TPM RISK TOOL

MASTER

Bank Name		**Criticality**	TOTAL BSRs _____ TOTAL CRITICAL _____	TOTAL MCS _____	TOTAL OSP _____
HQ Address		**Materiality**	TOTAL HIGH _____	Medium _____	LOW ____
Bank ID #		**Bank Risk Rating**			
Document #		**Instructions:** Grade each item according to how well the response meets OCC requirements: 1=Outstanding, 2=Very Good, 3=Satisfactory, 4=Needs Improvement, 5=Unsatisfactory or No Response. (Mid-range ratings are also acceptable i.e., 2.5, 3.75, etc.) Note: EDD = Enhanced Due Diligence required.			

#	Check if Yes	Description	Bank Source Docs	Page #	Comments	Raw Rating	Weight	Weighted Rate	Risk Appetite	Result
1	☐	**Planning**								
1.1	☐	**SENIOR MGT PLANNING PRIOR TO ENGAGEMENT: Before entering into a third-party relationship, did senior management develop a plan to manage the relationship?**	CSSMP _____ Planning Require-ments (PR)	1, 3, 4 _____ 1.1-1.6.1	1.1 Bank should have a Management Plan policy statement that (1) includes all of these requirements, (2)includes a template, and (3) determines when a Supplier will be required to have an MP based on its risk and complexity. (Citi requires an MP only for Critical and High Risk Suppliers; should be expanded to include all OSPs and Major Spends above $XXX,XXX.)					
1.2	☐	Is the management plan commensurate with the level of risk and complexity of the third-party relationship?	PR*	1.6.1	1.2 The MP template should be a smart form that expands based on risk factors and categories. (*PR req'd for Critical, Very High Risk, Core OSP, Cust Interaction, Legal/ Reg Compl, Essential Prod, Credit Risk, Ext hosted Citi- branded internet facing app BSRs.)					
1.3	☐	Does the management plan discuss the risks inherent in the activity?	CSSMP _____ PR	_____1.3. 1	1.3 Inherent risks are not quantified or considered, other than simple referencing at Citi. I don't think BSRMs or CPS understands how to assess or mitigate inherent risks.					
1.4	☐	Does the management plan outline the strategic purposes of using third parties (e.g., reduce costs, leverage specialized expertise or technology, augment resources, expand or enhance operations)?	CSSMP	1 (Objective)	1.4 Yes, I have seen references to this in some CPS documentation.					
1.5	☐	Does the management plan outline the legal and compliance aspects, and inherent risks associated with using third parties?	PR	1.4.1	1.5 The Supplier's MP should (1) identify and quantify all risks, (2) be risk rated, and (3) be Centurion rated as part of the Selection process. All identified risks should be referenced in the Supplier's Exit Strategy.					
1.6	☐	Does the management plan discuss how the arrangement aligns with the bank's overall strategic goals, objectives, and risk appetite?	PR	2.5.5 (only for Critical, Very High Risk & Core OSP BSRs)	1.7 I never saw Citi's risk appetite or strategic goals and objectives defined, nor referenced in their SRM governance but it is addressed in the PR so it is considered for some BSRs. Need to expand the list.	3.75				
1.7	☐	Does the management plan assess the complexity of the arrangement, such as the volume of activity, potential for subcontractors, the technology needed, and the likely degree of foreign-based third-party support?	CSSMP		1.8 Possibly CPS questionnaires address this.					
1.8	☐	Does the management plan determine whether the potential financial benefits outweigh the estimated costs to control the risks (including estimated direct contractual costs and indirect costs to augment or alter bank processes, systems, or staffing to properly manage the third-party relationship or adjust or terminate existing contracts)?	PR	1.51 (only for Critical & Very High Risk BSRs)	1.9 Finance or CPS performs a Cost/Benefit analysis. Comment: recommend the Bank expands the list to include all OSPs, Essential Products, and High Risk BSRs.	4				
1.9	☐	Does the management contract consider how the third-party relationship could affect other strategic bank initiatives, such as large technology projects, organizational changes, mergers, acquisitions, or divestitures?	CSSMP		1.10 I never saw a reference to this.					
1.10	☐	Does the management plan consider how the third-party relationship could affect bank and dual employees and what transition steps are needed to manage the impacts when the activities currently conducted internally are outsourced?	CSSMP		1.11 Define dual employees. If the MP defines transition steps, they should be referenced in the Supplier's Exit Strategy.					
1.11	☐	Does the management plan assess the nature of customer interaction with the third party and the potential impact the relationship will have on the bank's customers—including access to or use of those customers' confidential information, joint marketing or franchising arrangements, and handling of customer complaints—and outline plans to manage these impacts?	CSSMP		1.12 I never saw a Citi Management Plan so I don't know what it covers; however, their iCRF covered some of this; now CASP+ does it apparently.					
1.12	☐	Does the management plan assess potential information security implications including access to the bank's systems and to its confidential information?	CSSMP	Appendix D plus Section 2.8 (page 8)						
1.13	☐	Does the management plan consider the bank's contingency plans in the event the bank needs to transition the activity to another third party or bring it in-house?	Exit Strategy		1.14 The Supplier's MP's transition strategy should be referenced in its Exit Strategy.					
1.14	☐	Does the management plan assess the extent to which the activities are subject to specific laws and regulations (e.g., privacy, information security, Bank Secrecy Act/Anti-Money Laundering (BSA/AML), Anti-Bribery), and fiduciary requirements)?			1.15 The Supplier's MP should identify all specific U.S. laws and regs that apply to them to they can be referenced (identified) in the contract and monitored.					
1.15	☐	Does the management plan consider whether the selection of the third party is consistent with the bank's broader corporate policies and practices including its diversity policies and practices?	CSSMP	Section 2.2 Guiding Principles						
1.16	☐	Does the management plan detail how the bank will select, assess, and oversee the third party, including monitoring the third party's compliance with the contract?		Section 2.1 plus Sections 2.4-8 plus Appendix B, C, D, G & H						
1.17	☐	Is the management plan presented to and approved by the bank's board of directors especially when CRITICAL activities are involved?			Check to see if the SRMC approves all CRITICAL Suppliers?					

#	Check if Yes	Description	Bank Source Docs	Page #	Comments	Raw Rating	Weight	Weighted Rate	Risk Appetite	Result
2	☐	**Due Diligence and Third-Party Selection**								
2.1	☐	Does the bank conduct due diligence on *all* potential third parties before selecting and entering into contracts or relationships?			2.1 At Citi, CPS conducts due diligence for new BSRs prior to contract, but they make exceptions; for example, Citi PO's can bypass DD. (Need more details about timing of Finance & Compliance involvement; CPS may disapprove a prospect before they are involved.)					
2.2	☐	Confirm the bank does not rely solely on experience with or prior knowledge of the third party as a proxy for an objective, in-depth assessment of the third party's ability to perform the activity in compliance with all applicable laws and regulations and in a safe and sound manner.			2.2 Not sure. Once a BSR is approved as Master Agreement or Evergreen, they may not be reevaluated in depth. FE updates and Annual Reviews probably are it.					
2.3	☐	Is the degree of due diligence commensurate with the level of risk and complexity of the third-party relationship?			2.3 Confirm CPS has smart forms that expand DD based on increasing risk factors and categories, i.e., OSP, MCS, Critical and Major Spend.					
2.4	☐	Is more extensive due diligence performed when a third-party relationship involves critical activities?			(see 2.3 above)					
2.5	☐	Are on-site visits performed to fully understand the third party's operations and capacity?			(see 2.3 above)					
2.6	☐	If the bank uncovers information that warrants additional scrutiny, does it broaden the scope or assessment methods of the due diligence as needed?			(see 2.3 above)					
2.4		**Does the bank consider the following during due diligence:**								
2.4.1	☐	**Strategies and Goals**								
2.4.1.1	☐	Does the bank review the third party's overall business strategy and goals to ensure they do not conflict with those of the bank?								
2.4.1.2	☐	Does the bank consider how the third party's current and proposed strategic business arrangements (such as mergers, acquisitions, divestitures, joint ventures, or joint marketing initiatives) may affect the activity?								
2.4.1.3	☐	Does the bank review the third party's service philosophies, quality initiatives, efficiency improvements, and employment policies and practices?								
2.4.2	☐	**Legal and Regulatory Compliance**								
2.4.2.1	☐	Does the bank evaluate the third party's legal and regulatory compliance program to determine whether the third party has the necessary licenses to operate and the expertise, processes, and controls to enable the bank to remain compliant with domestic and international laws and regulations?			This is a critical one. The MP should identify the specific laws & regs and Compliance should review the Supplier's governance, audits, licenses, CAPs, etc.					
2.4.2.2	☐	Does the bank check compliance status with regulators and self-regulatory organizations as appropriate?			This should be built into the App & Annual Review smart forms for higher risk Suppliers.					
2.4.3	☐	**Financial Condition**								
2.4.3.1	☐	Does the bank assess the third party's financial condition, including reviews of the third party's audited financial statements?			Yes, the Finance Dept performs an FE initially and rates it annually or semi-annually.					
2.4.3.2	☐	Does the bank evaluate growth, earnings, pending litigation, unfunded liabilities, and other factors that may affect the third party's overall financial stability? (Note: Depending on the significance of the third-party relationship, the bank's analysis may be as comprehensive as if extending credit to the third party.)	PR	**2.5.3** (only for Critical, Very High Risk, Core & Non-Core OSP, Cust Interaction, Essential Prod, Credit Risk.) **2.5.4**	1-This should be built into the App & Annual Review smart forms for higher risk Suppliers 2-PR does not indicate which BSRs get financial evaluation for credit risk exposure (See Third Party Credit Risk Policy.) 3-List should be expanded to match 1.6.1.					
2.4.4	☐	**Business Experience and Reputation**								
2.4.4.1	☐	Does the bank evaluate the third party's depth of resources and previous experience providing the specific activity?								
2.4.4.2	☐	Does the bank assess the third party's reputation, including history of customer complaints or litigation?	PR	2.5.6 & 2.5.7 (only for Critical, Very High Risk & Core OSP BSRs)	List should be expanded to match 1.6.1	3.75				
2.4.4.3	☐	Does the bank determine how long the third party has been in business, its market share for the activities, and whether there have been significant changes in the activities offered or in its business model?								
2.4.4.4	☐	Does the bank conduct reference checks with external organizations and agencies such as the industry associations, Better Business Bureau, Federal Trade Commission, state attorneys general offices, state consumer affairs offices, and similar foreign authorities?								
2.4.4.5	☐	Does the bank check U.S. Securities and Exchange Commission or other regulatory filings?								
2.4.4.6	☐	Does the bank review the third party's Web sites and other marketing materials to ensure that statements and assertions are in-line with the bank's expectations and do not overstate or misrepresent activities and capabilities?								
2.4.4.7	☐	Does the bank determine whether and how the third party plans to use the bank's name and reputation in marketing efforts?								

#	Check if Yes	Description	Bank Source Docs	Page #	Comments	Raw Rating	Weight	Weighted Rate	Risk Appetite	Result
2.4.5	☐	**Fee Structure and Incentives**								
2.4.5.1	☐	Does the bank evaluate the third party's normal fee structure and incentives for similar business arrangements to determine if the fee structure and incentives would create burdensome upfront fees or *result in inappropriate risk-taking* by the third party or the bank?								
2.4.6	☐	**Qualifications, Backgrounds, and Reputations of Company Principals**								
2.4.6.1	☐	Does the bank ensure the third party periodically conducts thorough background checks on its senior management and employees as well as on subcontractors who may have access to critical systems or confidential information?								
2.4.6.2	☐	Does the bank ensure that third parties have policies and procedures in place for removing employees who do not meet minimum background check requirements?								
2.4.7	☐	**Risk Management**								
2.4.7.1	☐	Does the bank evaluate the *effectiveness* of the third party's risk management program, including policies, processes, and internal controls?								
2.4.7.2	☐	Where applicable, does the bank determine whether the third party's internal audit functions independently and effectively tests and reports on the third party's internal controls?								
2.4.7.3	☐	Does the bank evaluate processes for escalating, remediating, and holding management accountable for concerns identified during audits or other independent tests?								
2.4.7.4	☐	If available, does the bank review Service Organization Control (SOC) reports, prepared in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No.16 (SSAE 16)?								
2.4.7.5	☐	Does the bank consider whether these reports contain sufficient information to assess the third party's risk or whether additional scrutiny is required through an audit by the bank or other third party at the bank's request?								
2.4.7.6	☐	Does the bank consider any certification by independent third parties for compliance with domestic or international internal control standards (e.g., the National Institute of Standards and Technology and the International Standards Organization).								
2.4.8	☐	**Information Security**								
2.4.8.1	☐	Does the bank assesss the third party's information security program?								
2.4.8.2	☐	Does the bank determine whether the third party has sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities?								
2.4.8.3	☐	When technology is necessary to support service delivery, does the bank assess the third party's infrastructure and application security programs, including the software development life cycle and results of vulnerability and penetration tests?			TPISA plus Vulnerability Assessment					
2.4.8.4	☐	Does the bank evaluate the third party's ability to implement effective and sustainable corrective actions to address deficiencies discovered during testing?								
2.4.9	☐	**Management of Information Systems**								
2.4.9.1	☐	Does the bank gain a clear understanding of the third party's business processes and technology that will be used to support the activity?								
2.4.9.2	☐	When technology is a major component of the third-party relationship,does the bank review both the bank's and the third party's information systems to identify gaps in service-level expectations, technology, business process and management, or interoperability issues?								
2.4.9.3	☐	Does the bank review the third party's processes for maintaining accurate inventories of its technology and its subcontractors?								
2.4.9.4	☐	Does the bank assess the third party's change management processes to ensure that clear roles, responsibilities, and segregation of duties are in place?								
2.4.9.5	☐	Does the bank understand the third party's performance metrics for its information systems and ensure they meet the bank's expectations?								

#	Check if Yes	Description	Bank Source Docs	Page #	Comments	Raw Rating	Weight	Weighted Rate	Risk Appetite	Result
2.4.10	☐	**Resilience**								
2.4.10.1	☐	Does the bank assess the third party's ability to respond to service disruptions or degradations resulting from natural disasters, human error, or intentional physical or cyber attacks?								
2.4.10.2	☐	Does the bank determine whether the third party maintains disaster recovery and business continuity plans that specify the time frame to resume activities and recover data?								
2.4.10.3	☐	Does the bank review the third party's telecommunications redundancy and resilience plans and preparations for known and emerging threats and vulnerabilities, such as wide-scale natural disasters, distributed denial of service attacks, or other intentional or unintentional events?								
2.4.10.4	☐	Does the bank review the results of business continuity testing and performance during actual disruptions?								
2.4.11	☐	**Incident-Reporting and Management Programs**								
2.4.11.1	☐	Do the third party's incident reporting and management programs provide clearly documented processes and accountability for identifying, reporting, investigating, and escalating incidents?								
2.4.11.2	☐	Do the third party's escalation and notification processes meet the bank's expectations and regulatory requirements?								
2.4.12	☐	**Physical Security**								
2.4.12.1	☐	Does the third party have sufficient physical and environmental controls to ensure the safety and security of its facilities, technology systems, and employees?								
2.4.13	☐	**Human Resource Management**								
2.4.13.1	☐	Does the bank review the third party's program to train and hold employees accountable for compliance with policies and procedures?								
2.4.13.2	☐	Does the bank review the third party's succession and redundancy planning for key management and support personnel?								
2.4.13.3	☐	Does the bank review training programs to ensure that the third party's staff is knowledgeable about changes in laws, regulations, technology, risk, and other factors that may affect the quality of the activities provided?								
2.4.14	☐	**Reliance on Subcontractors**								
2.4.14.1	☐	Does the bank evaluate the volume and types of subcontracted activities and the subcontractors' geographic locations?								
2.4.14.2	☐	Does the bank evaluate the third party's ability to assess, monitor, and mitigate risks from its use of subcontractors and to ensure that the same level of quality and controls exists no matter where the subcontractors' operations reside?								
2.4.14.3	☐	Does the bank evaluate whether additional concentration-related risks may arise from the third party's reliance on subcontractors and, if necessary, conduct similar due diligence on the third party's critical subcontractors?								
2.4.15	☐	**Insurance Coverage**								
2.4.15.1	☐	Does the bank verify that the third party has fidelity bond coverage to insure against losses attributable to dishonest acts, liability coverage for losses attributable to negligent acts, and hazard insurance covering fire, loss of data, and protection of documents?								
2.4.15.2	☐	Does the bank determine whether the third party has insurance coverage for its intellectual property rights, as such coverage may not be available under a general commercial policy. (Note: The amounts of such coverage should be commensurate with the level of risk involved with the third party's operations and the type of activities to be provided.)								
2.4.16	☐	**Conflicting Contractual Arrangements With Other Parties**								
2.4.16.1	☐	Does the bank obtain information regarding legally binding arrangements with subcontractors or other parties in cases where the third party has indemnified itself, as such arrangements may transfer risks to the bank?								
2.4.16.2	☐	Does the bank evaluate the potential legal and financial implications to the bank of these contracts between the third party and its subcontractors or other parties?								
2.4.16.3	☐	Does senior management review the results of the due diligence to determine whether the third party is able to meet the bank's expectations and whether the bank should proceed with the third-party relationship?								

#	Check if Yes	Description	Bank Source Docs	Page #	Comments	Raw Rating	Weight	Weighted Rate	Risk Appetite	Result
2.4.16.4	☐	If the results do not meet expectations, does management recommend that the third party make appropriate changes, find an alternate third party, conduct the activity in-house, or discontinue the activity?								
2.4.16.5	☐	As part of any recommended changes, does the bank supplement the third party's resources or increase or implement new controls to manage the risks?								
2.4.16.6	☐	Does management present results of due diligence to the board when making recommendations for third-party relationships that involve critical activities?								
3	☐	**Contract Negotiation**								
3.1	☐	Once the bank selects a third party,does management negotiate a contract that clearly specifies the rights and responsibilities of each party to the contract?								
3.1.1	☐	Additionally, when a third-party relationship will involve critical activities, does senior management obtain board approval of the contract before its execution?								
3.1.2	☐	Does the bank review existing contracts periodically, particularly those involving critical activities, to ensure they continue to address pertinent risk controls and legal protections?								
9	☐	Where problems are identified, does the bank seek to renegotiate at the earliest opportunity?								
3.2	☐	**Contracts should generally address the following:**								
3.2.1	☐	**Nature and Scope of Arrangement**								
3.2.1.1	☐	Does the contract specify the nature and scope of the arrangement? For example, a third-party contract should specifically identify the frequency, content, and format of the service, product, or function provided.								
3.2.1.2	☐	Does the contract include, as applicable, such ancillary services as software or other technology support and maintenance, employee training, and customer service?								
3.2.1.3	☐	Does the contract specify which activities the third party is to conduct, whether on or off the bank's premises, and describe the terms governing the use of the bank's information, facilities, personnel, systems, and equipment, as well as access to and use of the bank's or customers' information?								
3.2.1.4	☐	When dual employees will be used, does the contract clearly articulate their responsibilities and reporting lines?[7]								
3.3	☐	**Performance Measures or Benchmarks**								
3.3.1	☐	Does the contract specify performance measures that define the expectations and responsibilities for both parties, including conformance with regulatory standards or rules? (Note: Such measures can be used to motivate the third party's performance, penalize poor performance, or reward outstanding performance.)								
3.3.2	☐	Do performance measures incentivize undesirable performance, such as encouraging processing volume or speed without regard for accuracy, compliance requirements, or adverse effects on customers?								
3.3.3	☐	Industry standards for service-level agreements may provide a reference point for standardized services, such as payroll processing. For more customized activities, there may be no standard measures. Instead, the bank and third party should agree on appropriate measures.								
3.4	☐	**Responsibilities for Providing, Receiving, and Retaining Information**								
3.4.1	☐	Does the bank ensure that the contract requires the third party to provide and retain timely, accurate, and comprehensive information such as records and reports that allow bank management to monitor performance, service levels, and risks?								
3.4.2	☐	Does the contract stipulate the frequency and type of reports required, for example: performance reports, control audits, financial statements, security reports, BSA/AML and Office of Foreign Asset Control (OFAC) compliance responsibilities and reports for monitoring potential suspicious activity, reports for monitoring customer complaint activity, and business resumption testing reports?								

#	Check if Yes	Description	Bank Source Docs	Page #	Comments	Raw Rating	Weight	Weighted Rate	Risk Appetite	Result
3.5	☐	**Does the bank ensure that the contract sufficiently addresses:**								
3.5.1	☐	the responsibilities and methods to address failures to adhere to the agreement including the ability of both parties to the agreement to exit the relationship.								
3.5.2	☐	the prompt notification of financial difficulty, catastrophic events, and significant incidents such as information breaches, data loss, service or system interruptions, compliance lapses, enforcement actions, or other regulatory actions.								
3.5.3	☐	the bank's materiality thresholds and procedures for notifying the bank in writing whenever service disruptions, security breaches, or other events pose a significant risk to the bank.								
3.5.4	☐	notification to the bank before making significant changes to the contracted activities, including acquisition, subcontracting, off-shoring, management or key personnel changes, or implementing new or revised policies, processes, and information technology.								
3.5.5	☐	notification to the bank of significant strategic business changes, such as mergers, acquisitions, joint ventures, divestitures, or other business activities that could affect the activities involved.								
3.5.6	☐	the ability of the third party to resell, assign, or permit access to the bank's data and systems to other entities.								
3.5.7	☐	the bank's obligations to notify the third party if the bank implements strategic or operational changes or experiences significant incidents that may affect the third party.								
3.6	☐	**The Right to Audit and Require Remediation**								
3.6.1	☐	Does the bank ensure that the contract establishes the bank's right to audit, monitor performance, and require remediation when issues are identified?								
3.6.2	☐	Does the third-party contract include provisions for periodic independent internal or external audits of the third party, and relevant subcontractors, at intervals and scopes consistent with the bank's in-house functions to monitor performance with the contract?								
3.6.3	☐	Does the contract include the types and frequency of audit reports the bank is entitled to receive from the third party (e.g., financial, SSAE 16, SOC 1, SOC 2, and SOC 3 reports, and security reviews)? (Note: The bank should consider whether to accept audits conducted by the third party's internal or external auditors and reserve the bank's right to conduct its own audits of the third party's activities or to engage an independent party to perform such audits. Audit reports should include a review of the third party's risk management and internal control environment as it relates to the activities involved and of the third party's information security program and disaster recovery and business continuity plans.)								
3.7	☐	**Responsibility for Compliance With Applicable Laws and Regulations**								
3.7.1	☐	Does the bank ensure the contract addresses compliance with the specific laws, regulations, guidance, and self-regulatory standards applicable to the activities involved, including provisions that outline compliance with certain provisions of the Gramm-Leach-Bliley Act (GLBA) (including privacy and safeguarding of customer information); BSA/AML; OFAC; and Fair Lending and other consumer protection laws and regulations.								
3.7.2	☐	Does the bank ensure that the contract requires the third party to maintain policies and procedures which address the bank's right to conduct periodic reviews so as to verify the third party's compliance with the bank's policies and expectations.								
3.7.3	☐	Does the bank ensure that the contract states the bank has the right to monitor on an ongoing basis the third party's compliance with applicable laws, regulations, and policies and require remediation if issues arise.								
3.8	☐	**Cost and Compensation**								
3.8.1	☐	Does the contract fully describe compensation, fees, and calculations for base services, as well as any fees based on volume of activity and for special requests?								
3.8.2	☐	Does the bank ensure the contracts do not include burdensome upfront fees or incentives that could result in inappropriate risk taking by the bank or third party.								
3.8.3	☐	Does the contract indicate which party is responsible for payment of legal, audit, and examination fees associated with the activities involved?								
3.8.4	☐	Does the contract outline the cost and responsibility for purchasing and maintaining hardware and software? (If not, the bank may want to consider adding it.)								
3.8.5	☐	Does the contract specify the conditions under which the cost structure may be changed, including limits on any cost increases?								

#	Check if Yes	Description	Bank Source Docs	Page #	Comments	Raw Rating	Weight	Weighted Rate	Risk Appetite	Result
3.9	☐	**Ownership and License**								
3.9.1	☐	Does the contract state whether and how the third party has the right to use the bank's information, technology, and intellectual property, such as the bank's name, logo, trademark, and copyrighted material?								
3.9.2	☐	Does the contract indicate whether any records generated by the third party become the bank's property?								
3.9.3	☐	Does the contract include appropriate warranties on the part of the third party related to its acquisition of licenses for use of any intellectual property developed by other third parties?								
3.9.4	☐	If the bank purchases software, does the contract establish escrow agreements to provide for the bank's access to source code and programs under certain conditions (e.g., insolvency of the third party)?								
3.10	☐	**Confidentiality and Integrity**								
3.10.1	☐	Does the contract prohibit the third party and its subcontractors from using or disclosing the bank's information, except as necessary to provide the contracted activities or comply with legal requirements?								
3.10.2	☐	If the third party receives bank customers' personally identifiable information, does the contract ensure that the third party implements and maintains appropriate security measures to comply with privacy regulations and regulatory guidelines?								
3.10.3	☐	Does the contract specify when and how the third party will disclose, in a timely manner, information security breaches that have resulted in unauthorized intrusions or access that may materially affect the bank or its customers?								
3.10.4	☐	Does the contract prohibit the third party and its subcontractors from using or disclosing the bank's information, except as necessary to provide the contracted activities or comply with legal requirements? (same as 3.10.1)								
3.10.5	☐	Does the contract address the powers of each party to change security and risk management procedures and requirements, and resolve any confidentiality and integrity issues arising out of shared use of facilities owned by the third party?								
3.10.6	☐	Does the contract stipulate that intrusion notifications include estimates of the effects on the bank and specify corrective action to be taken by the third party?								
3.10.7	☐	Does the contract stipulate whether and how often the bank and the third party will jointly practice incident management plans involving unauthorized intrusions or other breaches in confidentiality and integrity?								
3.11	☐	**Business Resumption and Contingency Plans**								
3.11.1	☐	Does the bank ensure the contract provides for continuation of the business (COB) function in the event of problems affecting the third party's operations, including degradations or interruptions resulting from natural disasters, human error, or intentional attacks?								
3.11.2	☐	Does the bank ensure that the contract requires the third party to provide the bank with operating procedures to be carried out in the event business resumption and disaster recovery plans are implemented?								
3.11.3	☐	Does the contract include specific time frames for business resumption and recovery that meet the bank's requirements, and when appropriate, regulatory requirements?								
3.11.4	☐	Does the contract stipulate whether and how often the bank and the third party will jointly practice business resumption and disaster recovery plans?								
3.12	☐	**Indemnification**								
3.12.1	☐	Does the contract include indemnification clauses that specify the extent to which the bank will be held liable for claims that cite failure of the third party to perform, including failure of the third party to obtain any necessary intellectual property licenses? (If not, the bank may wish to consider adding it.)								
3.12.2	☐	Does the contract include indemnification clauses that require the bank to hold the third party harmless from liability? (If so, has the bank carefully assessed those?)								

#	Check if Yes	Description	Bank Source Docs	Page #	Comments	Raw Rating	Weight	Weighted Rate	Risk Appetite	Result
3.13	☐	**Insurance**								
3.13.1	☐	Does the contract stipulate that the third party is required to maintain adequate insurance, notify the bank of material changes to coverage, and provide evidence of coverage where appropriate? (Note: Types of insurance coverage may include fidelity bond coverage, liability coverage, hazard insurance, and intellectual property insurance.)								
3.14	☐	**Dispute Resolution**								
3.14.1	☐	Does the contract establish a dispute resolution process (arbitration, mediation, or other means) to resolve problems between the bank and the third party in an expeditious manner? (If note, the bank may wish to consider it.)								
3.14.2	☐	Does the contract establish whether the third party should continue to provide activities to the bank during the dispute resolution period?								
3.15	☐	**Limits on Liability**								
3.15.1	☐	Does the contract limit the third party's liability and, if so, is the proposed limit in proportion to the amount of loss the bank might experience because of the third party's failure to perform or to comply with applicable laws?								
3.15.2	☐	Would the contract subject the bank to undue risk of litigation, particularly if the third party violates or is accused of violating intellectual property rights?								
3.16	☐	**Default and Termination**								
3.16.1	☐	Does the bank ensure that the contract stipulates what constitutes default, identifies remedies and allows opportunities to cure defaults, and stipulates the circumstances and responsibilities for termination?								
3.16.2	☐	Does the contract include a provision that enables the bank to terminate the contract, upon reasonable notice and without penalty, in the event that the OCC formally directs the bank to terminate the relationship?								
3.16.3	☐	Does the bank ensure the contract permits the bank to terminate the relationship in a timely manner without prohibitive expense?								
3.16.4	☐	Does the contract include termination and notification requirements with time frames to allow for the orderly conversion to another third party?								
3.16.5	☐	Does the contract provide for the timely return or destruction of the bank's data and other resources and ensure the contract provides for ongoing monitoring of the third party after the contract terms are satisfied as necessary?								
3.16.6	☐	Does the contract clearly assign all costs and obligations associated with transition and termination?								
3.17	☐	**Customer Complaints**								
3.17.1	☐	Does the contract specify whether the bank or third party is responsible for responding to customer complaints?								
3.17.2	☐	If it is the third party's responsibility, does the contract specify provisions that ensure that the third party receives and responds timely to customer complaints and forwards a copy of each complaint and response to the bank?								
3.17.3	☐	Does the contract specify that the third party should submit sufficient, timely, and usable information to enable the bank to analyze customer complaint activity and trends for risk management purposes?								
3.18	☐	**Subcontracting**								
3.18.1	☐	Does the contract stipulate when and how the third party should notify the bank of its intent to use a subcontractor?								
3.18.2	☐	Does the contract specify the activities that cannot be subcontracted or whether the bank prohibits the third party from subcontracting activities to certain locations or specific subcontractors?								
3.18.3	☐	Does the contract detail the contractual obligations—such as reporting on the subcontractor's conformance with performance measures, periodic audit results, compliance with laws and regulations, and other contractual obligations?								
3.18.4	☐	Does the contract state the third party's liability for activities or actions by its subcontractors and which party is responsible for the costs and resources required for any additional monitoring and management of the subcontractors?								

#	Check if Yes	Description	Bank Source Docs	Page #	Comments	Raw Rating	Weight	Weighted Rate	Risk Appetite	Result
3.18.5	☐	Does the contract reserve the right to terminate the contract without penalty if the third party's subcontracting arrangements do not comply with the terms of the contract?								
3.19	☐	**Foreign-Based Third Parties**								
3.19.1	☐	Do contracts with foreign-based third parties include choice-of-law covenants and jurisdictional covenants that provide for adjudication of all disputes between the parties under the laws of a single, specific jurisdiction?								
3.20	☐	**OCC Supervision**								
3.20.1	☐	Do contracts with service providers stipulate that the performance of activities by external parties for the bank is subject to OCC examination oversight, including access to all work papers, drafts, and other materials? (Note: The OCC treats as subject to 12 USC 1867(c) and 12 USC 1464(d)(7), situations in which a bank arranges, by contract or otherwise, for the performance of any applicable functions of its operations. Therefore, the OCC generally has the authority to examine and to regulate the functions or operations performed or provided by third parties to the same extent as if they were performed by the bank itself on its own premises.[8])								
4	☐	**Ongoing Monitoring**								
4.1	☐	Ongoing monitoring for the duration of the third-party relationship is an essential component of the bank's risk management process. More comprehensive monitoring is necessary when the third-party relationship involves critical activities. Does senior management periodically assess existing third-party relationships to determine whether the nature of the activity performed now constitutes a critical activity?								
4.2	☐	After entering into a contract with a third party, does bank management dedicate sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the third party commensurate with the level of risk and complexity of the relationship?								
4.3	☐	Does bank make regular on site visits to understand fully the third party's operations and ongoing ability to meet contract requirements?								
4.4	☐	Does management ensure that bank employees that directly manage third-party relationships monitor the third party's activities and performance?								
4.5	☐	Does the bank pay particular attention to the quality and sustainability of the third party's controls, and its ability to meet service-level agreements, performance metrics and other contractual terms, and to comply with legal and regulatory requirements?								
4.6		The OCC expects the bank's ongoing monitoring of third-party relationships to cover the due diligence activities discussed earlier. Because both the level and types of risks may change over the lifetime of third-party relationships, a bank should ensure that its ongoing monitoring adapts accordingly. This monitoring may result in changes to the frequency and types of required reports from the third party, including service-level agreement performance reports, audit reports, and control testing results. **In addition to ongoing review of third-party reports, some key areas of consideration for ongoing monitoring may include assessing changes to the third party's:**								
4.6.1	☐	business strategy (including acquisitions, divestitures, joint ventures) and reputation (including litigation) that may pose conflicting interests and impact its ability to meet contractual obligations and service-level agreements.	PR	2.5.6 & 2.5.7 (only for Critical, Very High Risk & Core OSP BSRs)	List should be expanded to match 1.6.1					
4.6.2	☐	compliance with legal and regulatory requirements.								
4.6.3	☐	financial condition.								
4.6.4	☐	insurance coverage.								
4.6.5	☐	key personnel and ability to retain essential knowledge in support of the activities.								
4.6.6	☐	ability to effectively manage risk by identifying and addressing issues before they are cited in audit reports.								
4.6.7	☐	process for adjusting policies, procedures, and controls in response to changing threats and new vulnerabilities and material breaches or other serious incidents.								
4.6.8	☐	information technology used or the management of information systems.								
4.6.9	☐	ability to respond to and recover from service disruptions or degradations and meet business resilience expectations.								
4.6.10	☐	reliance on, exposure to, or performance of subcontractors; location of subcontractors; and the ongoing monitoring and control testing of subcontractors.								
4.6.11	☐	agreements with other entities that may pose a conflict of interest or introduce reputation, operational, or other risks to the bank.								

#	Check if Yes	Description	Bank Source Docs	Page #	Comments	Raw Rating	Weight	Weighted Rate	Risk Appetite	Result
4.6.12	☐	ability to maintain the confidentiality and integrity of the bank's information and systems.								
4.6.13	☐	volume, nature, and trends of consumer complaints, in particular those that indicate compliance or risk management problems.								
4.6.14	☐	ability to appropriately remediate customer complaints.								
4.7	☐	Do bank employees who directly manage third-party relationships escalate to senior management significant issues or concerns arising from ongoing monitoring, such as an increase in risk, material weaknesses and repeat audit findings, deterioration in financial condition, security breaches, data loss, service or system interruptions, or compliance lapses?								
4.7.1	☐	Additionally, does management ensure that the bank's controls to manage risks from third-party relationships are tested regularly, particularly where critical activities are involved?								
4.7.2	☐	Based on the results of the ongoing monitoring and internal control testing, does management respond to issues when identified, including escalating significant issues to the board?								
5	☐	**Termination**								
5.1	☐	A bank may terminate third-party relationships for various reasons, including:	Exit Strategy							
5.1.1		expiration or satisfaction of the contract.								
5.1.2		desire to seek an alternate third party.								
5.1.3		desire to bring the activity in-house or discontinue the activity.								
5.1.4		breach of contract.								
5.2	☐	Does management ensure that relationships terminate in an efficient manner, whether the activities are transitioned to another third party or in-house, or discontinued?	Exit Strategy		Citi's Exit Strategy should be revised to include all of these points, including appropriate training.					
5.3	☐	In the event of contract default or termination, does the bank have a plan to bring the service in-house if there are no alternate third parties?	Exit Strategy							
5.4	☐	**Does the bank's termination plan cover the following:**								
5.4.1	☐	capabilities, resources, and the time frame required to transition the activity while still managing legal, regulatory, customer, and other impacts that might arise?								
5.4.2	☐	risks associated with data retention and destruction, information system connections and access control issues, or other control concerns that require additional risk management and monitoring during and after the end of the third-party relationship?								
5.4.3	☐	handling of joint intellectual property developed during the course of the arrangement?								
5.4.4	☐	reputation risks to the bank if the termination happens as a result of the third party's inability to meet expectations?	Exit Strategy							
5.4.5	☐	The extent and flexibility of termination rights may vary with the type of activity.								
6	Acknow-ledge	**Oversight and Accountability**								
6.1	☐	The bank's board of directors (or a board committee) and senior management are responsible for overseeing the bank's overall risk management processes. The board, senior management, and employees within the lines of businesses who manage the third-party relationships have distinct but interrelated responsibilities to ensure that the relationships and activities are managed effectively and commensurate with their level of risk and complexity, particularly for relationships that involve critical activities:[9]								

#	Check if Yes	Description	Bank Source Docs	Page #	Comments	Raw Rating	Weight	Weighted Rate	Risk Appetite	Result
7	☐	**Board of Directors**								
7.1	☐	Does the board ensure an effective process is in place to manage risks related to third-party relationships in a manner consistent with the bank's strategic goals, organizational objectives, and risk appetite?								
7.2	☐	Does the board approve the bank's risk-based policies that govern the third-party risk management process and identify critical activities?								
7.3	☐	Does the board review and approve management plans for using third parties that involve critical activities?								
7.4	☐	Does the board review summary of due diligence results and management's recommendations to use third parties that involve critical activities?								
7.5	☐	Does the board approve contracts with third parties that involve critical activities?								
7.6	☐	Does the board review the results of management's ongoing monitoring of third-party relationships involving critical activities?								
7.7	☐	Does the board ensure management takes appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring?								
7.8	☐	Does the board review results of periodic independent reviews of the bank's third-party risk management process?								
8	☐	**Senior Bank Management**								
8.1	☐	Does senior management develop and implement the bank's third-party risk management process?								
8.2	☐	Does senior management establish the bank's risk-based policies to govern the third-party risk management process?								
8.3	☐	Does senior management develop plans for engaging third parties, identify those that involve critical activities, and present plans to the board when critical activities are involved?								
8.4	☐	Does senior management ensure appropriate due diligence is conducted on potential third parties and present results to the board when making recommendations to use third parties that involve critical activities?								
8.5	☐	Does senior management review and approve contracts with third parties? Board approval should be obtained for contracts that involve critical activities.								
8.6	☐	Does senior management ensure ongoing monitoring of third parties, respond to issues when identified, and escalate significant issues to the board?								
8.7	☐	Does senior management ensure appropriate documentation and reporting throughout the life cycle for all third-party relationships?								
8.8	☐	Does senior management ensure periodic independent reviews of third-party relationships that involve critical activities and of the bank's third-party risk management process?								
8.9	☐	And does senior management analyze the results, take appropriate actions, and report results to the board?								
8.10	☐	Does senior management hold accountable the bank employees within business lines or functions who manage direct relationships with third parties?								
8.11	☐	Does senior management terminate arrangements with third parties that do not meet expectations or no longer align with the bank's strategic goals, objectives, or risk appetite?								
8.12	☐	Does senior management oversee enterprise-wide risk management and reporting of third-party relationships?								

#	Check if Yes	Description	Bank Source Docs	Page #	Comments	Raw Rating	Weight	Weighted Rate	Risk Appetite	Result
9	☐	**Bank Employees Who Directly Manage Third-Party Relationships (BSRMs)** (Note: include all of these items in BSRM Job Description revision)								
9.1	☐	Conduct due diligence of third parties and report results to senior management?								
9.2	☐	Ensure that third parties comply with the bank's policies and reporting requirements?								
9.3	☐	Perform ongoing monitoring of third parties and ensure compliance with contract terms and service-level agreements?								
9.4	☐	Ensure the bank or the third party addresses any issues identified?								
9.5	☐	Escalate significant issues to senior management?								
9.6	☐	Notify the third party of significant operational issues at the bank that may affect the third party?								
9.7	☐	Ensure that the bank has regularly tested controls in place to manage risks associated with third-party relationships?								
9.8	☐	Ensure that third parties regularly test and implement agreed-upon remediation when issues arise?								
9.9	☐	Maintain appropriate documentation throughout the life cycle?								
9.1	☐	Respond to material weaknesses identified by independent reviews?								
9.11	☐	Recommend termination of arrangements with third parties that do not meet expectations or no longer align with the bank's strategic goals, objectives, or risk appetite?								
10	Acknow-ledge	**Documentation and Reporting**								
10.1	☐	A bank should properly document and report on its third-party risk management process and specific arrangements throughout their life cycle. Proper documentation and reporting facilitates the accountability, monitoring, and risk management associated with third parties.								
10.2		**Does the bank's third party documentation and reporting include:**								
10.2.1	☐	a current inventory of all third-party relationships, which should clearly identify those relationships that involve critical activities and delineate the risks posed by those relationships across the bank?10			Citi had a real challenge identifying all of its BSRs, including Criticals.					
10.2.2	☐	approved plans for the use of third-party relationships?								
10.2.3	☐	due diligence results, findings, and recommendations?								
10.2.4	☐	analysis of costs associated with each activity or third-party relationship, including any indirect costs assumed by the bank?								
10.2.5	☐	executed contracts?			It was difficult at Citi to identify active contracts, SOWs, and Pos.					
10.2.6	☐	regular risk management and performance reports required and received from the third party (e.g., audit reports, security reviews, and reports indicating compliance with service-level agreements)?			BSRMs sometimes requested TP reports but it seemed to be rare, with the exception of Heidi and Jody.					
10.2.7	☐	regular reports to the board and senior management on the results of internal control testing and ongoing monitoring of third parties involved in critical activities?			MCAs may be Citi's response to this.					
10.2.8	☐	regular reports to the board and senior management on the results of independent reviews of the bank's overall risk management process?								
11	☐	**Independent Reviews**								
11.1	☐	Does senior management ensure that periodic independent reviews are conducted on the third-party risk management process, particularly when a bank involves third parties in critical activities?								
11.2	☐	Does the bank's internal auditor or an independent third party perform the reviews, and does senior management ensure the results are reported to the board?								
11.3		**Do the reviews assess the adequacy of the bank's process for:**								
11.3.1	☐	ensuring third-party relationships align with the bank's business strategy?								
11.3.2	☐	identifying, assessing, managing, and reporting on risks of third-party relationships?								

#	Check if Yes	Description	Bank Source Docs	Page #	Comments	Raw Rating	Weight	Weighted Rate	Risk Appetite	Result
11.3.3	☐	responding to material breaches, service disruptions, or other material issues?								
11.3.4	☐	identifying and managing risks associated with complex third-party relationships, including foreign-based third parties and subcontractors?								
11.3.5	☐	involving multiple disciplines across the bank as appropriate during each phase of the third-party risk management life cycle?11								
11.3.6	☐	ensuring appropriate staffing and expertise to perform due diligence and ongoing monitoring and management of third parties?								
11.3.7	☐	ensuring oversight and accountability for managing third-party relationships (e.g., whether roles and responsibilities are clearly defined and assigned and whether the individuals possess the requisite expertise, resources, and authority)?			Citi failed in this objective. BSRMs had neither the expertise, training, nor time to do what was required of them.					
11.3.8	☐	ensuring that conflicts of interest or appearances of conflicts of interest do not exist when selecting or overseeing third parties?								
11.3.9	☐	identifying and managing concentration risks that may arise from relying on a single third party for multiple activities, or from geographic concentration of business due to either direct contracting or subcontracting agreements to the same locations?								
11.3.10	☐	Does senior management analyze the results of independent reviews to determine whether and how to adjust the bank's third-party risk management process, including policy, reporting, resources, expertise, and controls?			Citi apparently does this, but reacts ineffectively.					
11.4	☐	Does senior management use the results to better understand the effectiveness of the bank's third-party risk management process so that they can make informed decisions about commencing new or continuing existing third-party relationships, bringing activities in-house, or discontinuing activities?			They try but are unsuccessful.					
11.5	☐	Does management respond promptly and thoroughly to significant issues or concerns identified and escalate to the board if the risk posed is approaching the bank's risk appetite limits?								
12	Acknow-ledge	**Supervisory Reviews of Third-Party Relationships**								
12.1	☐	The OCC expects bank management to engage in a robust analytical process to identify, measure, monitor, and control the risks associated with third-party relationships and to avoid excessive risk taking that may threaten a bank's safety and soundness. **A bank's failure to have an *effective* third-party risk management process that is commensurate with the level of risk, complexity of third-party relationships, and organizational structure of the bank may be an unsafe and unsound banking practice**.								
12.2	Acknow-ledge	**When reviewing third-party relationships, examiners will:**								
12.2.1	☐	assess the bank's ability to oversee and manage its relationships.			Citi's ability to manage was deemed unsatisfactory.					
12.2.2	☐	highlight and discuss material risks and any deficiencies in the bank's risk management process with the board of directors and senior management.								
12.2.3	☐	carefully review the bank's plans for appropriate and sustainable remediation of such deficiencies, particularly those associated with the oversight of third parties that involve critical activities.								
12.2.4	☐	follow existing guidance for citing deficiencies in supervisory findings and reports of examination, and recommend appropriate supervisory actions. These actions may range from citing the deficiencies in Matters Requiring Attention (MRAs) to recommending formal enforcement action.								
12.2.5	☐	consider the findings when assigning the management component of the Federal Financial Institutions Examination Council's (FFIEC) Uniform Financial Institutions Rating System **(CAMELS ratings)**.12 Serious deficiencies may result in *management* being deemed less than satisfactory.								
12.2.6	☐	reflect the associated risks in their overall assessment of the bank's risk profile.								
12.3	☐	Acknowledge: When circumstances warrant, the OCC may use its authority to examine the functions or operations performed by a third party on the bank's behalf. Such examinations may evaluate safety and soundness risks, the financial and operational viability of the third party to fulfill its contractual obligations, compliance with applicable laws and regulations, including consumer protection, fair lending, BSA/AML and OFAC laws, and whether the third party engages in unfair or deceptive acts or practices in violation of federal or applicable state law. The OCC will pursue appropriate corrective measures, including enforcement actions, to address violations of law and regulations or unsafe or unsound banking practices by the bank or its third party. The OCC has the authority to assess a bank a special examination or investigation fee when the OCC examines or investigates the activities of a third party for the bank.								
Centurion Name			**Review Date**			**Rating**				