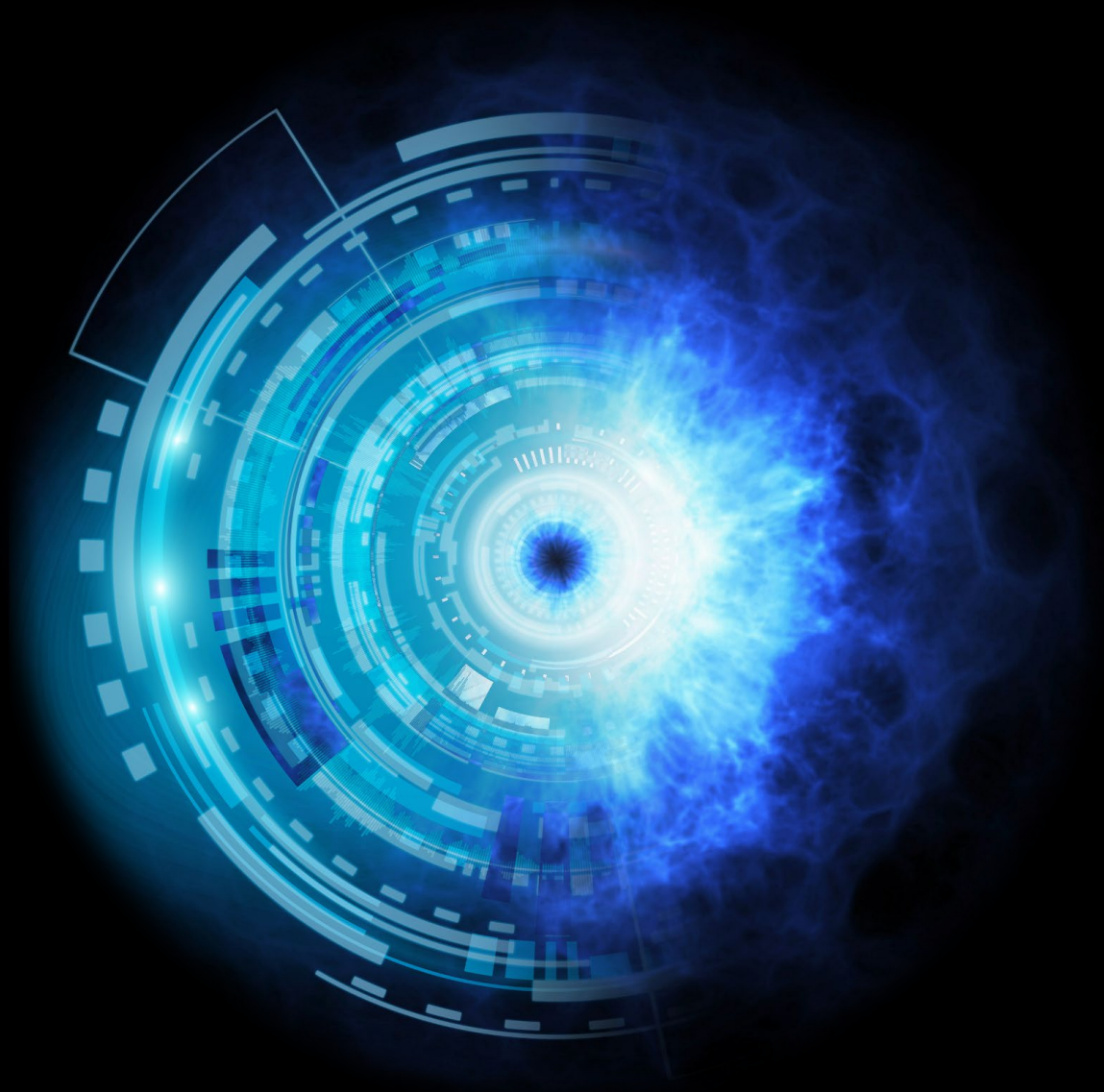
Deloitte.



Fintech risk and compliance management

A framework to empower the organization

The financial technology (fintech) industry continues to invest in innovations that create exciting new products and support evolving customer preferences. Emerging technologies such as artificial intelligence, robotics, and machine learning are increasingly the core elements of fintechs' product portfolios and customer interactions. In addition, many fintechs find themselves optimizing their business model by way of new products or services in response to customer needs, and in their partnerships with more regulated firms (e.g., banks and insurance companies).

Evolving fintech risk management functions are tasked with addressing the potential exposures created by their innovation, partnerships, and ongoing financial and regulatory market developments. Consistent with this, there is increasing pressure for fintech firms to elevate their risk management capabilities, including the development of a responsive operational risk and compliance program. As these capabilities evolve, the callout of roles and responsibilities is occurring with a delineation of a more traditional "three lines of defense" financial service model.

One source of such pressure is regulator expectations: in a recently published report,[1] the OCC (Office of the Comptroller of the Currency) urges traditional financial institutions to consider risk assessing and managing the impact of fintechs on their organizations. This points to a broader concept discussed in our previous point of view[2] that regulators continue to emphasize the importance of fintechs on the financial ecosystem—be it as a standalone organization, as a third-party service provider, or a partner. By looking to financial institutions to risk assess fintechs, regulators like the OCC are indirectly placing some of their regulatory requirements on fintechs via their expectations of the institutions they regulate. In response, many fintechs are working to achieve robust risk and compliance capabilities.

Like other investments, effective risk and compliance management spend involves a cost-benefit analysis; however, regulatory compliance is sometimes hard to measure until noncompliance becomes apparent to the public and regulators. As fintechs continue to gain momentum and attention from regulators, they should have risk and compliance capabilities that scale with their operations and strategy. For example, fintech lenders went from the lowest volume of origination to the highest volume of origination in the unsecured personal lending market in just over three years and show signs of increased participation in other areas of financial services, including mortgage, commercial, other retail, and small business lending[3]. In this third and final point of view on risk management considerations for fintechs, we outline six steps that fintechs can take to ramp up a comprehensive and fit-for-purpose program.

Elements of a broad-based risk management approach

Fintechs that have interest in becoming a bank, expanding their portfolio of bank-like products and services, or partnering with more traditional financial services firms will be expected by regulators to have a risk and compliance framework that sufficiently addresses their inherent risks as generated by their book of business. In general, some of these risks would include but not be limited to anti–money laundering for marketplace firms, or the potential for misrepresentation in disclosures and marketing material for lending and wealth services firms. When risk and compliance programs are effected correctly by a fintech, they can be a revenue enabler and may put them in an advantageous position to collaborate with banks and other traditional financial service institutions who are required to have robust risk management practices in place. Fintechs can "get it right" and potentially save costs by taking advantage of synergies between and among risk domains and designing their capabilities to cut across them as outlined below.

The three lines of defense

1. **First line of defense** is the busness, who owns the risks as generated by their operating business as well as the controls to mitigate those risks
2. **Second line of defense** is risk management who provides the framework by which the first line is able to effect the control of risks. Risk managemt oversees the first line's execution of the framework and provides effective challenge to the business
3. **Third line of defense** is internal audit whose remit is direct from the board to audit the processes and policies as effected.

Figure 1. Risk & Compliance program framework

Risk & compliance program framework

Figure 1 portrays a risk and compliance program framework derived from regulatory expectations that consists of capabilities responsive to the inherent risk of the operating business.

- **People and culture:** The risk and compliance management program aligns with company culture and can be operationalized to meet regulatory and industry expectations. Company culture empowers its people to effect proper risk management and achieve business objectives
- **Business risk strategy:** Risk and compliance strategy are aligned to the business's strategy, with risk management having a seat at the table. Risk management has a view and advises the business, management, and board on its strategy
- **Governance and policy:** Clear and well-articulated roles, responsibilities, and decision rights support the risk culture and strategy. Established committees with defined mandate of advising and/or decisioning and the genesis of their remittance are well understood. Policy framework is in place and implemented effectively, aligning to culture, strategy, regulatory requirements (e.g., as in the case of a payments business, compliance with state money transmission regulations), and sound risk management practices
- **Risk assessment and regulatory change:** Control identification and implementation, combined with an understanding of regulatory requirements, exist within a successful customer journey. Associated control vulnerabilities and applicable regulatory obligations are known, controlled, and follow an established change process
- **Monitoring and testing:** A controls testing and monitoring program for at minimum high-risk activities with applicable reporting of risks and issues is established. Further development and implementation of key performance indicators (KPIs) and key risk indicators (KRIs) are monitored with defined thresholds
- **Data capture:** Consistent capture, measurement, and reporting of data that informs management and board for decisioning is in place
- **Issue management:** Issues decisioned at various levels, including the business, risk management, executive management, and board, are identified, escalated, and remediated. Focus is on the early identification of systemic/thematic issue and resolution of issues to sustainability

- **Awareness and training:** The training program includes risk management–related trainings applicable across businesses and the firm more broadly (e.g., segregation of duties and PATRIOT Act)
- **Regulatory interaction:** Internal coordination of communication and messaging to requisite regulators (e.g., state regulators, attorney generals, Federal Trade Commission, and Consumer Financial Protection Bureau) that is consistent and accurately reflects business and risk performance and strategy execution. In addition, capabilities are in place for ready responsiveness to regulatory exams and requests

Using this type of framework as a guide, fintechs can tailor for their needs a broad-based risk management program:

Step #1
Define roles and responsibilities through a governance model

A defined risk and compliance governance program can establish minimum standards and guidelines for committee activities, including the development of committee charters and templates for meeting agendas and minutes. Such a consistent construct can support committee design and alignment with the organization's risks, as well as allow for efficient committee oversight for those risks (e.g., through establishing and monitoring the organization's risk appetite). A governance model can also empower the organization and committees to determine how much risk the fintech is willing to onboard, as in the case of fraud risk, and at what transaction level and/or dollar threshold such risk is not sustainable or desirable for the company to do business. Selection of relevant committee members with knowledge of the subject matter can help ensure the integrity of the committee.

Step #2
Understand applicable risks and rank them

Like financial institutions, fintechs are subject to multiple risk types, including credit, liquidity, operational, compliance, and reputation. To that end, attention should be given to identifying and scoring the inherent risks specific to activities undertaken. Business managers across the organization can outline the risks related to activities in their part of the organization. An example of a more comprehensive and advanced technique is to identify and map critical business processes, noting operational vulnerabilities and regulatory requirements. Further, the nature of a business and its operations will highlight certain risks as more critical than others. Risk scoring or ranking them can promote a more transparent and consistent prioritization process that can help determine risk treatment decisions collaboratively with executive management and help action and prioritize critical risks.

Step #3
Evaluate the controls environment

Once the fintech understands the risks unique to its products and services and evaluates them according to its risk ranking methodology and framework, the next step is to determine what controls are in place to address exposures and identify gaps. A common methodology within the financial services industry is to complete a risk and control self-assessment (RCSA), which allows a business to determine the current state of its control environment by evaluating existing (formally and/or informally documented) controls for design and operational effectiveness. The RCSA process can help identify control vulnerabilities and missing controls and provide the opportunity for the business to evaluate whether a control should be created or if the residual risk can be mitigated by other existing controls or accepted as part of their

overall risk appetite thresholds. Efficiencies can be gained in this process if a common risk taxonomy is developed and used to evaluate and measure controls.

Step #4
Evaluate risk and response options

Once risk assessments have been conducted, risk professionals can review the results for consistency and accuracy of ratings, as well as the scope and coverage of the identified controls, based on their understanding of the greater organization. They can then aggregate the assessments to identify common findings across business lines and find singular solutions.

Once the commonality of issues is identified, the results can be aggregated by theme. Over time, trending analyses can be performed to identify instances of both increasing and decreasing risk. This can inform trends, emerging risks, testing plans, and resource management and deployment.

Step #5
Consider the organization's maturity level and technology use

Risk and compliance maturity can be evaluated based on three classifications: existing, evolving, and mature.

An existing designation means the organization is meeting core risk and compliance requirements and expectations and has a basic operating model in place with identified roles and responsibilities. Methodologies and processes, although they may be manual in nature, exist to evaluate and remediate any risk challenges.

Evolving organizations may utilize a common risk taxonomy to enhance synergies between operations and risk functions, leading to improved efficiencies and rationalized oversight. Process, risk, and control mapping is at a point of maturity where the organization uses this construct to proactively identify vulnerabilities and noncompliance so they can be mitigated properly.

Mature organizations have advanced oversight and execution processes, defined reliance models, and a clear vision and strategy embedded across the organization driven by measurable KRI results. Tools such as a Governance, Risk and Compliance (GRC) platform enable consistent and repeatable risk management activities, which add to the overall strength of the control environment.

Step #6
Engage management through effective reporting and communication

With the risk and compliance management program up and running, the management team can begin to formalize the metrics by which they measure their risk management practices. Thresholds and tolerance levels are established, which translate into KRIs to primary stakeholders, including executive management, the board, shareholders, and regulators. Leading functional units can then seek to strike a balance between broad value for the organization and fiduciary responsibility under their respective regulatory obligations.

An effective, forward-looking approach

As fintechs evolve and grow, they are faced with the challenge of keeping current their risk and compliance capabilities commensurate with their business operations and strategy. Limitations to capital and manpower exacerbate this challenge, but fintechs can respond effectively by establishing a risk framework that enables their operating model. The suggested risk and compliance framework provides needed structure while allowing for transparency and effective cost decisioning and efficiency so fintechs can continue their market disruption while adapting to ever-increasing expectations of risk management, accountability, and compliance.

Endnotes

1. Office of the Comptroller of the Currency, *Semiannual Risk Perspective for Spring 2019*, https://www.occ.gov/publications/publications-by-type/semiannual-risk-perspective/pub-semiannual-risk-perspective-spring-2019.pdf
2. Deloitte Center for Regulatory Strategy, Americas, *The future of fintechs: Risk and regulatory compliance*, https://www2.deloitte.com/us/en/pages/regulatory/articles/future-of-fintechs-risk-and-regulatory-compliance.html
3. OCC, *Semiannual Risk Perspective.*

Contacts

Peter Reynolds
Managing Director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 212 313 1660
pereynolds@deloitte.com

Gina Primeaux
Principal
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 714 436 7341
gprimeaux@deloitte.com

Harish Dakshina
Senior Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 404 388 2898
hdakshina@deloitte.com

Amanda Williamson
Senior Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 704 887 2069
amawilliamson@deloitte.com

James D Simpson
Senior Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 816 881 5197
jasimpson@deloitte.com

Tara Wensel
Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 347 224 4056
tawensel@deloitte.com

Deloitte.