MANAGING INSURERS’ COMPLIANCE RISKS IN A CHANGING ENVIRONMENT

FOCUS ON WHAT YOU SHOULD DO, NOT ON WHAT YOU CAN’T DO
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 82 offices in 46 countries. For more information, please visit bcg.com.
MANAGING INSURERS’ COMPLIANCE RISKS IN A CHANGING ENVIRONMENT

FOCUS ON WHAT YOU SHOULD DO, NOT ON WHAT YOU CAN’T DO

MATTEO COPPOLA
OFIR EYAL
LORENZO FANTINI
GIACOMO TESTA
## CONTENTS

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>FOREWORD</td>
</tr>
<tr>
<td>5</td>
<td>EXECUTIVE SUMMARY</td>
</tr>
<tr>
<td>10</td>
<td>COMPLIANCE MATURITY MODEL</td>
</tr>
<tr>
<td>12</td>
<td>GROWING IMPORTANCE OF COMPLIANCE</td>
</tr>
<tr>
<td>15</td>
<td>BCG RISK ASSESSMENT RESULTS</td>
</tr>
<tr>
<td>19</td>
<td>GOVERNANCE AND ORGANIZATION</td>
</tr>
<tr>
<td>30</td>
<td>COMPLIANCE PROCESSES AND METHODOLOGIES</td>
</tr>
<tr>
<td>37</td>
<td>LEVERS FOR COMPETITIVE ADVANTAGE</td>
</tr>
<tr>
<td>42</td>
<td>POTENTIAL ROADMAP FOR INSURERS</td>
</tr>
<tr>
<td>47</td>
<td>CONCLUDING REMARKS</td>
</tr>
<tr>
<td>48</td>
<td>NOTE FOR THE READER</td>
</tr>
</tbody>
</table>

### GROWING IMPORTANCE OF COMPLIANCE

- An evolving business environment and new strategic imperatives
- Consumers’ increased awareness of their rights and a regulatory focus on business conduct
- Fast growing regulatory requirements
- Emerging risks such as terrorism financing and data protection
- Growing sanctions for non-compliance

### BCG RISK ASSESSMENT RESULTS

### GOVERNANCE AND ORGANIZATION

- Roles and responsibilities
- Organizational structures and reporting lines
- Adequate number of resources, new skill sets and competencies

### COMPLIANCE PROCESSES AND METHODOLOGIES

- Compliance risk taxonomies
- Risk assessments
- Managing compliance risks
- Structured compliance reporting

### LEVERS FOR COMPETITIVE ADVANTAGE

- Ensure Board of Directors steering role
- Embed compliance into strategic thinking
- Ensure appropriate level of investments

### POTENTIAL ROADMAP FOR INSURERS

- Rapid compliance health check
- Risk assessment and mitigation programs (compliance programs)
- Compliance governance review
- Compliance function strengthening
- End-to-end control framework review
- Training program setup and launch

### CONCLUDING REMARKS

### NOTE FOR THE READER

- About the authors
- Acknowledgments
- For further contacts
MANAGING COMPLIANCE RISKS is crucial in the challenging environment of financial services, particularly in the Insurance industry. Today, increased client awareness, expectations and litigation, evolving business models, new technologies with emerging risks, a new wave of regulations and an unprecedented level of sanctions require a radically different approach.

Banks have invested heavily in compliance over the last five years, with many institutions completely revising their models. We believe the Insurance industry is at the onset of a similar transformation.

This paper offers an in-depth look at current market practices and emerging compliance risk management trends. To prepare it, we interviewed Chief Compliance Officers (CCOs) and other senior managers at 17 Insurers across eight countries, including global and regional players.

The paper is designed to provide deep analysis along several dimensions. As such, it can be consumed in different ways by different readers, depending on individual needs. After a short Executive Summary, the paper is structured as follows:

- **Section 1** makes a case for Boards of Directors and executive managers to actively manage compliance;
- **Section 2** outlines risk assessment results conducted within the study, highlighting current priorities of CCOs;
- **Section 3** focuses on governance and organization, including Compliance roles and responsibilities, organizational structures, reporting lines, sizing, skills and capabilities;
- **Section 4** identifies emerging best practices for compliance methodologies and processes, with a focus on risk taxonomies, risk assessments, risk management and reporting;
- **Section 5** explains levers to turn compliance into a competitive advantage, focusing on Board engagement and main initiatives to be launched;
- **Section 6** outlines a suggested roadmap for Insurers to tackle the compliance challenge, outlining different action plans according to Insurers' starting points.
The intended audience of this study is Boards of Directors, executive managers, General Counsels, Chief Compliance Officers and other heads of control functions. The study also is of interest and use to heads of business functions (such as in distribution, underwriting and marketing) who would like to better understand the compliance aspects of their organizations’ activities.

Please note that the considerations and statements presented in this paper are those of The Boston Consulting Group only, except for aggregate figures and individual opinions explicitly quoted from study participants. All quotes, tables and figures presented in the paper reflect information as of February 2016.

We hope the report’s findings and recommendations can help Insurers to respond effectively and efficiently to the challenges posed by compliance risk management in today’s changing environment.

NOTES
1. US, UK, France, Germany, Italy, Belgium, Portugal and Hong Kong. BCG asked each Insurer to complete a detailed survey before meeting with their Chief Compliance Officers and other senior managers (i.e., General Counsels).
EXECUTIVE SUMMARY
FOCUS ON WHAT YOU SHOULD DO,
NOT ON WHAT YOU CAN’T DO

COMPLIANCE HAS GONE THROUGH a fundamental transformation in the Banking industry in the last five years, moving from a reactive “tick-in-the box” control mechanism to a strategic function at the core of key business processes. Insurance is at the onset of a similar transformation, yet with some industry specificities.

Growing importance of compliance
Compliance risk management is in fact a significant concern of Boards of Directors and executive managers across the Insurance industry, driven by:

1. An evolving business environment requiring more focus on customer and data protection, and privacy;

2. Increasing regulatory requirements across different jurisdictions, many with a compliance focus, with an upcoming regulatory wave in the next two to three years;

3. Emerging risks like terrorism financing and data protection, which Insurers also must manage proactively;

4. Increased consumer awareness of insureds' rights, and greater regulatory focus on conduct and risk culture, with scrutiny of behaviors, customer outcomes and true value delivered to customers (as seen in United Kingdom and United States);

5. Growing sanctions for non-compliance, following the precedent set in the Banking industry.

The last point deserves consideration by Insurance executives. Banks’ fines, settlements and redress costs over the last five years have reached a cumulative total of approximately € 200 billion. Profits of European Union G-SIB institutions in this period would have been a third higher without litigation costs and provisioning for future litigation.¹
In Insurance, penalties have been orders of magnitude lower. While one could argue that business models differ across industries, Insurance is possibly the next sector to face this wave of regulatory pressure. Scrutiny may accelerate quickly if the Insurance sector finds itself in crises similar to the Banks, or if public debate and political attention to compliance escalates into the Insurance sector.

Today, Insurance executives have the opportunity to make their compliance model more robust along several key dimensions, potentially avoiding large sanctions as well as significant additional costs (full time employees [FTEs], investments, etc.) like those already borne by the Banking industry. This is a crucial step considering the compliance risks that our study highlighted.

**BCG risk assessment result**

Client and data protection, and financial crime, are the two most critical risk categories for our panel of Insurers. Within the first risk category, mis-selling and fiduciary risk, privacy and data protection, and product adequacy and disclosure represent the most critical risks. Within financial crime, AML is the most critical risk. Going forward, we expect financial crime (especially AML and sanctions) to become an even more significant factor, as the Banking industry has already experienced.

**Governance and organization**

Managing compliance risks is first of all a business duty. The front line should proactively manage compliance risks, run risk assessments, and define and implement controls and mitigating actions. The Compliance department should set methodologies and support the identification of risks and their management, suggesting the best course of action while considering business objectives. The Audit function should provide independent assurance on the adequacy of the compliance risk management framework.

Compliances’ mandate and scope should be clearly differentiated from Legal and Operational Risk functions. With regard to compliance risks, Legal should provide advice on current and new regulations, as well as judiciary practices. Operational Risk should maintain an overall view on non-financial risks, focusing day-to-day activity on identifying and measuring risks, and applying a common approach across all operational risks, including compliance.

Compliance should instead take the lead on more specialist activities: supporting the Business function for controls definition, policies and mitigating actions to properly manage compliance risks, and supporting the Operational Risk function for the qualitative element of risk assessments. Splitting responsibilities between Operational Risk and Compliance functions based purely on a risk taxonomy definition has proven difficult, as implementation differences in day-to-day activities (for instance fraud) could result in inconsistent methodologies, processes and outcomes for similar risks.

Having established a solid “three lines of defense” framework does not diminish the need for a strong and modern Compliance function, built on several key cornerstones:
1. An organizational structure that combines content specialization and operational efficiency, typically including both risk-type units (i.e., financial crime, customer protection, etc.) and cross-risk activities units (i.e., methodologies, monitoring and controls, reporting, etc.);

2. Reporting lines that safeguard the independence of the Chief Compliance Officer. Different CCO reporting models exist (to Chief Executive Officers [CEOs], General Counsels or Chief Risk Officers [CROs], etc.) but direct access to Board of Directors also should be granted;

3. A clear split between Group and Local compliance activities. Local CCOs should have a strong and codified functional reporting line to Group CCO, with the latter having significant input on HR decisions (hiring, termination, promotions, MBO, etc.) and the budgets of Local CCOs;

4. An appropriate mix of competencies. Compliances’ traditional focus on legal, still crucial to understanding regulations, should be complemented with business knowledge and risk management skills, to proactively manage compliance risks with the business;

5. Adequate sizing. Group Compliance functions currently range from 10-20 FTEs for regional Insurers to 25-35 FTEs for global organizations, depending on overall scale. Local Compliance functions must adequately cover all main risks at the local level and core cross-risk activities (i.e., risk assessments, controls, reporting).

Compliance processes and methodologies

At the basis of any compliance methodology, Insurers must establish a structured risk taxonomy integrated with operational risks. However, our survey suggests that, while most Insurers identified Group-wide compliance risks, assessed in all business units, few of them aligned their taxonomies with operational risks. The result is a potential duplication of processes and, possibly, different assessments of the same or similar risks. Furthermore, at many Insurers, some risks still do not have clear oversight of second-line functions such as accounting, tax, employee protection, cybersecurity and IT risks. These risks are typically assigned to first-line functions only.

Insurers must evaluate compliance risks by running ad hoc risk assessments, now a standard practice in the industry. Yet most Insurers still view risk assessments as operational exercises, focused on detailed regulatory requirements, mostly run by Compliance, with a backward-looking view toward current regulations, business model and processes. Instead, we believe that risk assessments should:

- Be forward-looking, assessing Insurers’ strategy and strategic priorities;
- Be risk-based, i.e., they should focus on most critical risks;
- Have strong involvement from the Board of Directors, executive managers and business functions, with Compliance mainly providing methodological support and guidance.
As shown further ahead, this model is quite advanced and not in place at most Insurers, which have significant work to do in this area.

Most advanced Insurers are also developing a Compliance Risk Appetite Framework, setting tolerance limits for compliance risks and linking them to the results of compliance risks assessments. In this way, Insurers are adding to the traditional “zero appetite” philosophy for non complying with regulations a clear appetite for the risks related to them. This approach enhance the calibration of risk assessment scales and the identification of unacceptable compliance risks.

For most Insurance players, managing compliance risks means having a solid control system in place. Many Insurers have a very comprehensive approach, perhaps correlating the number of controls with the solidity of the control system. We believe instead that controls should be focused on critical risks, designed in a lean and efficient way, and positioned upstream in processes to avoid costly loops and duplications.

In the Banking industry, controls have exploded, as well as FTEs and investments to manage them, but arguably without a commensurate increase in compliance levels. Conversely, an efficient control system can improve effectiveness, as well, focusing the business on a select group of crucial controls.

Furthermore, Compliance reporting should incorporate the strategic perspective. Insurers should move from very detailed, “long list” reporting, (difficult to understand for “non-technicians”) to a synthetic overview of compliance risks, ongoing programs and actions. Compliance risks should be fully integrated with the Insurer’s overall risk map, enabling a comprehensive but synthetic view of its risk profile. Respectively, Insurers should also develop a way to synthesize the overall compliance risk profile into few figures, the Key Risk Indicators (KRIs) of compliance. Only a few of the Insurers interviewed in our survey are working in this direction.

Finally, leading Insurers plan to include early warning compliance risk indicators in their monitoring and reporting system, leveraging emerging technology to provide a forward looking view of the risks arising from the market place and the external environment.

**Levers for competitive advantage**

We believe that managing compliance risks goes beyond controls and reporting. Insurers should be proactively involved in strategic initiatives (i.e., customer centricity, big data, etc.) by establishing structured ways to engage Boards of Directors and executive management. This could take the form of dedicated sessions with strategic plan cycles, as well as dedicated Board committees.

Interviews conducted with CCOs highlighted three strategic priorities to turn compliance from a burden into a key source of competitive advantage for Insurers:

- Support Boards of Directors to understand compliance risks and make informed compliance decisions, holding training sessions, and estab-
lishing direct communication channels and structured interactions with Boards, moving from pure reporting to facilitating strategic discussions;

• Embed compliance in business, translating regulatory requirements into management actions “upfront,” rather than remediating breaches ex-post and building costly controls later;

• Ensure that required investments in Compliance are made, particularly in operating model enhancement (governance, organization, etc.), reporting and supporting IT tools, as well as training for Compliance and Business functions.

Potential roadmap for insurers
While Insurers start with different compliance capabilities, processes and methodologies — and will need to contend with varying degrees of complexity depending on size, footprint and business mix — all must assess their readiness for upcoming challenges and build more robust models if required. Some players have already started this journey with specific projects.

A roadmap for effective and efficient compliance risk management over the next one to two years can comprise several key building blocks:

1. A health-check to assess an Insurer’s starting point versus peers, and Regulators’ expectations;

2. Review of critical risks embedding Board of Director and executive managers’ view, and launch of remedy actions;

3. Compliance governance review toward a management- and business-driven approach;

4. Compliance function enhancement with stronger organization and more robust skills;

5. End-to-end review of the control framework with a risk based approach

6. Comprehensive training program for business and Compliance functions.

As mentioned above, regulatory compliance will affect Insurers in many dimensions in the next few years. The Insurance industry has the opportunity today to get ahead of the curve. The players that proactively take this challenge will build a critical defense infrastructure and a significant competitive advantage.

NOTES
INSURERS CAN ASSESS THE maturity of their compliance model vis-à-vis competitors and quickly identify gaps to be addressed.

In line with the main results of this paper, we suggest measuring Insurers’ maturity on three key dimensions (see Exhibit 1):

- Governance (split of responsibilities between Compliance, business, Legal, etc.) and organization (organizational structure, skills, reporting model, etc.);
- Compliance processes and methodologies (risk assessment, controls, reporting, etc.);
- Levers for competitive advantage (Board of Directors engagement, integration of strategy and compliance, etc.).

Our market study clearly shows that we can group compliance models in three main categories:

1. Dinosaurs (legacy): Compliance responsibilities are not clearly allocated among the three lines of defense (business, Compliance, Risk Management and Audit); in particular, Compliance manages compliance risks independently from operational risks, with great inefficiencies. Compliance resources are very limited, mainly with a legal background and without a clear, formalized organizational structure at Group, Region and Local levels. Group coordination is very limited as well; Local departments operate without strong oversight. Compliance risk assessments are not performed, and controls are usually manual and not prioritized. Reporting on compliance risks occurs on a spot basis. The Board of Directors and executive managers discuss compliance topics only when serious breaches emerge.

2. Bears (standard): Compliance responsibilities are clear, but the approach to managing compliance and operational risks is still siloed. Compliance resources are adequate in number and clearly organized, but mainly with a legal background. The Compliance organizational structure is mainly driven by historical reasons, not leveraging clear synergies or areas of expertise. Group coordination has been formalized but not properly enforced; Local Compliance departments do not have a strong central radar. Compliance risk assessments are performed bottom-up, typically with low business engagement and without a prioritization of risks, controls and efforts. Reporting on compliance risks is frequent but separated from operational risks and not tailored to specific audiences (i.e., Board of Directors). The Board of Directors and executive managers discuss compliance topics on a spot basis.
3. Eagles (best practice): Compliance and control functions are very clear on their roles and fully cooperating. Operational Risk and Compliance exploit maximum synergies. Compliance resources are adequate in number, with a mix of business, Legal, Risk Management and Audit skills. The Compliance organizational structure enables both risk specialization and synergies. Group coordination is enforced with a strong functional reporting line model, as well as by active Group management of Local Compliance departments (i.e., budget approval, hiring and termination, management by objective [MBO] targets, performance evaluation and reporting flows). Top-down compliance risk assessment is done with the Board of Directors and executive managers, concurrent with the strategic planning cycle to prioritize bottom-up assessments, with a strong risk-based approach. Reporting on compliance risks is frequent and integrated with all risks, tailored to different audiences by adopting different languages and granularity levels. The Board of Directors and executive managers regularly discuss compliance topics and proactively consider the impacts of strategic decision on the Insurer’s compliance risk profile.

### EXHIBIT 1 | Compliance Maturity Model

<table>
<thead>
<tr>
<th>Governance and organization</th>
<th>Processes and methodologies</th>
<th>Levers for competitive advantage</th>
<th>% of Insurers in our sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Unclear responsibilities (i.e. of Business, Compliance, Risk)</td>
<td>• Manual / not formalized processes and controls</td>
<td>• Very limited engagement of BoD and exec. managers on compliance topics, usually in correspondence of serious threats and potential sanctions</td>
<td>~25%</td>
</tr>
<tr>
<td>• Compliance and operational risk with siloed approaches</td>
<td>• Bottom up risk assessment</td>
<td>• BoD and exec. managers engagement requested on a spot basis and limited to reviewing compliance criticalities</td>
<td>~60%</td>
</tr>
<tr>
<td>• Small orga structure</td>
<td>• Controls not always prioritized</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Skill set legal oriented</td>
<td>• Granular level reporting, but still detailed and siloed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Local compliance not reporting to parent company</td>
<td>• Bottom up and top down risk assessment</td>
<td>• Structured and proactive engagement of BoD and exec. managers</td>
<td>~15%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Compliance embedded into strategic decisions</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gradual move towards more sophistication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dinosaurs (legacy)</td>
<td>Bears (standard)</td>
<td>Eagles (best practice)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: BCG

1 i.e. budget approval, hiring and firing, MBO targets, performance evaluation, reporting flows, on-site visits
Several factors drive the increasing importance of compliance risk management and its rising profile with Insurers’ Boards of Directors and executive managers. These include:

- An evolving business environment and new strategic imperatives;
- Consumers’ increased awareness of their rights and a regulatory focus on conduct;
- Fast-growing regulatory requirements, with a regulatory wave focused on compliance;
- Emerging risks such as terrorism financing and data protection;
- Growing sanctions for non-compliance, following the precedent set in the Banking industry.

**An evolving business environment and new strategic imperatives**

Insurers face unprecedented changes to traditional business models and new strategic imperatives, requiring proactive management of compliance risks. Specifically, new imperatives put increased focus on compliance risk management; the impact can be readily illustrated by analyzing common strategies such as:

- Customer centricity instead of a traditional product focus;
- The digital revolution, particularly as it drives change in products and distribution;
- Big data and advanced analytics initiatives.

Undertaking any of these strategies will expose Insurers to significant compliance risks:

- Customer centricity emphasizes the importance of customer protection, including adequate product design and transparency, as well as proper distribution;
- A digital sales model raises concerns on financial crime and buyer verification, which is more difficult in a digital environment (i.e., AML for online customers);
- Use of big data will demand that privacy and data protection requirements be met on a much broader set of information.

**Consumers’ increased awareness of their rights and a regulatory focus on business conduct**

Severe misconduct in the Financial Services industry during the financial crisis, and the...
The public debate that followed in Europe and the US, increased consumers’ awareness of their rights. Litigation with Banks and other financial institutions soon followed.

Partially in reaction to increased consumer and political pressure, Regulators honed in on business conduct and risk culture, particularly in the US (Consumer Financial Protection Bureau) and in the UK (Financial Conduct Authority). These Regulators promoted a new approach to supervision, requiring that financial institutions put customers at the heart of their business models, to ensure customer satisfaction, deliver true value and not discriminate across customer types. Regulators are now empowered to directly challenge management and business behaviors, product design and information, sales network incentives and the underlying risk culture of any organization under their purview. Organizational structures, policies and procedures, and control frameworks are no longer sufficient if they are not reflected in tangible business practices and aligned with good business conduct.

**EXHIBIT 2 | Key upcoming regulations with compliance focus**

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMIR$^2$</td>
<td>Up to 2015</td>
<td>Clearing, reporting and risk mitigation techniques for derivative contracts negotiated over the counter</td>
</tr>
<tr>
<td>CRS$^3$</td>
<td>Jan 2016</td>
<td>Due diligence on all customers for tax purposes, reporting of certain clients financial incomes to competent authorities</td>
</tr>
<tr>
<td>MAD II/ MAR$^4$</td>
<td>July 2016</td>
<td>European definitions of market abuse crimes and related criminal sanctions, extension of liabilities to legal entities</td>
</tr>
<tr>
<td>AML Directive IV</td>
<td>Jan 2017</td>
<td>Stronger DD$^5$ of new clients with extended perimeter, more severe process to identify beneficial owners with follow the money approach</td>
</tr>
<tr>
<td>PRIIPs$^6$</td>
<td>Jan 2017$^7$</td>
<td>Comprehensive “Key Information Documents” to be distributed together with specific investment products</td>
</tr>
<tr>
<td>IDD II$^7$</td>
<td>Jan 2017$^7$</td>
<td>Conduct requirements for distributors of insurance products and transparency requirements on products/services offered to clients</td>
</tr>
<tr>
<td>MIFID II / MIFIR$^8$</td>
<td>Jan 2018$^8$</td>
<td>Full disclosure to customers of product features and profitability, enhanced product governance and review of market infrastructures</td>
</tr>
<tr>
<td>IFRS 4 (Phase II)</td>
<td>Jan 2018$^9$</td>
<td>Economic balance sheet rules (i.e. market based valuation of insurers’ assets and liabilities) and granular reporting requirements</td>
</tr>
<tr>
<td>GDPR$^9$</td>
<td>Jan 2018$^9$</td>
<td>Strong limitations in personal data usage and enhanced protection of clients sensitive information</td>
</tr>
</tbody>
</table>

Sources: BCG

$^1$BCG Estimate; $^2$European market infrastructure regulation; $^3$Common reporting standards; $^4$Market abuse directive/regulation; $^5$Due Diligence; $^6$Packaged retail and insurance-based investment products; $^7$Insurance Distribution Directive II; $^8$Markets in Financial Instruments directive II/ regulation; $^9$General data protection regulation.

Fast growing regulatory requirements

Following a well-established trend in the Banking industry, Insurance Regulators are expanding their focus from capital and balance sheet risks to less quantifiable risks, mainly in the compliance space. A growing number of regulatory requirements and audits now touch every Insurance business, product, process, legal entity and region. We expect this trend to accelerate in the next two to three years, with major new regulations focusing on distribution and customer protection, market abuse, anti-money laundering, information and disclosure requirements, tax and data protection, and other compliance topics (see Exhibit 2).

Emerging risks such as terrorism financing and data protection

Insurers’ evolving footprints continuously expose them to new risks. Insurers are becoming more complex in many ways, including products, distribution channels and geographies, and as legal entities. They have more
jurisdictions and regulations to comply with (i.e., for asset management), and many Regulators to manage. Hence, they are increasingly vulnerable to a set of emerging risks.

For instance, terrorism financing is an emerging risk of raising concern within the Banking and Insurance industries, particularly for players with significant international operations. In the past, a significant challenge has been posed by the absence of a clear definition of terrorism activities that could guide the countering initiatives of financial institutions. Recently, the focus of international authorities has risen, and new regulatory initiatives, such as the fourth European Directive on AML, were launched to provide a more prescriptive guidance on how to mitigate the risk of financing terrorism. The new prescriptions and the raising instability of several geographical areas pose new challenges to Insurers, requiring a deep knowledge of the business environment, in order to understand where the predicate offences are committed and how the funding of terrorism is carried out.

Data protection is another emerging risk in the Insurance industry. Despite being historically recognized as a compliance risk it is changing in nature, following the evolution of business models and regulatory requirements. On one side, the technological innovation brought by digital marketing and distribution channels requires a more intense and complex usage of personal data, which adds to the already thorny treatment of personal data typical of insurance products. On the other side, regulators are planning to completely review consumers’ rights (i.e., with the European “right to be forgotten”, “data portability”, etc.) and to harden requirements on security controls by institutions, with significant impacts on their compliance risk profile.

Growing sanctions for non-compliance

Growth in the number and severity of sanctions is the companion of increased compliance risks in the Insurance industry. While compliance sanctions can easily reach several billion euros for leading Banks, Insurers have been fined up to 150-200 million euros over the last five years, mainly for customer protection and market integrity violations.

Interconnections of Regulators across Banking and Insurance industries, and overlap of common risks and regulations, suggest that sanctions will further increase for Insurers. Regulators may focus on risks heavily fined in Banking, largely in the category of financial crime and conduct (i.e., AML, sanctions, etc.).

Compliance sanctions can impact not just the Insurance company, but also individual executive and non-executive members of the Board of Directors, and executive managers. Personal fines can add up to several million euros and criminal liabilities also apply. Liability for a wide variety of risks, not always known and understood, is a growing concern for senior executives and Board members.
Within our study, we ran a risk assessment of the relative importance of different compliance risks, with qualitative ranking from 1 (very low risk) to 5 (very high risk) of four risk categories and 14 specific risk types (see Exhibit 3 for detailed explanation):

1. Financial crime: Obligations to verify clients’ and other business counterparties’ misbehavior. Risk types within this category include:
   a. Anti-money laundering
   b. Tax evasion
   c. Bribery and corruption
   d. Sanctions (prohibited businesses)

2. Client and data protection: Obligations to check company and employee misbehavior toward customers. Risk types within this category include:
   a. Privacy and data protection
   b. Discrimination
   c. Product adequacy and disclosure
   d. Mis-selling and fiduciary risk

3. Market integrity: Obligations to avoid manipulation and distortion of markets and their proper functioning. Risk types within this category include:
   a. Market manipulation
   b. Insider trading
   c. Antitrust and competition
   d. Accounting standards

4. Professional ethics: Company obligations towards employees and related business parties. Risk types in this category include:
   a. Conflicts of interest
   b. Employee protection.

Risk assessment results for risk categories (see Exhibit 4) show that client and data protection, and financial crime, are the two most critical risk macro categories in our sample (for both global and regional players) with an average ranking of 3.0. Market integrity and professional ethics are perceived as less relevant, with average rankings of 2.5 and 2.4 respectively.

Interestingly, while all global players agree on the relevance of financial crime risks, regional players do not share a common view. For
example, several regional players without significant US-related business believe financial crime risks to be less relevant for them. Conversely, global players are looking very carefully at the Banking industry and preparing for regulatory scrutiny on sanctions and AML. “AML has always been a regulation to monitor and we do not see any relevant changes.”

CCO of a Regional Insurer

Risk assessment results for specific risk types show that Insurers rank Mis-selling and Fiduciary Risk, Privacy and Data Protection, Product Adequacy and Disclosure, and AML the most critical risk types (see Exhibit 5). CCOs quotes (see Exhibit 6) add depth and color to the rationale behind the rankings:

- Mis-selling and Fiduciary Risk is a key concern for agents and dealer networks, as well as the sales force in general, reinforced by more stringent upcoming regulations in US, UK and continental Europe (i.e., MIFID II).
- Privacy and Data Protection is considered an emerging risk in the context of digital, technological innovation and increased clients’ awareness of their rights.
- Product adequacy and disclosure is ranked high due to the very complex nature of products, particularly in the Life business, as well as the concern of not selling products that actually fulfill customers’ needs.
- Renewed focus on AML is clearly driven by recent US, UK and continental Europe regulatory pressure and new regulations (i.e., AML Directive IV in Europe).

Excluding AML, all top risks relate to company and employee behavior versus customers and other business counterparts. These are “business conduct” risks.

If we draw a comparison across industries, the largest fines and most intense regulatory focus in Banking are related to financial crime risks
(i.e., AML, sanctions, tax evasion, etc.), not on conduct risks — although Regulators have recently extended their attention to conduct, as noted. Despite the proximity of Insurance and Banking Regulators suggesting that financial crime risks will remain relevant for Insurers, we believe that “business conduct” could be the industry’s most important risk category.

The differing nature of Banking and Insurance businesses can explain variances in risk rankings across industries. In Banking, trans-
actions and client interactions are very frequent and difficult to monitor. Several standard products with high volumes (deposits, investments, etc.) can be conduits for money laundering and other financial crime schemes. Conversely, if we exclude investment products in the Life business, it is less easy to use insurance policies for financial crime. Insurers have less frequent interactions with their customers and could monitor better each transaction.

On the other hand, while Banks are discovering the importance of proper "conduct,” following recent scandals such as Payment Protection Insurance mis-selling in the UK, Insurers have been familiar with conduct risks from the very beginning. Insurance products are more complex in nature and their functionality less apparent to the public (particularly on the Life side) than Banking products. They have complex exposures and trigger factors, and their promise to pay is valid only if kept properly when the claim is made. They also require sophisticated treatment of a broad set of customers’ sensitive data, exposing Insurers to a high risk of breaching individuals’ privacy rights. Conduct risks are thus more “embedded” in the Insurance business and more complex to manage, since the boundaries of a good Life policy, from a customer conduct point of view, are sometimes less clear than those of a good deposit account or loan.

Finally, Insurers’ recent focus into alternative asset classes (even if still limited) and innovative investments in a low-yield environment will expose them to a set of risks currently considered to be of lower criticality, within the market integrity category. More sophisticated investment strategies and asset classes, and a battle for returns, will push Insurers closer to market manipulation, conflicts of interest and accounting standards risks, which we expect to rise over the next few years.

---

**EXHIBIT 6 | CCOs quotes on most critical risks**

<table>
<thead>
<tr>
<th>Global Insurers</th>
<th>Regional Insurers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy and Data Protection</strong></td>
<td><strong>Evolution of technology, digital and client’s higher awareness are making privacy risk more and more critical</strong></td>
</tr>
<tr>
<td><strong>Mis-selling and Fiduciary Risk</strong></td>
<td><strong>Conduct regulation is not rule-based and lawyers cannot interpret it. They are principle-based, and you have to struggle to find your way</strong></td>
</tr>
<tr>
<td><strong>Product adequacy / disclosure</strong></td>
<td><strong>We fear especially to design and distribute products not adequate to the target customers</strong></td>
</tr>
<tr>
<td><strong>AML</strong></td>
<td><strong>We noticed an increasing pressure by the authorities and now tax evasion is considered similarly to money laundering</strong></td>
</tr>
</tbody>
</table>

*Source: BCG*
GOVERNANCE AND ORGANIZATION

Roles and responsibilities

Compliance risks should be managed where the risks are taken; compliance risk management is inherently ineffective without the strong involvement of business functions. Mitigation of compliance risks is primarily a front-line responsibility.

Therefore, the business should be held accountable for compliance violations. Business functions should implement adequate controls for their respective processes to ensure that risk is adequately managed. Moreover, business should proactively run risk assessments, with the guidance and support of Compliance, launching mitigating actions where residual risks cannot be accepted.

The Compliance function, and the other control functions, should support business by providing standards, methodologies and policies. Compliance should also coordinate risk assessments and provide guidance to design controls and define mitigating actions. Frequent training sessions, delivered by Compliance, will enable the Insurer’s business functions to actively perform their duties in a compliant manner. Compliance should also periodically review risk assessments, controls and actions run by business, ensuring their appropriateness.

Finally, Compliance should report compliance risks internally and externally. The CCO of a global Insurer in our study explained the Compliance function’s engagement model with the business:

“We have a four-stage process to support the first line of defense: inform (risk identification), support (advisory and implementation), challenge (monitor and require what is expected) and report (to the Board).”

CCO of a Global Insurer

As a third line of defense, the Audit function should provide independent assurance on the efficacy and effectiveness of compliance risk management, within the broader effectiveness of control system. Audit should challenge all functions involved in compliance when required (see Exhibit 7).

Identifying and enforcing the right mix of roles and responsibilities between front-line and control functions in general, and Compliance in particular, is perhaps the most crucial part of the compliance risk management framework. This governance structure is frequently assessed by Regulators during audits, inspections and more informal conversations with Insurers.

Our study confirms that Chief Compliance Officers largely share the view outlined in the Three Lines of Defense Framework. This detailed assessment of the ownership of compliance-related activities is illustrated in
Exhibit 8. However, three points of attention have emerged from our interviews with CCOs:

- Risk assessments are sometimes exclusively run by the Compliance function with limited business engagement, reducing ownership by the first line and the effectiveness of the assessments themselves. In these situations, Compliance is less close to the source of risk origination.

- Even if formally assigned to business, control functions (Compliance, Audit, etc.) can find themselves executing controls and launching mitigating actions across business processes. This compromises testing independence and limits the effectiveness of the controls.

- Control key performance indicators (KPIs) appear to be outside the domain of Compliance, despite they are a fundamental part of the compliance control system.

In particular, if Compliance and other control functions execute risk assessments and/or controls instead of business functions, the effectiveness of compliance risk management may be reduced by:

- Business functions’ discharging their responsibilities, declining to recognize compliance as their duty but rather as an optional task.

  “The business involvement is still left to the individual, for sure we have to enhance it.”

  CCO of a Global Insurer

- Lower effectiveness of risk assessments and controls, since the Compliance function typically has lower proximity to, and knowledge of, the business.

- Reduced second line of defense and independent verification role of the Compliance function, which could struggle to design, perform and test controls at the same time.

Limited engagement of business functions in compliance risk management is due to a variety of reasons: lack of awareness, poor compliance culture, limited compliance skills and resource constraints.

Banking and Insurance Regulators’ audits and issued statements show that limited business involvement in compliance is no longer acceptable, and typically leads to the most severe sanctions. This has been recently evi-
enced in the US and UK, for example with AML and prohibited businesses sanctions in the Banking industry.

Best-practice Insurers launch initiatives to effectively tackle limited business engagement and enhance the compliance culture of the organization. We assessed five different measures to enhance the compliance culture in our study (Exhibit 9). Dedicated training programs executed by Compliance and periodic newsletters on the topic have been already adopted by most Insurers. A minority of players are starting to explore new ideas, such as:

- Training done by other functions or external professionals (i.e., real case experience from business executives of other companies, practical business cases on compliance, etc.);
- Economic disincentives and sanctions linked to compliance behavior;
- Staff rotation programs that work bi-directionally between business and Compliance, and can provide Compliance officers with front-line business experience.

That said, having a strong business involvement in Compliance is not enough. Another key element of a solid compliance governance framework is the clear distinction between Compliance and other advisory and control functions, particularly Legal and (Operational) Risk Management.

All Insurers participating in our report had Compliance as a standalone function, separated from Legal and Risk Management. However, some differences across players emerged in the role of Compliance, and the interactions across the three functions for compliance-related activities.

The main difference between Legal and Compliance is that Legal is an advisory function (arguably the first line of defense), while Compliance is a control function (second line of defense). Legal carries out legal assessments and gives legal opinions on current and new regulations, as well as support on litigation in court. Legal is usually focused on supporting and defending business functions’ interests.

Conversely, Compliance takes the valuable input of the Legal function and supports the business in formulating the response to these regulations. Moreover, Compliance ensures that regulations are properly enforced. It supports business functions in managing compliance risks, while verifying and questioning the

---

**EXHIBIT 8 | Ownership assessment of compliance activities**

<table>
<thead>
<tr>
<th>Compliance related activities</th>
<th>Business</th>
<th>Compl.</th>
<th>Risk</th>
<th>Legal</th>
<th>Audit</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define compliance risks</td>
<td>0%</td>
<td>92%</td>
<td>8%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Assign compliance risks ownership</td>
<td>0%</td>
<td>83%</td>
<td>8%</td>
<td>0%</td>
<td>0%</td>
<td>8%</td>
</tr>
<tr>
<td>Set standards and define policies and methodologies</td>
<td>0%</td>
<td>83%</td>
<td>8%</td>
<td>0%</td>
<td>0%</td>
<td>8%</td>
</tr>
<tr>
<td>Define control KPIs</td>
<td>33%</td>
<td>42%</td>
<td>25%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Design controls</td>
<td>42%</td>
<td>42%</td>
<td>8%</td>
<td>0%</td>
<td>0%</td>
<td>8%</td>
</tr>
<tr>
<td>Approve controls</td>
<td>42%</td>
<td>42%</td>
<td>8%</td>
<td>0%</td>
<td>0%</td>
<td>8%</td>
</tr>
<tr>
<td>Execute controls</td>
<td>58%</td>
<td>25%</td>
<td>0%</td>
<td>0%</td>
<td>8%</td>
<td>8%</td>
</tr>
<tr>
<td>Monitor adherence to control policies</td>
<td>17%</td>
<td>50%</td>
<td>0%</td>
<td>0%</td>
<td>33%</td>
<td>0%</td>
</tr>
<tr>
<td>Run compliance risk assessments</td>
<td>0%</td>
<td>91%</td>
<td>9%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Report compliance risks (i.e. to Board)</td>
<td>0%</td>
<td>92%</td>
<td>8%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Define mitigating actions</td>
<td>17%</td>
<td>75%</td>
<td>8%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Implement mitigating actions</td>
<td>64%</td>
<td>27%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Provide efficacy assurance on compliance risk mgmt</td>
<td>9%</td>
<td>36%</td>
<td>9%</td>
<td>0%</td>
<td>45%</td>
<td>0%</td>
</tr>
<tr>
<td>Provide legal advisory</td>
<td>0%</td>
<td>8%</td>
<td>0%</td>
<td>92%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Contract management (legal matters)</td>
<td>0%</td>
<td>17%</td>
<td>0%</td>
<td>83%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Research on compliance topics</td>
<td>0%</td>
<td>92%</td>
<td>8%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Lead trainings on compliance</td>
<td>0%</td>
<td>75%</td>
<td>8%</td>
<td>0%</td>
<td>0%</td>
<td>17%</td>
</tr>
<tr>
<td>Engage with regulators (excl. litigation issues)</td>
<td>8%</td>
<td>33%</td>
<td>8%</td>
<td>42%</td>
<td>0%</td>
<td>8%</td>
</tr>
<tr>
<td>Engage with regulators for litigation issues</td>
<td>0%</td>
<td>8%</td>
<td>8%</td>
<td>83%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Source: BCG

Potential market best practice in BCG view
appropriateness of their business practices in the interest of the company and external stakeholders. The primary focus of the Compliance function is not legal advice, but rather implementing and enforcing regulations in business processes, since they can be applied very differently to current business practices. Despite having a legal background and legal knowledge be a key requirement for any senior Compliance role, sound business judgement becomes increasingly important.

Although differing in focus, Legal and Compliance are still required to work closely together.

“We think that Legal and Compliance have many things in common. Compliance, to become a successful business partner, needs to be perceived much more as an advisor (as Legal is) and, rather than limiting business, should be able to manage risks in business activities. Compliance is not an external arm of the Regulator.”

CCO of a Global Insurer

Risk Management and Compliance share many common features, as both functions need to identify, measure, monitor and report risks, as well as support the business in managing them. However, the measurement approach varies significantly between the two functions. Risk Management focuses mainly on producing rigorous, quantitative metrics to determine capital regulatory requirements. Compliance mainly aims to identify and prioritize business processes that are exposed to potential breaches of regulation or compliance risks.

Our interviews revealed, however, that the split of responsibilities between Operational Risk and Compliance is typically not fully defined, with partial overlap of many activities across the two functions (risk identification, risk assessments, reporting, etc.).

“The overlap really materializes when things go wrong; then everyone is looking at the incident,” even if “our governance policy allocates the risks very clearly between control functions.”

CCO of a Global Insurer

Leading Insurers focus Operational Risk departments on identifying and measuring risks with a standardized quantitative approach, including compliance risks. For example, conduct risk could be captured within specific operational risks and event types, such as internal fraud and business practices, as the European Banking Association (EBA) suggested for the 2016 banking stress test.

Conversely, Compliance takes the lead on controls and mitigating actions to properly
manage compliance risks within day-to-day operations, supporting Operational Risk for the qualitative portion of risk assessments, as well, typically focused on controls. Within our sample, at least three Insurers are evolving their operating models in this direction.

It is not feasible instead to fully separate operational versus compliance risks, since these risks and the respective risk takers are very similar. Lack of collaboration between the two functions, with a split of risks, could result in different methodologies, processes and outcomes obtained for similar risks. Resulting actions toward the same business owners could also be duplicated, ensuing in a loss of credibility for both functions.

Organizational structures and reporting lines
The correct assignment of roles and responsibilities between lines of defense is a necessary but insufficient condition for sound compliance risk management. It’s equally important to establish a modern Compliance function, with a solid organizational model built around three cornerstones that emerged clearly from top Insurers in our study:

1. Organizational structure combining specialization in risk types and operational efficiency
2. Group Compliance reporting models to ensure adequate independence of the function
3. Clear division of roles and responsibilities between Group and Local Compliance, with Local CCOs having strong functional reporting lines into Group.

**ORGANIZATIONAL STRUCTURE COMBINING SPECIALIZATION AND OPERATIONAL EFFICIENCY**
The organizational structure of the Compliance function should ensure that the compliance mandate toward internal (business, management, control functions, etc.) and external (policyholders, regulators) stakeholders is properly achieved. In this area, the study identified four main organizational models that can be deployed, each with specific pros and cons (see Exhibit 10):

1. By risk type
2. By activity type

**EXHIBIT 10 | Group compliance organizational model**

![Organizational Model Diagram]

Source: BCG
3. Mixed by risk and activity

4. By geography or legal entity.

In the first model, oriented around risk, organizational units cover specific risks (i.e., AML, sanctions, mis-selling, etc.). This model enables strong risk specialization and creates a unique point of contact for external regulators and other authorities. However, the operational efficiency of this model may be sub-optimal, since similar activities can be split into different units (i.e., reporting, etc.). In our sample, 30% of Insurers have adopted this model.

“We designed risk units to focus on specific regulations and develop the technical skills of our officers.”

CCO of a Regional Insurer

In the second model, each organizational unit performs a set of cross-risk activities (i.e., standards and polices, risk assessments, enabling and training, reporting, etc.). This model leverages synergies across risks, ensuring strong operational efficiency and good communication within the company due to using the same interface for training, risk assessments, etc. The drawback is a limited specialization on single risk matters, which is of rising importance with certain risks (i.e., sanctions, AML, conduct, etc.). In our sample, 10% of Insurers have adopted this model.

In the third model, each organizational unit has a risk or an activity specialization (i.e., AML, mis-selling, risk assessments, etc.), exploiting advantages of both models already outlined: strong specialization on the most important risks, and synergies for concentrating activities that are cross-risk in nature. At this stage, such a model has been adopted by 30% of Insurers in our sample. Notably, we see a clear trend toward this solution, which is also very common in the Banking industry, where players challenged with Compliance organizational choices in 2012-13 have shifted to specialize in specific risks and activities.

In the last organizational model, units mirror the legal, geographical and business structure of the Insurer (i.e., units dedicated to a specific business unit, division or region). The advantages of this model are a focus on country-specific regulations and clear internal interfaces with each business unit. While this is a common model for Insurers (30% of our sample), it appears a “legacy” organization, in which specialization by risk type or activity was not as critical as it is today. We expect this model to be integrated with risk or activity specialization in the future.
We are currently organized by business unit, but lack the specific expertise required on some specific topics such as AML.”

CCO of a Regional Insurer

Independent of the organizational model, most innovative Compliance functions are incorporating regulatory intelligence on future regulations (such as a regulatory map, etc.) and trends in their domain. For most Insurers, this activity is instead carried out in the strategy department or in the business lines, with increasing involvement of the Compliance function.

**Group compliance reporting model ensuring adequate independence**

The survey identified three main reporting models of the Group Compliance function (see Exhibit 11):

1. Standalone Compliance reporting to the CEO or the Board of Directors (35% of respondents);
2. Compliance reporting to the General Counsel, together with Legal (35% of respondents);
3. Compliance within Risk Management, reporting to the CRO (18% of respondents).

The remaining 12% of Insurers have other reporting models (i.e., to Chief Financial Officer [CFO], to Regulatory Director, etc.).

In the first model, Compliance is a standalone function, not grouped with other functional areas. The Chief Compliance Officer can report directly to the CEO or the Board of Directors, assuring the highest level of independence and the highest visibility of compliance topics.

In the second model, Compliance and Legal functions are placed in the same functional area of Risk Management, and both report to a Chief Risk Officer. The rationale is to group control functions and leverage synergies from strict cooperation of Operational Risk and Compliance, since these functions’ activities can overlap, as already discussed.

The choice of organizational design and reporting line is the result of many factors, including organizational history of the role of the Compliance function. It is paramount that, regardless of organizational choices, the Compliance function be granted independence. This is typically achieved by an additional “dotted line” reporting to Board of Directors or Board committees. This structure is becoming increasingly common in the market. The Board must have true and clear oversight of the Compliance function, granting all means necessary to adequately manage compliance (budget, resources, etc.). In addition to independence, the Board’s dotted reporting line can help Compliance to influence more of Insurers’ strategy and key decisions, as described in the fifth section of this paper.

**Split between Group and Local compliance and strong functional reporting lines**

Group, Local and business unit Compliance functions’ mandate should be clearly differentiated, driven by the principle that risks should be managed where risks are taken:

- Group Compliance should be in charge of defining frameworks, policies, standards and methodologies for the Group, a Group-wide risk taxonomy, as well as coordinating Local and business unit compliance activities (i.e., risk assessments). Group Compliance should report compliance risks and initiatives at the Group level and manage the relationship with Group regulators.

“There are better synergies with Legal than with Risk, because we need more often legal advice rather than quantitative support. Risk is too focused on quantitative measurements rather than business operations, and the majority of Risk staff has a financial focus.”

CCO of a Global Insurer
Local and business unit Compliance should support the business in identifying, measuring and managing compliance risks for the business unit. It should provide all the required guidance and methodological support, as well as validate business results and suggest actions. Local Compliance should manage the relationship with the Local regulator.

“Group Compliance must provide local Compliance officers with common tools and methodology to run local risk assessments, ensuring that local Compliance officers do their job, and reporting risk assessments results to the Group Board of Directors.”

CCO of a Global Insurer

Given this model, Local and business unit Compliance independence is usually more at risk than Group Compliance, since Local Compliance has to liaise, on a daily basis, with business functions to assess and mitigate risks and push/verify business functions’ behaviors.

In order to strengthen Local and business unit CCOs independence, some Insurers established a solid reporting line between these groups and Group Chief Compliance Officers (or to Group General Counsels). However, more than 34% of Insurers (see Exhibit 12) have Local and business unit CCOs reporting to Local Directors or Local managers. This creates the risk of their being overruled on business priorities and not being able to influence excessive risk-taking.

To better safeguard the independence of the Compliance function across the Group, Insurers can establish functional reporting lines that includes at least six dimensions:

1. Local and business unit Compliance budget to be approved at Group Compliance level (without substituting, but adding to the approval role of Local and business unit management)
2. Hiring and termination of Local and business unit CCOs must be approved by Group Compliance
3. MBO targets for Local and business unit CCOs must be defined by Group Compliance
4. Performance of Local and business unit CCOs is to be evaluated by Group Compliance
5. Local and business unit Compliance will frequently report to Group Compliance
6. Group Compliance will interact frequently on-site with Local and business unit Compliance.
As reported in Exhibit 12, the industry is not fully aligned with the above model. Group Compliance typically conducts reporting, on-site visits, and hiring and termination of local Compliance Officers. Conversely, MBOs, performance evaluation and budget are largely defined at the Local level, by Local CEOs only. While we understand that these matters are quite sensitive and have an impact on local financial results, we believe that Group Compliance (or General Counsel) must play a significant role in compensation and budget decisions.

Budget has been the most controversial topic in our interviews. Some Chief Compliance Officers stressed that Local management must be held accountable for compliance risks in their business unit, and therefore should have a predominant role in approving Compliance budget.

"Local management must be held accountable for compliance risks in their business units; if I get control of the budget, this accountability would be on me."

CCO of a Global Insurer

Other CCOs suggest more balance and equilibrium in Local Compliance budget approval:

"A strong central oversight is fundamental to ensure control. However, decentralization of power is also important, in order to make local structures more responsible. Therefore, budgets are usually approved locally, but I am strongly involved in Compliance planning and I have a relevant say in this process."

CCO of a Global Insurer

Adequate number of resources, new skill sets and competencies
Compliance functions must be adequately staffed with the required competencies to perform required duties and fulfill responsibilities.

Compliance staff should be balanced between a central Group function and Local units that primarily engage with business to manage risks. We observed different levels of Compliance staff centralization in our sample, usually correlated with the dimension, footprint and complexity of the Insurer. The ratio between Local and business unit Compliance FTEs and Group FTEs ranges from around five for regional Insurers to over 30 for the largest global players.

However, we see large variability even within the same “clusters” of Insurers. For instance, some global players consciously choose to have double the amount of Local Compliance officers, compared to others with a similar number of Group Compliance officers and commensurate gross written premium. Very strong reporting of Local CCOs to Group CCO is associated to this model, as described in the previous section. We certainly see the value of this decentralized organizational model, which ensures that risks are managed in a timely fashion at the local level, with a higher proximity to risk takers, before they become a Group concern.

"Our Compliance framework is very decentralized. We provide minimum standards and general methodology, while Local Compliance designs controls and runs assessments. They better understand local regulatory requirements."

CCO of a Global Insurer

As far as Group Compliance FTEs are concerned, our study assessed typical sizing of these units (see Exhibit 13). Scale plays an important role: Group Compliance size ranges from 10–20 FTEs for the regional players in our sample, to only 25-35 FTEs for their global competitors, which in some cases have more than 10x larger gross written premiums. Of course, the dimension and complexity of the Insurer do not always explain the FTE numbers observed. Other reasons include a different split of activities between Group, Local and business unit Compliance functions, and a recent history of mergers or acquisition, and/or Group restructuring.

Interviews with Insurers revealed that Group Compliance FTEs are expected to increase over the next two years by an average of 10-15%, following changes in the regulatory environment and increasing regulatory pressure, in particular with regard to global players.
“We see an increasing regulatory pressure in the financial crime area and we expect to strengthen our unit.”

CCO of a Global Insurer

Compared to Banking, Group Compliance functions are definitely smaller. In regional Banks they have approximately 50-100 FTEs, while in global Banks they range from 300 FTEs to over 2,000 FTEs (with larger numbers for US-based players). A similar picture applies comparing Compliance FTEs (Group plus Local) to total FTEs, with Banking staff levels being 10-15 times larger than Insurers’ (0.5–2.0% vs. 0.02–0.05%). We do not foresee staffing levels similar to Banking for Insurers in the near future. However, to avoid building up unnecessarily large Compliance departments, Insurers should learn from precedent in the Banking industry. From the onset, Insurers should deploy efficient organizational models with strong business involvement. This approach helps to avoid duplication of activities, extremely large numbers of controls without a risk-based approach, and large departments carrying out manual tasks.

Looking at the distribution of Compliance resources by activity (see Exhibit 14), Compliance staff is mostly focused on setting standards, policies and methodologies, driving compliance risk assessments, and defining (and executing) controls. This entails a total absorption of, on average, over 50% of total FTEs. Reporting and enabling activities, such as training, currently absorb around 17% of resources, but most of the Insurers interviewed recognize the need to invest further in this area.

“We must design and coordinate, centrally, global training programs for business and Compliance.”

CCO of a regional Insurer

The distribution of resources by risk category shows that Insurers are currently focused on client and data protection, and financial crime, deploying around 65% of total FTEs in these areas. The remaining 35% of total FTEs is dedicated to the other risk categories combined.

The next section illustrates how this distribution of resources maps neatly with the risk categories Insurers perceive to be most critical, as determined in the risk assessment portion of our study. The differing nature of Insurance and Banking businesses, whereby insurance products are more complex and less familiar to consumers, often require more sophisticated usage of personal data. This makes us believe that “conduct”-related risks, such as client interest, will remain predominant in Insurance (also versus financial crime risks, which significantly dominate the Banking industry).
Beyond current risk and activity allocation, Chief Compliance Officers are realizing the importance of having new skills in their departments. There is a new emphasis on business and risk management knowledge, compared to the legal background traditionally required.

“I think the most important skills for Compliance officers to have are business knowledge and soft skills; these are fundamental to carry out our job independently and effectively, and to be perceived as a valuable function in the company.”

CCO of a Regional Insurer

Finding Compliance officers with business skills is not easy, as noted in our study: “The challenge now is making Compliance interesting for business people, as they would be better than long-term Compliance professionals.”

“Interpretation and understanding of current principle-based regulation is much easier than it used to be (from a legal point of view). It’s plain and simple language. However, the challenge is now more complex, requiring to understand risks around the rules, and help and guide business to manage risks in business processes”

CCO of a regional Insurer

Compliance officers must manage risks like Risk Management officers, and they need business skills to effectively engage with their business colleagues to become trustworthy, credible partners. Many CCOs believe the ability to integrate these new skills in the current compliance environment will be a key success factor for the future effectiveness of their departments. Chief Compliance Officers need to deploy a full set of levers to achieve this target, including external targeted recruiting, training courses, staff rotational programs and other internal relocations.

Some of the most advanced Compliance departments we interviewed are considering introducing “big data” analytic skills into this group. In their view, data analysis could be a key to identifying trends in potential compliance breaches. However, to our knowledge, none of the interviewed Insurers have fully adopted such an approach.

**NOTES**
1. BCG global Banking compliance benchmarking, 2015.
Compliance risk taxonomies

Establishing clear, structured compliance risk taxonomies is not a formal exercise, but the necessary starting point of any compliance methodology and process. If compliance risks cannot be clearly described, they cannot be measured in risk assessment with the business. Nor can they be managed with appropriate mitigating actions, or reported on across the organization in a consistent and coherent manner.

Best-practice compliance risk taxonomies should be clearly integrated with an operational risk taxonomy and event types. In addition, a distinction between Group-wide risks, homogeneous across the Group, and Local risks helps to determine priorities when formulating mitigating actions, as well as decisions on creating centers of excellence at the Group level to manage specific risks.

However, our interviews revealed (see Exhibit 15) that while ~80% of Insurers differentiate Group-wide risks from Local risks, only ~30% of players integrated compliance and operational risk taxonomies. Both conditions were present in just ~20% of Insurers.

Once again, taxonomy definition is not a formal requirement or a mere methodological exercise, but rather an important prerequisite to effectively manage the entire spectrum of Insurers’ risks. Such an approach would avoid potential overlaps between compliance and operational risks that can result in:

- Duplication of risk assessment activities with the business (risk takers);
- Unclear risk priorities, if similar risks are ranked differently in different assessments;
- Incoherent control framework on similar risks, if different or overlapping and partially contradictory controls are defined for similar risks.

All of these pitfalls have been pointed out by Insurers in our study. For example, one CCO explained:

“We manage data privacy, and risk management manages data protection separately, despite great similarities between them.”

CCO of a Regional Insurer

Leading Insurers in our panel have been very explicit in their opinions on the advantages of an integrated approach. The CCO of a global Insurer mentioned:

“We have an integrated taxonomy with Operational Risk …Operational Risk drives the design and deployment of risk measurement, while Compliance usually performs gap analysis and operationalizes regulatory requirements into business processes.”

CCO of a Global Insurer
Risk assessments

Risk assessments are the first pillar of a comprehensive compliance risk management. They aim at prioritizing risks based on objective evidence, expert opinions and business feedback, providing clear views of the risks and the processes they affect. As such, they cannot be run as gap assessments on each of the regulatory requirements. Conversely, they require to measure the risks underlying each regulation, with deep understanding of the Insurer’s business model. Risk assessments should provide clear guidance on where to focus remedial actions and controls.

“A risk assessment is not a gap analysis but rather putting a price to risks”

CCO of a global Insurer

Our survey identified two categories of risk assessment processes: a traditional bottom-up assessment used by most of the Insurers and a top-down assessment used by only a few Insurers (see Exhibit 16).

In the bottom-up assessment, Compliance officers engage risk owners (up to 20-30 for each business unit) to measure the current level of inherent risk and the impact of internal control system (hence, residual risk), based on a detailed taxonomy that links each regulatory requirement to a certain risk. This is a long and time-consuming exercise, to be completed for all significant business units, Legal Entities and processes, on a very broad set of regulations. The bottom-up approach typically lacks an ex-ante prioritization (it is not risk-based), necessary to focus assessment efforts and to facilitate executive decisions on risk mitigation.

In the top-down risk assessment, Chief Compliance Officers 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 (not more than 15–20 risks);
- Determine the business processes in which these risks are particularly relevant;
- Discuss the impact of new strategies and strategic initiatives on the compliance risk profile.
We believe top down-risk assessments, which require much less time and effort than a bottom-up approach, can help Insurers to:

- Prioritize efforts on a risk-based approach, which has been suggested by many regulations (i.e., the new AML Directive in Europe); these risks will be the main focus of a more traditional and detailed bottom-up assessment;
- Encourage Board of Director and executive manager involvement and ownership of compliance as a business imperative;
- Link compliance to the company strategy (discussed in depth in the next section of this paper);
- Adopt a forward-looking perspective to assess not only current but also emerging risks over the planning horizon.

The common standard to measure risks is the inherent versus residual risk framework. Inherent risk is the gross risk level (without any control or with previous period controls); residual risk is obtained from inherent risk considering the current level of controls (see Exhibit 17).

Despite widespread use of this framework, significant differences remain in the methodology used for inherent risk calculations. Some Insurers adopt a quantitative approach, comparing expected losses, which include sanctions and other costs (litigation, etc.), with certain thresholds of financial results (i.e., operating income). The obtained risk level could be adjusted for expected reputational damages, leveraging other pre-defined scales with different severity levels.

Conversely, other Insurers adopt a purely qualitative (but still rigorous) approach, in which inherent risks are divided into a series of drivers. These are assessed on qualitative scales from risk owners and verified by Compliance officers. This approach is not necessarily less rigorous, since the objective of risk assessments is to prioritize compliance risks to launch appropriate actions, not to forecast their expected level next year.

As already noted in the Governance and Organization section of this paper, most innovative Insurers are putting together compliance risk assessment and operational risk self-assessments. In many cases the assessment feeds the operational risk internal model.
Here, Insurers usually use a scenario-driven approach, combining compliance with operational risk. For each business unit, 20 to up to 70 scenarios (descriptions of potential loss events in a specific business context) are chosen to represent all operational risks. Together, Compliance and Operational Risk support executive managers and business functions to assess the impact of scenarios with ad hoc workshops. When possible, they leverage external data and expert opinions as a starting point for the discussion. Given the potential synergies of a coherent approach between Compliance and Operational Risk, we encourage Insurers to take this direction.

The level of involvement of the Board of Directors, executive managers and the wider business in risk assessments can vary significantly across Insurers. Players using a top-down risk assessment method typically engage the business significantly. Others running only bottom-up exercises can delegate most of the risk assessment to Compliance officers only, with the role of business limited to an ex-post validation. To make a risk assessment truly reflective of the business’ risk profile, Compliance needs to take into account the business owners’ point of view, since they are typically the actual risk takers.

Finally, most advanced Insurers are developing a Compliance Risk Appetite Framework to embed shareholders appetite for compliance risks into risk assessments. The Board of Directors of these Insurers, supported by the CCO, sets tolerance limits for compliance risks that are subsequently cascaded into business units and linked to the results of compliance risks assessments (see Exhibit 18).

“We draw a risk map with the inherent risk on one axis and the controls environment on the other axes, which give us a very good positioning of the different risks. Then we compare the positioning of each risk against our Risk Appetite Framework to identify priorities and the risks where to focus on”

( CCO of a global Insurer)

In this way, Insurers are adding to the traditional “zero appetite” philosophy for non-complying with regulations a clear appetite for the risks related to them. Compliance

---

**EXHIBIT 17 | Risk assessments and quantification models**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherent risk</td>
<td>Gross compliance risk, without taking into account controls or with previous period controls, it usually include:</td>
</tr>
<tr>
<td></td>
<td>• Sanction loss</td>
</tr>
<tr>
<td></td>
<td>• Reputational damage</td>
</tr>
<tr>
<td></td>
<td>• Other losses (i.e. legal expense)</td>
</tr>
<tr>
<td>Control measures</td>
<td>Organizational and control measures put in place to mitigate the risk under analysis:</td>
</tr>
<tr>
<td></td>
<td>• Risk specific control activities</td>
</tr>
<tr>
<td></td>
<td>• Contingency plans and procedures</td>
</tr>
<tr>
<td>Residual risk</td>
<td>Compliance risk level after all efforts to reduce risk have been made, it results in:</td>
</tr>
<tr>
<td></td>
<td>• Risk acceptance - within risk appetite</td>
</tr>
<tr>
<td></td>
<td>• Risk rejection - requires further control measures</td>
</tr>
</tbody>
</table>

---

**Models for inherent risk quantification**

1. **Quantitative rating**
   - Expected loss
   - Economic value of reference
   - Rating system
   - Reputational damage
   - Qualitative rating:
     - High – significant potential loss, reputational damage and risk of criminal investigations against BoD and top mgmt
     - Medium – moderate potential loss and increase in complaints, damage to brand image
     - Low – no material risk (loss or reputational)

2. **Qualitative rating**
   - High – significant potential loss, reputational damage and risk of criminal investigations against BoD and top mgmt
   - Medium – moderate potential loss and increase in complaints, damage to brand image
   - Low – no material risk (loss or reputational)

---

Source: BCG
risks levels will never be equal to zero. Realizing that compliance risks can only be mitigated, not completely eliminated, helps to understand priorities and maximizes the efficacy and efficiency of mitigating actions.

Many challenges remain in this space, such as identifying rigorous indicators to define the risk appetite given the more qualitative nature of compliance risks compared to financial risks.

“We thought about integrating conduct in the risk appetite framework with quantitative indicators, but we decided not to do it. Conduct is currently in the risk appetite statement, and the business assesses itself against it qualitatively.”

(CCO of a regional Insurer)

Managing compliance risks

Most of the Insurers we interviewed specified establishing an effective control system as the most important way to manage and mitigate compliance risks. As observed in the Governance section of this report, Compliance should provide guidance to design and test controls, with a second-line-of-defense lens, while business functions should effectively execute and implement them.

Again, the parallel with Banking is illustrative. The relatively recent proliferation of new regulations and regulatory pressure pushed several Banks to put in place very costly controls systems. As controls have been designed over time without a clear and complete picture of risks, they usually lack of coherent framework. For example, duplicated checks (sometimes with contradictory outcomes) or controls for low risks (e.g., for environmental matters) having the same intensity of those applied to high risks (i.e., for sales and distribution). This results in compliance stifling business, sometimes without decreasing risk exposure. The insurance industry can learn from these mistakes and take a clean sheet approach. Hence, Insurers should rigorously review their controls framework, updating guidelines and policies, understanding risk factors, reviewing controls objectives and risk indicators and rationalizing controls activities. As a starting point, they could launch an effective control framework review based

---

**EXHIBIT 18 | Risk Appetite Framework**

![Risk Appetite Framework Diagram](diagram.png)

Source: BCG
on the 10 levers presented in Exhibit 19, which combine market best practices observed in this study.

One of the key concepts is to clearly link the strength and number of controls to the level of residual risk measured by the risk assessments. Controls must be focused where the perceived residual risk is significant, with the “risk-based” logic that is embedded in several recent national and international regulations (i.e., AML Directive IV in Europe).

Structured compliance reporting

Reporting of compliance risks varies significantly across the industry. We believe that structured compliance reporting must include at least three levels (see Exhibit 20):

- Aggregated compliance risk level indicators, which should provide an immediate and simple view on overall compliance risks;

- A synthetic overview of critical compliance risks, external early warning indicators, and ongoing mitigating actions and compliance programs;

- Detailed deep dives on single risks and risk indicators, engaging specific risk owners as a way to monitor and measure progress on mitigating actions, controls and programs.

While detailed deep dives are common at most Insurers, a synthetic, simple and clear view of compliance risks is typically more difficult to provide. In addition, this synthetic view is very rarely integrated with operational risks, which would be the most useful reporting for interaction with Boards of Directors and executive managers.

Few insurers are also working on aggregated Key Risk Indicators of compliance. The most difficult element of such indicators involves merging very different metrics and qualitative information into a KRI number. Usually, the first step is to define the “risk tree” containing all the drivers that contribute to the indicator. Once the risk tree is defined and syndicated with Board of Director and executive managers, Compliance will find the appropriate way to measure and compare each of the drivers, and build the overall indicator.
An even lower number of Insurers is working to include early warning compliance risk indicators in their monitoring and reporting system. These indicators usually leverage emerging technology, such as Big Data, to provide a forward looking view of the risks arising from the market place and the external environment. Examples of early warning indicators include comprehensive data on industry sanctions (by geography, sector and risk), semantic analysis of regulators’ statements and public interviews, customer research and public sentiment on conduct risks.

Notes
1. “Business-wide risk assessments should help firms understand where they are exposed to ML/TF (money laundering/terrorism financing) risk and which areas of their business they should prioritize in the fight against ML/TF.”
LEVERS FOR COMPETITIVE ADVANTAGE

The relevance and breadth of compliance risk management is a strong incentive for Insurers to go beyond merely complying with regulation; it presents an opportunity to turn compliance into a competitive advantage. Our study suggests that best-in-class Insurers:

- Enable the Board of Directors to understand compliance risks and take informed compliance decisions;
- Embed compliance in Insurers’ strategic thinking, and optimize the business model around regulatory requirements and compliance risks, structurally engaging Compliance in finding solutions ex-ante rather than checking compliance ex-post;
- Ensure the right level of critical investment in compliance, including operating model enhancements, risk assessments, reporting, IT tools and training programs.

Ensure Board of Directors steering role
The volume of current and upcoming regulatory requirements affecting insurance companies and their Boards of Directors, together with Board members’ new responsibilities, are pushing Boards’ interest in compliance topics to unprecedented levels (see Exhibit 21).

With the support of specific committees, the Board of Directors should:

- Define a compliance strategy that is integrated into the overall business strategy;
- Ensure proper functioning of a strong, independent Compliance function;
- Monitor relevant compliance risks and approve required mitigating actions.

For more than 75% of the Insurers interviewed, Board committees (i.e., Risk, Control or Audit) meet at least on a quarterly basis to discuss compliance topics. Even if compliance discussions are quite frequent, Chief Compliance Officers’ specific contribution still needs to be codified for most players (see Exhibit 22). All CCOs interviewed are invited to Board committees only on an ad hoc basis to discuss compliance issues or present periodic reports. Very few CCOs are proactively involved in strategic discussions on compliance risk profile and regulatory strategy.

CCOs highlighted common challenges to engage Boards of Directors, including:

- Limited Board knowledge of compliance topics;
• Technical compliance concepts are difficult to translate into simple and managerial messages;

• Uncertainty about the type of information to be reported.

To cope with these challenges, leading players are launching training programs for Boards of Directors, including self-assessments and regulatory inductions, already quite common for Banks.

---

**EXHIBIT 21 | Board of Directors involvement in compliance topics**

<table>
<thead>
<tr>
<th>BoD involvement – CCOs’ view</th>
<th>BoD committees discussions of compliance topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>BoD involvement on compliance is increasing; the challenge is now to find a good way of reporting to them, but we are still quite far from an effective support</td>
<td>% of respondents</td>
</tr>
<tr>
<td>Regional Insurer</td>
<td>Monthly 8</td>
</tr>
<tr>
<td></td>
<td>Quarterly 50</td>
</tr>
<tr>
<td></td>
<td>Half-yearly 17</td>
</tr>
<tr>
<td></td>
<td>Yearly 0</td>
</tr>
<tr>
<td></td>
<td>Other 25</td>
</tr>
</tbody>
</table>

Source: BCG

---

**EXHIBIT 22 | CCOs contribution for Board of Directors**

<table>
<thead>
<tr>
<th>CCO participation to steering</th>
<th>Different levels of CCOs contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member of the Board of Directors?</td>
<td>We prepare reports and answer questions off-line; sometimes I make tailored presentations</td>
</tr>
<tr>
<td>Yes</td>
<td>Regional Insurer</td>
</tr>
<tr>
<td>No</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Member of Board Committees?</th>
<th>I participate to Risk Committee’s sessions when relevant compliance issues emerge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Regional Insurer</td>
</tr>
<tr>
<td>6%</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>94%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Invited to Board Committees?</th>
<th>I prepare a report to the Audit Committee and attend the Committee only if required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Global Insurer</td>
</tr>
<tr>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>0</td>
</tr>
</tbody>
</table>

| CCOs not member of steering bodies but participant to selected Committees’ sessions | From off-line explanations to quarterly dashboards presented to a BoD Committee |

Source: BCG
Embed compliance into strategic thinking

We believe that forward-looking management of compliance is of critical importance for Insurers. All players should establish a structured, periodic and codified way to engage with the Board of Directors and executive managers in order to embed compliance into strategic thinking. This could take the form of dedicated sessions with strategic plan cycles, as well as dedicated Board committees or subcommittees.

At current stage only approximately 15% of Insurers bring compliance risk management up to strategic level (see Exhibit 23), typically those with a top-down risk assessment in place. In this way, they proactively embed compliance thinking into the strategy of the company and the main strategic initiatives launched by Business. The integration of such forward-looking perspective with the ex-post perspective of standard controls enhances dramatically current and emerging compliance risks mitigation.

Most advanced Insurers fully integrate compliance risks into their Own Risk and Solvency Assessment (ORSA). CCOs of these Insurers produce synthetic managerial reports on compliance risks embedded in current and perspective business model, which feed a “living ORSA” used to establish a dialogue between Risk Management, Compliance, executive managers and business leaders.

“We are going to setup a double signature model for new products and strategic initiatives: the first addressing the product financial profile (by risk management), and the second addressing the product conduct profile (by compliance)”

(CCO of a regional Insurer)

“We call our ORSA a “living ORSA”, being an evolving document always updated for the BoD and executive managers. We avoid the tick-the-box approach in order to make the ORSA useful, providing an effective view of risks and facilitating informed decisions. For this reason we include business plan impacts on the compliance profile, reviewing the plan if necessary and linking everything back to the ORSA”

(CCo of a global Insurer)
Embedding compliance into strategic thinking would enable Insurers to perceive compliance not only as a cost or potential threat of doing business, but also as a source of strategic competitive advantage. Regulatory requirements can be turned into new opportunities in a broad set of domains such as distribution, product design, customers and customer data, etc.

As a case study, the Insurance Distribution Directive II in Europe is bringing fundamental changes to the relationship between Insurers and their intermediaries, as well as required information disclosure to customers. This raises several strategic questions (see Exhibit 24).

A best-practice compliance risk management approach proactively incorporates the expected changes from the new regulations into the distribution strategy. It leverages new information requirements to develop innovative products targeting specific customers with focused marketing campaigns. Such an approach would deliver tangible value for the Insurer and dramatically reduce compliance risks from inception, with a forward-looking perspective.

Ensure appropriate level of investments

Insurers must allocate the required budget to enhance their compliance risk management framework, keep current with regulatory requirements and integrate compliance into business strategy. Chief Compliance Officers outlined three main areas of current investments (see Exhibit 25):

- Review of operating models, including roles and information flows between control functions, compliance processes to engage business and Compliance function review;
- Design of risk dashboards and risk reporting, an increasingly common request from Boards of Directors that additionally requires integration with risks presented by Risk Management;
- Training programs for Compliance officers, and management and business functions, including methodologies, processes and business cases to understand compliance risks.

Exhibit 24 | Insurance Distribution Directive II key questions

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Strategic points to be addressed</th>
</tr>
</thead>
</table>
| BoD roles and responsibilities | • Management of professionalism requirements for members of BoD (knowledge certificates, continuing professionalism requirements, etc.)  
• Identification of the functions involved in BoD assessment and training  
• Potential change of BoD composition due to new requirements |
| Business and Strategy          | • Identification of the customer segments whose profitability is affected the most  
• Management of customer behavior changes in response to additional information available  
• Review of policies and interfaces for services and claims  
• Management of the impacts on distribution channels (i.e. brokers, online, etc.), especially on intermediaries subject to new strict requirements (i.e. registration, capital, etc.)  
• Identification of implications on the product mix (i.e. bundled products, IBIP2, etc.) and on products features  
• Identification of consequences of ban of inducements2 and prohibition of tying practices3  
• Identification of implications on volumes, prices and products margin |
| Organization and Processes     | • Review of the product development process (identify target market, assess risks,...)  
• Management of the increase in documentation volumes (on costs, nature of advices, etc.), also reviewing the processes behind (i.e. customer suitability assessment, etc.)  
• Review of the policy for assessment/training of the staff involved in products distribution |

Source: BCG

1Insurance based investment products.  
2Prohibition for intermediaries to receive commissions from third parties as incentive/other.  
3Selling products in a package with ancillary products/services where the single products are not available to be purchased separately (i.e. obligation to open a current account when purchasing an insurance)
As a final remark, we assessed qualitatively the level of compliance investments made by each Insurer. Not surprisingly it is significantly lower — on the order of five times lower — than Banks. Investment levels range from <$1 million a year for regional Insurers, up to $5-10 million annually for very large global Insurers. However, we believe that investments in the Insurance industry will dramatically increase during the next several years, raising the importance of prioritizing interventions and focusing on those that truly matter.
LOOKING AT THE RESULTS of the study, we foresee five levels of intervention that global and regional Insurers should consider to evolve their compliance capabilities:

1. Perform a rapid health check to quickly benchmark a starting point versus peers, and regulatory expectations on a pre-defined set of dimensions;

2. Launch compliance risk assessments and mitigation programs, focusing on the most critical risks, and embedding a strategic and forward-looking view;

3. Revise compliance governance to reflect priority risks and move toward a more business oriented approach, making compliance governance “Regulator-ready”;

4. Strengthen Holding company and Local Compliance functions, ensuring that the right organization, activities, sizing and competencies are in place;

5. End-to-end review of the control framework with a risk based approach, including policies and procedures, risk factors, controls objectives and control activities

6. Launch ad hoc training programs to apply compliance risk management to real business cases, with different training types for Board of Directors, management, business and Compliance.

RAPID COMPLIANCE HEALTH CHECK

We encourage Insurers to perform a rapid health check of their starting point, comparing it with:

- Most representative competitors, in terms of business type, geographical footprint and, consequently, risks the Insurer is exposed to;

- Regulatory requirements and underlying Regulators’ expectations.

The health check should consist of a standard survey with qualitative and quantitative questions, plus selected interviews with executive managers, business and Compliance functions. Insurers can use these inputs to assess their own compliance maturity and compare it with external benchmarks, leveraging the dimensions outlined above in the Maturity Model.

RISK ASSESSMENT AND MITIGATION PROGRAMS (COMPLIANCE PROGRAMS)

Whenever Insurers believe they are exposed to specific compliance risks, whether driven by industry trends, change initiatives, regulatory findings or internal sentiment, they should assess these risks across their business processes and mitigate them. The “golden rules” for assessment and mitigation programs include:
• Ensure executive sponsorship and endorsement to mobilize the organization;

• Embed a forward-looking view, considering business strategy and regulatory evolution, with active engagement of the Board of Directors and executive managers;

• Involve business functions, which should drive risk assessment and mitigation;

• Leverage the Compliance function to design frameworks, support business and validate results;

• Actively engage with Regulators (i.e., preparing ad hoc communication plans);

• Build enabling elements during the exercise (i.e., dashboards, training programs).

As an example, an Insurer with significant business in the US might want to launch a global assessment of financial crime risks, focused on sales, distribution and asset management processes. The assessment starts by designing (centrally with Group Compliance) ad hoc surveys, whose focus should be based on the top down view of executive managers. The surveys are then answered by business units with support of their Compliance functions and validated centrally (see Exhibit 26).

Having identified specific business units and business processes that bear the highest financial crime risks, Insurers could then strengthen their controls and launch remedy actions, if needed.

Compliance governance review

Insurers can review and enhance Compliance governance and responsibilities, ensuring a stronger involvement of business functions and clear interfaces among control functions. Successful projects to review a Compliance operating model include:

• Board of Directors and executive managers driving the review by defining underlying compliance principles and strategy, as well as guidelines to split responsibilities across functions;
- Group and Local senior business executives and management syndicating and agreeing on new roles and responsibilities to be taken;

- The Compliance function discussing and tailoring agreed-upon general principles to the specific context, processes and controls of the Insurer;

- Orga/HR function supporting the review of guidelines, policies, procedures and processes, together with Compliance.

Such projects can be carried out with limited internal resources and bring clear tangible benefits:

- Internally, they align all key functions (at least at the senior level) on new responsibilities and favor their proactive engagement;

- Externally, they clarify the compliance strategy of the company and make compliance documents Regulator-ready; governance is typically the entry point of many inspections.

### Compliance function strengthening

Strong business involvement in compliance and clear split of responsibilities among control functions is not a substitute for the role of the Compliance function itself. If anything, it requires a stronger Compliance function, which has the structure, the knowledge and skills to support and challenge the business. Compliance function strengthening includes several streams:

- Ensure the right reporting line of Local and business unit CCOs to the Group CCO. A strong reporting line goes well beyond reviewing organizational charts and typically entails Group CCO power on HR and budget decisions. This stream is typically performed with the support of the Orga/HR function and involves syndication with executive managers.

### Potential objectives of privacy controls

<table>
<thead>
<tr>
<th>Regulation and internal policies</th>
<th>Potential objectives of privacy controls</th>
<th>Aligned vs requirement?</th>
</tr>
</thead>
<tbody>
<tr>
<td>External regulation on privacy</td>
<td>Ensure the password policy is applied to every insurer's application and system</td>
<td>![Blank]</td>
</tr>
<tr>
<td></td>
<td>Ensure adequacy of digital certificates-based authentication tools and other authentication tools</td>
<td>![Blank]</td>
</tr>
<tr>
<td></td>
<td>Ensure usage of a common workflow to manage applications authorization and authentication</td>
<td>![Blank]</td>
</tr>
<tr>
<td></td>
<td>Ensure passwords are changed at least every 2 months for general data and monthly for critical data</td>
<td>![Blank]</td>
</tr>
<tr>
<td></td>
<td>Ensure passwords contain numerical, alphanumeric and special characters</td>
<td>![Blank]</td>
</tr>
<tr>
<td></td>
<td>Ensure that processes to manage client credentials do not involve direct participation of insurer's employees</td>
<td>![Blank]</td>
</tr>
</tbody>
</table>

---

**Source:** BCG

---

**EXHIBIT 27 | Interpretation of regulations in line with market practices**

<table>
<thead>
<tr>
<th>Regulation and internal policies</th>
<th>Potential objectives of privacy controls</th>
<th>Aligned vs requirement?</th>
</tr>
</thead>
<tbody>
<tr>
<td>External regulation on privacy</td>
<td>Ensure the password policy is applied to every insurer's application and system</td>
<td>![Blank]</td>
</tr>
<tr>
<td></td>
<td>Ensure adequacy of digital certificates-based authentication tools and other authentication tools</td>
<td>![Blank]</td>
</tr>
<tr>
<td></td>
<td>Ensure usage of a common workflow to manage applications authorization and authentication</td>
<td>![Blank]</td>
</tr>
<tr>
<td></td>
<td>Ensure passwords are changed at least every 2 months for general data and monthly for critical data</td>
<td>![Blank]</td>
</tr>
<tr>
<td></td>
<td>Ensure passwords contain numerical, alphanumeric and special characters</td>
<td>![Blank]</td>
</tr>
<tr>
<td></td>
<td>Ensure that processes to manage client credentials do not involve direct participation of insurer's employees</td>
<td>![Blank]</td>
</tr>
</tbody>
</table>

---

**Example**

"The treatment of personal data by electronic means is allowed only to appointees provided with security credentials"
Perform a gap analysis of Compliance officers’ skills to build an HR plan to strengthen the talent pool. This stream is typically performed with the support of Human Resources.

Based on our experience, Compliance function strengthening typically does not entail a significant FTE increase, but rather a redefinition of Compliances’ role and positioning in the organization, as well as a significant enhancement of Compliance officers’ skill sets. In a few cases, it can lead to a FTE decrease, for instance when Compliance carries out first-line-of-defense activities (investigations, controls) that can be moved to business or middle-back office.

End-to-end control framework review

Once Insurers have obtained a clear understanding of their compliance risk exposure and have set up a strong compliance governance and organizational model, they should focus on revising their control framework. A best practice approach should aim at optimizing controls ensuring coherence, standardization, prioritization, automation and, most importantly, a strong focus on relevant risks. Insurers could optimize their control framework in line with these general principles using the 10 levers illustrated above in this study. For example, a more precise interpretation of regulations could reduce controls over-scoping and consequent effort (see Exhibit 27).

Training program setup and launch

The revision of the control framework may result insufficient to effectively enhance compliance, particularly for large organizations that require higher mobilization and education of resources to change behaviors, rather than just reviewing policies and procedures, prescribing control activities or even discussing compliance issues with Boards of Directors and senior executives.

Training programs should explain the underlying philosophy of Compliance governance. These programs should train business and control functions to apply compliance principles and methodologies to everyday business
activities. Based on our experience, these training programs should cover at least three sets of stakeholders, with customized content and training solutions:

- Board members and Group/Local executive managers, who need to understand and debate new Compliance governance and strategy, and who can engage in top-down risk assessments;

- Local business functions, which need to master basic compliance concepts and apply them to their respective processes, with a clear grasp of what must change;

- Local Compliance officers, who need to have the same knowledge as their Group counterparts on compliance methodologies, tools and, most importantly, how to support Local business functions effectively.

Training programs start with a three- or four-day workshop to establish common ground, and then move into vertical training on specific processes and risks. In parallel, Compliance officers can reinforce business skills with short rotational programs. Finally, Compliance officers can be trained on soft skills, such as communication (see Exhibit 28).
REGULATORY CHANGES AND EMERGING business models are making compliance risk management a top concern for Insurers’ Boards of Directors and executive managers, not merely a formal exercise. Awareness of compliance risks has risen dramatically in the Insurance industry and, as our study showed, many players have already started the journey toward structured, business-driven and forward-looking compliance risk management practices.

Nonetheless, we found that there is still significant work to be done. In this paper, we outlined three dimensions that many Insurers could benefit in strengthening:

1. Governance and organization: strong and proactive engagement of business functions, clear compliance roles and responsibilities across controls and advisory functions, specialized and efficient Compliance functions, strong reporting lines of Local CCOs to the Group CCO, and Compliance officers with the right set of legal, business and risk management skills;

2. Methodologies and processes: structured and integrated risk taxonomies, top-down risk assessment complementing a bottom-up approach, a compliance risk appetite, a risk based, efficient control system, and managerial reporting integrated with operational risk;

3. Levers for competitive advantage: Board of Directors proactive engagement model, compliance embedded into overall strategy, and adequate investments to ensure a level of compliance risk in line with Risk Appetite.

Finally, we suggested a practical roadmap for Insurers to tackle and implement the new compliance paradigm, outlining different initiatives according to an Insurers’ starting point.
About the authors
Matteo Coppola is a partner and managing director in The Boston Consulting Group’s Milan office, and the global leader of the risk and compliance segment of the Insurance practice.

Ofir Eyal is a principal in The Boston Consulting Group’s London office, leading risk management projects within the risk and compliance segment of the Insurance practice.

Lorenzo Fantini is a principal in The Boston Consulting Group’s Milan office, leading compliance projects within the risk and compliance segment of the Insurance practice.

Giacomo Testa is a member of the consulting team in The Boston Consulting Group’s Milan office, actively involved in risk and compliance projects in the Insurance and Financial Institutions practices.

Acknowledgments
The authors would like to thank the external stakeholders who generously supported the realization of the study, providing insights and bringing visibility, in particular:

- The 17 Insurers who discussed with us current industry trends and best practices to manage compliance risks, through dedicated interviews with their Chief Compliance Officers, General Counsels and other senior executives;
- The members of national and international authorities, who engaged in discussions on the results of this study;
- The members of the Global Insurance Chief Compliance Officers Forum, who gave us the opportunity to present the results of this study.

For Further Contact
To discuss the findings of our study in greater detail, please contact one of the authors.

Matteo Coppola
Partner and Managing Director
BCG Milan
+39 02 65599 406
coppola.matteo@bcg.com

Ofir Eyal
Principal
BCG London
+44 207 753 5653
eyal.ofir@bcg.com

Lorenzo Fantini
Principal
BCG Milan
+39 02 65599 729
fantini.lorenzo@bcg.com

Giacomo Testa
Associate
BCG Milan
+ 02 65599 604
testa.giacomo@bcg.com

NOTE TO THE READER
Managing Insurers’ compliance risks in a changing environment