POLICY & MEDICINE
COMPLIANCE UPDATE
Reprinted from
Volume 4.9 | September 2018

Where is the Grass Greener?

Banking or Life Science Compliance Part II

*By Jenny McVey, Ph.D.**

Summary: In the August issue of the Update, we discussed key regulatory mandates that large banks are expected to adhere to. Although the overall principles of banking compliance mirror that of the life science industry, there is a concerted emphasis around the engagement, responsibility, and accountability of a bank's Board of Directors, which is unseen within life sciences. This article discusses how large banks operationalize regulatory mandates by reviewing the organizational structure of a compliance function within a bank.

In last month's edition of the *Update*, we discussed the efforts banking regulators have been focusing on around enterprise-wide risk management to avoid another crisis.[1] "*Where is the Grass Greener? Banking or Life Science Compliance*" touched upon key regulatory guidance and compliance mandates for the financial services industry. This month we continue our discussion by examining how large and complex banks have structured and operationalized compliance within their organizations to meet regulatory mandates.[2]

Risk Management Framework

The financial services industry operates in a fiercely dynamic regulatory environment, influenced by emerging technology, market globalization, industry consolidation, as well as competitive services and products. It also performs a crucial role in maintaining financial stability and driving economic growth that is central to overall economic health. Therefore, it is no surprise that scrutiny given to managing and controlling risk has been constant and continues to increase, especially since the 2008 global financial crisis.

As discussed in our last article, banking risk management frameworks are required to be designed by an independent risk management function, approved by the institution's Board of Directors, reviewed annually and updated to reflect changes in the regulatory environment or business activities. These frameworks should cover a broad category of risk such as credit, earnings, operational, interest rate, capital, liquidity, pricing, strategic, reputational, and compliance.

As a result, financial services organizations consider corporate compliance as one of its multiple risk functions, and compliance is therefore typically woven into a bank's overall risk management framework. As in any industry, the compliance function has the responsibility to establish a company-wide compliance program and policies and sets the standards for compliance monitoring and testing, and reports compliance issues on an aggregate basis. For banks, the responsibility to manage day-to-day compliance risk, as with other risk categories, falls on the shoulders of the three lines of defense.

The Three Lines of Defense

Fundamental to the design and implementation of the overall risk management framework, the 'lines of defense' are structured with the intention to focus on the broad categories of risk, which includes compliance, and identifies responsibilities of different parts of an institution to address and manage potential risks. To summarize:

The First Line of Defense ("FLOD") refers to the business or functional units. The FLOD is responsible for 'owning' and managing the risk that incurs through its business activities and is responsible for aligning overall business risk assessments with components of the compliance program. From an operational standpoint, the FLOD develops and adheres to set standards and policies

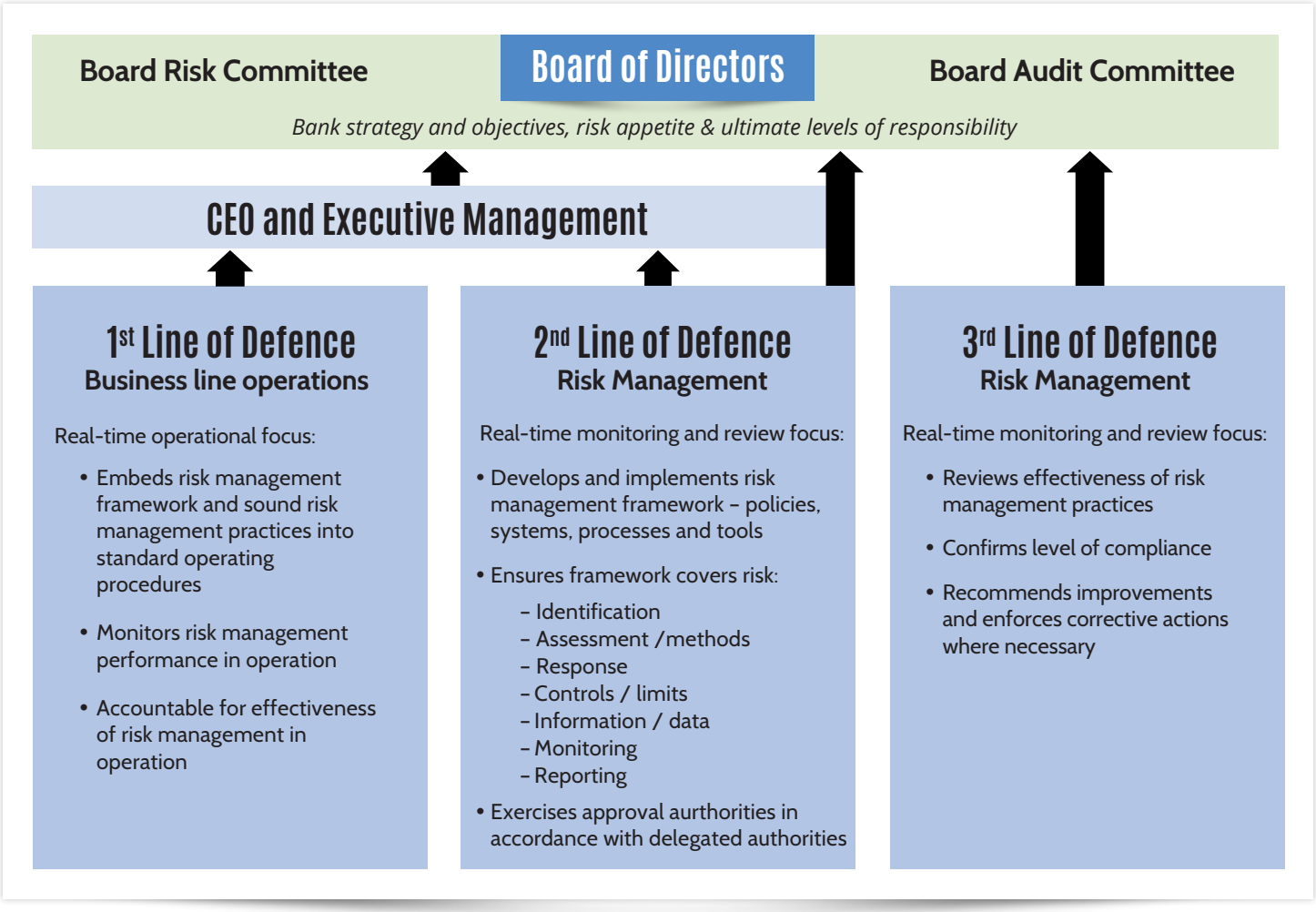
that are relevant to their respective business area and in line with the organization's risk appetite. This means that the FLOD is typically responsible for defining, developing and implementing key compliance controls and activities, and remediates control failures or compliance breaches. Of course, the level of granularity is variable organization to organization, and generally, these responsibilities are rarely delegated outside of the business unit.

The Second Line of Defense ("SLOD") refers to the risk management function, which may include the organization's compliance function that is independent of the FLOD and is responsible for further identifying, assessing, measuring, monitoring, and reporting risk on an enterprise-wide level. The SLOD defines and develops core compliance standards, activities and policies by which the FLOD further builds upon for their respective business activities. Typically, we see the SLOD assessing the overall design and monitoring of controls and failures, as well as reporting on control failure and compliance breaches.

The Third Line of Defense ("Third Line") is the internal audit function, which is charged with conducting risk-based audits and reviews, part of which assesses the effectiveness of company governance, risk management, and internal controls, and evaluates compliance with laws and regulations and identifies.

The International Finance Corporation ("IFC")[3] offers high-level best-practices of how banks may structure their organizations. As can be seen in Figure 1, the FLOD reports compliance matters directly to an executive or senior management, which is typically comprised of committees that focus on specific risk areas and are responsible for

FIGURE 1: *High-level organization of three lines of defense[7] as presented by the International Finance Corporation.*



setting risk limits within the corporation's overall risk appetite and tolerance limits. Depending on the organization, the compliance function and the Third Line may report directly to Board committees, which, like the executive committees, are developed to focus on specific areas of risk (Figure 2).

Managing Compliance by Committee

As discussed previously, the accountability of the Board goes beyond demonstrating support and commitment and necessitates responsibility for key aspects of compliance.[4] This includes setting and communicating clear expectations about compliance, and reviewing, approving, and adopting clear key compliance policy statements. Simply put, the Board is responsible for overall oversight and approval of the Framework. This is very different than what we experience in the life science industry, where banking regulators impose many governance standards and expectations on the Board.

It is not unusual for large banks to have several senior management committees managing compliance,[5] aggregating and reporting significant compliance matters along with the effectiveness of the risk management framework, to the Board. Having multiple and focused committees allows the Board to fulfill regulatory mandates to be more involved in the oversight of the effectiveness of overall risk management,[5] such as "reviewing, approving, and adopting clear key compliance policy statements."[6]

Organizational Structure

Where does compliance reside?

Similar to life sciences, compliance functions within the financial services industry vary significantly in structure between organizations. For example, in large banks, compliance leads, and staff may reside in the business or functional area, while the compliance function in smaller institutions may be centrally located within one area. Additionally, in some organizations, stand-alone units can be established for focused risk areas such as anti-money laundering and sanctions, terrorist financing, and privacy.

The positioning compliance functions within the banking organization continues to evolve. To meet regulatory and compliance demands, global banks have shifted their compliance functions to become either integrated as part of their risk management functional area, or as a stand-alone function.[9] Either structure lends to establishing compliance as a focused and core area within the organization and

FIGURE 2: *High-level risk governance structure as presented by the IFC.[8] The risk management department, which in this model, includes the compliance function, identifies, assesses, monitors, and mitigates risk, while the business units are responsible for day-to-day risk management.*

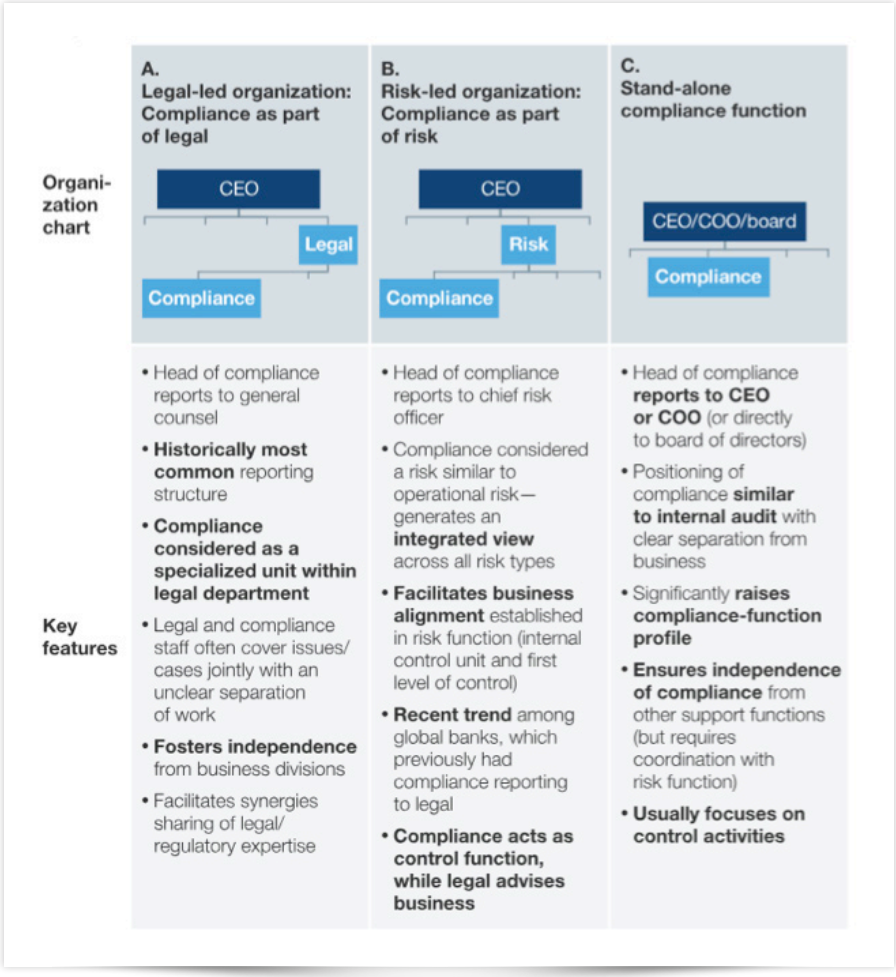
demonstrates the commitment to doing business 'the right way.' McKinsey clearly outlined three common types of organizational compliance structures:[10]

A. **Legal-led compliance:** Within this 'historical' structure, compliance is part of the organization's legal function, where the head of compliance reports to general counsel, who then may report to the CEO.

B. **Risk Management-led compliance:** This model is where many large banks are migrating towards, where the head of compliance may report to the Chief Risk Officer, and acts as a control function, independent from the lines of business.

C. **Stand-alone compliance:** Life science compliance professionals are familiar with this model, where the head of compliance may report directly to the CEO or COO, or to the Board.

Similar to maturing life science companies, global banks have moved away from compliance residing within the legal function as companies continue to seek effective risk mitigation. Banking compliance functions are trending to be more part of the overall risk management function. This allows compliance to have an integrated view across all risk types across departmental lines, to access all operational areas, and to oversee the implementation and consistency of compliance activities with potential enterprise-wide compliance standards.



JPMorgan Chase & Co.

JPMorgan Chase & Co's governance and framework structure provides an excellent example of the effort banks undertake to emphasize the importance of compliance.[11] For starters, JPMorgan separated their compliance group from their legal function. They also included compliance as part of their "four functions," which includes Risk, Finance, and Legal, as part of their control framework (Figure 3).

With over 250,000 employees, JPMorgan's compliance department is comprised of more than 3,000 employees or an 83 to 1 ratio of employees to compliance staff. Those compliance professionals are under the direction of the enterprise-wide Chief Compliance Office ("CCO"), who directly reports to the Chief Operating Officer ("COO"). Each business unit or regional area has dedicated CCOs, which support JPMorgan's enterprise-wide CCO.

In 2012, an enhanced centralized compliance program was initiated globally in an effort to instill appropriate coverage, oversight and consistent standards and practices. Familiar to life sciences, their program is designed around the following "seven core principles" or functions:

1. Governance and oversight;
2. Regulatory management;
3. Policies and procedures;
4. Training and awareness;
5. Monitoring and testing;
6. Issue management; and
7. Compliance risk assessment and reporting.

To provide the ability to cross operational and regional lines, JP Morgan developed enterprise-wide governance committees, who are ultimately responsible for implementing and having oversight of their overall compliance program. They explained:

> "[These] committees enable us to better understand and address issues by serving as central forums for discussing and resolving issues that affect the company as a whole or one or more lines of business. Equally important, these committees give us the opportunity to share best practices and lessons learned across the company."[13]

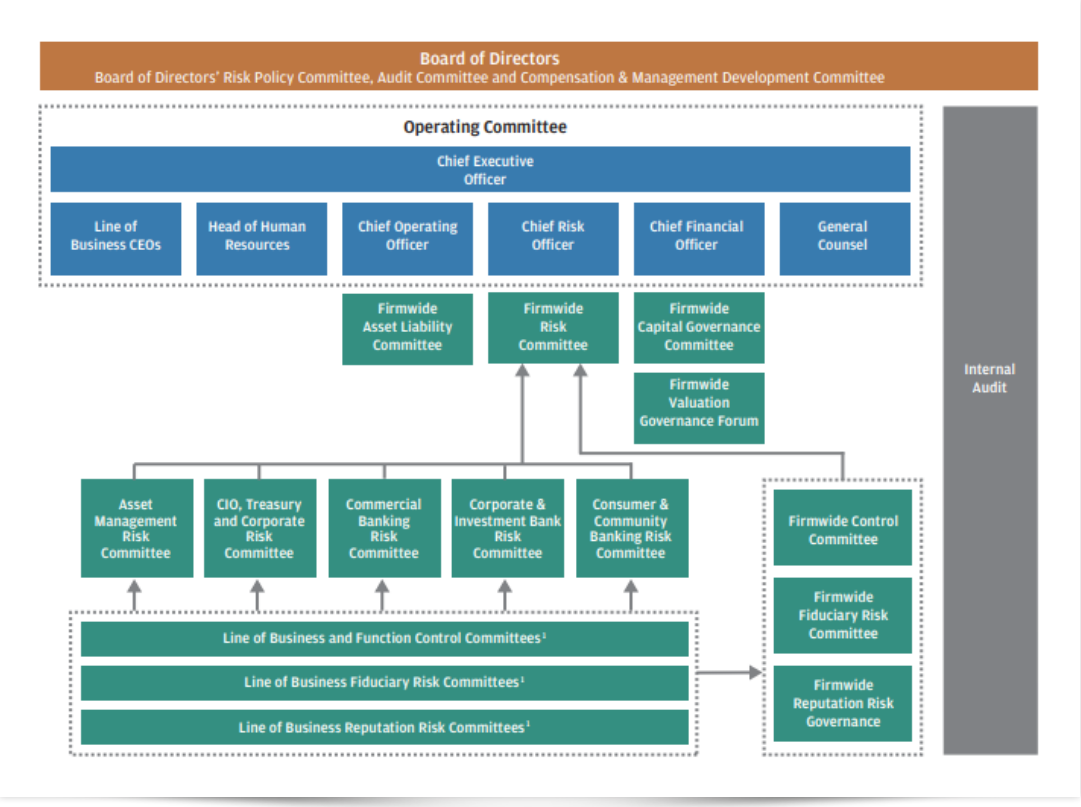
As shown in Figure 3, JPMorgan has Risk and Control committees in place to "oversee inherent risk" within each line of business or region, which then will escalate issues to their 'Firmwide Risk Committee.'

Considerations

At first glance, it appears that large banks within the financial services industry have figured effective compliance out. From a high level, it appears that banks are having the FLOD own and manage business unit compliance risk effectively embed compliance throughout the organization such that employees can make risk-based decisions on a daily basis. Furthermore, by executing Board and senior level committees, banks have found a way to address the OCC's expectations of Board actions, such as "questioning, challenging, and when applicable, opposing recommendations and decisions made by senior management," and "establishing and adhering to an ongoing training program".[14] Have banks operationally found the 'golden ticket' to establishing and maintaining a compliant organization?

The principles of the lines of defense are not foreign to life science companies. We see business and regional areas developing and implementing their respective sets of compliance policies and procedures that align with core company compliance standards. However, many would argue that it is not a well-oiled machine, especially considering repeated enforcement action,[15] the uptick in Foreign Corrupt Practices Act ("FCPA") matters for life science companies in the last two years,[16] as well as the Department of Justice's views that the healthcare industry "faces serious compliance and corruption challenges not only in high-risk markets overseas but right here at home as well."[17] The life sciences industry is far from being out of the enforcement woods. Similarly, recent scandals in the financial services sector, such as subprime loans and a multitude of settlements entered into by Wells Fargo over this past year,[18] suggest that the financial services industry is in the same boat - the compliance structure and organization sounds good in theory, but actual effectiveness in practice is hard to determine.

FIGURE 3: *Their structure reflects the model where JPMorgan's[12] core compliance function resides*



Closing Thoughts

As discussed in our previous article, although the financial industry has made strides since the 2008 financial crisis, there is a question if the heightened regulatory demands are sufficient. In June of this year, the President and CEO of the Federal Reserve Bank of New York cautioned that although the U.S. and global economic data are trending upwards, this may not provide a full picture to illustrate if "people are cutting corners, taking excessive risks, or violating rules and regulations." Finally, while we can say that the life sciences industry can learn from financial services, it is impossible to conclude that banks have figured it out – at least, for now.

References

* *Ms. McVey is an Associate Director with Forensic Risk Alliance. FRA provides multi-jurisdictional expertise in financial and electronic forensics to help companies manage risks in an increasingly regulated business climate. www.forensicrisk.com*

1 *See Jenny McVey, "Where is the Grass Greener? Banking or Life Science Compliance" (August 2018) available at https://www.lifescicompliance.com/*

2 *Office of the Comptroller of the Currency defines large banks as "a bank with average total consolidated assets equal to or greater than $50 billion as of the effective date of the Guidelines". See United States Department of the Treasury – Office of the Comptroller of the Currency – 12 CFR Parts 30 and 170; see also OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations (2014) available at www.occ.tres.gov*

3 *IFC is a sister organization of the World Bank and is the largest global development institution focused on the private sector in developing countries. See www.ifc.org.*

4 *Id. at 1.*

5 *United States Department of the Treasury – Office of the Comptroller of the Currency – 12 CFR Parts 30 and 170 OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations (2014), available at www.occ.tres.gov.*

6 *The Board of Governors of the Federal Reserve System – Divisions of Banking Supervisions and Regulation - "Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance profiles," SR 08-8 (2008), available at https://www.federalreserve.gov/boarddocs/srletters/2008/SR0808.htm.*

7 *See "The Governance of Risk Management," International Finance Corporation at www.ifc.org*

8 *Id. at. 4*

9 *See McKinsey & Company, "A best-practice model for bank compliance" (Jan. 2016), available at https://www.mckinsey.com/business-functions/risk/our-insights/a-best-practice-model-for-bank-compliance.*

10 *Id.*

11 *See JPMorgan Chase & Co., "How We Do Business – The Report," available at https://www.jpmorganchase.com/corporate/investor-relations/.*

12 *Id.*

13 *Id.*

14 *Id. at 9.*

15 *Zimmer Biomet Holdings Inc. had been in breach of a 2012 deferred prosecution agreement and was placed under a second deferred prosecution agreeing in 2017, in what the SEC called "repeat" violations of the Foreign Corrupt Practices Act and Pfizer, Inc. entered a second corporate integrity agreement in 2018. See www.justice.gov.*

16 *At least 26 LS companies were involved in FCPA matters since 2016. Data can be found at www.traceinternational.org/compendium – preferable to include search methodology or list the 26 LS companies cited for FCPA violations.*

17 *Melissa L. Jampol and Matthew Savage Aibel, DOJ Targets Healthcare with FCPA Enforcement, FCPA BLOG (Aug. 10, 2017, 8:22 A.M.), http://www.fcpablog.com/blog/2017/8/10/jampol-and-aibel-doj-targets-healthcare-with-fcpa-enforcemen.html.*

18 *See e.g., Press Release, US Dep't of Justice, Wells Fargo Agrees to Pay $2.09 Billion Penalty for Allegedly Misrepresenting Quality of Loans Used in Residential Mortgage-Backed Securities (Aug. 1, 2018), https://www.justice.gov/opa/pr/wells-fargo-agrees-pay-209-billion-penalty-allegedly-misrepresenting-quality-loans-used; Press Release, U.S. Sec. & Exchange Commission, Wells Fargo Advisors Settles SEC Charges for Improper Sales of Complex Financial Products (June 25, 2018), https://www.sec.gov/news/press-release/2018-112; Emily Flitter and Glenn Thrush, Wells Fargo Said to Be Target of $1 Billion U.S. Fine, N.Y. TIMES (Apr. 19, 2018), https://www.nytimes.com/2018/04/19/business/wells-fargo-cfpb-penalty.html.*

www.forensicrisk.com

Jenny McVey
FRA Life Sciences
202 - 627- 6597
jmcvey@forensicrisk.com