How to Ensure Your Major Vendor Contracts Are Rock Solid

By: Peter Jeye, Founder & CEO of FintechVendors.com

Crafting robust contracts with key system vendors is a paramount concern for financial institutions, and it's a topic that sparks much debate among industry professionals. Such agreements go far beyond just securing a good price; they are fundamental to safeguarding the institution's operational integrity and regulatory standing. The intricate details within these contracts can either provide a solid foundation for a long-term partnership or create headaches down the road.

♦ **A critical focus must be on managing business risks**.

This includes clearly defining liabilities, indemnification clauses, and stringent provisions for confidentiality and security breaches. Given the sensitive nature of financial data, contracts must explicitly outline data protection protocols and breach response mechanisms. It's not enough to simply state that a vendor will handle data securely; the contract should detail the specific security standards they will adhere to, such as encryption protocols, access controls, and regular security audits. Furthermore, commitments must be included to ensure the vendor timely provides system updates to stay in compliance with new and changing regulations. This is particularly important in a dynamic regulatory environment where rules around data privacy and transaction security are constantly evolving.

Another vital consideration is the impact of your institution's growth on pricing. The contract should contain transparent and acceptable terms for how pricing will adjust as your volume or usage increases, avoiding unforeseen costs as your institution scales. Be wary of clauses that allow vendors to unilaterally change pricing, or that tie price increases to broad economic indicators without a clear cap. A good contract will define specific triggers for price adjustments and set a reasonable limit on how much prices can increase over a given period, providing predictable cost management for your budget.

♦ **Service Level Agreements (SLAs) are the backbone of vendor performance.**

These should detail performance metrics, uptime guarantees, response times for issues, and clear penalties for non-compliance/non-performance, ensuring accountability and continuity of critical services. Well-defined SLAs should include:

- **Uptime Guarantees**: A specific, measurable percentage with clear consequences if this metric isn't met.

- **Support Response Times**: Defined timeframes for a vendor to acknowledge, respond to, and resolve issues based on severity level (e.g., critical, high, medium, low).
- **Performance Metrics**: Specific performance benchmarks, such as transaction processing speed or data retrieval times, that are essential for your daily operations.
- **Escalation Process**: A clear path for escalating unresolved issues, including contact information for key personnel and management.

♦ **Fair and practical termination provisions are essential**.

A well-structured exit strategy, including clear notice periods and data de-conversion assistance, is crucial to minimize disruption if the relationship needs to end. The contract should spell out who owns the data and ensure that the vendor will provide your institution with its data in a usable format within a reasonable timeframe. It should also outline the costs associated with de-conversion to prevent a vendor from holding your institution hostage with exorbitant fees. These protections should also extend to scenarios such as mergers, where system transitions and data portability are equally critical. It's also important to check for fine print regarding clawbacks, where you owe back to the vendor any credits/discounts received if your institution is acquired prior to end of term.

♦ **Term length and renewal provisions must be tailored to meet specific needs.**

Ideal contract durations vary depending on the type of system and its importance to the institution. A key consideration is maintaining sufficient flexibility to mitigate risks such as outdated technology or declining vendor performance, while also avoiding excessive administrative, legal, or evaluation burdens. For example, core system contracts typically span 5 to 7 years, while digital banking systems are commonly contracted for 3 to 5 years. It's essential to carefully review and negotiate renewal provisions, including notification requirements and any pricing implications—such as changes to original or newly offered discounts and credits—upon renewal.

♦ **Promises, conversion schedule, and best pricing must be covered.**

Sales presentations often highlight capabilities that might not make it into the final legal document, so careful review is needed. The implementation and conversion schedule must also be formally agreed upon and detailed, setting clear expectations for both parties. Of course, while all these elements are crucial, it goes without saying that securing the best possible pricing remains a fundamental objective throughout the negotiation process, including integration costs. A thorough contract review by legal counsel specializing in financial technology is a non-negotiable step to ensure every clause serves to protect your institution's interests and operational stability.

Prior to FintechVendors.com, Peter Jeye was Founder & CEO of Next Step, a leading consulting firm to community banks and credit unions that helped negotiate countless number of major vendor contracts.