CAPCO

CONDUCTING DUE DILIGENCE ON FINANCIAL TECHNOLOGY COMPANIES:

A GUIDE FOR COMMUNITY BANKS

a **wipro** company

INTRO

For financial institutions in today's rapidly changing market, remaining on top of trends in products and services can be the difference between growing effectively and losing customers to competition. Partnering with fintech companies may expand product availability, increase revenues and decrease expenses, furnish expertise, and assist the financial institution in meeting strategic goals. But, as with all third-party partnerships, the use of fintechs does not diminish the responsibility of an institution's board of directors and management to ensure that fintechs operate in a safe and sound manner and in compliance with applicable laws, regulations, and internal policies.

On Aug. 27, 2021, the federal bank regulatory agencies (Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC)) released "Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks" (The Guide). The Guide is intended to assist community banks with assessing the risks and benefits as part of a financial institution's due diligence process.

"Due diligence" involves a financial institution collecting and analyzing information to determine whether a third-party relationship would support strategic and financial goals, and whether the relationship can be implemented in a safe and sound manner, consistent with legal and regulatory requirements. The scope of due diligence depends on the risk to the financial institution.

The Guide focuses on six due diligence areas for financial institutions to evaluate for fintech companies.

1. BUSINESS EXPERIENCE AND QUALIFICATIONS

Business experience in the financial services sector and with the desired product or service should be evaluated. Financial institutions must evaluate a fintech's business experience and qualifications when considering a fintech's experience in conducting the desired activity and its ability to meet the financial institution's needs.

Considerations for business experience include, but are not limited to:

- Operational history, which should provide insight into a fintech's ability to meet the financial institution's needs. Considerations here include the ability to adequately provide the activity(ies) being consider in a manner that enable the financial institution to comply with regulatory requirements along with meeting customer needs.
- References for and any complaints lodged against the fintech. This evaluation would address whether the fintech has sufficient experience and expertise to meet the financial institution's needs, as well as the ability to address issues that may arise.
- Legal or regulatory actions against the fintech can be indicators of the fintech's history with offering the desired products and/or services.

A business strategy is defined as the determination of the basic long-term goals of an enterprise and the adoption of courses of action and the allocation of resources to carry out goals.

To determine the fintech's business strategies and plans, financial institutions should discuss with the fintech any key decisions it is considering. Here look for plans to launch new products or pursue new arrangements, such as mergers, acquisitions, joint ventures, or joint marketing. Financial institutions should evaluate the fintech's business strategies and plans when considering if the fintech would affect the prospective activity. Furthermore, financial institutions should inquire about the fintech's management style to determine if the fintech's culture, values, and business style fit those of the financial institution.

Lastly financial institutions, as part of its due diligence, should look to the background and expertise of the fintech's board of directors and executive management. Consideration may also be given to evaluating if there is sufficient management and staff with expertise to handle the desired activity.

Potential sources of information for financial institutions to review as part of the fintech's business experience and qualifications, include organizational charts, client references, public records, media reports, geographic footprint, expansion plans, ownership information, and professional information on management.

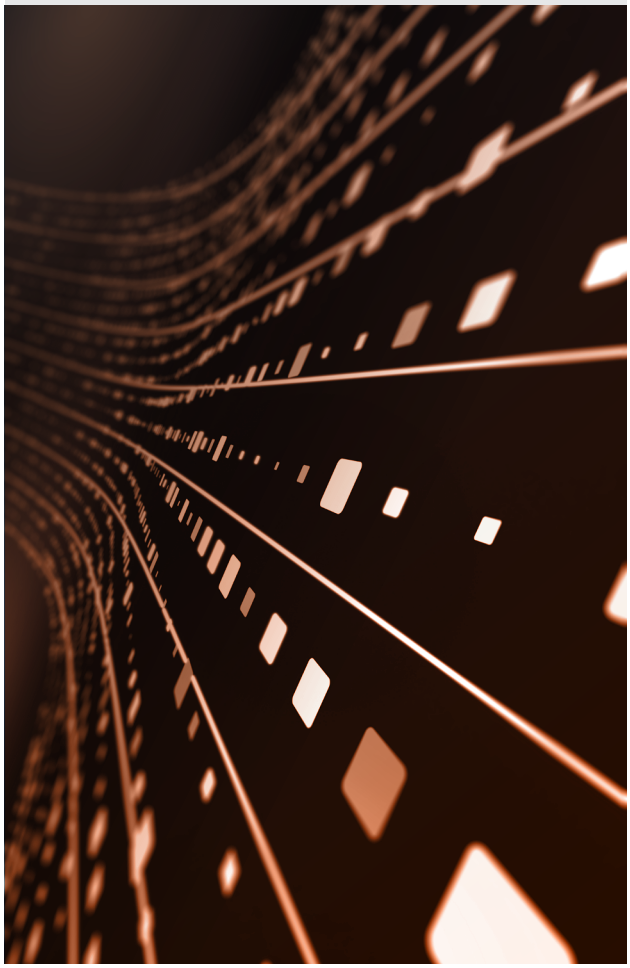
2. FINANCIAL CONDITION

Financial institutions must evaluate a fintech's financial condition to assess its ability to remain in business and fulfill any obligations credited by the third-party relationship. Look at the fintech's financial analysis and funding and market information.

For financial analysis and funding, financial institutions should review the fintech's financial reports when evaluating the fintech's capacity to provide the desired activity, to remain a going concern, and fulfill any if its obligations to the financial institution. Furthermore, being aware of a fintech's funding sources provides information when reviewing a fintech's financial condition. How is the fintech going to fund operations? Will it be through cash flow and profitability? Will the fintech rely on loans, capital injections, venture capital, or planned public offerings. Financial institutions should ask these questions as part of its analysis of the fintech's financial condition.

Due diligence also includes looking at market information. Is there a competitive environment for the desired product or service? If so, this could give some measure of the company's viability. Don't stop there. If possible, obtain a list of fintech's clients and client base. Does the fintech have a few significant clients or does it have a wide client base? If there are just a few critical clients, this could affect revenue if the client is lost or hinder a fintech's ability to fulfill its obligations with a community bank. Lastly, determine if the fintech is susceptible to external risks that may affect the fintech's financial condition.

Potential sources of information for financial institutions to review as part of the fintech's financial viability include: financial statements, auditors' opinions, annual reports, lists of funding sources, publicly available information on competitors, and information on the fintech's client base.



3. LEGAL AND REGULATORY COMPLIANCE

Financial institutions should evaluate a fintech's legal standing, its knowledge about legal and regulatory requirements, and its experience working within the legal and regulatory framework to determine if the fintech has the ability to comply with applicable laws and regulations.

The Office of the Comptroller of the Currency (OCC) issued FAQs to supplement OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance" to clarify its existing guidance and reflect evolving industry standards. FAQ#21 speaks to a financial institution's ability to outsource the development, maintenance, monitoring, and compliance responsibilities of its compliance management system. Financial institutions may outsource some or all aspects of their compliance management system to third parties, so long as the financial institution monitors and ensures that third parties comply with current and subsequent changes to consumer laws and regulations. Financial institutions cannot shift the compliance responsibility to third parties to avoid liability, fines, and penalties.

As part of its due diligence efforts, financial institutions should consider the following regulatory compliance considerations:

- Review the fintech's risk and compliance processes to determine its ability to support the financial institution's legal and regulatory requirements, including but not limited to privacy, consumer protections, fair lending, and anti-money laundering.
- Determine if the fintech has experience working with other financial institutions and if it is familiar with the institution's regulatory environment.
- Review information pertaining to any consumer facing applications, delivery channels, disclosures, and marketing materials to determine if there are any potential consumer compliance issues.
- Consider industry ratings and the nature of any complaints against the fintech, which can provide insight into potential customer-service and compliance issues or consumer protection matters.

Sources of information for regulatory considerations include policies, procedures, training materials, contract terms detailing legal and compliance performance responsibilities, information regarding customer-facing delivery channels or applications, marketing materials, disclosures, and consumer complaint processes and history.

Financial institutions should also consider the following legal considerations:

- Review organizational documents and business licenses, charters, and registrations, which provide information on where a fintech is domiciled and authorized to operate. These documents may also provide permissible activities under applicable governing laws and regulations.
- Review the nature of the proposed relationship to include roles and responsibilities of all parties to help the financial institution identify potential legal considerations.
- Assess any outstanding legal or regulatory issues in search of insight into a fintech's management, its operations, and its ability to provide certain activities, products, or services.

Source of information for legal considerations include charters, articles of incorporation, certificates of good standing, licenses, records related to patents and intellectual property, lawsuits, settlements, fines, consumer complaints and regulatory filings if a publicly traded company.

4. RISK MANAGEMENT AND CONTROLS

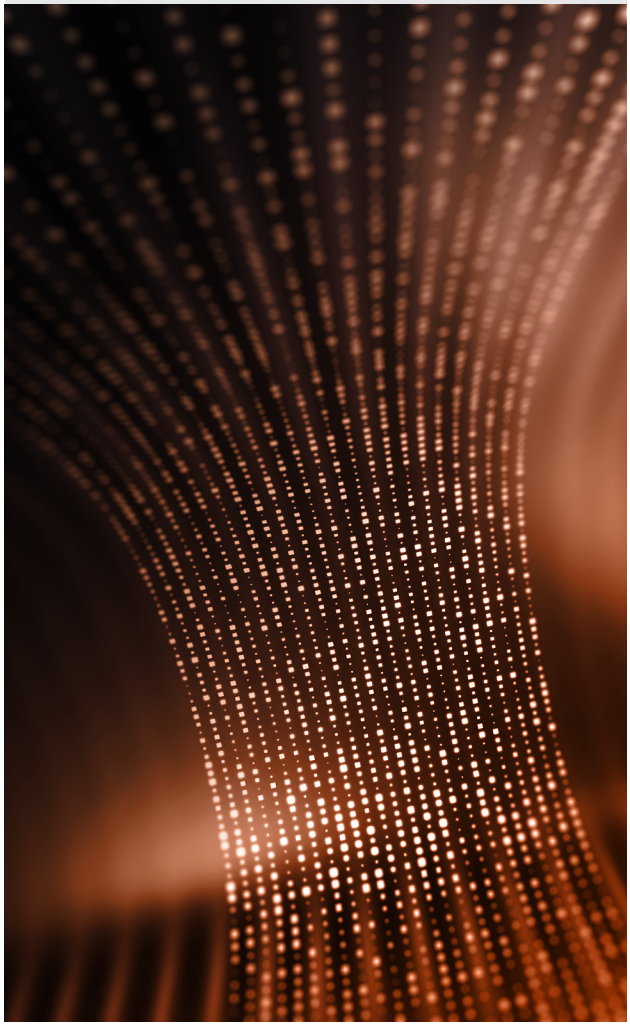
Due diligence for risk management and controls determines if the fintech can conduct the desired activity in a safe and sound manner, consistent with the financial institution's risk appetite and in compliance with applicable legal and regulatory considerations.

Financial institutions should review a fintech's policies and procedures for the desired activity to gather intelligence into how the fintech outlines its risk management responsibilities and reporting processes, and how the fintech's employees are responsible for complying with policies and procedures. Reviewing these documents will also assist a financial institution to determine whether the fintech is in line with its own risk appetite, policies, and procedures. Furthermore, financial institutions should look to the nature, scope, and frequency of controls reviews as part of its due diligence.

Financial institutions should evaluate the independence and qualifications of those that are part of the testing control. Regarding audits, look to see if the fintech has an in-house or outsourced audit function. Review the scope and results to determine if the fintech's risk management and controls are effective. Review any findings, conclusions, and action plans to determine if the fintech is responsive. Determine if the fintech's reporting would assist the financial institution in monitoring key risks, performance, and control indicators and whether such reporting processes would identify and escalate risk issues and control testing.

Staffing and training are a necessary component for any risk management and control processes due diligence efforts. Determine if the fintech's staff has the relevant expertise for the desired activity. Lastly, make sure the fintech has an adequate training program. The training goal should be to keep staff informed about regulatory requirements, risks, technology, and any other factors that may affect the quality of the desired activity.

Sources of information to assist with this due diligence aspect include but are not limited to relevant policies and procedures, information on staffing, recent audit reports, self-assessments, training materials and schedule, and project plans.



5. INFORMATION SECURITY

The Interagency Guidelines Establishing Information Security Standards set forth standards pursuant to section 39 of the Federal Deposit Insurance Act, 12 U.S.C. 1831p-1, and sections 501 and 505(b), 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act. The Interagency Guidelines also address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

Financial institutions should evaluate a fintech's information security measures to determine if it has processes in place for handling and protecting sensitive information pursuant to the proposed relationship and activity. Financial institutions should consider the fintech's security framework in place to manage cybersecurity risks – the security framework being its information security program.

Look to the fintech's information security control assessments to determine if the fintech identifies any weaknesses, mitigates such weaknesses or corrects vulnerabilities in its security program. Look to the program to see if the fintech can perform the desired activity in a safe and sound manner. Determine if the fintech trains and tests its employees and subcontractors on its information security program and processes. Does the fintech comply with safeguarding requirements and privacy and information security requirements? Lastly, does the fintech have solid incident response and notification procedures?

Potential sources of information include but are not limited to:

- Completed information security controls assessments
- Incident management and response policies
- Incident reports with post-mortem and remediation activities
- Information security policies
- Information security training programs
- Policies addressing safeguarding and privacy laws and regulations

A fintech's information systems should also be reviewed as part of the financial institution's due diligence. Financial institutions should understand the fintech's operations infrastructure and its security measures for managing operations risk. Financial institutions should determine if the fintech's existing security infrastructure is adequate for the desired activity or if the fintech would need to invest in additional IT resources to successfully perform the desired activity. Lastly, financial institutions should evaluate the fintech's procedures for deploying new hardware or software along with policy toward patching or using unsupported hardware or software which could create a potential security hazard.

Sources of information to evaluate include information technology policies, overview of the fintech's technology and processes supporting the desired activity, and controls or standards assessments.

6. OPERATIONAL RESILIENCE

Operational resilience identifies business continuity planning and incident response, service level agreements, and reliance on subcontractors as key components in a financial institution's due diligence.

Continuity planning and incident response due diligence should include:

- Evaluating the fintech's business continuity plan, incident response plan, disaster recovery plan, and related testing to determine the fintech's ability to continue operations in the event of disruption.
- Evaluating the fintech's recovery objectives, including any established recovery time objectives and recovery point objectives to determine whether the company's tolerances for downtime and data loss align with the financial institution's expectation.
- Addressing how a fintech considers changing operational resilience processes to account for changing conditions, threats, or incidents. Also consider how the fintech handles threat detection to determine incident preparation.
- Discussing responses to actual cyber events or operational outages and if there was any impact on other clients or customers.
- Knowing the locations of a fintech's data centers allows the financial institution to consider which laws and regulations would apply to the financial institution's business and customer data.
- Considering whether a fintech has appropriate insurance policies and whether the fintech has the financial ability to make the financial institution whole in the event of a loss.

Sources of documentation for business continuity and incident response evaluation include business continuity plans; disaster recovery plans; incident response plans; documented system backup processes; test results of business continuity, disaster recovery, and incident response plans; cybersecurity reports and audits; and insurance documents.

Financial institutions should review service level agreements between it and the fintech to ensure the rights are responsibilities of each party are set forth regarding expected activities and functions. Financial institutions may consider the reasonableness of the proposed service level agreement. Consideration should be given to incorporating performance standards to ensure key obligations are met. Also, consider whether defining default triggers and recourses in the event the fintech fails to meet performance standards should be included in the service level agreements, which should be reviewed by counsel experienced with such agreements prior to execution.

Lastly, financial institutions should know if the fintech intends to rely on subcontractors to meet any of its performance obligations. Ask if the fintech depends on a small number of contractors for operations and if so, what activities do the subcontractor provide. Inquire as to how the fintech will address a subcontractor's inability to perform. Lastly, consider if the fintech conducts background checks on subcontractors. Don't forget to incorporate any performance measures into the contract.

Potential sources of information for this due diligence aspect include the fintech's policies on outsourcing and its use of subcontractors, independent reports or certifications regarding contractors, and a listing of third parties used by the fintech.

CHALLENGES REGARDING DUE DILIGENCE

Some of the challenges around due diligence for any third-party vendor includes determining examiner expectations, starting the process, allocating resources, and obtaining needed documentation from the fintech. Examiners will expect the financial institution to evaluate risk in outsourcing activities, identify high risk vendors and conduct appropriate due diligence, know who their vendor's vendors are, and periodically review vendors based on risk as set forth in a financial institution's vendor management program.

If the financial institution is considering working with fintechs, the right consultants can help navigate entering into the relationship, due diligence, and ongoing relationship management.

As part of the due diligence, financial institutions should ensure the following contractual provisions during contract negotiations:

- Right to audit
- Measurable performance standards
- Contractual default and remedy for curing
- Rights and responsibilities of all parties
- Subcontractor requirements
- Liability limitations
- Business continuity testing
- Data governance
- Compliance responsibilities
- Security responsibilities
- Insurance responsibilities
- Contract term and renewals
- Termination rights

CONTACT

Becky Breland, Senior Consultant, Becky.Breland@capco.com

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy specializing in driving digital transformation in the financial services industry. With a growing client portfolio comprising of over 100 global organizations, Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to deliver end-to-end data-driven solutions and fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its Innovation Labs and award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Twitter, Facebook, YouTube, LinkedIn Instagram, and Xing.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
a wipro company