Reflecting on an optimal framework

Many financial institutions, consistent with regulatory expectations, organize their risk management framework into a model with three lines of defense (LOD):

1. The business line, which generates, owns, and controls the risk
2. The support functions, which provide oversight to the first line, and include the risk disciplines of operational risk and compliance, among others
3. Internal audit, whose remit is derived from the board to process-audit the first and second lines of defense

The global financial crisis generated years of significant spend on the remediation of identified regulatory (and, at times, internal audit and risk management) issues. In response to addressing these issues and executing their oversight responsibilities, operational risk and compliance may have created multiple functions and activities, and in certain cases, generated duplicative requests for the first line of defense.

With the global financial crisis behind us, institutions now have an opportunity to reflect on what an optimal operating risk management model may look like—and where synergies may be garnered from the existing capabilities of operational risk and compliance. For the purposes of this paper, we will discuss the first and second lines of defense. Further, we will explore the activities performed by each risk discipline and the capabilities where synergies may exist.

Operational risk and compliance functions have a shared mandate to provide oversight to the first line and challenge the execution of their risk management practices. But depending on how the functions are organized, this may create some challenges that result in inefficient processes. For example, operational risk and compliance may request that the first line perform the same or similar activities (e.g., risk identification, risk assessment, controls testing, issue identification, and issues reporting). So today, some institutions are exploring ways to optimize the execution of their risk management activities at both the first and second lines of defense.

Figure 1 illustrates different regulatory definitions of operational risk and compliance risk and the implication of each.

Why do potential synergies between operational and compliance risk disciplines exist? For a simple and obvious reason: if there is a breakdown in process, a compliance breach may occur, and vice versa.
Figure 1. Operational risk and compliance definitions

The Basel Committee on Banking Supervision (BCBS)

- **Operational risk:** The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk.

- **Compliance risk:** The risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer. Usually, this is the result of failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to banking activities.

Federal US regulators

- **Operational risk:** The failure to establish a system of internal controls and an independent assurance function—one that tests the effectiveness of internal controls and exposes the bank to the risk of significant fraud, defalcation, and other operational losses.

- **Compliance risk:** The risk of legal or regulatory sanctions, financial loss, or damage to reputation resulting from failure to comply with laws, regulations, rules, other regulatory requirements, or codes of conduct and other standards of self-regulatory organizations applicable to the banking organization (applicable rules and standards).

Important to note: Tension can exist between the definitions of BCBS and the federal US regulators, as BCBS takes a measurement approach to risk. This includes compliance as a sub-risk category, while in the United States, regulators define compliance as its own discrete risk discipline.

However, there is consensus among these regulators on the importance of maintaining the integrity of each risk discipline and recognizing the need for separate operational risk and compliance functions.

Many institutions are reevaluating their risk management operating models across lines of defense. Now they are looking to transform their risk management processes to address specific challenges as outlined in figure 2.

Figure 2. Drivers for change

Process/cost inefficiency
Challenges, post-global financial crisis, arising from inefficiencies due to siloed risk management practices of the same or similar activities across various risk and compliance functions and business lines. These may be the result of a historic tactical response vs. strategic response to regulatory remediation and associated increases to headcount.

Outdated technology
Segmented data sources, along with a historic underinvestment of disparate legacy systems, sometimes impede the capture, measurement, and reporting of data.

Inability to assess/quantify risk
Challenges in providing management and the board with data that transforms into information. Data that is concise, on-point, timely, and comprehensive for them to be advised and make informed decisions.

Stakeholder expectations (management, board, and regulators)
The need for more effective and efficient communications and reporting to stakeholders of an integrated view of risk.

Need for clarity and transparency
The need for second LOD risk and compliance functions to break down silos that often appear to overlap in roles and responsibilities.

Cost reduction
Increasing pressure on first and second LOD to find new ways to reduce costs, increase efficiencies, and still control risk.

Data and technology opportunities
High potential for automation and emerging technologies (such as artificial intelligence, the use of bots, etc.) to help improve risk effectiveness.
Opportunities for synergies

In transforming risk management operating models, many institutions are beginning to identify potential synergies across their risk management efforts. These synergies can bring greater transparency and higher-value intelligence to management and the board. Synergies can also provide greater transparency of issues and risks, and their potential impacts.

Figure 3 illustrates a selection of discrete capabilities of operational risk and compliance, as well as opportunities for potential synergies between these risk disciplines.

Figure 3. Operational risk and compliance capabilities

To realize the opportunities of synergies, a common and consistent taxonomy is foundational for effective risk management. A definition of terms is considered a leading practice to advance the consistent interpretation, measurement, execution, and reporting of issues and risks within the two risk disciplines. There are five critical data elements where a common and consistently applied taxonomy is crucial: risks, controls, processes, policies, and obligations.

Synergies become most evident when performing a risk assessment, regardless if it is a self-assessment at the first LOD or a compliance assessment performed by the second LOD. The ability to map processes from obligations to policies, and then to risks and controls, can assist in the identification, reporting, and escalation of issues. Figure 4 highlights specific opportunities for synergies.
Figure 4. Key opportunities for synergies

**Governance**
The rationalization of governance committees and risk management frameworks that support the organization model across the first and second LOD.

**Issue management**
Holistic issue management that enables effective identification and aggregation of systemic issues, along with the prioritization and coordination among functions to achieve single issue remediation that is sustainable.

**Evaluation of controls**
A common taxonomy enables effective evaluation and measurement of controls associated with key risks and obligations. Potentially, a shared services unit for conducting second-line testing could be established to promote single testing for both disciplines, including validation and oversight of the first-line testing results.

**Issue management**
Issues identified in isolation across operational risk and compliance may create inefficiencies regarding issue management and remediation, specific to solving for the same or like issues twice. A centralized system of identification, analysis, reporting, and tracking of issues may promote the successful systemic identification and prioritization of issues.

**Reporting**
This process can be more comprehensive when collaborative analysis by operational risk and compliance create common risk and performance indicators and metrics to produce shared and insightful reports. Centralized reporting across operational risk and compliance can bring about a reduction of overlaps.
Options for realizing synergies

Baseline maturity and sustainable processes for both operational risk and compliance functions are needed before real efficiencies and synergies can be considered. A defined vision—one shaped by tone from the top—is a critical factor for a successful transformation. Also crucial to transformation are identified and effective agents of change with requisite skill sets.

As financial institutions explore different ways to realize synergies and touchpoints between operational risk and compliance, some examples of organizational construct include:

1. **Coordination between operational risk and compliance.** Streamline processes for risk management requests of the first LOD while having the two risk disciplines remain independent functions.
   - **Potential advantages:** Minimal disruption to people, process, and technology to reduce redundancies and costs and maintain desired independence and authority of respective risk discipline, which enables them to continue to meet regulatory requirements and expectations.
   - **Potential disadvantages:** May not result in optimal long-term operating model objective of supporting cost reduction associated with risk management. Also, there is potential to create confusion between operational risk and compliance roles and responsibilities with the first line unless communicated properly.

2. **Centers of Excellence (CoE).** Some institutions are considering, or have already established, a shared service model across operational risk and compliance using CoEs for same or similar risk management activities. This includes controls testing, issue management, reporting, etc. The CoE may have a dual reporting line to both operational risk and compliance senior officers with a single interface to the first line. In addition, some institutions are opting for a managed services model where they outsource selected risk management processes.
   - **Potential advantages:** Reduction in overall effort and cost of activities, greater consistency in results and applied methodologies, and streamlined coordination with first line and alignment to the enterprise risk strategy and vision.
   - **Potential disadvantages:** Regulatory constraints and possible dilution of subject matter expertise specific to each respective risk discipline.

3. **Singular ownership for operational risk and compliance.** Some institutions have considered merging the two risk disciplines under one organization to take advantage of the synergies between exposures.
   - **Potential advantages:** Strategic alignment of visions and objectives with limited or no conflicting requirements and processes, and reduced burden and touchpoints with the first line.
   - **Potential disadvantages:** Different approaches and perspectives to managing risk, which can cause inherent conflict between the two functions. For example, operational risk often anchors risk management activities to a process, whereas compliance manages risk to an obligation. Further, compliance must manage regulatory requirements and expectations for legal obligations (e.g., laws and regulations), which does come under an operational risk mandate. Requisite knowledge and understanding of such is generally not resident in an operational risk function.
Conclusion

With the global financial crisis in the past, financial institutions can now revisit their organizational construct and required capabilities across the first and second LOD. In doing so, these organizations can optimize risk management processes and create efficiencies.

The transformation of the risk management operating model and culture may be warranted based on potential synergies. But it is also important to retain the integrity of each respective risk discipline, consistent with regulatory definitions. For success in this transformation, it is critical to establish a clear, well-articulated, and communicated vision combined with an appropriate tone from the top.

Contact us:

Monica O’Reilly
Principal
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 415 783 5780
monoreilly@deloitte.com

Vikram Bhat
Principal
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 973 602 4270
vbhat@deloitte.com

Alok Sinha
Principal
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 415 783 5203
asinha@deloitte.com

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

Edward Appert
Managing Director
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 212 436 7511
eappert@deloitte.com

Yana Parfenyuk
Senior Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 201 685 5283
yparfenyuk@deloitte.com

Joanna Connor
Senior Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 215 982 6535
jconnor@deloitte.com

Arun Chandra Akalamkam
Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche AERS India Pvt Ltd.
+1 404 487 7449
aakalamkam@deloitte.com

Param Gupta
Senior Consultant
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 212 436 3283
paragupta@deloitte.com

As used in this document, “Deloitte” means Deloitte Tax LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright © 2019 Deloitte Development LLC. All rights reserved.