



September 2018

The Benefits of First- and Second-Line Monitoring

An article by Clayton J. Mitchell, CAMS, and Matthew J. Schuster, CPA, CRCM



As the regulatory environment shifts to an agenda of decreased regulatory enforcement by the current U.S. administration, and as availability of customer data increases, banks find themselves in a unique position to adjust their vision and overall approach to risk management and regulatory compliance. With corporate conduct, transparency, and accountability increasingly on the minds of customers, the closer that risk and compliance monitoring functions are to the customer, the more beneficial it is for financial services companies.

These shifts in risk management and compliance strategy are good for the customer in terms of service and experience. However, they are also beneficial for organizations since a more agile and holistic approach to risk and compliance efforts leads to increased efficiencies and decreased costs of compliance-related activities, including remediation and restitution. Such shifts also help risk and compliance management functions to increase focus on the enterprise-level strategies and risk appetite across their organizations.

Closer to the customer

As perceived regulatory pressure eases, compliance officers still face many challenges. Banks must still answer to ever-increasing customer expectations of secure, fair, and equitable treatment. For example, on April 20, 2018, the OCC fined Wells Fargo \$500 million for failure, among other items, to develop and implement an effective enterprise-wide risk management function in connection with the opening of fraudulent customer accounts as originally identified by the Consumer Financial Protection Bureau in a 2016 regulatory action.¹ While in the current environment, banks might face less costly fines from the federal government, lax risk management can lead to even costlier loss of business from disgruntled customers. Wells Fargo reported that its consumer checking account opening percentage for January 2017 was down 31 percent for deposit accounts compared to the previous year.² This outcome can likely be attributed in part to the widespread coverage of the regulatory actions in traditional and social media.

With the perceived decrease in regulatory scrutiny and the increased risk of supervision by social media, financial institutions are now looking to move compliance monitoring and testing into the first line of the three-lines-of-defense (3LOD) model and to position remediation efforts closer to the customer. Doing so can allow them to identify issues quicker and remediate faster, leading to a more protected and loyal customer base, which translates to growth and increased business opportunities. Additionally, by pushing the day-to-day monitoring into the first line, risk and compliance functions – the second line of defense – have more time to focus on higher-level tasks, such as providing consultation to the lines of business or other compliance management initiatives, thereby increasing their value to the organization.

In essence, pushing monitoring nearer to the customer shifts the focus and strategy from avoidance of fines to offering the best possible service to customers by treating everyone fairly and equitably and obtaining insights on the effectiveness of processes through shortening the time it would normally take to get feedback, such as through audit results. These insights can influence decision-making, ultimately improve client experience, and maximize business results via better information and data.

Three lines of defense

The 3LOD model defines roles and specific duties across the lines of business, risk and compliance functions, and the internal audit function of banks. This approach enables a framework of monitoring and accountability across the bank. While all three lines operate within the same organizational risk strategy and enterprise governance framework, a best-case scenario, high-level breakdown of responsibilities in each line of defense (LOD) is as follows:



- **First LOD, line of business:** Manage and own risks, implement processes, complete risk assessments over the operations of their specific line of business, determine and execute appropriate controls to mitigate those risks, and incorporate monitoring around the effectiveness of those controls and take corrective action when identified.
- **Second LOD, compliance and risk management:** Coordinate enterprise-wide compliance risk assessment, provide advisory services related to compliance management to the line of business, perform ongoing monitoring and testing to the line of business, and oversee and enforce compliance management policies and processes.
- **Third LOD, internal audit:** Provide assurance through independent testing to senior management over first-line control design and effectiveness and second-line compliance management program activities, including monitoring and testing.

Challenges arise if unclear delineation of responsibilities and poor communication exist within the 3LOD. Poor communication can lead to control or monitoring coverage gaps or inefficiencies in the overall monitoring of the financial services company, which can misalign resources and cause chaos among the lines of business. Because monitoring and testing efforts can be expensive, many financial institutions find that resources might become limited or stretched thin. Even with the best intentions, organizations under such constraints can misidentify risks or mismanage the controls, which can result in noncompliance.

Effective self-monitoring

An organization succeeds in achieving its risk management objectives if each line of defense performs its specific monitoring and testing duties efficiently and cohesively. The business line managers who have day-to-day ownership of risk and controls take on the responsibilities of first LOD in the 3LOD model. As subject-matter experts, business line managers drive the design of monitoring processes that identify and remediate issues when they happen. Without effective monitoring in the first LOD, unidentified issues can linger and exacerbate over months or years until the second or third LOD identifies the issue – or even worse – when a customer or regulator does.

Complementary compliance monitoring

The second LOD functions as oversight of the stated risk management policies and processes, and effectively challenges the line of business process effectiveness by performing separate monitoring, focused on consequences such as compliance violations or consumer harm. The second-line monitoring should rely, in part, on the outcomes of the first-line monitoring that the line of business is performing. Effective and thorough second LOD monitoring should focus on the higher-risk areas of the financial institution but also build upon the monitoring that the line of business is completing.



Data and analytics for compliance

The sands are shifting for risk and compliance officers. With significant annual advances in data availability and technological applications, banks are increasingly turning to these technologies to help streamline their overall risk and compliance efforts. Such advances include tools and techniques that enable the automation of what used to be manual testing efforts, which frees up resources and drives testing consistency. It also allows the institution to widen its risk and compliance focus to advisory and remediation efforts rather than spending all of its resources on issue identification.

Business leaders increasingly acknowledge the opportunity that exists to utilize data analytics to reduce overall costs related to compliance. When paired with a holistic organizational approach to compliance, banks can realize numerous benefits, including:

- Improved quality of information
- Identification of market trends
- Overall cost reduction for compliance efforts
- Improved customer experience
- Reduced compliance-related person-hours
- Ability to test populations of transactions, rather than samples

These advantages do not come easily, though, and they are typically accompanied by significant data-related challenges.

Take for example a merger or acquisition. Such activity often results in a vast amount of disparate information systems, and the types of data found within these organizations might include numerous incompatible systems and data sources. Yet organizations must focus on accurate and complete data in order to realize the value of monitoring and testing activities. As a result, institutions adopting technology solutions in their compliance environments should anticipate potentially significant initial efforts. However, the reward is worth the effort. In the end, utilizing data analytics in compliance can lead to an environment focused more on how to best service the customer and enable business growth rather than on avoiding fines. Any bank that can spot trends and predict answers before problems arise can position itself ahead of its competitors and regulators and can reap the fiscal rewards of a satisfied and secure customer base.

A balancing act

Ultimately, risk management is everyone's responsibility, and organizations need to find the right balance of traditional monitoring and newer, data-driven techniques to develop an approach that meets compliance obligations and aligns with the specific risk appetite of the organization. With changes to the regulatory environment, banks have an opportunity not only to adapt and grow, but also to embrace technologies that can ultimately deliver customers a higher-quality experience and provide businesses with accurate, proactive, and cost-effective approaches to compliance efforts.

Using business data to augment and replace traditional testing and monitoring can help define more accurate risk strategies and establish a better control environment. It can also support accountability enforcement while speeding up the evaluation and communication of deficiencies. These strategies can translate positively to the customer and can lead to better market position for organizations.





Learn more

Clayton Mitchell
Principal
+1 317 208 2438
clayton.mitchell@crowe.com

Matt Schuster
+1 317 208 1965
matt.schuster@crowe.com

¹ "OCC Assesses \$500 Million Penalty Against Wells Fargo, Orders Restitution for Unsafe or Unsound Practices," Office of the Comptroller of the Currency, U.S. Department of the Treasury, April 20, 2018, <https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-41.html>

² "Wells Fargo Reports January Retail Banking Customer Activity," Wells Fargo, Feb. 17, 2017, <https://newsroom.wf.com/press-release/wells-fargo-reports-january-retail-banking-customer-activity>

crowe.com

"Crowe" is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. "Crowe" may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S. member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. © 2018 Crowe LLP.