Fintech Operations
Having explored risk from both an internal and external perspective, we are now turning to the topic of internal operations. The key operational categories explored below are key to helping Fintechs and their Issuing Bank Partners stay on the right side of regulators and making the Fintech Program a success. These operations are also part of what the Fintech's Issuing Bank Partner assesses through continuous communication and audits.

Because we have limited space, this is a 'taster' and is in no way complete. This article is divided into four main topics: Policies and Procedures; Disaster Recovery; BSA/AML/CTF/Cybersecurity; and Data Management.

Policies and Procedures
Policies and Procedures form your guardrails; they direct what you do and how you do it. The very act of creating your policies and procedures can help clarify your vision when setting up your Program. Policies must adhere to the regulations and laws governing Fintechs and their Banks. Policies incorporate regulations, showing how a Fintech is going to meet their legal obligations. For example, a comprehensive BSA policy incorporates the Bank Secrecy Act, the Currency and Foreign Transactions Reporting Act of 1970, the USA PATRIOT Act, and the AMLA 2020 Act, along with measures to ensure compliance with the Department of Treasury's Office of Foreign Assets Control (OFAC). Some are specific to one topic, such as a Privacy Policy, but even with a single focus policies can still incorporate multiple laws and regulations. Privacy, for example, will encompass the Gramm-Leach-Bliley Act (GLBA) and Federal Trade Commission (FTC) regulations, along with the Children's Online Privacy Protection Act (COPPA), and relevant state laws such as the California Consumer Privacy Act (CCPA).

While your policies reflect the 'what' of your Program - debit, credit, prepaid, specific customer profile - the Procedures are the "how." Once you have written your policies - typically between 20 to 40 policies per program[1] - you need to create your procedures. How will you ensure that your policies are put into action appropriately? What specific tasks, processes, and workflows will be implemented to ensure uniformity across your program? These are usually accompanied by training and give your staff the necessary detail of how to complete their jobs in line with the policies you have set.

A Program is required to submit its policies for their Issuing Bank Partner's review and approval and it is best practice for an Issuing Partner Bank to also request, review, and approve related procedures. This ensures adequate safeguards are in place and that the procedures support the policies, as approved. Once initial approval is received, policies and their associated procedures should be reviewed annually, or more frequently if changes to the program and/or its operations are made.

Disaster Recovery & Business Continuity
Like Fraud, disasters are things you hope won't happen to you but must be planned for. These can range from natural disasters, cyber events, or human made events but all types interrupt a

[1] The number can vary depending on whether multiple topics are included in a single policy, or whether you choose to create separate policies by regulation. A Fintech will be guided by their Issuing Bank Partner on how the Bank wants to see the policies completed.

Program's operations. Some may be specific to one Program; others may have a broader impact, affecting a region or the financial sector as a whole. The purpose of a Program's Disaster Recovery/Business Continuity Plan (DR/BCP) is to ensure the Program has a good chance of surviving extended service outages caused by factors beyond its control, and to restore services as quickly as possible. These plans should include all departments and cover technology, business operations, testing, and communication strategies critical to the continuity of the entire Program, including safeguarding employees, customers, products, and services. Additionally, think of a Business Continuity Plan as not just something for managing a disaster, but also to ensure ongoing maintenance of systems and controls for the resilience of operations.

A Program's DR/BCP should be aligned with the Program's risk appetite, strategic goals and objectives, and should be supported by a Business Impact Analysis (BIA) that identifies critical functions, analyzes interdependencies, and assesses impacts.

Once the DR/BCP is in place, remember to train your people and test, test, test the plan! This way, when disaster strikes, everyone will know what to do to get you up and running again in an efficient and effective manner.

BSA/AML/CTF/Cyber Security

Fintech companies are required to adhere to AML and CTF regulations established by international bodies like the Financial Action Task Force (FATF). The goal is to prevent illegal activities, such as money laundering and terrorist financing. To achieve this goal, Fintech companies must implement procedures to verify the identities of their customers by collecting and verifying personal information. In addition to that, continuous monitoring of transactions is necessary to detect and report suspicious activities. Companies must also maintain detailed records of transactions and customer information for regulatory review and audits.

Compliance with data protection laws, such as the General Data Protection Regulation (GDPR) in Europe, and the California Consumer Privacy Act (CCPA) in the U.S., is crucial for Fintech companies. Companies must ensure that personal and financial data are handled, stored, and processed securely, using encryption and other security measures to protect data from unauthorized access and breaches. Robust cybersecurity measures must be implemented to protect against data breaches and establish procedures for responding to security incidents. This also includes notifying affected individuals and regulatory authorities in the event of a breach. Companies must conduct regular security audits and risk assessments to identify and mitigate potential vulnerabilities.

Data Management

Fintech is an industry where data is the main asset that drives informed strategic decisions and fuels growth. From the moment data is collected, it starts its transformative journey from raw numbers to insights. It's stored, utilized, and analyzed to help Fintech vendors outperform competitors, improve user experience, increase operational efficiency, access credit risk, etc. The more seriously vendors treat data management, the more value they can extract from the numbers gathered.

Neglecting the data management aspect, in turn, can lead to ineffective use of resources,

missed business opportunities, and wrong business decisions. Fintech companies should lay the ground for risk-free and effective data management by leveraging the industry's best practices and tips to prevent this from happening.

Some common challenges in Fintech data management are Data Silos, Data Quality, Legacy Systems, Data Privacy and Compliance, and Scalability.

To improve data collection and storage in Fintech data management one or more of the following strategies can be used.

- Flexible data architecture and data sharing enhances decision-making by offering a comprehensive view of business results, processes, and operations.
- Shift to cloud-based solutions brings about cost savings and speed improvements for Fintech services.
- Robust data governance ensures accountability by verifying data accuracy, transparency, and adherence to regulations, which are all vital for informed decision-making.
- Data cataloging is valuable for the Fintech industry as it enhances data management processes. Data catalogs improve data accessibility and promote teamwork. Successful implementation leads to faster data analysis, increased engagement, and decreased cost of development.

With all of the above in place you will be well on your way to having a solid foundation that will serve you well as you develop your Program, and give your Issuing Bank Partner confidence that you know what you are doing and that, together, you will be successful. Of course, plans are just plans, the hard work starts after the plans are made and your doors, whether real or virtual, are open for business!

Check in next week for a discussion on turning data into valuable information

---

This is the fourth in a series of collaborative articles by iLEX Consulting Group and iDENTIFY

About iLEX

Since 2012, iLEX Group LLC has been a leader in delivering expertise in the FinTech industry, with a robust background in compliance, operations, and client management. We bring our client's visions to life with our ingenuity, partners, resources, and leadership.

About iDENTIFY iDENTIFY has become a leading fintech software company by providing banks with the tools necessary to unify their customer data. With several years of providing solutions for the banking industry, our vision is to streamline internal operations, create convenience for our clients, and give banks faster-to-market solutions.