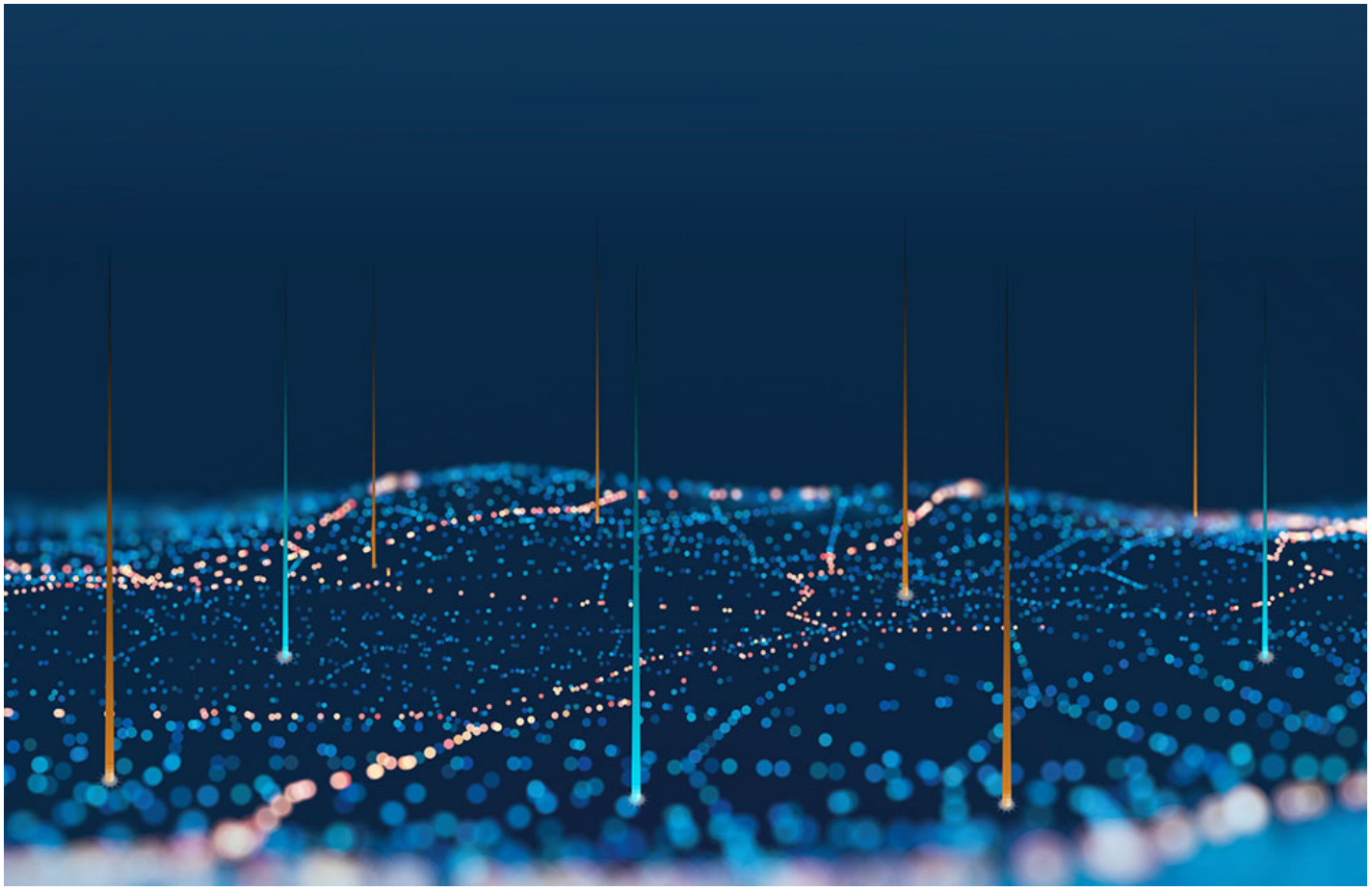
How to Help Your Fintech Partners Develop a COMPLIANCE ROADMAP

BY TRACEY LEVANDOSKI, CRCM



FINANCIAL TECHNOLOGY, OR FINTECH, continues to emerge with new products and services banks will undoubtedly want to explore through fintech partnerships. Bank compliance officers are well aware of the importance of an effective compliance management system (CMS) with regard to consumer protection and regulatory expectations. If the bank partners with fintechs to provide services to its customers, examiners expect the bank to manage these relationships just like any other third-party service provider. As the regulated entity in the relationship, the bank is ultimately responsible for ensuring its fintech partners have an effective CMS. However, the fintechs may not have a strong regulatory background or may have limited staffing resources to implement an effective CMS and may find themselves playing catch-up to meet expectations. Fintechs may need a roadmap to understand an effective path to building a compliance infrastructure. The destination is a fully functional, effective CMS that meets the regulators' requirements as well as the bank's expectations under its third-party risk management program. Depending on where the fintech partner is in its development cycle, the journey to

get there may take many detours. Bank management can take the driver's seat in creating a fintech compliance roadmap to help avoid wrong turns along the way.

The Fundamentals—Building the Infrastructure of the CMS

If you are already familiar with the fundamentals of an effective bank CMS, you know it has two interdependent control components:

1. Board and Management Oversight; and
2. Compliance Program, which includes:
    - Policies and procedures;
    - Training;
    - Monitoring and/or audit; and
    - Consumer complaint response.

The fintech's expected CMS should not vary significantly from the bank's program; it just needs to be tailored to the fintech's products, operations, and maturity level. If your fintech partner is a new player, it may not have the resources to execute or the transactional volumes to justify a fully functional CMS. Even if the fintech is more mature, it needs to make sure compliance staff are knowledgeable about applicable regulatory requirements as new product lines are added. In either case, focusing on the infrastructure can set the stage for the fintech to build its program and meet the bank's expectations.

Embarking on the Journey—Governance and Oversight

Banks are expected to have strong oversight by the Board of Directors. However, in a fintech's case, the Board may be comprised of the investors' principals who are focused on the financial performance of the company and far removed from general operations, including knowledge of the CMS. Board meetings may not occur on a regular or frequent basis. With these limitations, it may not be feasible for the fintech's compliance staff to have a direct connection with the Board. Even if this is the case, the fintech should still implement a governance body to oversee the CMS. This may be a committee comprised of the fintech's executive management or department heads. Regardless of the governance body's composition, a detailed charter should be ratified that includes the responsibilities under which the committee will operate covering all four elements of the compliance program.

In addition to the governance body for general oversight, the fintech should designate a compliance officer or specialist to oversee the day-to-day CMS activities and provide CMS-related reporting to the governance body.

On Ramp—CMS Policy

In conjunction with establishing the Oversight component, an overarching CMS policy should also be implemented which addresses each of the Compliance Program elements. Consider including the following sections at a minimum:

- Policies and Procedures—structure, review, and approval requirements
- Compliance Training
    - Minimum passing scores
    - New-hire training requirements
    - Frequency of ongoing training
    - Consequences of non-compliance
    - Management reporting and monitoring
- Monitoring, Testing, and Audit Program
    - Risk assessment requirements
    - Scope and frequency of reviews and audits
    - Methodology for selecting testing samples
    - Reporting requirements
    - Follow-up on remediation efforts
- Consumer Complaint Response Program
    - Definition of a complaint
    - Defined risk levels to be assigned to individual complaints
    - Resolution timelines based on assigned risk ratings
    - Analysis of complaints for trends, root-cause, and scope of accounts affected
    - Reporting requirements

While it may be advisable to perform baseline compliance testing for all areas included in the risk assessment during the first year of operation, continued testing should be completed based on the risk rating assigned during the risk assessment process.

In the developmental stage of the CMS policy, set forth the minimum requirements then build upon those as the CMS continues to grow. As the program matures, the fintech may find it more effective to have separate, more detailed policies for each of the areas of training, monitoring and audit, and complaint response to provide more comprehensive directives as indicated by the suggested elements outlined.

Detour—Define the Products

It may seem that the next logical step should be to create policies and procedures specific to the operations around the products or services to be offered. However, the fintech first needs to understand what regulatory requirements apply. Fintechs may be tempted to purchase an "off-the-shelf" policy program, but policies provided with such programs cover everything including the kitchen sink. Given its likely limited CMS resources, the fintech may not take the time to customize a template to its own needs, especially if management does not have a good understanding of what does apply. Therefore, before drafting policies, you should help your fintech partner create an "applicability matrix" for each of the applicable regulations. For example, if the product is a consumer credit card, the entirety of Regulation Z will not apply. By mining the regulation to be as granular as possible and identifying the sections that are applicable to and cover the full lifecycle of the product or service, policies and procedures will be more relevant.

CAUTION:

Depending on the complexity of the product or service, it may be advisable to seek legal counsel for assistance in completing the applicability matrix, especially as it relates to state consumer regulatory requirements.

As you assist with the creation of the applicability matrix, be aware of terminology the fintech uses that may differ from regulatory requirements. An example we often see is the use of the terms "cancelled" or "withdrawn" with regard to credit applications. If an application is initiated but the consumer never returns to complete it, the fintech may code it as "cancelled" when it is incomplete which requires notification under Regulation B. The fintech may also "withdraw" the application, a term which has its own Regulation B definition, rather than sending a notice of incompleteness.

Roadwork Ahead—Policies and Procedures

Now that the applicable sections of the regulations have been identified, the fintech's next step should be to build the policies that address those sections. A best practice would be to use a consistent policy template that incorporates the following elements at a minimum:

- Statement of purpose
- Scope
- Policy statements
- Policy ownership

- Roles and responsibilities
- Frequency of auditing or monitoring for compliance with the policy
- Training requirements applicable to the policy
- Record retention
- Version control which maintains the policy's implementation date, date of most recent approval, and brief history of revisions made since the policy's inception

In conjunction with policies, which should set forth the broad policy statements, procedures should also be drafted that drill deeper down into the nuts and bolts of the operation. The goal of a company's policy and procedure library should be that a new employee could read the documents and know what to do without significant additional guidance.

CAUTION:

Sometimes we see a set of policies and procedures that do not reflect the company's actual practices. Be sure your fintech partner's policies and procedures are living documents and revised as necessary when circumstances warrant such as the introduction of new products or services and new or amended regulations.

"Technology" is part of the fintech abbreviation, so it stands to reason that technology is the center of focus for generating and retaining electronic transaction records. However, bank management should work with fintech management early in the relationship to determine how record retention will be addressed. Reliance on electronic storage can create record retention issues if systems are not tested to determine that documents and disclosures can be recreated for review during audits and examinations. Often times, raw data is retained, but the actual documents are not. Keep in mind you will need to be able to prove how the consumer received and viewed documents, so be sure to test the fintech's processes for demonstrating this and recreating the documents.

Roadwork Ahead—Compliance Training

The fintech's management and staff should receive specific, comprehensive training that reinforces policies and procedures and is tailored to each staff member's responsibilities. Training is another area in which the fintech can purchase an off-the-shelf program from one of the online platform providers. However, if the course offerings are not detailed enough to cover the compliance requirements of the company's products and services, such a platform may not be adequate to meet the company's needs. Referring to the applicability matrix, it may be necessary to compare course offerings to determine the best platform. More generic courses can be supplemented with customized courses created with the assistance of the bank or another third party. After the training platform has been selected, the training program should be established as outlined in the CMS policy.

Speedbump—Consumer Compliance Response Program

All institutions are hopeful that a minimum number of consumer complaints are received related to any aspect of the bank's business. However, just like the bank has a consumer complaint response program in place, so should the fintech. Fintech employees should be trained on the company's complaint response policies and procedures before the first day of production. You can assist with this by helping the fintech define what will be considered a complaint, how complaints should be categorized by risk level, resolution periods, and mechanisms in place for reporting and logging complaints. The fintech's complaint program should mirror the bank's program to facilitate the integration of the fintech's complaint log into the bank's log for root cause analysis, trend analysis, and management reporting.

Going the Distance—Ongoing Reporting to the Governance Body and the Bank

After the infrastructure has been put in place, fintech management should establish a reporting template that covers all areas of the CMS. Reports should be presented on an established schedule to keep the governance body informed about the company's compliance program. The bank may require periodic reporting as well, so be sure to set the expectations for CMS reporting early in the partnership.

Beyond the Fundamentals—Continuing the Journey

The fundamentals as outlined above ideally should be in place at the outset of the partnership. As production volumes increase and the partnership matures, the bank will want to help the fintech build out the remainder of its CMS and set the stage for ongoing maintenance. Roadwork Ahead—Compliance Risk Assessment Referring once again to the applicability matrix, use it as a framework for generating the fintech's compliance risk assessment. Be sure to factor in the inherent risk and internal controls to arrive at the aggregate (residual) risk for each area assessed. Use the risk assessment as the basis for the monitoring, testing, and audit schedules.

Roadwork Ahead—Monitoring/Testing/Audit

Establish a monitoring and testing program as outlined in the CMS policy using the applicability matrix and compliance risk assessment as a guide. The bank may want to help the fintech identify the sections of the applicability matrix in which first line of defense monitoring can be completed within the department responsible for the operations. For second line of defense testing, particularly within fintechs whose compliance departments are not fully staffed or in the early stages of development, the bank may need to help the fintech identify individuals within the company who can assist with testing. The bank may even need to provide supplemental second line of defense testing on a temporary basis until the fintech is adequately staffed to complete the testing internally.

While it may be advisable to perform baseline compliance testing for all areas included in the risk assessment during the first year of operation, continued testing should be completed based on the risk rating assigned during the risk assessment process. Be sure to define testing frequencies based on the

risk rating. If the aggregate risk rating for a particular area is "high," that area should be tested more frequently than an area risk rated as "moderate" or "low."

After the testing schedule has been established, the next step is to create testing scripts and templates as well as a consistent reporting mechanism for each area identified in the applicability matrix. For the testing scripts, a good place to start is to use the examination procedures issued by the regulatory agencies. However, be sure to customize to the specific sections of the regulations applicable to the fintech's operations. Consideration should also be given to ongoing follow-up when corrective action is required based on testing results. An industry best practice is to implement an "issues tracking" log which provides a summary of the findings, action to be taken, due date, and department or person responsible. Compliance staff should review the log periodically and perform additional testing to ensure corrective action is being completed timely and effectively. All significant issues being tracked should be shared periodically with the governance body established within the fintech.

Bank management will need to determine if the fintech will be required to undergo periodic CMS audits as part of the third line of defense. If the fintech has its own internal audit department, it may be able to establish any required audits internally, or more likely, the fintech will have to look to a third-party audit firm for audit requirements. In either case, the bank should provide the fintech with audit guidance which establishes the bank's expectations for minimum requirements to be included in a CMS audit.

CAUTION:

Banking partners should be as specific as possible with audit guidance, including any minimum transaction testing requirements, especially if the fintech is early in its development and will need to seek third-party assistance. Fintech management may not know what to request in the statement of work which can result in payment for unneeded services at a time when financial resources may already be stressed.

Roadwork Ahead—Third-Party Risk Management

Just as the bank is expected to have a third-party risk management program, the fintech should also establish a program which includes all the same elements such as a detailed policy and defined vendor risk ratings to direct the level of initial and ongoing due diligence. Review of the third-party risk management program should also be considered in the monitoring and testing program.

Going the Distance—Change Management

As the fintech matures, change management policies and procedures are essential to outline actions to be taken as the business evolves or as external factors impact operations. At a minimum, change management policies and procedures should consider all business lines to be impacted and include due diligence in advance of proposed or required changes considering the entire life cycle of the product or service impacted. Additionally, postimplementation reviews should occur to ensure actions taken achieved the desired results.

Going the Distance—Ongoing CMS Evaluations and Adjustments

Now that an effective CMS has been established, reinforce the need for continued process improvement with your fintech partner. If a change is required anywhere in the product or service life cycle, run through all the stops on the roadmap and determine any adjustments to be made. Consider the CMS as a circular process. If a change was made to a policy or procedure, additional training may be required outside of the established training schedule, and additional or more frequent monitoring or testing may be prudent. If significant findings are noted during testing activities, audits, or examinations, changes to policies or procedures may be necessary. In addition, remedial training may be required, and the testing schedule for that area may need to be accelerated until corrective action has proven effective. In all cases for which changes need to be made to the CMS, the changes should be included in the periodic reporting to the governance body and the bank, and updates to the risk assessment might be warranted, as well. Even if there are no changes, the risk assessment should be refreshed annually. Additionally, policies should be reviewed and approved annually.

Conclusion

With so many considerations in the development and maintenance of a CMS, your fintech partner's management team can quickly become overwhelmed, given all the other elements they are tackling during the early stages of the partnership. If the team is unfamiliar with the bank's regulatory environment, that adds more stress, and they will look to the bank to help overcome the challenges involved in implementing an effective program. Providing a thoughtful roadmap as outlined herein can make the journey a little easier for both the bank and the fintech.

ABOUT THE AUTHOR

TRACEY LEVANDOSKI, CRCM, is a director at CrossCheck Compliance LLC, and a regulatory compliance and risk management professional with over 30 years of experience in the financial services industry. Having worked as both a prudential regulator and in banking institutions, Tracey has demonstrated expertise in compliance and the Community Reinvestment Act (CRA). Her expertise includes extensive knowledge of lending and deposit regulations, including fintech lending operations and the bank partner model. She is also experienced in financial institution accounting and operations. Tracey can be reached at **tlevandoski@crosscheckcompliance.com**.