaction and payment terms based on market rates. ICA may also be known as “Inter-Affiliate Agreements.” ICAs may be Domestic or Offshore Outsourcing.

Personally Identifiable Information is information that identifies or can be used to identify, contact, or locate a person. This encompasses information that is used in a way that is personally identifiable, including linking it with identifiable information from other sources, or from which other Personally Identifiable Information can easily be derived. To the extent unique information (which by itself is not Personally Identifiable Information) such as a personal profile, unique identifier, biometric information, and Internet Protocol (IP) address is associated with Personally Identifiable Information, then such unique information will also be considered Personally Identifiable Information.

Procure to Pay (P2P) is the Citigroup enterprise system utilized to purchase goods and services and to render payment to vendors for such goods and services.

Restricted Information is used in these Standards as defined in the [CISS](#).

SAS 70 Review is a review of an Outsource Service Provider's (OSP's) or vendor's internal controls as they relate to an audit of the provider's financial statements and is conducted by an independent firm in accordance with the Statement on Auditing Standards (SAS) 70. Such a review may be performed on an Outsource Service Provider's or vendor's organization outside of the United States; however, the review must be completed by an independent firm based in the United States that subscribes to the American Institute of Certified Public Accountants (AICPA). While a SAS 70 review may or may not be performed by a Certified Public Accountant (CPA) firm, a SAS 70 Report must be issued by a CPA. There are two types of SAS 70 Reports that may be issued following the completion of a SAS 70 Review as follows:

Type I SAS 70 Report is a SAS 70 Report that comments on an Outsource Service Provider or vendor's controls that are placed in operation and includes:

- A description of an organization's internal controls as it relates to an audit of financial statements
- Whether such controls are suitably designed to achieve the specified control objectives
- Whether the controls had been placed in operation as of a specific date
- The scope of a Type I SAS 70 review does not include a test of the documented controls

Type II SAS 70 Report is a SAS 70 Report that comments on an Outsource Service Provider or vendor's controls placed in operation and their operating effectiveness and includes:

- All items in a Type I SAS 70 Report above, as well as whether or not the controls that were tested were operating with sufficient effectiveness to provide reasonable assurance that the related control objectives were achieved during the period specified in the review (minimum of six month period)
- Information on and an evaluation of the following five Committee of Sponsoring Organizations of the Treadway Commission (COSO) components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring.
- The scope of a Type II SAS review generally includes a review of the controls over information technology and related processes.

Strategic Vendor Partner is defined within the emerging technology process and strategic vendor partnership program embedded in the Enterprise Technology Office (ETO). It describes a third party company that scores high in (1) the amount of fiscal year expenditure within the technology / telecom category; (2) technical capability in emerging technologies; (3) ability to serve Citigroup and execute well. These results are based on evaluations that use a specific set of criteria. The strategic vendor partnership program coordinates the relationship with such third parties until the technology is deployed.

Technology Product is any software, hardware, information services, or telecommunications product.

Technology Services are services connected with the design, development, testing, installation and operation of Technology Products. This includes, but is not limited to services provided in connection with: core processing; information and transaction processing and settlement activities; information security; security monitoring (including ethical hacking); systems development and maintenance; call centers; customer service; internet related services; data mining; data storage and archiving; telecommunications; continuity of business services and user acceptance.

Technology Vendor is any vendor providing a Technology Product or Technology Service to a Citigroup business.

Value Transfer Networks (VTNs) are the external financial infrastructure in each market that Citigroup relies on for payment trading, clearing, settlement and depository services. VTNs include payment systems, exchanges, clearinghouses, securities settlement systems, depositories, ATM networks, credit card associations and electronic communication networks.

Vendor Manager is responsible for managing the vendor's operational performance to the Contract. This includes day-to-day dealings with Critical Vendors and Most Critical Vendors with respect to support and service deliveries and any required Contingency Plans. Responsibilities also include compliance to information security requirements and requirements for Outsource Service Providers, when applicable. A Vendor Manager typically resides within the business. There may be more than one Vendor Manager assigned to a vendor.

Vendor Risk Management Committee (VRMC) is an executive-level committee designed to integrate senior technology, functional and business representatives to manage Citigroup's risk with its Most Critical Vendors (MCVs). The committee's objectives include heightening awareness regarding risks associated with MCVs, providing global assessments of MCVs, discussing overall risk to Citigroup posed by MCVs, ensuring appropriate risk mitigation efforts are taken, and gauging the status of risk mitigation activities.

Vendor Risk Management Unit is a unit within CBS Procurement assigned to facilitate and monitor Citigroup's risk mitigation activities with a Most Critical Vendor.

APPENDIX A – ITEMS TO CONSIDER WHEN EVALUATING A VENDOR’S FINANCIAL CONDITION

- **Vendor Financial Evaluation (VFE) Report Fulfillment:**
 - The performance of VFEs for Critical and Major Vendors and OSPs is coordinated and overseen by CBS Procurement or another business organization authorized by CBS Procurement. Information on CBS Procurement representatives is located on the CBS Procurement website at: [CBS Procurement Website](#).
 - The performance of VFEs for vendors with other classifications may be overseen by the businesses.
 - VFEs may be performed internally or by an approved third-party service provider. If a third party is utilized to perform VFEs, the agreement or Contract with the third party should include terms or provisions that protect the confidentiality of non-public financial statements provided by Citigroup or Citigroup’s vendors.
- **Vendor Financial Evaluation (VFE) Guidelines:**
 - In the performance of a VFE, the vendor’s financial condition should be assessed through the analysis of recent financial statements, utilizing tools such as relevant ratio and trend analysis and other research materials, as available.
 - The financial statements utilized in performing an VFE should meet the following criteria:
 - The financial statements should cover at least the previous two fiscal years, if possible.
 - Audited Financial Statements should be obtained, if available. If the vendor does not have Audited Financial Statements, the following should be obtained, in descending order of preference:
 - Reviewed Financial Statements
 - Compiled Financial Statements
 - Management Statements
 - Tax Returns
 - The financial statements should include Balance Sheets, Income Statements, Cash Flow Statements, and Notes to the Financial Statements, if available.
 - Consolidated Financial Statements for the vendor’s Parent Company should be utilized, if available. If Consolidated Financial Statements are not available, the financial statements utilized should pertain to the Subsidiary designated as Critical, Major, or an OSP for the responsible business or country.
 - If the vendor is a Joint Venture, the financial statements of the jointly owned entity should be utilized, if available, instead of the Financial Statements of the separate companies holding joint ownership.
 - If the vendor refuses or is unable to provide financial statements or other quantitative information regarding its financial condition, an exception should be documented with CBS Procurement or another organization authorized by CBS Procurement.
 - If the vendor’s financial statements are not publicly available, as with most Privately Held Companies, and a third-party service provider is utilized to perform the VFE, the vendor being evaluated should either agree in writing to allow

- Citigroup to provide its financial statements to the third party or should provide the financial statements directly to the third party.
- The VFE should result in the assignment of a Low, Medium, or High Vendor Financial Risk Rating. If the third-party service provider utilized assigns financial risk ratings based on a different scale or schema, the scale should be mapped to Low, Medium, or High Vendor Financial Risk Ratings.

DEFINITIONS

“Audited Financial Statements” are financial statements which have been prepared and certified by an auditor. In the United States, the auditor certifies that the financial statements meet the requirements of the United States’ Generally Accepted Accounting Principles (GAAP). Outside the United States, the auditor certifies that the financial statements meet the requirements of the accepted accounting principles of a given country.

“Balance Sheet” is a quantitative summary of a company's financial condition at a specific point in time, including assets, liabilities and net worth. The first part of a Balance Sheet usually shows all the productive assets a company owns, and the second part shows all the financing methods (such as liabilities and shareholders' equity).

“Cash Flow Statement” is a summary of a company's financial health, measured as cash receipts minus cash payments over a given period of time or net profit plus amounts charged off for depreciation, depletion, and amortization.

“Compiled Financial Statements” are financial statements that are read by an auditor. The auditor’s report issued with Compiled Financial Statements contains the auditor’s opinion regarding whether the financial statements are in proper form and appear to contain appropriate disclosures. The report issued will state that the auditor has not audited the financial statements and is not expressing an opinion on their fairness.

“Consolidated Financial Statements” are financial statements consolidated at the Parent Company level, including its Subsidiaries.

“Income Statement” is an accounting of sales, expenses, and net profit for a given period.

“Joint Venture” is a contractual agreement joining together two or more parties for the purpose of executing a particular business undertaking. All parties agree to share in the profits and losses of the enterprise.

“Management Statements” are financial statements that are internally prepared by a company. A company’s management uses these financial statements to obtain reasonable assurance regarding the achievement of the company’s financial objectives. No auditor is involved in the preparation of these financial statements.

“Notes to the Financial Statements” provide text to explain the data in the financial statements. They are largely descriptive and include material information on accounting methods, contingencies, and items in the financial statements. Notes may also contain

information regarding significant events affecting the company between the end of the fiscal year and the publication of the financial statements.

“Parent Company” is a company that includes the financial results of its Subsidiaries in its Consolidated Financial Statements.

“Privately Held Company” is a company for which securities are not currently traded on the open market.

“Reviewed Financial Statements” are financial statements analyzed by an auditor to determine if any unusual relationships exist. If there are none, the auditor will state that no material changes are needed to make the financial statements conform to GAAP (or to accounting principles in the country in question). A review has a narrower scope than an audit and does not include an auditor’s opinion regarding the financial statements.

“Subsidiary” is a company for which financial results are included in the Consolidated Financial Statements of the Parent Company.

“Vendor Financial Risk Rating” is a risk rating assigned to a vendor based on the findings of the VFE. The Vendor Financial Risk Rating definitions utilized by the CBS Procurement Vendor Financial Evaluation Unit (VFEU) are included below for reference. These definitions are internal and reflect a given vendor’s viability and its ability to meet contractual and commercial obligations.

“Low Financial Risk Rating”: Vendors receiving this rating will demonstrate good overall financial strength and stability. This is usually evidenced by a history of continuous earnings, sufficient cash flow to meet financial commitments and a strong capital base. Vendors in this rating category are either active in a stable industry or are industry leaders in a more cyclical industry. They will usually show sufficient liquidity to weather short-term market disturbances or financial volatility and will have a proven management team. These vendors appear to have long-term viability.

“Medium Financial Risk Rating”: Vendors receiving this rating will demonstrate an adequate or marginally adequate capacity to meet financial obligations. They usually exhibit deteriorating trends. This might be evidenced by an already inconsistent operating performance or by adverse business, financial or economic conditions, which would likely impair the Company’s ability to maintain operating performance. Vendors in this rating category are active in an industry with weak revenue or profit characteristics or excess capacity. They typically show marginally adequate cash flow for debt service, high leverage or strained liquidity. Management is generally adequate, but may be limited in depth. Although there are no immediate viability concerns, long-term viability is not assured for these vendors.

“High Financial Risk Rating”: Vendors receiving this rating exhibit a well-defined weakness that jeopardizes the timely servicing of liabilities. Such weaknesses may include adverse trends or developments of a financial, managerial or economic nature. If deficiencies are not corrected, there is a

distinct possibility of default with these vendors. Other characteristics of vendors in this category might include start-up operations, uncomfortably tight debt service coverage, dependence on external sources of liquidity, and vulnerability to industry cycles or trends that could impair capacity to meet credit obligations. There are serious short-term viability concerns with these vendors.

“Tax returns” are tax forms filed by businesses with a government entity or agency.

APPENDIX B – SOME TERMS AND CONDITIONS TO CONSIDER FOR OSP CONTRACTS

Scope of Arrangement	Description of required activities, and assignment of responsibilities; obligations of, and services performed by, the service provider; change control process
Term and Termination	Term of the agreement, default and termination
Relation of Parties	Citigroup's right to retain other vendors; customer complaints; and human resource issues
OSP's Policies and Procedures	OSP's CoB; and adherence to applicable Citigroup policies and standards
Reports	Specification of the frequency and types of reports the business will receive. Notification of certain events that impact service, and requirement to provide financial statements
Proprietary Rights	Data and system ownership, access, and license
Fees and Payment Terms	Cost and compensation, including incentives and penalties; payment schedules; responsibility for applicable taxes; responsibility for payment of fees and purchase of software and hardware
Representations and Warranties	Service levels, performance standards, and penalties; warranties; and disclaimers
Confidential Information	Confidentiality and security of data shared with service provider; if OSP will have access to Citigroup Confidential or Restricted Information as outlined in the CISS , requirement for vendor to disclose any security breaches that affect Citigroup or customers

Indemnification	OSP indemnification of Citigroup
Insurance Requirements	Notification of changes in insurance coverage
Limitation of Liability	Limitation of liability for lost profits or for special, incidental, indirect, consequential or exemplary damages arising out of the agreement
Subcontractors	Requirement for Citigroup approval for OSP to use subcontractors
Assignment	Any assignment of the agreement by OSP requires Citigroup's prior written consent; Citigroup can assign to an Affiliate without consent upon notice to OSP
Regulatory Requirements	Compliance with all applicable regulatory requirements
Choice of Law and Jurisdiction	Choice of law and jurisdictional covenants
Force Majeure	In the event an excusable delay by OSP continues more than a certain period, Citigroup may terminate
Right to Audit	Citigroup's right to audit OSP or obtain third party audit of OSP; access to information and operations by regulating authorities
Additional Terms and Conditions	Protection of privacy and Personally Identifiable Information given legal and regulatory requirements as deemed necessary. Dispute resolution mechanisms, escalation procedures. Additional terms and conditions as recommended by appropriate Citigroup legal counsel

APPENDIX C – ITEMS TO CONSIDER WHEN DETERMINING APPROPRIATE ONGOING VENDOR MANAGEMENT

Quality of Service and Support

- Is the vendor's performance relative to its contract obligations adequate?
- Do any changes in the business' needs require an adjustment in the vendor's service levels?
- Does the quality and frequency of communication between the vendor and business result in meaningful real-time discussion of performance and operational issues?
- Has the vendor addressed and improved any documented service issues in a timely manner?
- Are reports, where appropriate, documenting the vendor's performance adequate to provide a meaningful assessment of the vendor's performance?

Operational Performance

- Has the vendor demonstrated flexibility with changing priorities and/or requirements?
- If the vendor is a Critical Vendor, are deficiencies noted in the Critical Vendor's internal, external or regulatory review reports adequately addressed in a timely manner?
- Is the vendor in compliance with applicable Citigroup policies as required in the contract?
- Have there been any changes in the vendor's key management team? If so, have escalation contact lists been updated?
- Does the vendor continue to maintain adequate insurance coverage required by the contract?

Continuity of Business, Contingency Planning and Other Information Security Practices

- When applicable, has a Third Party Information Security Assessment (TPISA) been performed?
- If the vendor is a Critical Vendor:
 - Have there been any significant changes to the Critical Vendor's policies related to internal controls, information security, and contingency planning since Contract execution? If so, have the changes been reviewed to ensure continued compliance with applicable Citigroup policies?
 - When applicable, has the vendor's CoB Plan relative to business been updated to ensure all critical functions can be restored within an acceptable timeframe?
 - Are the Critical Vendor's subcontractors or other interdependent service provider systems included, as appropriate, in the vendor's contingency plan relative to the business?

Financial Condition

- Where applicable, is the frequency at which the vendor's financial stability is monitored commensurate with the financial risk assigned?

APPENDIX D – ONGOING VENDOR MANAGEMENT FOR OSPs

Ongoing vendor management requirements for OSPs are outlined below. If the OSP falls under two or more types of agreements (e.g. Core Business Process and Offshore), the higher frequency requirement applies. Suggested forms to utilize in ongoing vendor management can be found on the [CASP website](#).

		<u>Non-Core Business Process</u>	<u>Core Business Process</u>	<u>ITO</u>	<u>Offshore</u>
1	Citigroup business review of OSP's operations including assessment of quality of service and support, customer complaint resolution, and compliance to applicable Citigroup and business policies and standards	Annual	Annual	Annual	Semi-Annual
2	Quality assurance reviews	As needed	Annual	Annual	Semi-Annual
3	Review transaction procedures	Every two years, at minimum	Annual	Annual	Semi-Annual
4	Review OSP's internal operational assessment	Every two years, at minimum	Annual	Annual	Semi-Annual
5	Review of OSP's internal and/or external audit reports regarding its operations or controls pertaining to the services provided	As needed	Annual	Annual	Semi-Annual
6	Review OSP's insurance coverage	Annual	Annual	Annual	Annual
7	Review Citigroup-Specific CoB plan from OSP and test results	Annual	Annual	Annual	Annual
8	Financial evaluation	Every two years, at minimum.	Low Financial Risk = Every two years - High or Medium Financial Risk = Annual	Low Financial Risk = Every two years - High or Medium Financial Risk = Annual	Low Financial Risk = Every two years - High or Medium Financial Risk = Annual
9	Review of the status of the Contract which may include, but is not limited to Contract expiration date and verification that terms and conditions are still appropriate	Every two years	Annual	Annual	Annual
10	TPISA, if applicable	Annual	Annual	Annual	Annual
11	Documentation of business Contingency Plan	N/A	Annual	Annual	Annual
12	English Language documentation on file for U.S. regulators	N/A	N/A	N/A	As needed
13	Monitor Country Risk	As needed	As needed	As needed	As needed
14	Monitor other risk factors such as price and foreign currency exchange rate	As needed	As needed	As needed	As needed