Recommendations for fintech startups navigating the procurement process

Marc GilmanContributor 11:15 am PST • February 7, 2020

Marc Gilman is general counsel and VP of compliance at Theta Lake. He is also an adjunct professor at Fordham University School of Law.

The expanding scope of fintech has been well documented in these digital pages. Payments, investing, financial planning and lending often spring to mind as "classic" fintech startups, but other business models like regtech, compliance, human resources and marketing are on the ascent.

For passionate and talented founders, the tireless pursuit of building innovative technology is critical and fundamental. That said, to be successful in financial services, significant time and effort needs to be dedicated to other business fundamentals: corporate setup, privacy and security. The financial services customer base presents unique challenges for fintech startups as the regulatory and operational requirements for third-party vendor assessment and management are, in comparison to most other industries, brutal. Issues that might go overlooked during the early stages of product design and team-building could turn into obstacles during the sales process.

Understanding the dynamics of the financial services procurement process is essential if you want to negotiate it as quickly and seamlessly as possible. And before diving head-first into the development of your killer fintech app, consider the following questions:

- Is my technical architecture secure?
- Who is responsible for cybersecurity in the organization?
- What types of business insurance do I have and do they cover the right risks?
- How do I manage privacy regulations like GDPR and CCPA?
- Does the company understand the outsourcing mandates of Appendix J, the SEC and FINRA?

If you have trouble answering these questions, take a breath and let the heart palpitations subside. These issues are likely going to be very important for your fintech startup; however, answering these questions — and including them in your early stage strategy — will reduce friction down the road.

In this article, I'll offer practical observations about the preparatory work you can do to set your fintech startup up for success. We'll discuss ensuring you have the right agreements in place, building a security and privacy framework,

auditing practices, procuring insurance and regulatory requirements for third-party vendor assessment. The list is not exhaustive but points to baseline competencies that will build trust with your financial services clients, ensure that your practices match customer expectations and expedite procurement.

The right agreements

The first critical element (and I may be biased here as a General Counsel) is to have the right agreements in place for your organization. From employee non-disclosure and privacy to invention and advisory agreements, protecting confidential information and company IP is key. In some instances, customers may ask you to provide these agreements as part of the due diligence process. Given the risks of data breaches, cybersecurity events and non-compliance under GDPR and CCPA, having the right data protection agreements in place is essential for managing potential legal liability.

You can find good law firm resources on the Web to help you get started with NDAs and IP ownership agreements. Goodwin's Founders Workbench Document Driver and Cooley's GO platform both offer solid, free templates. (Full lawyerly disclaimer here: I'm not endorsing either of those platforms or vouching for their legal advice.). Incorporating these agreements into your employee and vendor onboarding process will then safeguard your fintech startup against obvious legal risk.

Security

For any product — whether consumer or business, hosted in the cloud or on premises — prioritizing security is critical. In fact, concerns about how you approach security may be as important to financial services firms as your product itself. Regulators from the SEC and FINRA to the FFIEC and state AGs are all deeply concerned about security. A data breach or other security event

not only erodes customer confidence, it often carries with it harsh financial and regulatory penalties. As a result, developing and deploying a robust security framework is important. What follows are a few high-level suggestions for creating a basic security program.

First, you must nominate a Chief Information Security Officer ("CISO") or equivalent at your organization. Smaller organizations may parse out security responsibilities among two or three employees. Many different arrangements might be acceptable so long as duties are clearly defined and well understood by those involved. Some firms who don't have the requisite expertise in-house look externally at providers like Coalfire, Vanta, and Tugboat Logic for outsourced CISO services or assessments. Note that while leveraging third parties for CISO duties creates efficiencies, responsibility and liability always remain with the fintech startup itself.

Designating a CISO ensures that you have a single point of contact for issues like outages, data breaches and threat assessments. In many startups, the CISO will often liaise with customers and prospects directly to explain the company's security architecture and processes. Since CISO-to-customer interactions are becoming more common, people skills are now as important as technical know-how in this domain. The CISO may lead the customer though detailed security assessments and run point on the elaborate dance of questions and answers that transpires during negotiation of a Master Service Agreement.

Your CISO will also define your organization's security policies and procedures. The policy framework is typically anchored by the Information Security policy, which describes the fintech's protocols for everything from access controls to data classification and the use of company systems. Additional standalone policies will cover themes as diverse as security incident response, business continuity and disaster recovery planning, and employees who bring their own

devices. Policies are often requested as part of the security assessment process, so making sure that your framework addresses not only the appropriate breadth of topics, but also covers them in sufficient detail is important. Your financial services clients may request targeted changes to policies and procedures to validate that they align with industry- or firm-specific requirements.

Having meaningful policies and procedures in place is important, and equally as important is testing them on a routine basis. You must be able to demonstrate that you can restore critical information from backup and maintain secondary production environments that can be leveraged in the event of a failure. Additionally, conducting routine tests of your incident response plan by gathering your team and walking through a mock scenario is essential.

From an operational perspective, enterprise cloud-based hosts like AWS, Azure and Google have tools that make many of these processes easier, if not seamless. Fintech startups often rely on the inherent redundancies of cloud providers for backup and business continuity. Financial services firms will likely have hard mandates around uptime, page and application response times and failover readiness baked into Master Service Agreements. Being always-on and nimble could make or break your company, so architect your platform to account for these requirements so they don't come as a surprise when you enter due diligence.

Auditing

Another key step that fintech startups should take to address security and privacy and tee up a smooth procurement is to obtain audited, third-party certifications that the security protocols stated in policies and procedures are, in fact, followed. There are several such certifications from SOC to ISO and

beyond. It seems that the SOC has become the most popular and comprehensive such audit, at least for U.S.-based finservs, so we will discuss it in some detail.

The SOC, or System and Organization Controls, come in several flavors and the language of SOC-dom can be hard to decipher— do you have a SOC 1 or a SOC 2? Is it a Type 1 or Type 2? Confusing for the uninitiated.

Basically, the SOC 1 tests accounting controls and a SOC 2 tests security, availability and processing integrity controls. The less popular SOC 3 tests the same controls as the SOC 2, but the report generated by the auditor is essentially a summary that can be freely distributed without an NDA. (The detail of the SOC report is important as it describes the steps your company takes to meet the various security requirements, hence a sanitized SOC 3 may not be sufficient.)

SOC audits can be conducted in two ways: they can test that you have documented sufficient policies and procedures that align to the controls being tested — this is the "Type 1." Or the audit can examine the "design and operating effectiveness" of those controls, in other words — that you actually doing the stuff you describe in your policies and procedures — this is a "Type 2" audit.

The SOC 2, Type 2 audit has gradually become the generally-accepted standard for fintechs that cater to financial services. The SOC 2, Type 2 tests the technical controls financial services firms are most concerned with, such as user access controls, business continuity and disaster recovery, penetration testing protocols, adequacy of information security policies and conducting routine training. Hopefully those controls ring a bell as I mentioned most of them in the security section above. It's no coincidence that having a solid security framework in place makes achieving the SOC 2 audit much easier. Or,

at least, slightly less painful.

Other audits have proven useful and may suffice as supplements to the SOC 2. The International Organization for Standardization ("ISO") articulates several security frameworks. The ISO 27001 audit tests an organization's information security management system by examining 14 key areas including policies, access management, supplier relationships and compliance. Core to ISO 27001 are the collection, protection and use of data, creating a close conceptual alignment with SOC 2. Other frameworks such as NIST's Cybersecurity Framework, the CIS Critical Security Controls and the Cloud Security Alliance's Cloud Controls Matrix can be leveraged to demonstrate a vendor's maturity as it pertains to information security and data protection.

Testing your startup's information security posture is becoming a critical step in preparing for a financial services vendor assessment — the next is demonstrating that you are ready if problems arise.

Insurance

With a framework and practice for responding to incidents locked down, fintechs must have plans to deal with worst-case scenarios — that's where insurance comes into play. Like disaster recovery and redundancy, any enterprise agreement with a financial services firm will include minimum insurance coverage requirements.

Key here will be the procurement of a cyber insurance policy tailored to meet your startup's needs and the expectations of a large financial institution. These cyber policies have become increasingly common in the last few years, although no two policies are created equal. Unlike, say, employer's liability or workers' compensation insurance, there are no standard forms for cyber insurance, so you must examine each policy to confirm that it protects you

against threats unique to your business model. You'll need to consider how and where you store your data, what third parties may have access to it and what other measures (SOC 2?) you'll take to protect information and detect potential issues.

Vendor management requirements

We've focused on agreements, security protocols, audits and insurance, so it is worth covering a few of the vendor management regulations applicable to financial institutions that you may be responsible for complying with. Understanding these regs, even at a high level, provides insight into the practical considerations your finserv customers are grappling with when they select and onboard a new technology provider.

The Federal Financial Institutions Examination Council (FFIEC) is a group of regulators including the Federal Reserve System, the OCC, the **FDIC** and others who jointly issue guidance and standards applicable to banking institutions in the U.S. The FFIEC has issued guidance on several technology-related areas including social media, cybersecurity and, of course, vendor selection. In 2015, the FFIEC released a new Appendix to its Business Continuity Planning Booklet titled "Strengthening the Resilience of Outsourced Technology Services." The new Appendix is commonly referred to as "Appendix J" for short and includes, among other things, requirements to include provisions in agreements for audit rights, BCP, data governance and a host of other issues. Special care must be taken to monitor and oversee critical third-party vendors to ensure that the business would run smoothly in the event of a material outage or other significant catastrophes like extreme weather conditions or terrorist incidents.

The SEC's Office of Compliance Investigations and Examinations issues reports on annual exam priorities as well as periodic risk alerts on issues

critical to the entities it regulates, like broker-dealers and investment advisors. In fact, the SEC's 2020 Exam Priorities include vendor risk management as an area of interest — it is included as subset of information security. FINRA has also raised the issue of vendor management in the context of cybersecurity, having released Notice to Members 05-48 on Outsourcing and discussing the importance of vendor management in its 2017 Report on Examination Findings.

Since third-party vendors often hold critical confidential business information, including sensitive personal information of the firm and its clients, state regulators are mandating that financial services firms have rigorous methods for assessing and overseeing their vendors, often as part of cybersecurity requirements. The New York Department of Financial Services ("NYDFS") includes provisions for third party vendor access to sensitive data in Section 500.11 of its Cybersecurity Requirements for Financial Services Companies. And the NAIC's Insurance Data Security Model Law, based in part on the NYDFS Reg, includes oversight of third-party service provider arrangements. Given that the NAIC's law has been implemented by eight states including South Carolina, Ohio, Michigan, Alabama and Connecticut, fintech startups must be aware of these requirements and provide assistance to facilitate compliance.

As demonstrated by the breadth of issues discussed above, assessing and executing the tasks required to prepare for a financial services procurement process can be daunting. However, considering these issues early and building your product with them in mind will make for a smoother vendor assessment. Given heightened security, privacy and compliance concerns across industries, these financial services mandates are rapidly becoming table stakes for technology companies generally, across businesses and geographies. We're quickly moving toward a model where good security is synonymous with good business.