



# **A time of evolution for compliance: laying foundations for future success**

Global insurance Chief Compliance  
Officer survey



**EY**

Building a better  
working world

# Contents

Introduction **1**

Executive summary **2**

Compliance plays a significant role in  
facilitating organizational success **4**

Compliance activity levels are high,  
with widespread and increasing use of  
assessments, monitoring and testing **6**

Reporting of compliance  
activity is extensive **7**

Regulatory interaction is  
frequent **8**

Consumer protection is high on the  
Chief Compliance Officer agenda **9**

Huge scope remains for tapping  
into the power of technology **10**

Outlook: how do chief compliance  
officers see the future for compliance? **11**

Conclusion **12**



# Introduction



For today's Chief Compliance Officer (CCO), the insurance sector continues to pose new challenges and opportunities on a seemingly daily basis.

The requirements of regulators constantly evolve and expand, creating new demands of compliance functions, their working methods and enabling technology. At the same time CCOs sense growing expectations from senior management of what the Compliance function could – or should – be doing. No longer is defensive activity sufficient; increasingly compliance teams are called on to look ahead, anticipate risks and support operating businesses to help them perform better. Although compliance functions have continued to evolve, it is recognized that there is more to do if they are to be fully able to meet the challenges they face.

These indicators, noted from informal conversations and our ongoing work with CCOs, suggest this is an important moment in the development of many compliance functions. EY therefore decided to take a snapshot of compliance in today's insurance entities – seeking to understand the current structures, reporting, technology and other factors.

The report sets out the detailed findings from interviews, based on a standard question set, with CCOs from 20 global insurance entities with head offices across the world (Europe, North America, Africa and Asia) during 2015.\*

## EY's survey focused on seven topics:

1. **The role and stature of the Compliance function**
2. **Compliance management**
3. **Compliance MI and reporting**
4. **Regulatory interaction**
5. **Consumer protection**
6. **The use of technology**
7. **Future outlook**

EY's findings indicate that substantial changes have taken place in many compliance functions, while others are still underway and more are likely to follow. To help CCOs not only address their many challenges but meet the rising expectations of their function's capability, we pose some questions for consideration at the end of this report. Asking the right questions is often the first step towards finding the right way forward.

\*Not all respondents answered all questions and the charts reflect this

# Executive summary

Our survey findings indicate that the Compliance function is recognized as an important department in the control framework of insurance entities across the world. That importance, and the resources required to support it, are expected to increase in future. Compliance teams face evolving demands of regulators, boards and senior management.

## **Considerable consistency in compliance activity**

We found areas of consistency in compliance functions' activities across organizations and international jurisdictions. For example, compliance monitoring and reporting activities are widespread. The content of compliance reporting, both locally and from local functions to group compliance, is also highly consistent. Compliance management information is often reported to the board or senior management at least quarterly. Widely reported topics include the results of compliance monitoring and testing, compliance breaches and issues, information on the compliance risk profile of the organization, and updates on emerging regulations and hot topics.

## **The rising importance of consumer protection**

Compliance teams are also increasingly focusing on consumer protection in response to the shifting focus of regulators. Insurance entities are developing a variety of responses, such as developing group-wide consumer protection standards, strengthening the approval process for products exposed to regulatory or reputational risk, and enhancing product oversight and governance processes.

## **Local regulatory impact**

Local regulations do have a material impact on compliance activity and operations. While group compliance sets policies and standards, the operation of the Compliance function is driven by the local regulatory environment and local regulatory expectations. Similarly, the positioning of compliance within operating and reporting structures – specifically whether within the legal or risk area – is typically driven by both the location of the group and local regulatory expectations.

## **A growing focus on risk**

Compliance functions in insurance entities surveyed typically report either to the Legal or the Risk function and in some cases to the CEO. Regardless of these reporting lines, all compliance functions tend to apply a risk-based approach using accepted frameworks and tools (such as risk governance and risk registers).

The risk-based approach allows the CCO role to become more strategic, as it requires more forward-looking analysis of the business. It also allows the Compliance function to become better integrated with both risk and internal audit functions, which also take a risk-based view, and so enables improved efficiency.

Compliance functions reporting to Risk tend to be more advanced in their use of risk management tools and techniques, most notably the definition of risk appetites, risk registers and risk metrics. They also can be more forward looking in terms of seeking to manage potential regulatory risks before they crystalize.

Compliance teams reporting to the Legal function are more likely to refer to an inventory of laws and regulations (which may be a legal requirement), but still apply a risk-based approach to their work. Compliance and legal teams complement each other in terms of providing differing viewpoints. Both have a distinct role to play and specific responsibilities. The Legal function focuses on what needs to be done to defend the entity's position under the law, while compliance teams apply a more regulatory-oriented lens and focus more on what needs to be done in the best interests of the customer. But even in the US, where the legal reporting line still dominates, the skills required of compliance teams are evolving. When recruiting new compliance talent, US CCOs are becoming less inclined to hire individuals with a legal background and increasingly placing value on audit and advisory skills.

### **A snapshot of compliance today**

Our survey findings give a valuable snapshot of compliance as it is today – its organization, activities, regulatory involvement and other issues. Our detailed findings follow, grouped under the following themes:

- ▶ Compliance functions play a significant role in facilitating organizational success
- ▶ Compliance activity levels are high, with widespread and increasing use of risk assessments, monitoring and testing
- ▶ Reporting of compliance activity is extensive
- ▶ Regulatory interaction is frequent
- ▶ Consumer protection is high on the CCO agenda
- ▶ Huge scope remains for tapping into the power of technology
- ▶ Outlook: what do CCOs need to do in order to develop the next generation of compliance functions?



# Compliance plays a significant role in facilitating organizational success

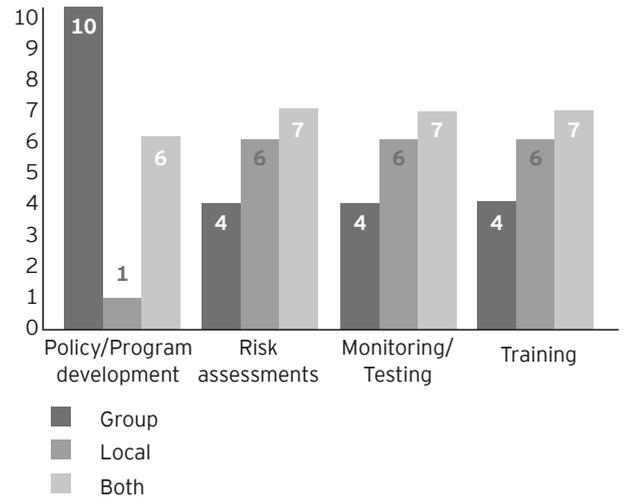
- ▶ The Compliance function is recognized as playing an important part in the control framework
- ▶ Compliance teams engage closely with C-suite or executive leadership
- ▶ Reporting lines tend to reflect the location of the group compliance function and the regulatory environment in which it operates
- ▶ Group and local compliance teams both play important roles

## CCO administrative reporting lines



- 35% General Counsel/Legal
- 15% Chief Risk Officer/Risk
- 20% CEO
- 30% Other

## Task undertaken by Compliance at group and local levels



Our survey and conversations with CCOs show that the Compliance function is recognized as being an integral part of entities' organizational control framework and that boards are keen to confirm that it operates effectively – internal audit reviews the effectiveness of the function in over 95% of survey participants. CCOs told us that the Compliance function generally has regular (quarterly or even monthly) meetings with internal audit, and often with the risk, actuarial and legal functions. Compliance is recognized as a “second line” control function but operating a Compliant business is recognized as a key responsibility of the business – nearly 75% of CCOs surveyed said that first line managers had Compliance-related annual objectives.

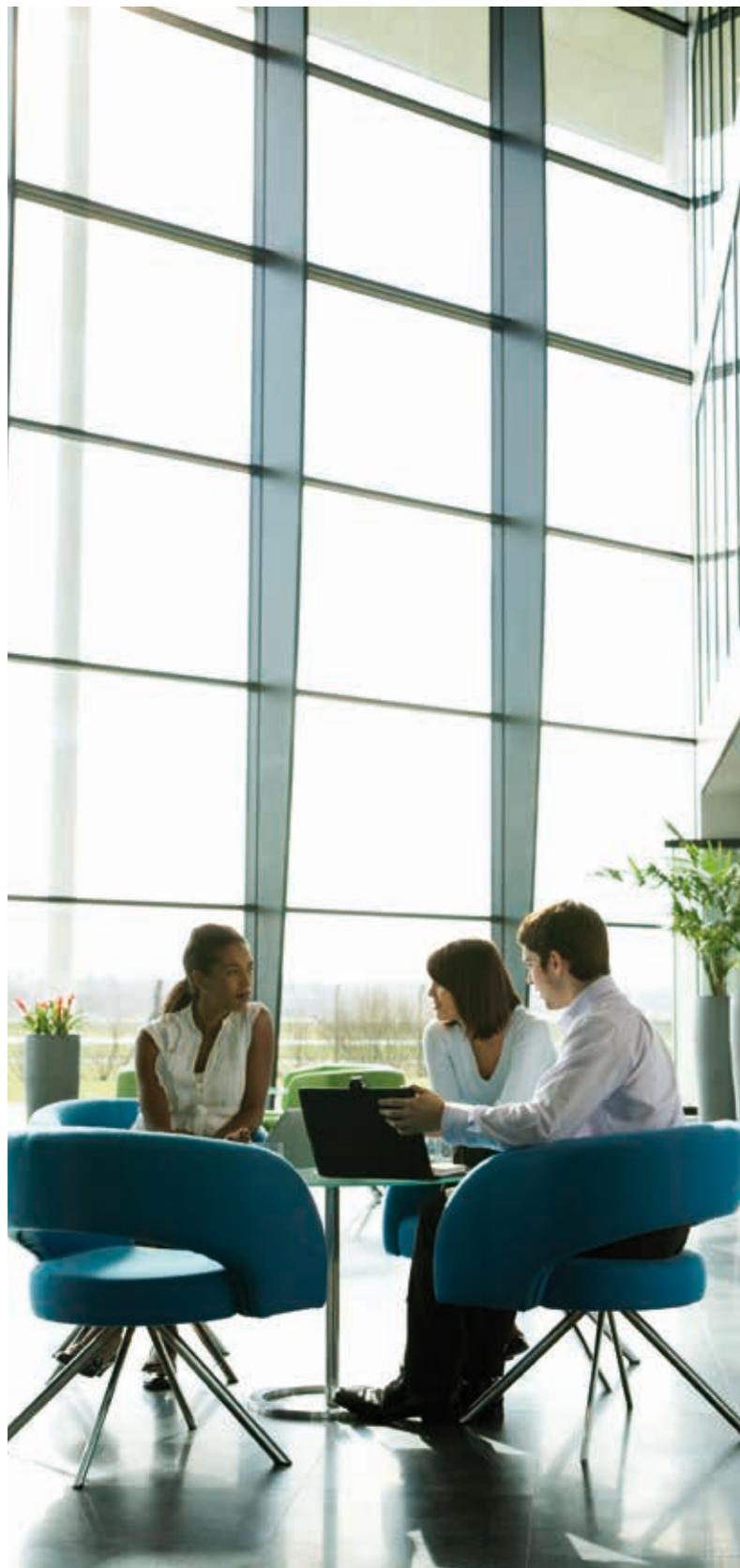
The importance of Compliance is also reflected in reporting lines, with the function always reporting at C-suite or executive level. Compliance officers engage closely with leadership teams to help develop strategic goals. They also work closely with senior management in addressing regulatory pressures. In the UK, for example, the Chief Risk Officer (CRO) will attend the board meeting, while the Compliance Director will often attend executive management meetings to provide an update on compliance activity and issues. Given the high levels of regulatory change, this attendance is likely to be regular and frequent. In Europe generally, the importance of the work undertaken by compliance directors is recognized, and their voices are heard at senior levels. In the US, CCOs are gaining more and more time with the board. There is also growing demand for the board to effectively challenge the CCO, creating a demand for new competencies among board members.

Who compliance reports to does vary: 35% report to the Legal function, 20% to the CEO and 15% to the risk department, while others report to the Audit Committee, the board of management or the board of directors. Reporting lines tend to reflect the location of the group compliance function and the regulatory environment in which it operates. For example, in most UK firms the CCO reports to the Risk function or the CEO directly, in continental Europe and the USA reporting to the legal department is more widespread. In Asia no survey participants report to risk or legal functions, but instead 50% report to the board of directors, 25% to the CEO and 25% to the CFO.

Reflecting the importance of compliance, the hiring and remuneration of the CCO is a matter for the board in 37% of insurance entities, and handled by the CEO in 19% of cases. General Counsel handles CCO appointment and remuneration in 31% of entities surveyed, and the CRO in 13%. However, the process is often collaborative with support provided by HR, internal audit or a board sub-committee.

Compliance reporting is often direct to the board, but can be indirect. Reports cover a range of content, such as general compliance overviews, common issues from local territories, and assessments of particular issues. While most board interaction is formal, CCOs also have informal interaction and open communication channels are maintained. Typical areas where compliance functions seek board approval include policies, compliance plans and codes of conduct.

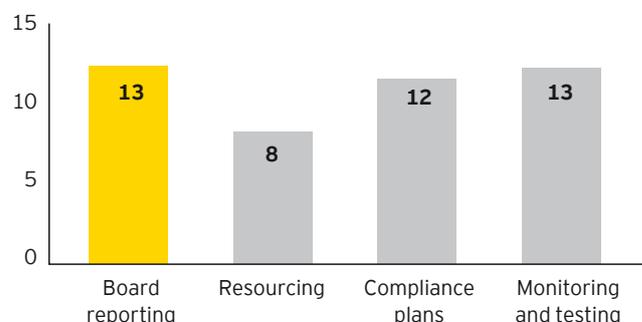
For most insurance entities, compliance activity takes place at both group and local level. Group compliance teams take responsibility for compliance policy development in two-thirds of entities surveyed. Other key compliance activities – risk assessment, monitoring and training – tend to be split between group and local compliance teams, though local activity would generally be greater. Resource demands are reflected in the relative size of group and local compliance teams. While total compliance headcounts are substantial, for most insurance entities, a larger proportion of resources tend to be positioned in the local businesses.



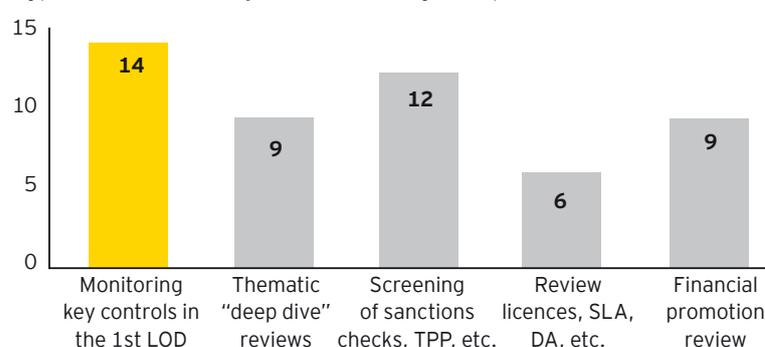
# Compliance activity levels are high, with widespread and increasing use of assessments, monitoring and testing

- ▶ Half (56%) of compliance functions define their risks using an inventory of laws, though the approach is most dominant in the US
- ▶ All compliance functions that we surveyed across the world conduct compliance risk assessments and use the results in a variety of ways
- ▶ Monitoring key controls in the business is standard practice, while screening of financial crime controls and the completion of detailed reviews and financial promotion reviews are also common

**Use of risk assessment results**



**Types of monitoring carried out by compliance**



When defining their risks, 50% of compliance functions surveyed use an inventory of laws and regulations as their reference point. Legal and regulatory inventories are less prevalent among European entities, which have tended to move towards a more risk-focused approach in line with current local regulatory thinking.

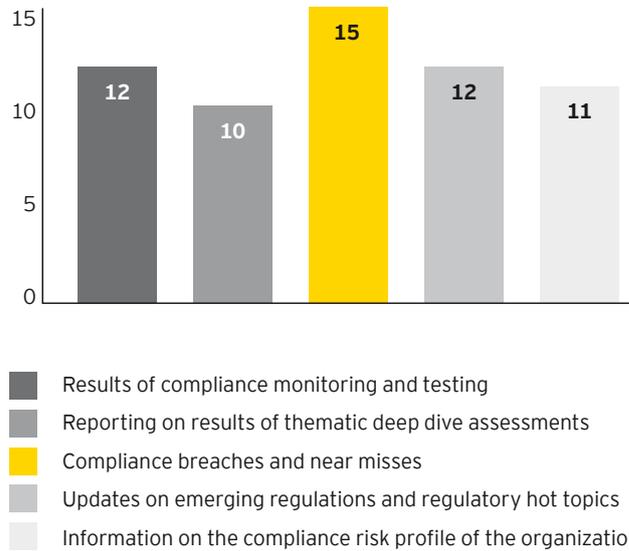
As expected, all survey participants conduct compliance risk assessments, and some firms are currently working to develop or further enhance their risk assessment process. Most use risk assessment results in reporting to the board, to inform compliance planning, and to focus monitoring and testing activity. Resourcing decisions may also be affected to some extent.

All the entities surveyed monitor key controls in the first line of defense. The majority of compliance functions surveyed also undertake screening of sanctions checks, third party payments or other financial crime controls, with some entities using dedicated teams from outside the Compliance function for such work. Reviews of financial promotions and marketing material are also common. A minority of insurance entities surveyed conduct reviews of licensees, service level agreements, and other legal requirements, but more often such activities are left to legal and/or procurement functions.

# Reporting of compliance activity is extensive

- ▶ In many insurance entities, compliance management information is reported to the board or senior executives at least quarterly
- ▶ The results of compliance activity is widely reported, both locally and to group compliance
- ▶ Local reports are often aggregated for group reporting purposes, with some firms having achieved a degree of standardization of quantitative information

**Local reporting to Group**



**Local Compliance aggregated at group level**



The vast majority of CCOs (95%) report at least quarterly to their board and/or to a board subcommittee such as the group audit committee or group risk committee. Just one survey participant (in Asia) reported less frequently (twice a year).

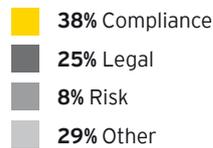
Compliance functions across the world are also highly consistent in terms of their local reporting, and in the content of reports to group compliance teams by local functions. Content typically includes the results of compliance monitoring and testing, compliance breaches and issues, information on the compliance risk profile of the organization, and updates on emerging regulations and hot topics. Entities that undertake detailed analysis on key risk issues also include their findings from such activity in local reporting.

Local reporting tends to be aggregated for group reporting purposes. Although no standard approach appears to be used for narrative reporting, some insurance entities have achieved a level of standardization of quantitative compliance management information.

# Regulatory interaction is frequent

- ▶ Compliance functions most frequently – though not always – own the organization’s relationship with regulators
- ▶ Primary regulator interaction is frequent, taking place at least monthly for the majority of compliance functions
- ▶ Regulatory visits take place at least annually for almost two thirds of entities surveyed
- ▶ The regulator relationship varies depending on factors such as legal and regulatory changes, market conditions and location

## Ownership of regulatory relationship



Compliance functions own the relationship with the regulator in 38% of insurance entities surveyed, the allocation of this responsibility sometimes being prompted by increases in regulatory requirements. Legal takes the relationship lead in 25% of entities, while CROs own the regulatory relationship in 8% of companies surveyed. In rare cases the CFO, company secretary or other function such as public affairs have this responsibility.

The frequency of interaction with regulators (whether by email, telephone or in person) varies greatly across the organizations we surveyed. The majority of insurance entities (58%) interact with regulators on at least a monthly basis – but some have continuous or daily contact. Interaction is ad hoc for 10%, while quarterly interaction is the norm for 10%. Interaction appears particularly frequent in Europe, with some relationship owners having multiple daily telephone calls with regulators.

We also found considerable variation in the frequency of regulatory visits, but these take place at least on an annual basis for 65% of survey participants. Other entities reported ad hoc, irregular or rare visits – perhaps every few years. The regulatory relationship including frequency of visits is influenced by a number of factors, such as legal and regulatory changes, market conditions and location. Systemic issues usually trigger less frequent but more intensive visits – perhaps taking place twice a year and lasting one or two weeks. Even where regulatory visits are short, they can still require significant preparatory time being spent by compliance teams.

# Consumer protection is high on the CCO agenda

- ▶ Insurance entities are facing new regulation and shifts in regulatory focus around consumer protection, with 72% of CCOs saying the business was feeling the impact
- ▶ Consumer protection compliance work is widely reported and at senior levels, including to the board
- ▶ Some entities are developing specific, group-wide responses to the growing importance of consumer protection

**Consumer protection/Conduct risk reporting escalation**



50% Senior Management  
36% Board of Directors  
14% Others

**Consumer protection/Conduct risk reporting in place**



76% Yes  
24% No

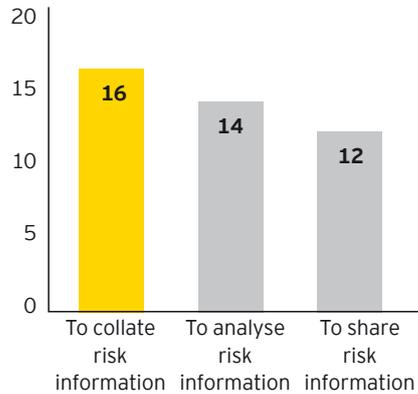
Consumer protection risks now feature highly on the agenda of most CCOs. This reflects the fact that new regulation or a new regulatory focus on consumer protection is affecting the majority (72%) of CCOs' businesses. New regulations are being introduced, or existing regulations enforced more stringently, while market expectations (as to how customers should be treated, for example) are extending even beyond strict regulatory requirements. Insurance entities are responding in a variety of ways, such as developing group-wide consumer protection standards to encourage consistency across the business, developing consumer protection strategies with business units and training staff. Other actions include strengthening the approval process for products exposed to regulatory or reputational risk, and enhancing product oversight and governance processes. Most insurance entities have a strategic goal of enhancing the customer experience, so focusing on the customer is seen as good business practice.

Work in relation to consumer protection risk is subject to widespread reporting: 76% of entities surveyed now report on such areas.

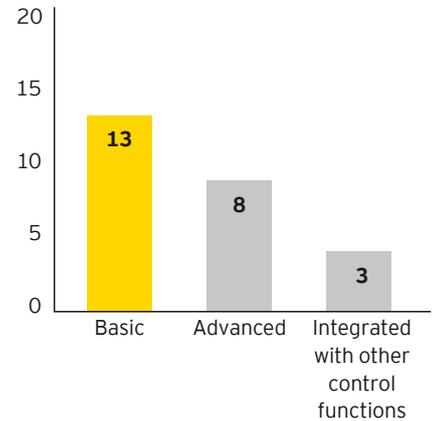
# Huge scope remains for tapping into the power of technology

- ▶ Most firms have the ability to collate, analyze and share information in some way
- ▶ Most CCOs (77%) describe their compliance technology as “basic”, at least in many areas of the organization
- ▶ Most entities surveyed do not have integrated technology in place, though some are working towards more integrated systems

**Use of Technology in managing compliance risks**



**Maturity of compliance systems**



All of the insurance entities that responded to the use of compliance technology question use technology to collate risk information, with most also using this to analyse (88%) and share (75%) information. However, two-thirds of those surveyed consider their systems (or parts of them) to be “basic”. Among this group, use of Excel spreadsheets is widespread (e.g., for third party assessments). More advanced systems may be used in some areas, for example, in relation to breaches, risks, policy exemptions or sanctions screening.

Among the minority of entities who consider their IT systems to be advanced, investment is significant or continuous. It may be used for a range of activities, including insider screening, monitoring of incidents or personal investments, and combating money laundering and other financial crime.

Only three survey participants said their systems were integrated with other control functions, although several firms are in the process of adopting technology to help them integrate their compliance systems. An important goal of such projects is to improve information sharing (e.g., in relation to group policies and risk assessment and testing capabilities).

# Outlook: how do CCOs see the future for compliance?

- ▶ Compliance functions have increased in size over the last year and further growth is likely
- ▶ Growth is being driven by:
  - ▶ The need to meet complex regulatory requirements
  - ▶ Growing management expectations for the role of compliance
  - ▶ The evolving nature of compliance work – becoming more supportive of business and forward looking
  - ▶ The many challenges of working in an international business
- ▶ Some CCOs, particularly in Europe, are finding it harder to recruit and retain the compliance talent they need

**Change in Compliance function size over 12 months**



■ 86% Increased  
■ 14% Stayed the same  
■ 0% Decreased

**Change in hiring and retaining compliance personnel over 12 months**



■ 39% Harder  
■ 38% Stayed the same  
■ 23% Easier

The majority (86%) of CCOs said their Compliance function had increased in size over the last year. Further growth is likely, driven by a range of factors.

The increasing complexity of regulations and their international reach (for example, Solvency II in Europe) is a key growth trigger. Assessing the impact on global business operations is challenging, calling for individuals with specialist, multi-functional expertise who can set out the business actions needed to comply with legal requirements. Emerging areas of regulatory emphasis also demand additional resource or people with new skills, as with the growing emphasis (in Europe) on culture and ethics. Compliance functions have an important role in helping to define what the organizational culture should be – translating regulatory expectations into business language, and in monitoring whether the desired cultural model has been delivered.

CCOs also believe that senior management teams have growing expectations of their Compliance function. Compliance teams are increasingly expected to provide an effective challenge to the business and act as a critical business partner for operating functions, rather than acting only as a second line monitoring function. This growing business focus is frequently identified by CCOs. Compliance personnel increasingly need to have good understanding of the business, processes and risks.

Compliance work is also developing a more forward-looking character, with the function expected to anticipate issues and understand correlations between different data in order to spot warning signs.

At the same time CCOs face a number of significant challenges related to the jurisdictions in which they operate and/or the nature of their organization. These include challenges around the liability of the compliance officer, changing local thinking to respond to issues emerging elsewhere, building global compliance systems, doing everything required within acceptable costs, and raising the profile of group compliance in order to have greater strategic input.

Perhaps not surprisingly given their growth and the challenges they face, some compliance functions (39% of respondents and particularly those in Europe) are finding it more difficult to hire – and retain – the talent they need. This is partly due to their need for particular competencies and experience – such as the ability to apply a forward-looking approach, to understand cultural issues and conduct detailed analysis. Where no natural pool of compliance resources exists, insurance entities are having to develop their own resources – but then risk losing them to competitors. They are also competing with banks and consultancies for the same compliance skills, making the recruitment challenge even tougher.

Some CCOs, however, said recruiting was becoming easier – because compliance functions are now more widespread, with the result that more qualified people are available. Given the increasing importance of compliance, the role of compliance officer has perhaps also become more attractive, with more people are interested in developing compliance careers.

## Conclusion

From what CCOs have told us it is clear that compliance in the insurance sector today is ever more “demanding” and “relentless” – descriptions we hear regularly. This is particularly due to continually evolving regulatory requirements and new emphasis being placed on issues such as customer protection and organizational culture. Senior management and boards within insurance companies increasingly appreciate the importance of compliance not only for addressing risk, but also for influencing strategy and supporting business operations.

**At the same time the, demands being placed on compliance teams to improve effectiveness are leading to a “raising of the bar” for how the function is expected to operate.**

So if CCOs are to meet the current and future expectations of regulators, C-suite executives and boards, what questions should they be asking themselves now in order to develop the next generation of Compliance functions?

- ▶ Is the scope of the Compliance function appropriate?
- ▶ Is there a consistent understanding of the role of the Compliance function in the business?
- ▶ Are my compliance resources engaged on the right activities and with members of the appropriate management and governance forums? Do we have the right access to senior management, and board members?
- ▶ Do we have an understanding of key regulatory risks and does our monitoring program reflect those risks?
- ▶ Do we manage our relationship with our regulators in an efficient and effective way?
- ▶ Could we do more to manage and measure our consumer protection risks?
- ▶ Can we use technology to better predict and understand our risks?
- ▶ Are we effectively working with the other control functions?
- ▶ What else can we use to assist in monitoring such as data analytics?
- ▶ Where is the future of changing regulatory environment and how should that play into our compliance strategy?

The answers will depend on the specifics of the business, jurisdiction, management and the current structures in place. Some answers may be challenging in themselves, identifying areas for priority action or investment. But gaining clarity now over future challenges and opportunities and how to address them is a vital first step in maximizing the potential of the Compliance function, both today and tomorrow.

## Participating companies

Ageas	Munich Re
AIA	NN Group
AIG	Old Mutual
Allianz	Prudential PLC
AON	Prudential Financial
Aviva	Sompo Japan Nipponkoa
AXA	Swiss Re
Marsh	Tokyo Marine
MetLife	Willis
MS&AD	Zurich

For further information on this report contact:



**Martin Bradley**  
Global

mbradley@uk.ey.com  
+ 44 20 7951 8815



**Tom Ward**  
Americas

tom.ward@ey.com  
+ 1 312 879 2234



**Steve Southall**  
EMEIA

ssouthall@uk.ey.com  
+ 44 20 7591 1004

## Country compliance contacts



**Rob Walsh**  
Australia

rob.walsh@au.ey.com  
+ 61 2 9248 4861



**Philip Rodd**  
Hong Kong

philip.rodd@hk.ey.com  
+ 85 228 469 028



**Trevor Rorbye**  
South Africa

trevor.rorbye@za.ey.com  
+ 272 144 302 90



**Roy Alexander Boukens**  
Belgium

roy.alexander.boukens@be.ey.com  
+ 32 277 49111



**Lorenzo Fattibene**  
Italy

lorenzo.fattibene@it.ey.com  
+ 39 066 7535 258



**Stefanie Gey**  
Switzerland

stefanie.gey@ey.com  
+ 41 58 286 3842



**Pauline de Chatillon**  
France

pauline.de.chatillon@fr.ey.com  
+ 33 1469 367 48



**Kiyoshi Katayama**  
Japan

katayama-kysh@shinnihon.or.jp  
+ 81 3 3503 1100



**Andrew L. Chenoweth**  
US

andrew.chenoweth@ey.com  
+ 1 312 879 3853



**Bernd Froehler**  
Germany

bernd.b.froehler@de.ey.com  
+ 49 89 14331 15811



**Wimjan Bos**  
Netherlands

wimjan.bos@nl.ey.com  
+ 31 88 407 1719



**Ranjit Jaswal**  
US

ranjit.jaswal1@ey.com  
+ 1 212 773 5839

**About EY**

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit [ey.com](http://ey.com).

© 2016 EYGM Limited.  
All Rights Reserved.

EYG No. EG0318  
52113.indd (UK) 03/16. Artwork by Creative Services Group Design.  
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

**[ey.com](http://ey.com)**