OLIVER WYMAN

JUMPING FORWARD

Compliance in Insurance

Elena Belov
Allen Meyer
Michael Moloney
Paul Ricard
Doris Li

INTRODUCTION

As we venture into 2020, evolving regulations and changing consumer behavior will impact insurers. Cybersecurity, data privacy, and customer protection continue to shape new challenges and trigger regulatory scrutiny.

As an insurance leader, you may already be considering how to address regulatory and risk management challenges—and it's a daunting task. At Oliver Wyman, we have been working with clients to solve these issues and more effectively manage compliance risks. Our paper delves into the challenges and impacts our clients are facing. We present the strategic changes and quick wins needed to effectively manage compliance, including how to develop a risk-based compliance program, increase engagement with the overall business, and fully align other non-financial risk functions.

BACKGROUND

The financial crisis highlighted the staggering financial and reputational impact compliance failures can have on institutions. Since 2008, regulators globally have sought to raise the bar for compliance risk management—imposing stricter standards on how financial services companies manage their obligations. Recently, there has been significant focus on compliance practices at insurers, in addition to new laws and regulations related to sales practices, market conduct, privacy, and individual accountability.[1] This, coupled with changes in customer expectations, business mix, and technology have only further increased the challenges insurers face to manage their compliance risks.

WHAT'S NEEDED? STRATEGIC CHANGES

In our experience, Compliance functions at insurers tend to be less mature than those at other regulated financial institutions. Similarly, insurers typically have fewer resources dedicated to compliance risk management and less influence and impact within their organizations than at other types of regulated financial institutions.

1 In the United States, constant changes in state-wide regulations such as the recent New York Department of Financial Services Best Interest regulation and the California Consumer Privacy Act have heightened the focus on the rights of customers. These initiatives are part of global trends around privacy (e.g., EU General Data Protection Regulation), and sales and market conduct (e.g., FCA Insurance Distribution Directive). In recent years, more stringent requirements around governance and accountability, as outlined in Solvency II or the UK's Senior Managers and Certification Regime have triggered similar regulations around the world, such as the China Risk-Oriented Solvency System ("C-ROSS"), Australia's Banking Executive Accountability Regime ("BEAR"), or Hong Kong's Manager-In-Charge ("MIC").

As a result, insurance companies need to take a hard look as to whether their Compliance functions are keeping pace with this heightened degree of complexity, scrutiny and change. In this paper, we recommend that insurers make three strategic changes to more effectively manage existing and evolving compliance risks:

- **Establish risk-based compliance programs** to focus on the most important compliance risks rather than applying similar intensity across all obligations.
- **Increase the engagement between Compliance and the business and corporate functions** to enable a broader firm-wide effort to manage the most important compliance risks rather than having these efforts shouldered by Compliance.
- **Work more closely with other non-financial risk management functions** in order to more seamlessly manage the firm's top risks (e.g., privacy and cyber) in a similar fashion.

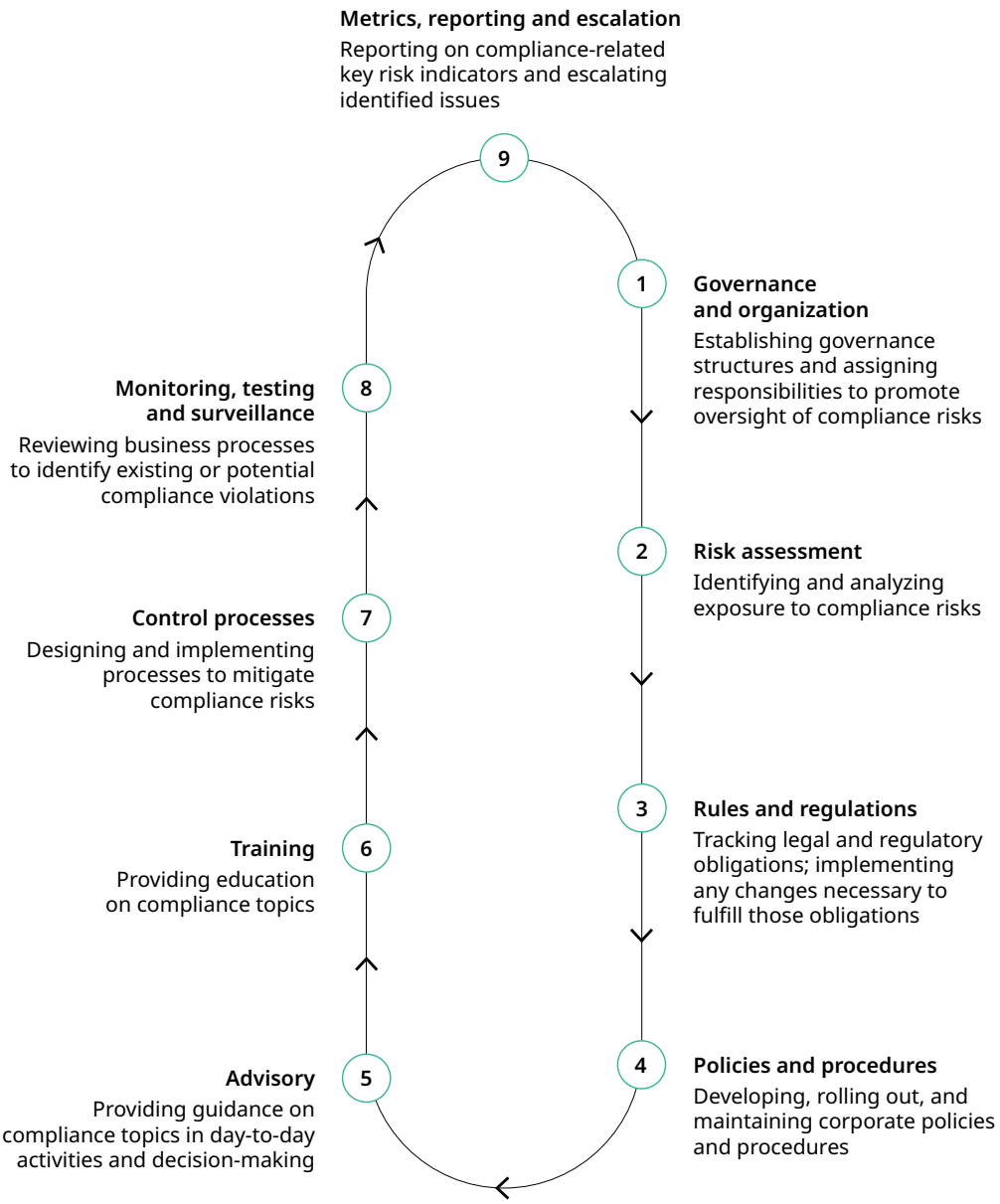
ESTABLISH
RISK-BASED COMPLIANCE PROGRAMS

In our experience, Compliance programs at most insurers are predominantly "rules-based" instead of also being "risk-based." Rules-based functions focus solely on the letter of the law and have broad but shallow programs to track relevant rules, laws, and regulations and test and train for compliance within them. The goal of a risk-based Compliance program is to reduce the overall compliance risk by focusing greater effort on managing the most material risks.

WHAT CAN BE DONE?

We believe that insurance companies should invest in the development of more "risk-based" compliance risk management programs. These changes can be implemented across the typical compliance risk management framework, outlined in Exhibit 1.

Exhibit 1. Oliver Wyman Risk Management Wheel

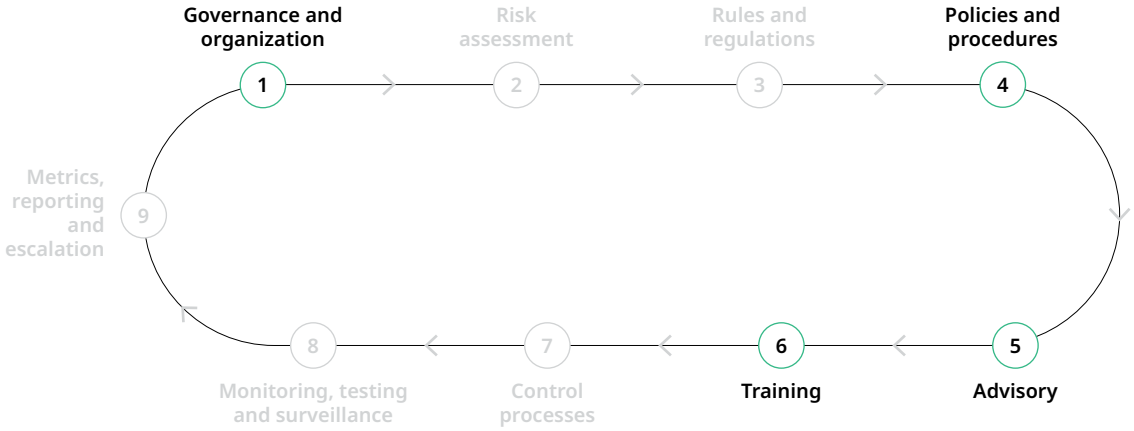


Source: Oliver Wyman analysis

RISK-BASED MANAGEMENT "MUST HAVES"

We recommend the following changes across the compliance risk management framework as insurance compliance moves from "rules-based" to "risk-based".

1. Establish a "culture of compliance"

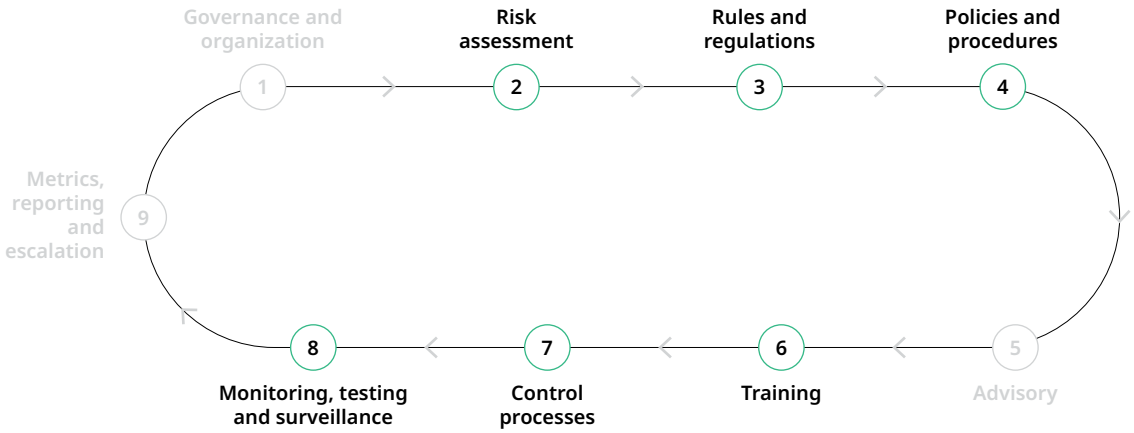


Implementation of risk-based programs is not possible without a mindset shift **within Compliance and the rest of the firm**. To make compliance management a true risk management discipline, senior management will need to deliver communications to the broader organization.

We recommend the following steps for senior leaders to help enact this change:

- Clearly articulate and cascade down the firm's compliance risk appetite.
- Establish governance committees dedicated to risk and compliance topics, where Compliance staff have a real seat at the table.
- Broaden the mandate of the Compliance function and compliance risk management to include the full breadth of regulatory, conduct, and cultural aspects (to capture the "spirit" vs. the "letter" of the law).
- Challenge existing practices and behaviors to examine whether they are appropriate to foster an environment where employees are encouraged to engage in healthy debate on "what's right."

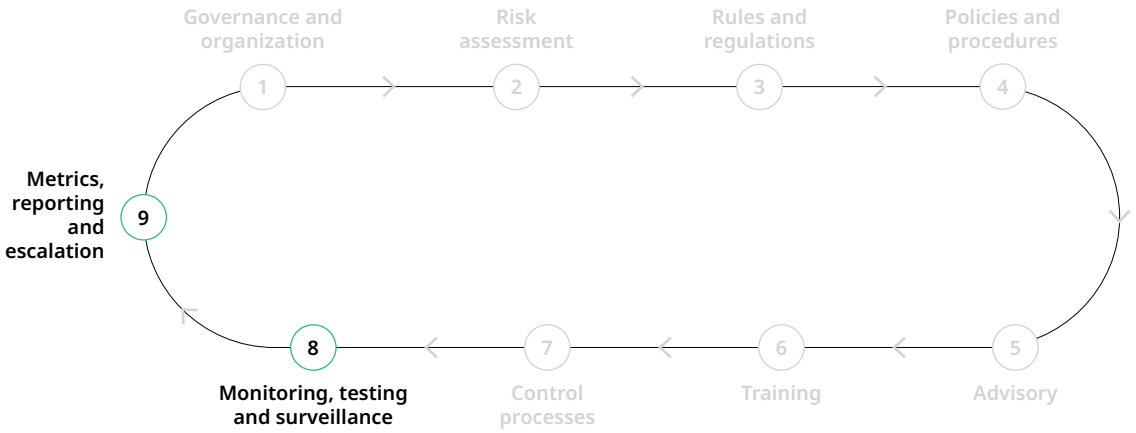
2. Increased focus on changing and emerging risks



The Compliance function of today typically focuses on a series of processes including **regulatory change management, policy management, training, controls operation and testing**. However, changes in business mix, operations and technology, and the regulatory landscape may change the insurer's exposure to existing risks, or introduce new compliance risks for which insurers need to be prepared. A more forward-looking Compliance function will focus a substantial amount of its time and resources on assessing risk rather than managing historical risks through existing processes.

A risk assessment methodology that captures changing and emerging risks should incorporate an appropriate mix of backward- and forward-looking inputs. Forward-looking inputs can be internal (e.g., key risk indicators such as number of complaints, disciplinary actions, testing results), or external (e.g., recent regulatory developments, fines at peer institutions, major changes in business strategy, or recent changes in systems). To do this, Compliance will need to have a robust controls inventory and assess the adequacy of those controls. This assessment should not only include whether the control is operating effectively, but also whether it has been designed effectively with the specific regulation in mind.

3. Monitoring and reporting of key compliance risk indicators



In many insurers, Compliance functions have **a principally narrative-based reporting model (e.g., regulatory exam results) and limited compliance risk metrics (e.g., monitoring and testing results)**. However, as the regulatory landscape changes, these programs will need to be increasingly dynamic, data-driven, and automated to support the nature and increasing number of risks insurers now face.

To address this trend, compliance reporting should be enhanced to include both lagging and leading key risk indicators. For example, metrics that point to potential poor insurance agent behavior may include the number of complaints or free look cancellations per agent. Any significant spikes should be reported to senior management with commentary on the changes, key trends, and drivers of risk levels.

Furthermore, to support a forward-looking risk management program, insurers will need to inject relevant data into their risk assessment processes. Examples of relevant data can include not only control details and control testing results, but also regulatory trends and key risk indicators.

Enhanced data analytics capabilities can also help a Compliance function become more forward-looking. The production of advanced metrics, surveillance programs, and dashboards (e.g., automated dashboards of key risk indicators across risks/geographies) can help Compliance officers gain deeper insights into the risks covered by Compliance. More advanced capabilities may include predictive analytics insights, or advanced scenario analysis for compliance risks which may not yet be covered by existing metrics/analysis.

INCREASE
ENGAGEMENT WITH THE BUSINESS AND OTHER FUNCTIONS

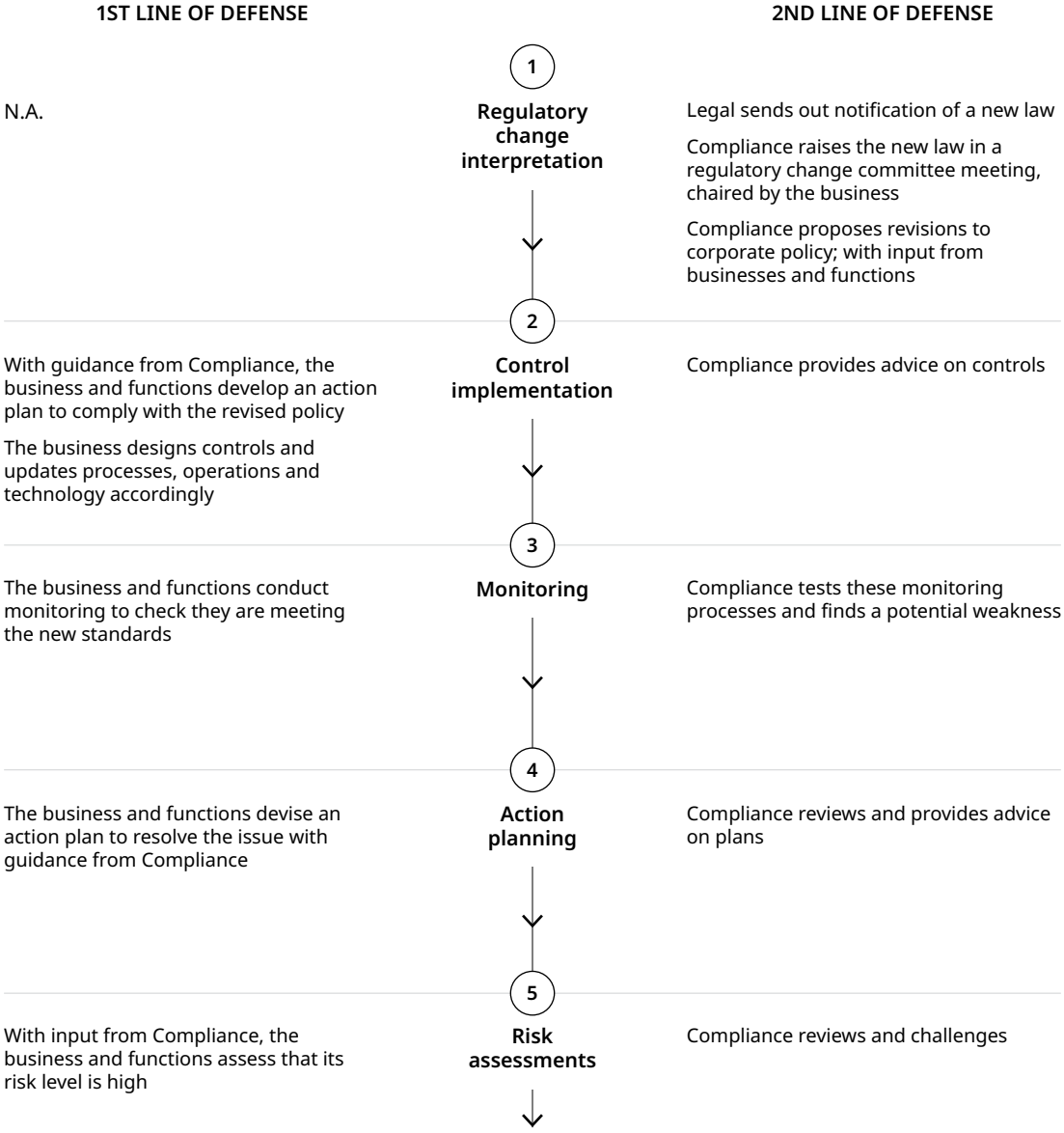
In global insurers, products and businesses tend to vary significantly by geography. As a result, Compliance functions at insurance companies need a deep understanding of the businesses and products they cover in order to maximize their effectiveness in helping the firm manage compliance risks.

In a model where Compliance partners work closely with the business, Compliance is involved in key business meetings, so that any risks associated with potential business decisions can be identified. Additionally, Compliance should provide effective review and challenge to the business, with compliance considerations factored into business decision-making, ultimately promoting first-line accountability of compliance risks.

This partnership model allows for stronger compliance processes to be built into the first line, enabling the business to better detect risks as they originate. When Compliance provides review and challenge of the business' design and implementation of controls, this allows for effective risk management to be embedded in everyday business processes.

When the business and Compliance work together to prioritize risks facing the firm, both teams are aware of the focus areas and can allocate resources more efficiently. This enables Compliance to concentrate on the most significant risks facing the business and better manage the firm's overall risk profile.

Exhibit 2. Ways to establish a strong compliance partnership with the business



Source: Oliver Wyman analysis

SHIFT THE MINDSET

To achieve this model of engagement and partnership between the business and Compliance, risk management functions need to have the adequate stature and influence within the organization to effectively challenge the business. Compliance may not always have a "seat at the table" in important business decisions, nor be perceived as an effective or strategic advisor to the business.

To shift this mindset within the organization, insurers can do a few things.

1. Refine the engagement model between compliance and the business and other functions

Although many insurers have adopted the three lines of defense model, this model is not always well communicated and the delineation of activities between the business, Compliance, and other functions is often unclear. Insurers can further refine this model by clearly defining what are the roles of the responsibilities of the first vs. second line, and identifying where the business and Compliance are expected to collaborate to better manage compliance risks.

This model also needs to be clearly communicated throughout the organization, which may require training as appropriate. Additionally, formal processes should be established to involve Compliance at an earlier stage (e.g., new product design processes).

Refining and communicating the engagement model will not be easy. Due to the historical perception of Compliance's role within the organization, business partners may react adversely to playing a bigger role than they are used to with regards to risk management.

However, having Compliance as a strategic partner rather than a naysayer will be important to communicate clearly and gain critical buy-in from the business. Keeping this in mind will help Compliance answer these questions that may be posed by the business:

- What's in it for us?
- How will this impact our teams?
- Will we need to make changes to systems and processes?

Thus, it will be important to bring the business along the journey to co-create a partnership model that works for the broader organization, not just from the perspective of the Compliance function.

Furthermore, communication from the top-down (e.g., C-suite level) can send a strong message throughout the organization that the Compliance function is a critical component to the organization's health and future strategy.

2. Align the organizational structure and operating model with the business

Aligning the organizational structure of the Compliance function with how the business itself is structured promotes better partnerships. Better alignment means the Compliance function has a single point of contact with an extensive working relationship with the business—developing specific product expertise and deep understanding of the business context which allows them to provide better advisory services.

However, as compliance risks become more global (e.g., privacy), risk management functions need to provide global oversight over these risks and identify where processes may be more efficient using central coordination. For example, insurance companies will need to build in global, end-to-end compliance processes to mitigate these risks. Legacy systems, which may vary significantly across geography, may benefit from a higher degree of centralization.

It is important to note, however, that centralization of activities may not be beneficial in all cases. For example, certain business units should be given the space to innovate without holding them to a higher global standard than is necessary. Compliance should work closely with the business to identify a solution that most effectively and efficiently manages compliance risk for the business. Thus, both the pros and cons of centralization need to be assessed given the business footprint and the changing risk landscape.

We recommend that Compliance functions take steps to assess whether their organizational structure is best suited for this changing landscape, and consider where activities should be more business-specific or may benefit from centralization. Some questions to consider include:

- Does the management of this risk vary significantly by region/business product?
- Is it important to provide senior management or external stakeholders a global view of this particular risk?
- Does this process benefit from consistency?

3. Upgrade skillsets and capabilities

The Compliance professional may need to upgrade their skillsets and capabilities in order to be an effective advisor to the business. Influencing capabilities, such as communicating effectively and gaining buy-in, and business understanding have not been traditionally valued in Compliance competency models. However, these capabilities are vital for Compliance professionals to be a true partner with senior management, and for risk management to be a key priority for the business. To build these capabilities, it is important to invest heavily in training, and source talent outside of traditional talent pools.

This may also require an investment in more senior professionals to lead the Compliance function. Regardless of skillset, a junior Compliance professional may be perceived as not having enough stature to be invited to key business decisions. Compliance professionals with commensurate experience and seniority relative to their peers in the business and other functions is one way to promote Compliance as an effective advisor to and challenger of the business. Additionally, having strong talent at the leadership level “trickles down” to the rest of the function, creating positive impacts on the broader culture and talent profile of the Compliance function.

Compliance as a strategic partner rather than a naysayer will be important to communicate clearly and gain critical buy-in from the business.

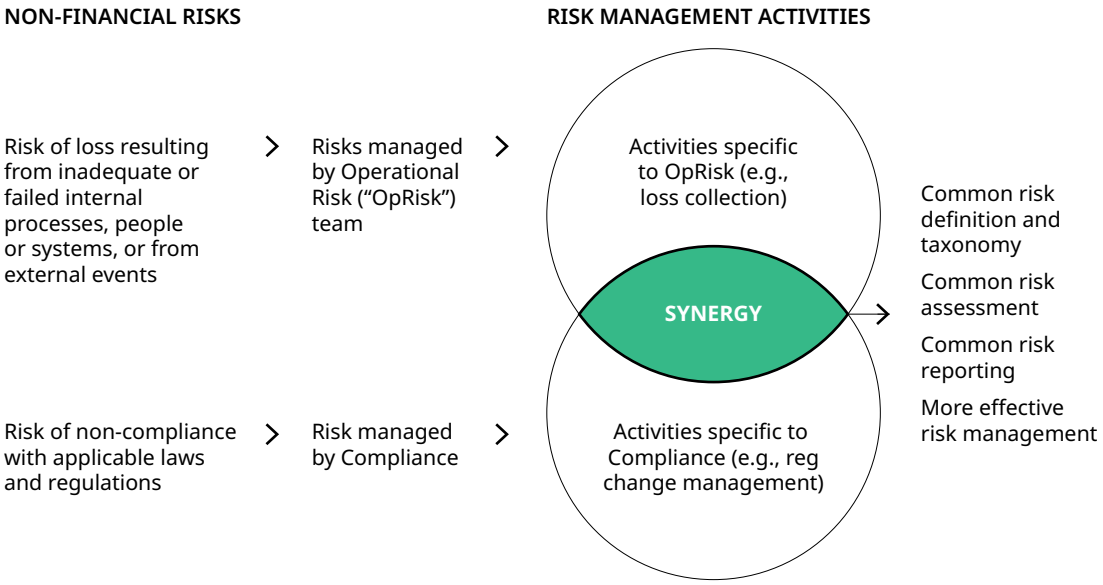
ALIGN
WITH OTHER NON-FINANCIAL RISK PROCESSES

As Compliance undergoes this transformation, there may be opportunities to align compliance risk processes with other non-financial risk processes. However, within many institutions, Compliance and other non-financial risk disciplines (e.g., operational, information technology and cyber, third-party) in insurance companies have organizationally operated in silos despite falling under the same non-financial risk umbrella. As a result, these disciplines have built various risk management processes (e.g., risk rating methodologies) that may not align.

Given the changing landscape, it has become increasingly important for senior executives at insurance companies to have a comprehensive understanding of their non-financial risk profile. However, methodologies between these various non-financial risk disciplines can differ, and reporting may not be comparable and may even send conflicting messages to senior management and the Board of Directors.

As a result, many institutions have started aligning their risk and compliance activities where appropriate. Areas where we have observed a high degree opportunity of alignment are the risk assessment process, controls processes, and reporting. Other areas of opportunity are interaction with the businesses/functions and training.

Exhibit 3. Opportunity to align compliance with other non-financial risk activities



Source: Oliver Wyman analysis

Exhibit 4. Risk alignment opportunities by compliance activity

Compliance activity	Degree level	Rationale	Example benefits
Risk assessment	High	Enables consistent definition and understanding of risk throughout the organization	A single non-financial risk taxonomy would set the foundation for alignment of other key processes (e.g. risk identification and assessment, reporting) Standardized risk assessment methodologies would allow for a common view of non-financial risk profile across the organization
Control processes	High	Promotes consistent management of risk throughout the organization	Control frameworks are standardized A single inventory reduces duplicative controls and better supports a rationalization of controls
Metrics, reporting, and escalation	High	Streamlines communication and escalation of compliance risks	Messaging to the Board and senior management (e.g. on the non-financial risk profile) are consistent Enables coordinated issue management and escalation pathways
Advisory	Medium	Streamlines communications via a single point of contact for the business/functions	Supports a more end-to-end view of risk events Uses business time more efficiently through coordinated requests from/ interactions with 2nd LOD
Training	Medium	Streamlines development and delivery of training where appropriate	Reduces duplicative trainings to the business on overlapping/similar non-financial risk types

Source: Oliver Wyman analysis

1. DEVELOP ONE NON-FINANCIAL RISK ASSESSMENT PROCESS

Given the increasing amount of overlap between the compliance risk assessment process and other non-financial risk assessment processes (e.g., the Risk Control Self Assessment (RCSA) in operational risk), insurers are starting to develop a single process to capture all types of non-financial risks. In order to achieve this, insurers should immediately start doing the following:

- Establish a common non-financial risk taxonomy to ensure consistency, comprehensive coverage, and sufficient clarity and granularity to assess all non-financial risks.
- Align risk assessment methodologies to produce a single view of the insurer's non-financial risk profile to senior management and the Board of Directors.

Please see our paper on this topic for further details.[2]

2. ENCOURAGE A CULTURE OF COLLABORATION

As Compliance functions become more closely aligned with risk, the Compliance professional will need to expand his or her skillset to not only have deep expertise in regulatory compliance, but also be a risk professional. Compliance professionals of the future will need to have a broad understanding of risks (including the interactions between risks), and increased collaboration and teaming. As the lines between compliance and operational risks become increasingly blurred (e.g., GDPR), Compliance and risk professionals need to actively work together.

To enable this alignment, some institutions have established governance structures to ensure coordination of non-financial risk processes between Compliance and other risk functions. This includes clear articulation of the governance and oversight of non-financial risks, and implementing joint committees where appropriate.

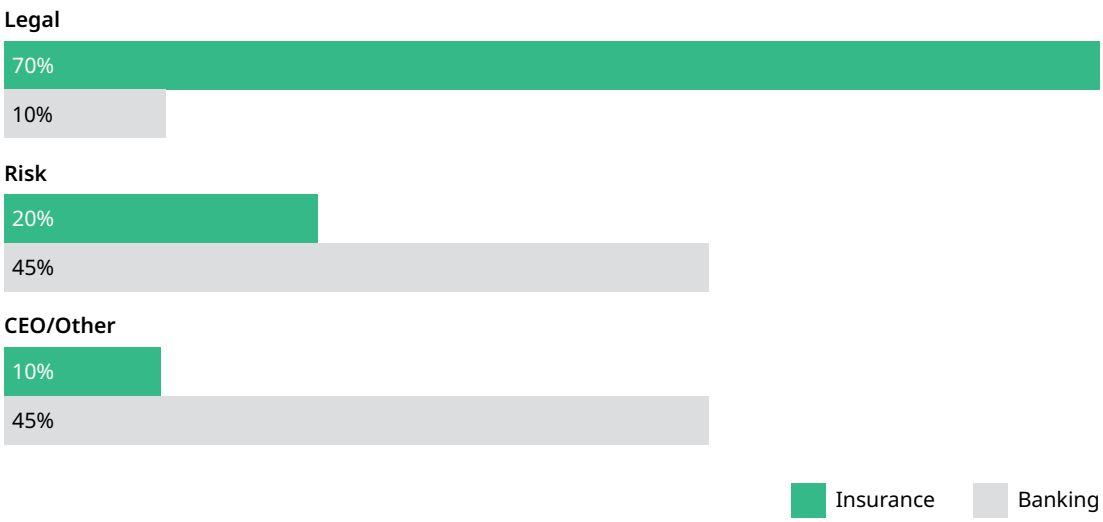
2 "Non-Financial Risk Convergence and Integration: Breaking Down the Silos," Oliver Wyman, March 2018.

Additionally, some institutions have also aligned their Compliance and risk functions organizationally. Across the financial services industry, we have observed a trend to shift Compliance's reporting line from Legal to Risk. Although most insurance Chief Compliance Officers (CCOs) report into Legal, select peers have begun to shift this to Risk.

However, organizational re-alignment should be made with careful consideration of the broader role of Compliance within the organization. In fact, some institutions have successfully aligned non-financial risk processes without shifting reporting lines to Risk. Additionally, there may be other considerations, such as talent and the potential impact to the stature of the Compliance function. This decision should be based on what's best for each individual institution.

More importantly, building effective non-financial risk teams requires a culture of collaboration, regular formal and informal interaction, knowledge sharing, coordinated strategy development, and the leveraging of synergies. By breaking down the silos between Compliance and other non-financial risk teams, your institution can better manage non-financial risks both efficiently and effectively.

Exhibit 5. CCO reporting lines for insurance and banking[3]



Source: Oliver Wyman analysis

3 Based on Oliver Wyman analysis as of May 2019; includes reporting lines for Compliance functions across select large financial institutions (Insurance, n=20; Banking, n=11).

CONCLUSION

In today's changing landscape, non-compliance is among the top risks for insurers given the potential regulatory, customer, and reputational impacts from violations. In our experience, Compliance departments are not yet meaningfully assisting insurers with these risks as a result of a historical process orientation and distance from the business. We believe that it is essential for insurers to begin a journey towards a more effective model for Compliance within their organizations.

To accomplish this, Compliance functions need to take a much more risk-based approach, along with substantially increasing engagement with the business and aligning more fully with other non-financial risk functions.

Enabling this transformation requires insurers to obtain strong support from senior management, clarify the first-line and second-line ownership of compliance risks, and upskill the Compliance team. While such a transformation will likely occur over multiple years, many quick wins can start to be implemented right away to progressively set the tone on the way forward.

AUTHORS

Elena Belov
Partner, Financial Services and Organizational Effectiveness
elena.belov@oliverwyman.com

Allen Meyer
Partner and Americas Compliance Practice Head
allen.meyer@oliverwyman.com

Michael Moloney
Partner and Head of Americas, Insurance
michael.moloney@oliverwyman.com

Paul Ricard
Principal, Insurance Practice and Organizational Effectiveness
paul.ricard@oliverwyman.com

Doris Li
Engagement Manager, Financial Services
doris.li@oliverwyman.com

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

Americas	EMEA	Asia Pacific
+1 212 541 8100	+44 20 7333 8333	+65 6510 9700