Edition September 2023

Third-Party Diligence (TPD)

The definitive guide to standardize third-party due diligence to build and maintain effective, compliant partnerships between banks and fintechs and other third parties.

ALLOY LABS Banking, unbound.

Crowe

Third-Party Diligence (TPD)

> "Knowing the key risks and vulnerabilities within partnerships and how to control for them is crucial in managing risks. This also allows each party to make informed decisions regarding those areas where they are willing to take on certain risks or where additional investments may need to be made to make the partnership thrive."
>
> Clayton Mitchell – Managing Principal, Fintech, Crowe LLP

Table of Contents

ALLOY LABS Banking, unbound. Crowe

Risk and compliance are often thrown up as roadblocks to exploring the new products and services that drive value for customers and keep community banks relevant.

These roadblocks, whether real or perceived, can be managed, and regulators are providing helpful guidance that can be translated to action."

Jason Henrichs, CEO Alloy Labs

Redefining Partnerships

Based on Fintech Stages of Growth

As a financial institution, when choosing to partner with a fintech at the startup or partnering stages, it is crucial for the fintech to demonstrate proactive risk management practices throughout its entire enterprise. Referring to the Crowe minimal acceptable maturity (MAM) model and the learnings from our work with business, risk, and compliance professionals across the Alloy Lab Alliance (Alliance), a fintech in the start-up or partnering stage often maintains a minimum score of 2, with more capable fintechs typically ranking at a 3. When conducting due diligence on a fintech with limited customer impact or controlled customer exposure, the acceptable maturity level, as per the MAM model, typically aligns with the developed stage. This helps to ensure effective measurement and that integration of systems and processes are in place across most departments, which will ensure comprehensive risk management. It is important for ownership, control, and documentation of data to be prioritized, with well-trained teams readily available to generate reports quickly and efficiently.

When a fintech moves from the initial stages of start-up or partnering to the growing or at-scale phase, we see the partnership requirements often undergo a significant shift. A minimum ranking of 4 (advanced) or 5 (optimizing) is now the benchmark, indicating a commendable advancement in strategy & business success, execution, and risk management. The partnership should be viewed as forward-thinking, with the fintech, at its best, operating at full-scale and utilizing data-driven decision-making to achieve their detailed, long-term growth objectives. There is often a full public offering available, and risk management practices should be deeply ingrained into the company's culture. At this impact stage, the partnering bank may have more lenience to exercise reduced oversight into risk management and triggering events.

We recognize the significance of the MAM model and emphasize the importance of organizations aligning their people, processes, and technology to support their strategic needs. As we engaged with different financial institutions within the Alloy Labs consortium, we proactively sought to determine the key factors that would drive their success in the next phase of third-party due diligence.

During these discussions, we focused on identifying the most significant areas of concern, anticipating potential challenges and risks that many occur, and in turn, formulated actionable steps to take to prevent and mitigate them. This iterative approach has been directed by the Alliance members, encouraging thought-provoking discussions and exploration, while enabling a proactive way to tackle oncoming challenges.

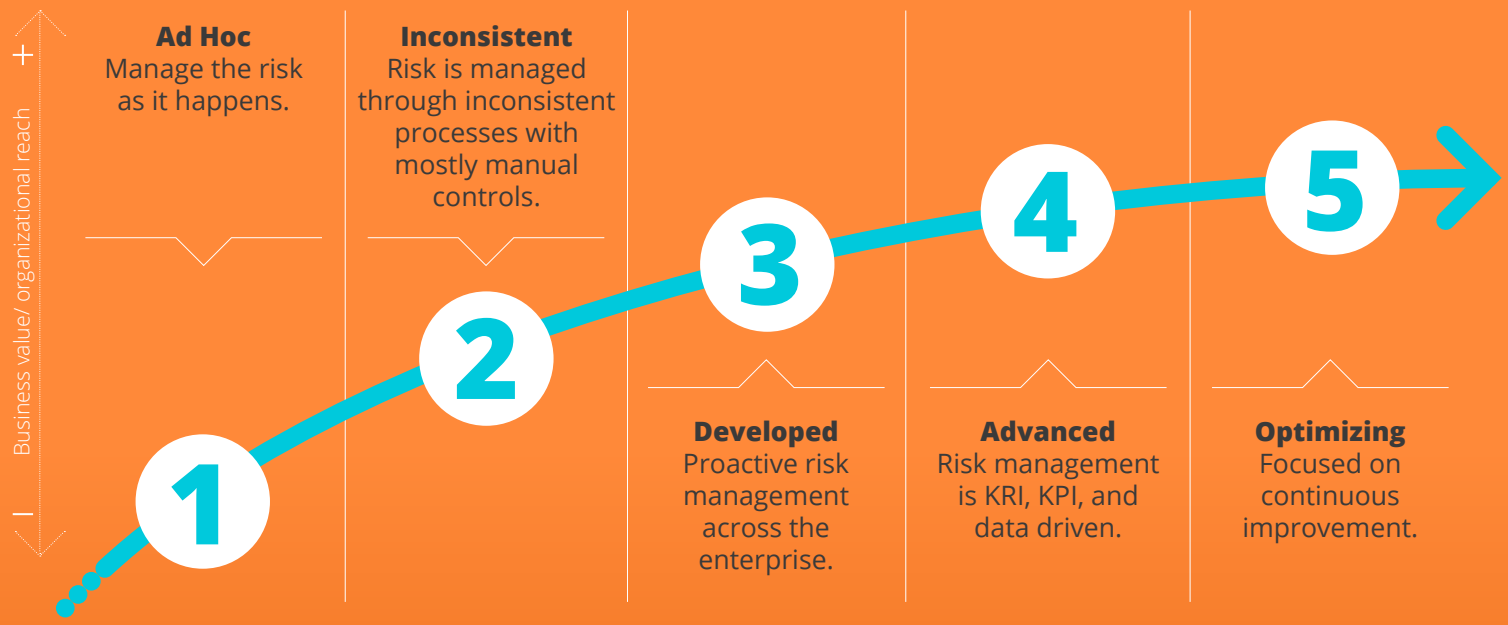
@

if you are interested in participating in any of the workstreams to contribute to this industry project reach out to

Emmett Shipman
VP Market Development at Alloy Labs
Emmett@alloylabs.com

Clayton Mitchell
Managing Principal, Fintech at Crowe LLP
Clayton.mitchell@crowe.com

Minimal Acceptable Maturity Model



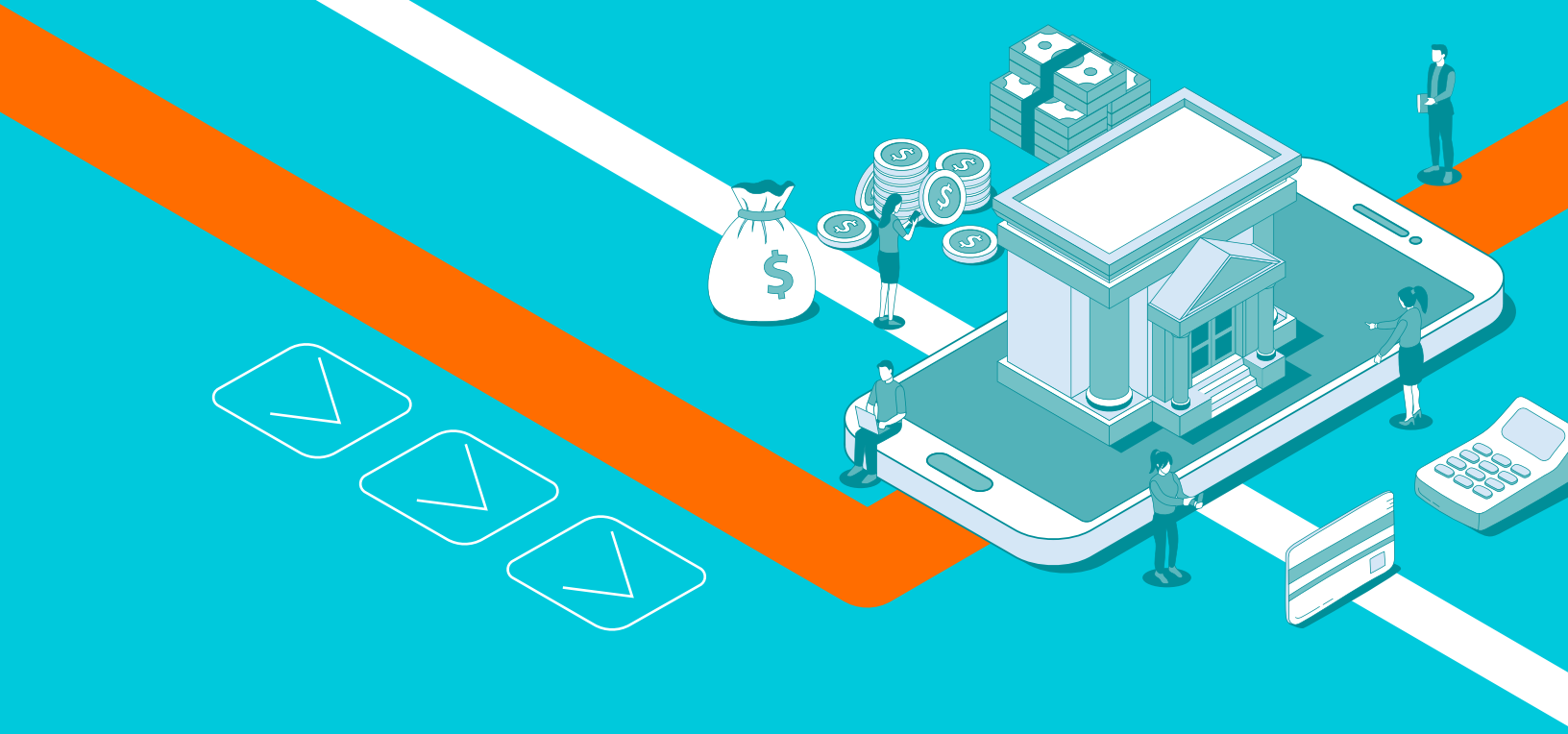
1	2	3	4	5
Ad Hoc Manage the risk as it happens.	**Inconsistent** Risk is managed through inconsistent processes with mostly manual controls.	**Developed** Proactive risk management across the enterprise.	**Advanced** Risk management is KRI, KPI, and data driven.	**Optimizing** Focused on continuous improvement.
Capability Maturity: Tactical				Capability Maturity: Strategic
People Success depends on people who put in extra effort beyond their normal responsibilities.	**People** Defined yet over- lapping roles and responsibilities lead to rework, confusion and higher resource costs.	**People** Risk management and execution roles and responsibilities are clearly defined.	**People** Risk management is embedded into the culture with seamless interactions across all three lines of defense.	**People** Organization has a gold-standard risk function that enables people and ideas to create value for the organization.
Process Processes are usually reactionary and often identify risk events after they happen.	**Process** Processes and controls are inconsistently documented and maintained across the organization.	**Process** Processes, controls, and effectiveness are consistently measured, tested, and reported.	**Process** Processes are managed over their life cycle and include analytics that leverage both leading and lagging indicators.	**Process** Risk management requirements are embedded in first-line process execution. Second-line challenge is established as an advisory and credible challenge function.
Technology Systems are paper or Microsoft Office based with little or no consistency in how they are used.	**Technology** Niche or point solutions have been implemented to address specific, high-visibility risks.	**Technology** Systems designed centrally and are integrated, working together to manage risk across risk areas and departments.	**Technology** Risk technology is integrated across the enterprise and is used to drive decisions leveraging automation.	**Technology** Continuous improvement is enabled by piloting innovative new ideas and technologies.
Data Inconsistent data with limited controls around accuracy and completeness or ownership of data; no data dictionary.	**Data** Each business area has their own “data hero” that knows where to find information, but has limited documentation.	**Data** Data has been prioritized and is owned and documented; teams and managers have ready access to data; reports can be easily run.	**Data** Data drives decision-making and is governed, cleaned, and audited. BU-specific analytics are available from a shared repository.	**Data** Best-in-class data governance and management and advanced predictive data analytics to drive business growth.

We are noticing regulatory agencies are putting in more “speed bumps” to slow down the process of using fintechs.

We are seeing more guidance, as well as more oversight during the audit/exam process as fintechs carve out their space in the financial institution world.

This is especially prominent where and when financial institutions’ customer data is being accessed.”

Keith Evans, Vice President/Vendor Management Officer, First Northern Bank



Significant Risks and Key Risk Management

As Pete Boergermann SVP, Director of Information Security stated: “Understanding the “What’s important” & “What could go wrong” guidance will provide a clear picture of potential risks in a new partnership. Taking action based on the “What I should do” builds confidence in the relationship to move forward, knowing that prudent steps have been taken to keep the customer’s data safe, thus enabling the business to achieve its strategic goals.”

In relationships with very few bright-line requirements, a risk-based approach is necessary. In this section, we have identified some of the most important areas where something might go wrong and tactics for mitigating those risks.

Enabling robust strategy & financial success

What's important	What could go wrong	What I should do
RELEVENT INDUSTRY EXPERIENCE AND REPUTATION within senior management & leadership team. Fintech should provide a formal written incident response plan to protect and recover all data without compromise or loss. The plan must be remediated and retested as necessary.	Financial mismanagement, such as miscalculating the allocation of resources and disproportionate levels of debt. A lack of positive company culture due to unsound management, resulting in high employee turnover. Failure to conduct adequate compliance and regulation filings, certifications, insurance, etc. Company suspected of fraud, money laundering, etc. due to corrupt leadership.	☐ Obtain a detailed business plan that includes long-term goals and strategies for the fintech, including its employee culture. This plan should outline how the fintech intends to achieve their objectives and what measures will be taken to create a supportive and productive work environment. ☐ Periodically conducting thorough background checks on all executive and senior management employees, as well as subcontractors who may have access to critical systems or confidential information. ☐ Conduct bi-annual reviews of the D&B report (Dun & Bradstreet) and request a certificate of good standing to ensure that the fintech is financially stable and has a sound reputation.
BUSINESS PLAN & STRATEGY in place to enable innovation	Executive leadership team unable to recognize and pursue new opportunities for growth and innovation. Company fails to adapt to changes in the market and stay ahead of competitors. Fintech's third-party vendors' goals and business strategies conflict with those of the financial institution. Fintech does not have enough revenue to support the relationship, resulting in a loss in sustainability of other clients.	☐ As the fintech begins to grow, a board of directors should be instated to aid decision-making. ☐ It is recommended to maintain a quarterly review of strategic group meeting minutes, as well as request insight into any project approvals completed by the board or executive committees. ☐ Request to be updated on conversations around mergers, acquisitions, joint ventures, significant modifications to customer base, etc. as the market continues to change.
STRONG financial condition	Fintech fails to create a strong financial plan, resulting in the inability to meet financial obligation, a loss in shareholder value, loss of market share, a reduced ability to acquire new customers and retain talented employees.	☐ Ensure there is documentation of the fintech driving revenue. ☐ Depending on the stage of the fintech, funding should align with the shared roadmap regarding the product, technology and partnership. ☐ Ensure the fintech has other strong clients that are also financially and legally regulated.

Aligning on a safe & strategic partnership

What's important	What could go wrong	What I should do
Ensure a **MUTALLY BENEFICIAL** business agreement	Failure to meet expectations, overstating or misrepresenting their capabilities to partner. One party gains more than the other party, resulting in a breakdown of strong communication and an unprofitable power dynamic. Distrust occurs between the bank and fintech.	☐ Ensure robust workstreams are in place to enable product advancement. Depending on the fintech's stage of growth, a project management team should be created. ☐ Together, agree upon and identify specific goals and objectives, as well as any key performance indicators (KPIs) that will be used to measure success. ☐ Identify potential areas of disagreement or conflict; discuss ways in which to stay ahead of future obstacles.
Monitoring **SUB-CONTRACTOR RELATIONSHIPS**	Failure to align goals with subcontractors, resulting in conflict and miscommunication, and preventing partnership from being executed. Legal issues could arise due to third party engaging in unethical or illegal activities. Inadequate security training and discipline via the subcontracting company, resulting in customer data being stolen. Unclear expectations written, which could result in the third party does not adhering to the agreed-upon budget.	☐ The fintech should provide updated due diligence when significant changes occur, and at the very least, annually. It is the fintech's responsibility to provide documentation to the financial institution. Review the fintech's subcontractor due diligence documents including agreements, financials, SOC, BCP, insurance, cybersecurity policies, etc. ☐ As the fintech partners with additional third-parties, it is required they have a formal vendor management program, including contract and due diligence documentation on key/critical 4th party vendors. ☐ Focus on high-risk 4th party vendors. The fintech and/or 4th party is responsible for identifying how they will mitigate against threats to their organizations.
STRONG NOFICATION POLICY in place	An incident occurs that disrupts fintech's ability to execute their business plan. Financial mismanagement, leading to a loss of funds.	☐ Fintech should provide a copy of their notification policy when issues and incidents arise that impact the services the fintech is providing your institution. A critical high-risk fintech should notify your institution as soon as possible, but no longer than 72 hours after the incident that may impact your institution. Include notification language in your fintech's agreement. Ask for additional documents or ask additional questions specific to your institution. ☐ It is suggested to have legal consultants review the notification policy to ensure the fintech and financial institution are aligned.

Ensuring operationally sound & mutally beneficial parternship

What's important	What could go wrong	What I should do
Enhanced safety for **DATA MANAGEMENT**	Failure to implement enhanced data protection tools for encryption and malware/firewall defense. Failure to create a proper test environment for internal testing prior to go-live updates, resulting in a loss of data or user protection. Inadequate data and disaster recovery tests and updates in place, resulting in miscommunication between employees and customers.	☐ Updates are tested in beta and if issues arise when rolled out, the company has systems in place to revert to the previous version in a timely manner. ☐ Fintech should provide information on security penetration testing and the results. ☐ Annual disaster recovery tests are completed and shared with customers. The disaster recovery site is a live failover and customers can participate in the test. ☐ Quarterly meetings are done with the company to go over updates, new services, and other new product offerings when the fintech is at the partnering stage of growth, with monthly meetings when the fintech is at the growing stage.
Executing partnerships with **OPERATIONAL RESILIENCE**	Fintech fails to identify triggering events such as loss of power, facilities, equipment, and personnel. as well as other localized, national, and global triggering events specific to their environment, including geographical locations. Failure to consider the impact and mitigate any operational risk of additional vendors and business partners, including the bank, if a triggering event should impact the fintech directly.	☐ Ongoing monitoring of the service level agreement (SLA) should occur annually, more frequently as necessary. Review should also occur at both the agreement renewal and in the case that a partnership is terminated. ☐ The financial institution may consider fintech on-site visits for additional monitoring, and the fintech should provide updated due diligence documentation at the time of review. ☐ Fintech should provide a BCP/DR plan that identifies where all data, including your institution's data, resides. The plan should also strictly identify how to protect and recover data and how that data is being used to enable operational resilience.
Implement **ILLNESS AND INCIDENT RESPONSE** plans	An illness or incident occurs; without a detailed response plan, the fintech will be unsure how to respond quickly and effectively, resulting in a delay in implementing necessary measures. Illness or incident occurs that can result in a negative impact on both the business operations and the culture of the company. Slow response times due to unpreparedness, resulting in customer disaffection and complaints.	☐ Ensure the fintech has a well-designed plan in place that will assist in minimizing the negative impact of such events, will protect the health and safety of employees and other stakeholders, and will make sure that the company follows legal and regulatory requirements. ☐ The formal written, mature incident response plan is approved by the board annually, identifying all processes, along with a formal testing and exercises of the incident response plan that should occur at least annually. Include a clause in the response plan that the fintech must alert the financial institution of an issue within the first 72 hours. ☐ Include a clause in the response plan that the fintech must alert the financial institution of an issue within the first 72 hours.

Abiding by compliance & regulatory needs

What's important	What could go wrong	What I should do
TREATING CUSTOMERS FAIRLY to meet regulatory requirements and enable customer success.	Inaccurate and deceptive marketing and disclosures. Lending and underwriting models that unfairly treat customers on a prohibited basis. Failure to provide adequate consumer protections (e.g., disputes and error resolution). Inappropriately or unethically use customers' non-public personal information.	☐ Product and service compliance related processes and controls effectiveness are consistently measured, controls are appropriately tested and reported, and processes are quantitatively understood. ☐ Document and standardized complaint program documents (standards, policies, and procedures). Processes for the complaint management program are now consistent and in compliance with the established guidelines. ☐ Periodic root cause analysis is completed and used as feedback to impact operational processes. ☐ Reporting to corporate compliance regarding overall complaints volumes and escalated complaints occurs on regular intervals.
FIGHTING FINANCIAL CRIME, together	Have inadequate procedures to identity the true customer and complete adequate identity verification. Have inadequate controls that would allow for account takeovers to occur. Fail to appropriately screen customer transactions for suspicious or unusual activity and sanctions lists.	☐ Established risk-based customer identification and verification procedures and clearly defined standards for partners, with periodic monitoring and reporting of compliance with established standards. ☐ Systems and processes that use alternative data sources and access management to limit account takeover risk. ☐ Established risk-based customer and transaction screening, based on products and services offered. Further a robust referral program from partners regarding any unusual or suspicious activity identified.
ADAPTIVE COMPLIANCE MANAGEMENT SYSTEM to support an expanded ecosystem	Fail to establish appropriate guidelines and risk management expectations to fintech partners. Failure to effectively challenge the activities of the partners on an ongoing basis. Inadequate reporting to senior management and the board regarding risk events, identified issues, and customer complaints.	☐ Compliance standards are operationalized and enforced through a culture of compliance throughout the ecosystem. Clearly defined roles and responsibilities are put into place that support the regularly updated and maintained standards. ☐ Standards for governance and oversight of all pieces of the partnership ecosystem are established, facilitating an overarching governance and oversight process that fits a bank's risk appetite. ☐ The test scripts and monitoring tools are in place, data is available, and testing has been completed. Results are reported and any noted exceptions are flowing through an issues management process and being tracked.

Risks are controlled

What's important	What could go wrong	What I should do
HAVING CLEAR EXPECTATIONS about the bank's risk appetite, communications, and reporting.	Misalignment or unrealistic expectations regarding risk-taking activities between partners can lead to breakdown of delivery, trust, and have negative customer confidence.	☐ Establish clear expectations regarding minimal acceptable maturity of the control environment. This would include how the fintech outlines risk management responsibilities, reporting processes, and how its employees are responsible for complying with policies and procedures. ☐ Set clear understanding about the nature, scope, and frequency of control reviews, especially those related to the prospective activity. This provides a community bank with insight into the quality of the fintech company's risk management and control environment. ☐ The bank and fintech should agree on outcomes regarding key risk indicators (e.g., complaints, issues management, etc.)
OPERATIONAL RESILIENCE to support adequate delivery and grow the business.	If the bank or fintech fails to execute, this could increase financial, operational, and reputation risk. This increased risk profile could cost both parties a significant amount of time and money and deteriorate the trust and value of the organization.	☐ Evaluating a fintech company's operational resilience includes evaluation of key personnel, technology, redundancy, and ability to respond to incidents. Information on a fintech company's staffing and expertise, provides a means to assess the overall adequacy of the fintech company's operations. The fintech should provide a copy of their most recent DR exercise and testing results of their business processes that are used for your financial institution. Ask for additional documents or ask additional questions specific to your institution, as necessary. ☐ The bank and fintech should agree on service level agreements and key performance indicators (e.g., downtimes, customer service, errors, etc.). Ongoing reporting and monitoring helps a community bank to consider how the fintech company integrates into the organization's issues management. ☐ There should be the right to terminate the relationship within the contracts, quarterly business reviews, and transparent communication regarding cost sharing or other remuneration for non-performance.
Ongoing **MONITORING & TESTING** to identify and manage risks timely.	Deteriorating control environments may occur without proper oversight and testing.	☐ The bank should be comprehensive and include monitoring and testing for operations, information security and privacy and regulatory compliance. ☐ A testing schedule should be agreed to as part of the onboarding and contracting stage of establishing the relationship and monitored on an ongoing basis, typically quarterly. ☐ Areas of scope and coverage should be mutually agreed to, and frequency of testing should be risk-based. Testing could be done internally by the fintech, by the bank, or by an independent third-party. If relying on the fintech's testing, a periodic, typically annual, audit of the higher risk activities should be incorporated. The cost of these activities should also be considered within the contract and part of the profitability analysis.

Keeping information secure

What's important	What could go wrong	What I should do
Information **SECURITY and PRIVACY by DESIGN**	Organizations who are not thoughtful about the information that they receive and share with partners creates disproportionate risks regarding the handling of non-public personal information or other confidential information.	☐ Both the bank and fintech partner should be very deliberate about the information received, shared and maintained, beyond what is required by a law or regulation or necessary to do business. This allows for the thoughtful evaluation, gathering, and storing of information, only as necessary to reduce the threat of unauthorized access or improper or unethical use of the data. ☐ Better understanding the business case and security controls of partners will also support appropriate design. Further, evaluating adequacy of policies and procedures would further support risk management.
Managing **FOURTH-PARTY RISK**	When an organization's third parties are also using service providers, including business process outsourcing, the threat landscape extends, and without proper processes and controls in place, exposes the organization to further significant information security risk.	☐ Having a robust understanding of the vendors that your partners and third-parties work with is critical to managing against fourth party risk. ☐ Once the inventory of fourth parties is known, conducting a risk analysis of the types of information that they have access to, how it's accessed and used, and where it is stored will help to determine risk exposure. ☐ Gaining an understanding of contractual obligations and due diligence completed by your partner is also warranted for critical and higher-risk partners. Oversight, monitoring, and testing of such should then be deployed based on the risk exposure.
Gaining **ASSURANCE** over information security practices	Without proper assurance regarding the safety and security of information and how it's processed, stored, and shared, an organization exposes itself to unknown risk and vulnerabilities that could go unmanaged and expose the organization to significant regulatory, reputational, and financial risk.	☐ Fintech should provide a formal written cybersecurity and information security testing plans, which are risk-based and aligned to industry guidance and expectations. These plans should identify all processes along with formal testing and tabletop exercise results. ☐ The types of tests and evaluations that should be considered within these plans includes: • SOC reports • Penetration testing • Vulnerability scanning • Tabletop activities regarding breaches and loss, including notification practices. • IT general controls, including software development, access management, application security controls, etc. • An adequate level of cybersecurity insurance. ☐ Test results need to be documented, remediated, and retested as necessary. Test results need to be shared and reviewed by the board or other executives, or management team. Ask for additional documents or ask additional questions specific to your institution related to mitigation and corrective action regarding security.

Learn more and get involved

Join these Alloy Labs member banks and industry leaders that participated in developing this playbook

Learn more and get involved

Members of the Alloy Labs Alliance, alongside consultants from Crowe LLP, announce a second iteration of their guide to standardize third-party due diligence to build and maintain effective, compliant partnerships between banks, fintechs and other third parties.

Reach out to Emmett Shipman or Clayton Mitchell if you want to be involved in this or other projects helping to drive exponential growth in the industry or if you need support in the development of oversight of your bank-fintech partnership programs.

Emmett Shipman
VP Market Development at Alloy Labs
Emmett@alloylabs.com
Alloylabs.com

Clayton Mitchell
Managing Principal, Fintech at Crowe LLP
Clayton.mitchell@crowe.com
Crowe.com

ALLOY LABS Banking, unbound.

Crowe