**Vendor Contract Terms and Conditions Considerations**

There are many reasons for a written contract. The basic premise is to establish who does what, what restrictions there are on the two parties and what happens if a party fails to do what was agreed. The requirements of each party and the counter- party’s commitments should be clearly documented, as well as what successful fulfilment looks like. Outcomes and deliverables should be objective and measurable, with no grey areas or issues to be decided later. Once a contract is signed, there should be no surprises- today, during the term of the contract, and if/when we decide to terminate the contract. Remember*: if it is not included in the contract, it will be difficult to enforce*. Additionally, a vendor may be providing a contract that is in their best interest, not always in ours- review it carefully. Words matter!

Contracts with a vendor where the relationship is more complex, or the vendor risk score is Medium, or High may need to include all the categories listed below. For less complex relationships or vendors with a No or Low risk scores, all the following categories may not need to be included in the contract but should at least be part of your discussion with the vendor, before signing the contract, so all parties understand what is expected from the relationship.

Additionally, you will see several references to the vendor’s subcontractors (i.e., fourth party vendors). The issue here is if these vendors have significant impact on our vendor’s ability to provide services to us, we need to make sure the contract outlines the vendor responsibilities regarding these relationships throughout the contract. To determine if a vendor falls under this category, first determine if we consider this vendor to be critical to our business, and/or do they have a material impact on our business and/or do they host sensitive data (generally NPI)? If yes, does this vendor rely on any vendors/subcontractors to support the services to us and/or share our data with another organization? If yes, then we must make sure those relationships are addressed and included throughout the vendor contract.

Make sure you are clear on the effective date and how that pertains to contract termination. Sometimes the “effective date” is the date we first start using the service, or the first day of the month we start using the service, etc. and not the date the contract is signed. This may be a critical distinction. You will note this date in the Vendor Summary & Score tab within the vendor program document.

**The address for XXXX Bank should always be: XXXXXXXXXXXXXXXXXX, as this is our legal address.**

[ ]  **NATURE AND SCOPE**

**☐** Ensure that the term, including the commencement and expiration dates, are clearly defined.

**☐** Ensure the rights and responsibilities of both parties to the contract are clearly described.

**☐** The specific services that will be provided by the Vendor, including whether on or off the bank’s premises, i.e., physical location/s, 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 customer’s information.

**☐** If the vendor is a significant vendor, as outlined above, ensure the following language is incorporated in the contract: *Vendor represents and warrants that to the extent subcontractors or agents are used to perform the obligations under this Agreement, Vendor shall be liable for the performance and all actions and inactions by such subcontractors or agents to the same extent that Vendor would be responsible under the terms of this Agreement for such performance as if it had been Vendor’s own performance, including, but not limited to intellectual property rights, infringement and breaches of confidentiality.*

[ ]  **PERFORMANCE MEASURES**

[ ] Detail how performance will be measured. Specify performance measures that define the expectations and responsibilities for both parties including conformance with regulatory standards or rules.

[ ] Include penalties for unmet service level agreements (SLAs).

[ ]  **RESPONSIBILITIES FOR PROVIDING, RECEIVING AND RETAINING INFORMATION**

[ ] Make sure the contract requires the vendor to provide and retain timely, accurate and comprehensive information such as records and reports that allow the bank to monitor performance, service levels, and risks as well as the frequency of these reports and the type of reports.

[ ] Notification to the bank prior to making significant changes to the contracted activities, including acquisition, subcontracting, offshoring, management, or key personnel changes, or implementing new or revised policies, processes, and information technology.

[ ] The bank’s obligations to notify the vendor if the bank implements strategic or operational changes or experiences significant incidents that may affect the vendor.

[ ]  **THE RIGHT TO AUDIT AND REQUIRE REMEDIATION**

**☐** The contract should include the Bank’s right to audit and monitor performance annually, both onsite or offsite, and require remediation when issues are identified.

**☐** Ensure the contract includes a requirement for the vendor to permit annual independent audits, regulatory examinations, and provide all requested compliance reports and information at the Institution’s request at no cost, including the vendor’s response to relevant regulations, supervisory guidance, or other notices published by federal agencies and available audit reports addressing the vendor’s resiliency capabilities and interdependencies, BCP testing, and remediation efforts.

[ ] Generally, a third-party contract should include provisions for periodic independent internal or external audits of the vendor, and relevant subcontractors, at intervals and scopes consistent with the bank’s in-house functions to monitor performance with the contract. The contract should agree to provide the Bank with vendor audits/reviews (i.e., financials, SSAE 16, SOC 1, SOC 2 reports and security reviews) at no charge.

**☐** If the vendor has significant vendors, as outlined in the opening paragraphs of this document, then the contract must also stipulate our right to audit those significant subcontracts, as well.

[ ]  **RESPONSIBILITY FOR COMPLIANCE WITH APPLICABLE LAWS AND REGULATION**

[ ] The contract should address 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 GLBA, BSA/AML, OFAC, CAN- SPAM Act, and Fair Lending or any other consumer protection laws and regulations.

[ ] Ensure the vendor provides performance reports, control audits, financial statements, and security and business resumption testing reports as needed, including the guidelines and fees for obtaining such reports.

[ ] Ensure that the contract requires the vendor to maintain policies and procedures which address the bank’s right to conduct periodic reviews to verify the vendor’s compliance with the bank’s policies and expectations, ensuring that the contract states the bank has the right to monitor on an ongoing basis the vendor’s compliance with applicable laws, regulations, and policies and requires remediation if issues arise. This includes onsite audits, as appropriate.

[ ] Make sure the contract includes notification timelines to the bank for internal negative compliance events and subsequent timely program/system modifications.

[ ]  **COST AND COMPENSATION**

[ ] Cost and compensation details should be spelled out in the contract, including but not limited to, upfront set up fees, legal, audit and examination fees, and fees for purchasing and maintaining hardware and software. Specify the conditions under which the cost structure may be changed. Always include limits/caps on any cost increases.

[ ] Be cautious of excessive up-front fees due and payable before we start using the product/service.

[ ]  **OWNERSHIP AND LICENSE**

[ ] The contract should state whether and how the vendor has the right to use the bank’s information, technology, and intellectual property, such as the bank’s name, logo, trademark, and copyrighted material.

[ ] The contract should state whether any records generated by the vendor become the bank’s property. Include appropriate warranties on the part of the vendor related to its acquisition of licenses for use of any intellectual property developed by other third parties. If the bank purchases software, establish escrow agreements to provide for the bank’s access to source code and program under certain conditions (i.e., insolvency of the vendor).

[ ] In a servicing relationship, the contract should stipulate who owns the servicing rights.

**☐** Beware of exclusivity clauses where the vendor states we can only use them or their services for like services. This type of clause could prevent us from implementing a new, best- in- class product.

[ ] If the contract is for marketing content, ensure the contract is written in a way to unequivocally identify XXXXX Bank as the owner of all content so upon contract termination the content remains with XXXXX Bank.

[ ]  **RETURN OF INFORMATION**

[ ] The contract should stipulate the vendor and *any subcontractors or outsource partners* will, during and after the term of the contract, promptly return all Confidential Information held or used by the vendor in whatever form, or at our discretion, promptly destroy, or otherwise permanently delete, all Confidential Information, including all copies and/or residual data. They must also provide a Certificate of Destruction. Suggested wording: *Vendor shall, and shall instruct all authorized users, to destroy all copies, whether in written, electronic or other form or media, all confidential information in its possession or the possession of such authorized users within 30 days following termination of this Agreement and will provide a Certificate of Destruction within 30 days.*

[ ] Notwithstanding the foregoing data destruction provisions, the vendor may not be obligated to return Confidential Information that is required for archival, regulatory, or audit purposes or contained in an archived computer system backup made in accordance with the vendor’s security or disaster recovery procedures provided the retained. Confidential Information will remain subject to the terms and conditions of this Agreement until it is destroyed or deleted. When that retention period expires, the vendor must provide a Certificate of Destruction.

[ ]  **CONFIDENTIALITY AND INTEGRITY**

[ ] The terms of the contract must prohibit the vendor and its subcontractors from using or disclosing the bank’s information, except as necessary to provide the contracted services or to comply with legal requirements when providing these services.

[ ] If the vendor and subcontractors have access to the bank’s customer personally identifiable information, the contract should ensure that the vendor implements and maintains effective minimum industry standards for security and communications to comply with privacy regulations and regulatory guidelines as well as handling expectations (availability, transport methods, backup requirements, etc.) during and after the relationship is terminated.

**☐** If the vendor has access to the bank’s customer personally identifiable information, the contract should stipulate that we must be notified, ***in advance***, if they add any vendors who will also have access to this information. Suggested wording: *Neither party shall have the right to assign or subcontract any of its obligations or duties under this agreement without the prior written consent of the other party, which consent shall not be unreasonably withheld or delayed.*

[ ] The contract should specify the vendor’s responsibility to maintain effective minimum industry standards for security and communications.

[ ] Ensure the vendor will disclose to the Institution if Cloud services are used for the storage or transmission of customer non-public personal information.

[ ] Use caution if the vendor includes language indicating we can only use their services and no other vendors for like services. The vendor may be agreeing to future services they end up unable to provide, or their level of service for one component of the services they provide does not keep up with industry standards. An exclusivity clause would make it difficult for us to offer the level of service that is best for us.

[ ]  **BUSINESS RESUMPTION AND CONTINGENCY PLANS**

[ ] Ensure that the contract provides for continuation of the business function in the event of problems affecting the vendor’s operations, including degradations or interruptions resulting from natural disasters, human error, or intentional attacks, including but not limited to cybersecurity incidents. This also includes subcontractor deficiencies where the subcontractor’s services are critical to the vendor’s operations.

[ ] Stipulate the vendor’s responsibility for backing up and otherwise protecting programs, data, and equipment, and for maintaining current and sound business resumption and contingency plans, for themselves and their subcontractors where that subcontractor is critical to the vendor’s operations and/or that vendor has access to our customers’ non -public information. Include provisions (in the event of the vendor’s or subcontractor’s bankruptcy, business failure, or business interruption) for transferring the bank’s accounts or activities to another vendor without penalty. Additionally, the contract should include operating procedures to be carried out in the event business resumption and disaster recovery plans are implemented.

[ ] The bank’s materiality thresholds, including specific time frames for resumption and recovery, and procedures for notifying the bank in writing whenever service disruptions, security breaches, or other events pose a risk to the bank. 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. Intrusion notifications should include estimates of the effects on the bank and specify corrective action to be taken by the vendor 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 vendor.

[ ] Stipulate the vendor will practice annual BCP testing as well as incident management involving unauthorized intrusions or other breaches in confidentiality and integrity and the frequency at which the Bank will jointly participate in these tests.

[ ]  **INDEMNIFICATION**

[ ] Consider including Indemnification language that specifies the extent to which the bank will be held liable for claims that cite failure on the part of the vendor to perform, including failure of the vendor to obtain necessary intellectual property licenses, being careful to assess indemnification clauses that require the bank to hold the vendor harmless from liability.

[ ]  **INSURANCE**

[ ] The contract should stipulate that the vendor is required to maintain adequate insurance, notify the bank of material changes to coverage and to provide the bank with proper evidence of coverage. This is to be provided ANNUALLY for any Medium or High-risk vendors.

[ ] Types of insurance coverage may include fidelity bond coverage, liability coverage, cyber insurance, hazard insurance and intellectual property insurance. The amount of “adequate” coverage will vary based on the type and criticality of service provided by the vendor.

[ ]  Review deductible amounts for any required insurance to ensure this amount is within the means of the business to cover, including if there are multiple simultaneous events which would require the vendor to cover all at one time. Consider having the vendor attest, in writing, that it possesses the necessary amount of unencumbered liquid assets to finance its responsibilities for losses within the deductible.

[ ] All types of insurance, but especially Cyber insurance coverage, must be adequate to cover multiple clients; $1MM per incident will not be enough. All vendors who access, process, transfer or store data should have a baseline $5MM cyber security policy.

[ ]  **DISPUTE RESOLUTION**

[ ] The contract should establish a dispute resolution process to resolve problems between the bank and the vendor in an expeditious manner, and whether the vendor should continue to provide activities to the bank and whether recurring fees will temporarily cease during the dispute resolution period.

[ ] 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.

[ ] Review each party’s right to modify, re-negotiate, and/or change the contract.

[ ]  **LIMITS ON LIABILITY**

[ ] Determine whether the contract places a limit on the vendor’s liability. If it does, is the proposed limit in proportion to the loss the bank could expect to experience in the event of a failure by the vendor to perform or comply with applicable laws, i.e., compensation to the Bank should be commensurate with the vendor risk level. Consider requesting at least one year of fees for Medium and High-risk vendors.

[ ] Determine whether a contract would subject the Bank to undue risk of litigation, particularly if the vendor violates or is accused of violating intellectual property rights.

[ ]  **DEFAULT AND TERMINATION**

[ ] Review right to terminate without cause, right to terminate for cause, and costs for early termination.

[ ] The contract should define what constitutes a default, identify remedies, and allow for opportunities to cure defaults and stipulate the circumstances and responsibilities for termination in the event of an uncured default.

[ ] 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. It should also include an opt-out option without penalties to us, should this venture be contrary to our values or risk-assessments, etc.

[ ] The ability of the vendor to resell, assign, or permit access to the bank’s data and systems to other entities.

[ ] Termination notice timeframe should be commensurate with the criticality and complexity of the service. This timeframe could be 6 months, but 60 days may be better.

[x] Ensure that the contract permits the Institution to terminate the relationship without prohibitive expense, and that termination and notification provisions allow for the orderly conversion to another third-party, if applicable.

[ ]  **CUSTOMER COMPLAINTS**

[ ] The contract should specify whether the bank or vendor is responsible for responding to customer complaints. If so, ensure the vendor has a process in place to track customer satisfaction, performance metrics, and reporting.

[ ] If it is the vendor’s responsibility, specify provisions that ensure that the vendor receives and responds timely to customer complaints and forwards a copy of each complaint and response to the bank. The vendor should submit periodic summary reports that are timely and include sufficient and usable information, including the status and resolution of complaints, to enable the bank to analyze customer complaint activity and trends for risk management purposes.

[ ]  **ADDITIONAL COSTS**

**☐** The contract should specify the cost of all training, as part of the implementation process and ongoing, once the vendor solution is "live".

[ ] The contract should specify the cost of all training, as part of the implementation process and ongoing, once the vendor solution is "live".

[ ] The contract should specify which costs are included and which ones are on a per-use basis. If costs increase during the term of the contract, ensure the ongoing increases are reasonable and will not out- pace the market.

[ ]  **EXIT COSTS**

[ ] Exit costs should not be prohibitive to exit the relationship.

[ ] An ongoing relationship will be dependent on the vendor providing requested due diligence documents. Failure to do so could result in the contract being terminated, with no penalty to the bank.

[ ]  **SUBCONTRACTING**

[ ] If the vendor is outsourcing any of the contracted services to subcontractors, how will the vendor monitor these subcontractors and mitigate risk arising from its use of the subcontractors? The contract should clearly state the vendor’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 subcontractors.

[ ] Ensure the contract prohibits the vendor from using foreign-based subcontractors without the Institution’s ***prior*** consent. Ensure contracts with foreign-based vendors or vendors that back up and/or store data offshore clearly address the need for data security and confidentiality and require the vendor to adhere to U.S. regulatory standards. (Note to Vendor Manager: Failure by the vendor to provide this advance notification should be considered grounds for termination!)

[ ] The contract should stipulate Heritage Bank’s right to terminate the contract without penalty in the event the vendor’s subcontracting arrangements do not comply with the terms of the contract.

[ ]  **OCC SUPERVISION**

**☐** The contract should stipulate that the performance of activities performed by external parties for the bank is subject to OCC examination oversight, including access to all work papers, drafts, and other materials at no cost. The OCC 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.

[ ] There should be no contract early termination fee as a result of an OCC examination/ objection.

[ ]  **FINALLY**

[ ] Ensure the contract does not contain provisions or inducements that may have a significant, adverse effect on the bank.

[ ] If the contract is with an affiliate, does the contract reflect an arms-length relationship between the parties? DEFINE "AFFILIATE" (currently only PHI) AND "ARMS-LENGTH" i.e., both parties in the deal are acting in their own self-interest and are not subject to any pressure or duress from the other party.