bcg.perspectives
by THE BOSTON CONSULTING GROUP

ELEVATING COMPLIANCE RISK MANAGEMENT IN INSURANCE

By Matteo Coppola and Lorenzo Fantini

Long an afterthought for most companies, compliance risk management—in financial services generally, and in the insurance industry specifically—is becoming a strategic function at the core of multiple business processes as diverse as new-product development and financial reporting. A comprehensive study by BCG of chief compliance officers (CCOs) and business executives in the insurance industry shows that this trend is set to continue.

Following the 2008 financial crisis, compliance in banking underwent a fundamental transformation as lawmakers and regulators in North America and Europe placed a host of new requirements on financial institutions. Regulatory activity today, especially in Europe, suggests that the insurance industry is facing a similar situation. Many companies view increasing compliance requirements as simply another burden on an already heavily regulated sector. Smart insurers, however, see opportunities to differentiate themselves with customers and consumers and even to establish competitive advantage.

Our study of compliance in the insurance industry assessed current risks, the state of governance and organization in insurance companies, and today's compliance processes and methodologies. In this article, we summarize our findings, analyze the shifting compliance environment, and consider what that shift means for the insurance industry.

The Rising Importance of Compliance

A number of factors are compelling compliance risk management from backwater to boardroom:

- An evolving business environment that requires increasing attention to such issues as customer and data protection and privacy.
- A rising regulatory wave that is expected to build over the next two to three years and increase requirements in a number of jurisdictions, many of which focus on compliance. (See Exhibit 1.)

EXHIBIT 1 | New and Upcoming Regulations Focus on Compliance

NAME	DATE	DESCRIPTION
EMIR	Implementation in process	Clearing, reporting, and risk mitigation techniques for derivative contracts negotiated over the counter
CRS	Implementation in process	Due diligence on all customers for tax purposes and the reporting of certain clients' financial incomes to the appropriate authorities
MAD II AND MAR	July 2016	European definitions of market abuse crimes and related criminal sanctions, and the extension of liabilities to legal entities
AML DIRECTIVE IV	Jan 2017	Stronger due diligence for new clients, with a broader scope and a more severe process to identify beneficial owners with a follow-the-money approach
PRIIPS	Jan 2017E	Comprehensive Key Information Documents to be distributed together with specific investment products
IDD II	Jan 2017E	Conduct requirements for distributors of insurance products and transparency requirements on products and services offered to clients
MIFID II AND MIFIR	Jan 2018E	Full disclosure to customers of product features and profitability, enhanced product governance, and a review of market infrastructures
IFRS 4 (PHASE II)	Jan 2018E	Economic balance sheet rules (that is, a market-based valuation of insurers' assets and liabilities) and granular reporting requirements
GDPR	Jan 2018E	Strong limitations on personal data usage and enhanced protection of clients' sensitive information

Source: BCG analysis.
Note: EMIR = European Market Infrastructure Regulation; CRS = Common Reporting Standard; MAD = Market Abuse Directive; MAR = Market Abuse Regulation; AML Directive 4 = Anti-Money Laundering Directive IV; PRIIPs = packaged retail and insurance-based investment products; IDD II = Insurance Distribution Directive II; MiFID II = Markets in Financial Instruments Directive II; MiFIR = Markets in Financial Instruments Regulation; IFRS 4 = International Financial Reporting Standard 4; and GDPR = General Data Protection Regulation.

- Emerging risks, such as data protection and the inadvertent financing of terrorism, that insurers must manage.

- Growing awareness by consumers of their rights as insureds and greater regulatory focus on company conduct and risk culture, including closer scrutiny of behaviors, customer outcomes, and the value delivered to customers.

- Increasing sanctions for noncompliance, following the precedent set in banking, in which fines, settlements, and redress costs over the past five years reached a cumulative total of approximately €200 billion.

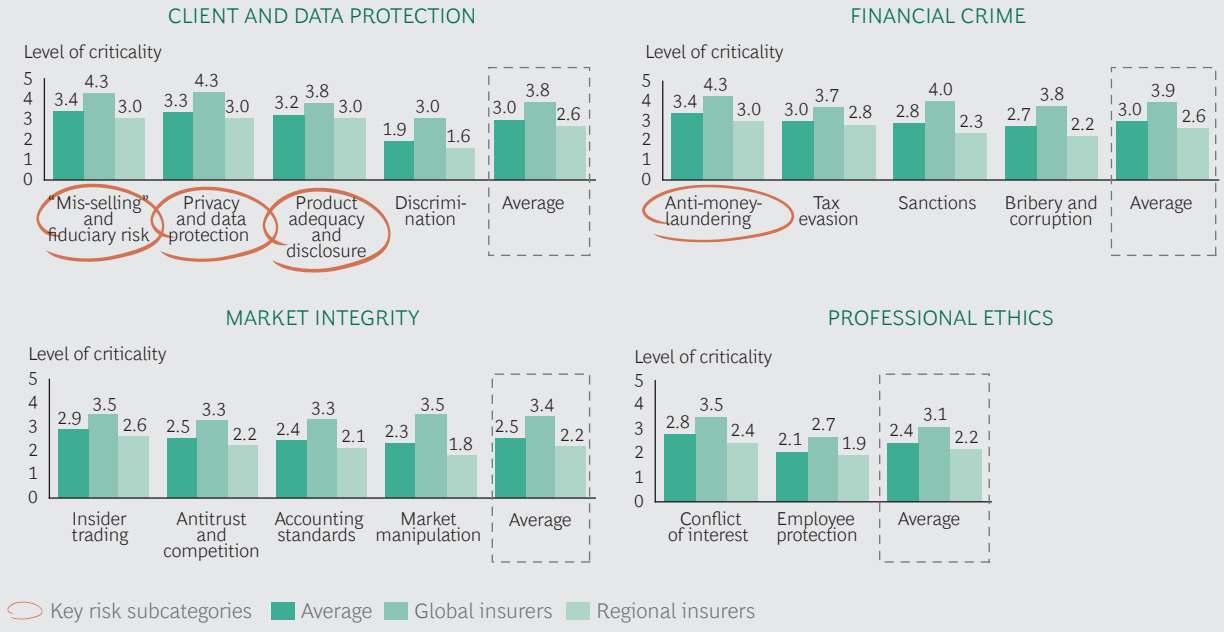
But perhaps most important, new business models and strategic imperatives require more-active management of compliance risks. For example, a growing focus on customer needs puts an emphasis on customer protection, including product design and transparency as well as distribution. Digital sales models raise new and more complex concerns over financial crime and buyer verification. And the increasing use of big data demands that privacy and data protection requirements be addressed for an ever-growing body of information.

These and other developments necessitate a compliance function that is much more active, sophisticated, and robust than the ones that most insurers currently have.

BCG's Compliance Risk Assessment

Our study consisted of in-depth interviews with CCOs and other senior managers at 17 insurers, including global and regional companies, in eight countries. Among other things, we asked these executives to rank the importance of various risks today. (See Exhibit 2.) Client and data protection and financial crime emerged as the two most critical risk categories in our sample for both global and regional players, with an average ranking of 3.0 on a scale of 0 to 5. Market integrity and professional ethics were seen as less relevant, with average rankings of 2.5 and 2.4, respectively.

EXHIBIT 2 | Industry Executives See Big Risks in Client and Data Protection



Source: BCG analysis.
Note: The qualitative score ranges from 0 to 5, where 0 is the least critical and 5 is the most critical.

Within the category of client data and protection, "mis-selling" and fiduciary risk, privacy and data protection, and product adequacy and disclosure are seen as the most critical risks. "My sentiment is that the industry is not doing a good job in screening customer data; the risk is high," said one senior executive. "Sales force mis-selling is a critical risk for our group, and it will be even more critical in Europe with MiFID II [the European Union's Markets in Financial Instruments Directive]," said another.

Within financial crime, anti-money-laundering (AML) risks are seen as the most critical. We expect the repercussions of financial crime (especially AML and related sanctions) to become an even more significant factor, as the banking industry has already experienced. As one member of our panel put it, "Money-laundering risk must be tackled in a tailored way, region by region, to be effective while minimizing costs."

Where Does the Compliance Function Fit?

Compliance risks should be managed by the part of the organization that takes the risks. What's more, that management is inherently ineffective without the strong involvement of business functions. Mitigation of compliance risks is primarily a frontline responsibility. Thus, company executives and their staffs are the first line of defense against poor or inadequate risk management.

The compliance function, along with other control functions, should support business by providing standards, methodologies, and policies. Compliance is the second line of defense, and, as such, it should coordinate risk assessments and provide guidance for designing controls and defining mitigating actions.

The audit function is the third line of defense. It should provide independent assurance about the adequacy of the framework for compliance risk management.

Compliance Governance and Organization

The compliance function itself should have the following key elements:

- **A strong organizational structure** that combines content specialization

and operational efficiency, typically including departments that focus on type of risk (such as financial crime and customer protection) and on activities across various risks (such as methodologies, monitoring and controls, and reporting).

- **Independent reporting lines** that safeguard the independence of the CCO. Companies use different CCO reporting models today (to the CEO, to general counsel, or to the chief risk officer, for example), but in all cases, direct access to the board of directors should be guaranteed.

- **A clear relationship between group-wide and local activities.** Local CCOs should have a strong and codified functional reporting line to the group CCO, who should provide significant input on HR decisions (such as hiring, termination, and promotions) and the budgets of local CCOs.

- **An appropriate mix of competencies.** Compliance's traditional focus on legal skills, which remain critical to understanding regulations, should be complemented with business knowledge and risk management skills in order to work with business personnel to manage compliance risks.

- **Adequate sizing.** Group-wide compliance functions currently range from 10 to 20 full-time-equivalent (FTE) employees for regional insurers and from 25 to 35 FTEs for global organizations, depending on overall scale. Local compliance functions must be able to adequately cover all principal risks at the local level and all core cross-risk activities, such as risk assessments, controls, and reporting.

To make sure that roles and responsibilities are clearly delineated, the compliance function's mandate and scope should be differentiated from those of the legal and operational-risk functions. With regard to compliance risks, the legal department should provide advice on current and new regulations, as well as judiciary practices. The operational-risk function should maintain oversight of nonfinancial risks, focusing on internal processes and procedures, people, and systems; identifying and measuring risks; and applying a common approach across all functions, including compliance. Compliance should take the lead on more-specialized activities, such as supporting the business function on definition policies regarding controls, taking mitigating actions, and supporting the operational-risk function on the qualitative element of risk assessments. Splitting responsibilities between the operational-risk and compliance functions on the sole basis of a risk taxonomy definition, as discussed in the following section, has proven difficult for many companies because implementing differences in day-to-day activities can result in inconsistent methodologies, processes, and outcomes for similar risks.

Compliance Processes and Methodologies

At the base of any compliance methodology, insurers must establish a structured risk taxonomy that is integrated with operational risks. If compliance risks cannot be clearly described, they cannot be measured, managed with appropriate mitigating actions, or reported within the organization in a consistent and coherent manner. Our survey findings suggest that while most insurers identify compliance risks at both the group-wide and local levels, few align their compliance risk taxonomies with operational risks. As the CCO of one regional insurer told us, "We manage data privacy, and risk management manages data protection separately, despite great similarities between them." The result is a potential duplication of processes and, possibly, different assessments of risks that are similar or even identical to one another.

Risk assessments that prioritize risks on the basis of objective evidence, expert opinions, and business feedback are the first pillar of comprehensive compliance risk management. They provide a clear view of the risks and the processes that the risks threaten. In our experience, however,

too many insurers view them as "gap assessments" focused only on regulatory requirements.

Risk assessments should be used to measure the risks underlying each regulation and should be based on an in-depth understanding of each insurer's business model. They should provide clear guidance on where to focus remedial actions and controls. The board of directors, executive managers, and business functions should be actively involved, and the compliance function should provide support and guidance regarding methodologies.

Most insurers today perform traditional bottom-up assessments, which are time-consuming exercises, especially when they need to be completed for multiple business units, legal entities, and processes affected by a broad set of regulations. The bottom-up approach typically does not prioritize risks before the assessment, so the subsequent efforts neither focus on the most significant risks nor facilitate executive decisions on risk mitigation.

In a top-down risk assessment, however, CCOs engage boards and top management to identify and prioritize the most important risks arising from current and new regulations with a very simple and high-level risk taxonomy that includes no more than 20 risks. Together, they determine the business processes in which these risks are particularly relevant and discuss the impact of new strategic initiatives on the compliance risk profile.

Not only do top-down assessments require less time and effort, but they also serve as a much more effective tool with which insurers can:

- Prioritize efforts on a risk-based approach, as has been suggested by many regulations (for example, the new AML Directive IV in Europe), so that these risks can be the subject of more traditional and detailed bottom-up assessments.

- Encourage the board of directors and executive managers to become involved and to view compliance as a business imperative.

- Link compliance more closely to company strategy.

- Adopt a forward-looking perspective to assess not only current risks but also risks that may emerge within the timeframe of the planning strategy.

- Gain an external perspective on emerging risks and trends through industry intelligence, which cannot be captured internally.

More advanced insurers are also developing so-called compliance risk appetite frameworks that embed shareholders' appetite for compliance risks into their risk assessments. The boards of these insurers, supported by the CCO, set tolerance limits for compliance risks that are linked to the results of compliance risk assessments. The CCO of a global insurer describes his company's approach this way: "We draw a risk map with the inherent risk on one axis and the controls environment on the other axis, which gives us a very good view of the positions of the different risks. Then we compare the positioning of each risk against our risk appetite framework to identify priorities and the risks to focus on."

Such companies are enforcing their "zero appetite" philosophy for noncompliance with regulations by establishing a clear appetite for the risks related to the regulations. Since compliance risk levels can never be reduced to zero, understanding that such risks can only be mitigated helps to set priorities and maximizes the efficacy and efficiency of mitigating actions.

For most insurance companies, managing compliance risks means having a solid controls system in place. But effectiveness is often equated with comprehensiveness, when in fact the actual effectiveness of such systems depends much more on prioritizing and focusing on the critical risks, employing a lean and efficient design, and positioning the controls upstream in busi-

ness processes to avoid costly loops and duplications. The experience of the banking industry is instructive in this regard. In the wake of the 2008 meltdown, controls and FTEs exploded, along with the investments required to manage them—but increases in compliance levels did not necessarily follow.

Insurers should rigorously review their controls framework, updating guidelines and policies, understanding risk factors, reviewing controls objectives and risk indicators, and rationalizing controls activities. We have developed a framework of best practices based on our study. (See Exhibit 3.) One of the key concepts is to link the strength and number of controls to the level of residual risk measured by the risk assessments so that controls are focused on the areas in which the perceived residual risk is significant.

Insurers can help top executives and members of the board to focus on and understand risk management by synthesizing the overall risk profile into a few figures—the key risk indicators (KRIs) of compliance. The most difficult challenge is to merge different metrics and qualitative information into a KRI number. The first step is to define the "risk tree," which encompasses all the drivers that contribute to the risk indicator. Once the risk tree is defined and agreed upon by the board and top management, the compliance function can find an appropriate way to measure and compare each of the drivers and then build the overall indicator into a useful reporting tool.

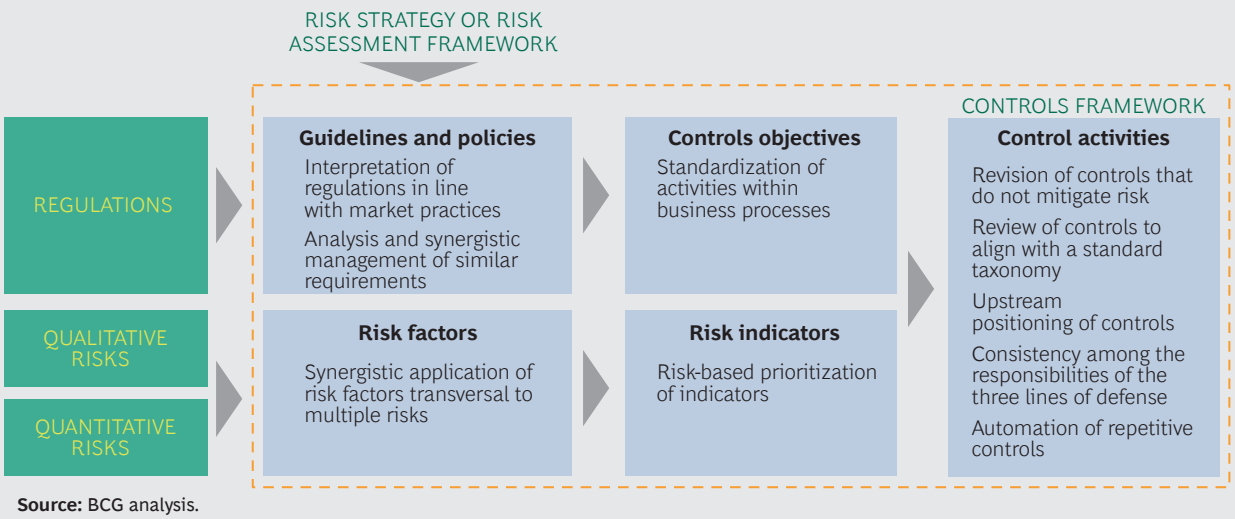
Levers for Competitive Advantage

Managing compliance risks goes beyond controls and reporting. Our study highlighted three strategic actions that companies should take to transform compliance from a burden into a source of competitive advantage.

Involve the board. Companies should actively help boards of directors to better understand compliance risks and their impact. At more than 75% of the insurers that we interviewed, board committees (such as risk, control, and audit) meet at least quarterly to discuss compliance topics. CCOs, however, are invited to these committee meetings only on an ad hoc basis to discuss current issues or to present periodic reports. Very few CCOs are actively involved in strategic discussions of compliance risk profile and regulatory strategy.

Changing this approach is not an easy task. CCOs highlighted several common issues that need to be addressed, including limited board knowledge of compliance topics, the difficulty of translating technical com-

Exhibit 3 | BCG Has Developed a Best-Practice Controls Framework



Source: BCG analysis.

pliance concepts into simple messages that focus on taking action, and uncertainty about the type of information to be reported at the board level. To handle these issues, a number of leading companies are launching training programs for board members, including self-assessments and regulatory inductions. Such sessions are already common in banking.

Embed compliance in insurers' strategic-planning processes. Forward-looking management of compliance is critically important for insurers, but only about 15% of insurers raise compliance risk management to the level of strategic planning. These tend to be the companies with top-down risk assessment processes in place. Such assessments help to embed compliance thinking into the strategy of the company and the main strategic initiatives launched by the businesses. For example, the European Union's Insurance Distribution Directive II is bringing fundamental changes to the relationship between insurers and their intermediaries and requiring new levels of information disclosure to customers, both of which raise key strategic questions. A best-practice compliance risk management approach would incorporate the expected changes from the new regulations into the distribution strategy and use new information requirements as the basis for developing innovative products targeting specific customers with focused marketing campaigns.

Make the necessary investments. Insurers need to allocate the required budget to ensure that their compliance risk management framework stays current with regulatory requirements and to integrate compliance into business strategy. CCOs outlined three main areas for investment:

- Reviews of current operating models, including the roles of, and information exchange among, control functions and compliance processes to ensure business engagement and compliance function involvement
- Better design of risk dashboards and risk reporting, an increasingly common request from boards of directors
- Training programs for compliance officers and business executives that address methodologies, processes, and business cases to build the necessary understanding of compliance risks

A Roadmap for Insurers

Each insurance company starts with different compliance capabilities, processes, and methodologies. And each will need to contend with varying degrees of complexity, depending on the insurer's size, footprint, and business mix. All companies need to assess their readiness for upcoming challenges and build more robust models if required. Most will benefit from taking the following steps:

- Perform a rapid health check to benchmark a starting point with respect to peers and regulatory expectations on a predefined set of dimensions.
- Launch compliance risk assessments and mitigation programs, focusing on the most critical risks and taking a strategic and forward-looking view.
- Revise compliance governance to reflect priority risks and move toward a more business-oriented approach, making compliance governance "regulator ready."
- Strengthen holding-company and local compliance functions, ensuring that the right organization, activities, sizing, and competencies are in place.
- Conduct an end-to-end review of the controls framework with a risk-based approach, including policies and procedures, risk factors, controls objectives, and control activities.
- Launch ad hoc training programs to apply compliance risk management to real business cases, with relevant training for boards of directors, business management, and the compliance function.

Regulatory changes and emerging business models are transforming compliance risk management from a formal exercise to a top concern for insurers. Awareness of compliance risks has risen dramatically, and as our study shows, many companies have already started the journey toward structured, business-driven, and forward-looking compliance risk management practices. There is still significant work to be done. Those that tackle the challenges and move quickly to establish best practices in their organizations will reap the rewards of leadership and competitive advantage.

About the Authors

Matteo Coppola is a partner and managing director in the Milan office of The Boston Consulting Group. You may contact him by e-mail at coppola.matteo@bcg.com.

Lorenzo Fantini is a principal in the firm's Milan office. You may contact him by e-mail at fantini .lorenzo@bcg.com.

The Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with 85 offices in 48 countries. For more information, please visit bcg.com.

6/16