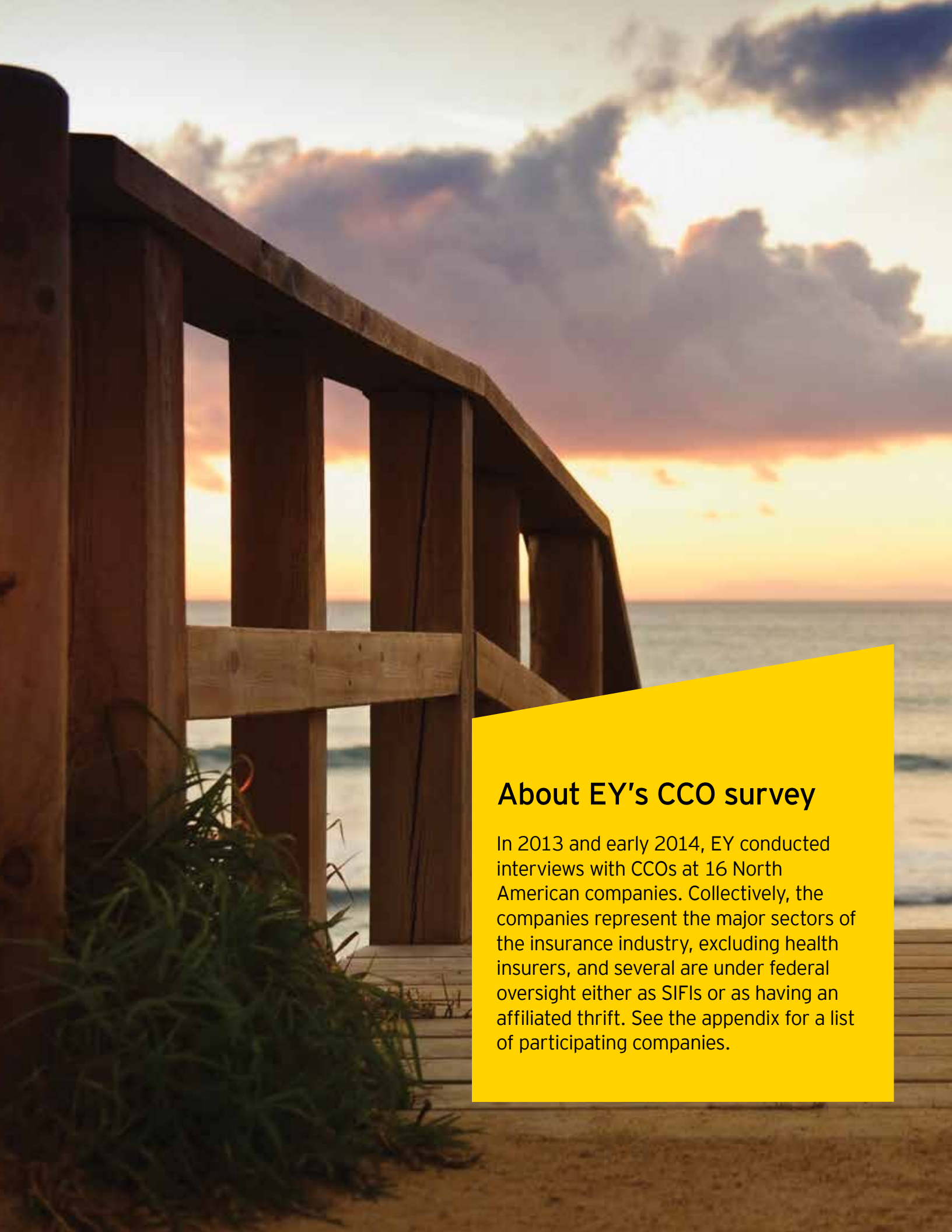
Compliance seeks a path to regulatory readiness

2014 insurance CCO survey

EY

Building a better working world



About EY's CCO survey

In 2013 and early 2014, EY conducted interviews with CCOs at 16 North American companies. Collectively, the companies represent the major sectors of the insurance industry, excluding health insurers, and several are under federal oversight either as SIFIs or as having an affiliated thrift. See the appendix for a list of participating companies.

The past several years have seen an unprecedented number of new regulations aimed at protecting the customers and shareholders of financial institutions. So far, most of these regulations have focused on banking and capital market institutions, leaving insurers out of the spotlight.

But that is changing. Several large insurers now face stricter regulatory oversight as a result of being deemed systemically important financial institutions (SIFIs) or global systemically important insurers (G-SIIs). Insurers with an affiliated thrift (a bank subsidiary) must now meet higher expectations as a result of the Dodd–Frank Wall Street Reform and Consumer Protection Act, which places them under the prudential supervisory oversight of the Federal Reserve Board.

An insurer's compliance function and its compliance activities will need to evolve as regulations and oversight continue to evolve. To set a benchmark for where insurers are today, our regulatory risk and compliance professionals interviewed chief compliance officers (CCOs) at 16 insurance companies in North America in 2013 through early 2014. All companies surveyed are life and property and casualty insurers, and several are under federal oversight either as SIFIs or as having an affiliated thrift.

The survey focused on the structure and governance of the compliance function and core compliance program activities. It also explored the use of technology within the compliance function and CCOs' outlook on the insurance industry.

Structure and governance of the compliance function

The structure of the compliance function and how it interacts with other groups in the organization help determine the function's effectiveness at keeping the company in line with regulatory requirements.

Our survey found that the overall structure, duties and roles vary broadly from insurer to insurer. Insurers that are subject to federal oversight tend to have more mature compliance functions than those that are not.

Organization and size of the compliance function

Most insurers in the survey have a central compliance function that has the responsibility to track key compliance events, such as market conduct exams, regulatory inquiries, and fines and sanctions. However, a number of insurers are strengthening the compliance role at the business unit level. They have established business unit compliance functions that report into the enterprise compliance group, or even business unit management, and help to oversee and advise business unit compliance activities.

All insurers surveyed have a designated CCO, but as Figure 1 shows, the size of the function (defined as the number of people with a direct reporting line into compliance) ranges widely, from a single person to more than 700. Among the insurers surveyed, 44% have 25 or fewer people reporting into compliance.

Stature of compliance in the organization

The stature of the CCO also varies from insurer to insurer, with the CCO at 75% of insurers having some level of direct involvement with the audit committee (or committee of similar function) or the full board of directors. CCOs need to have an independent voice with one or both of these groups to fulfill the role of the compliance function. Compliance should be included in new strategy and product development discussions, and must have the standing and freedom to meaningfully challenge these plans at the highest level, even when the impact to those strategies and products will be significant.

Compliance reports should be disseminated beyond the compliance channel. Most organizations do see that the board, the audit committee, the chief risk officer or some other group outside of compliance, such as business management or risk committees, receives copies of the organization's compliance reporting (see Figure 2).

CCOs and compliance in general must be free from undue influences that can result when their performance or compensation is controlled by the businesses they help to oversee or is tied too specifically to revenue or profit goals. The reporting line of the CCO is fairly consistent among insurers, with 69% indicating that the CCO reports to the insurer's general counsel (see Figure 3). The historically close ties between compliance and legal may explain this, as many of the early insurer compliance functions were spawned from the legal department.

Talent

Surveyed CCOs generally agree on the types of compliance professionals they are looking to attract and retain (see Figure 4). They appear to be moving away from the more traditional legal background as they seek to adapt their functions to the new regulatory landscape. Seventy-five percent indicated they look for inquisitive, savvy compliance professionals with the background and experience to know when something is amiss, and the investigative skills to get to the root causes of issues.

An equal portion of insurers stressed the need for compliance professionals who are knowledgeable about business operations. One of the most effective means to maintain compliance is to build it into existing business processes, which means that compliance personnel need to understand those processes.

A number of CCOs also seek communication and collaboration skills. While compliance professionals do not make decisions for the businesses they advise, they are responsible for communicating the relevant compliance risks and mitigation needs and working with the business units to address the effectiveness of related procedures and controls. The most effective compliance professionals will be able to provide an effective and valuable challenge to business management, just as the better business managers will cultivate this relationship and seek out those challenges.

Figure 1. Size of compliance function

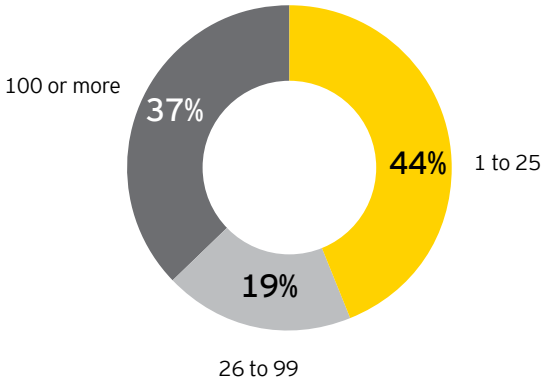


Figure 2. Compliance reporting recipients

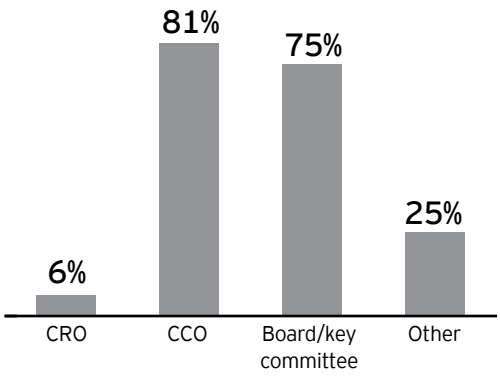


Figure 3. CCO reporting lines

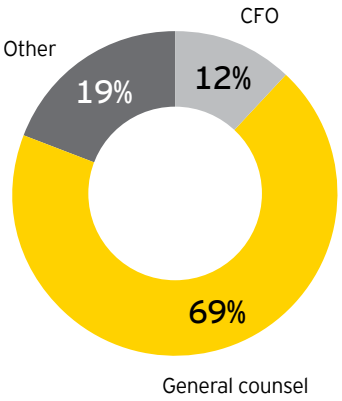


Figure 4. Skills critical to the compliance function

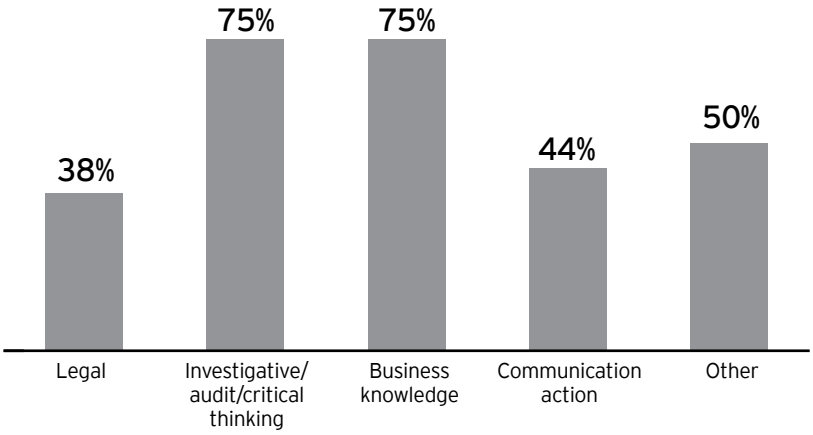
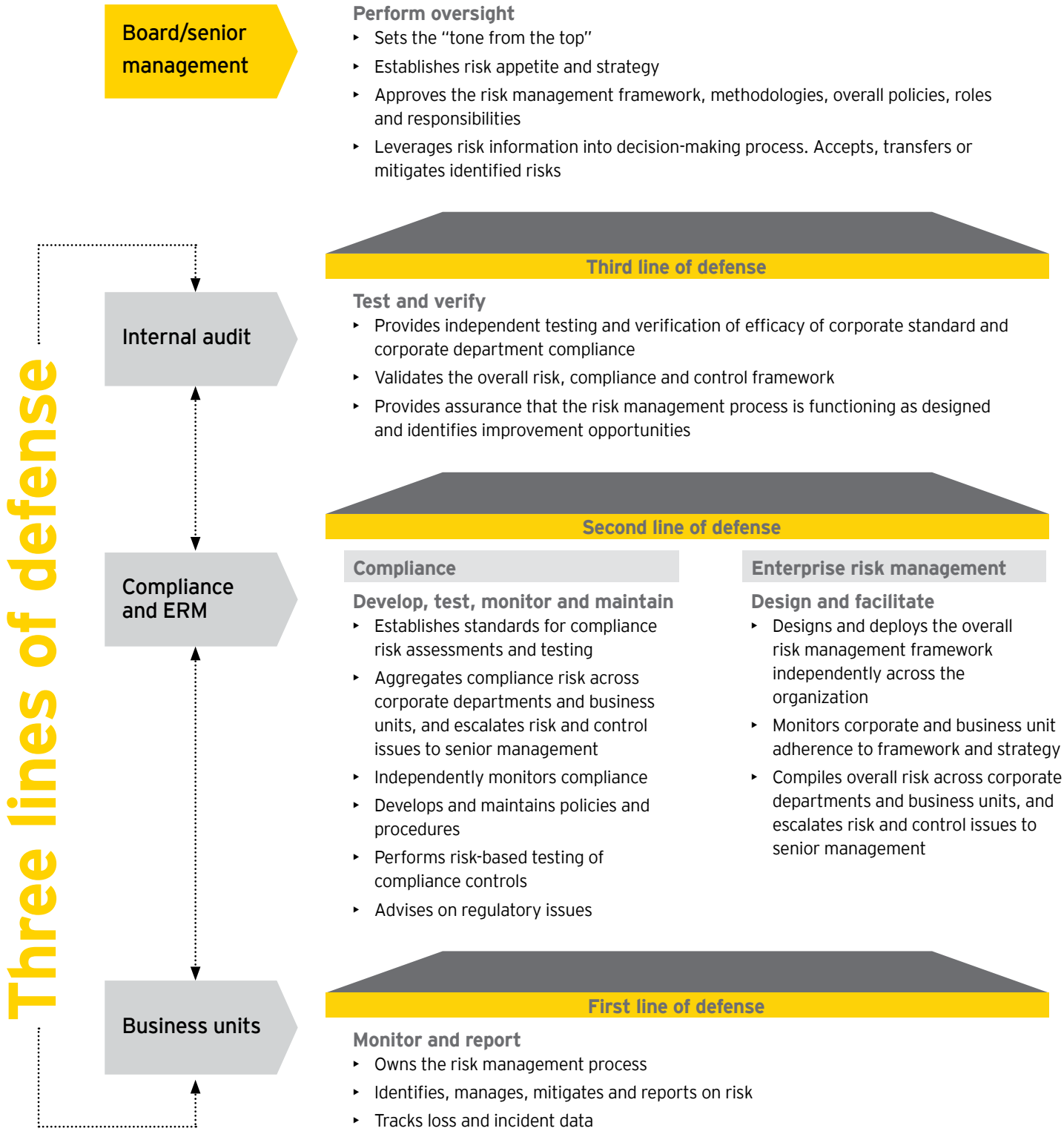


Figure 5. The three lines of defense model



Governance

The model showing the three lines of defense (Figure 5) lays out a key governance concept that regulators often apply when looking at how an organization assigns accountability for risks and risk management, including compliance risk. The model has become somewhat standard for large banking institutions, but it has not been applied as rigidly to the insurance industry. Although the base components may exist, many of the insurers surveyed do not have a formal governance framework that integrates all three lines of defense:

- Business units
- Compliance and enterprise risk management
- Internal audit

The first line of defense in the model is the business unit, including front line support units (such as operations). Businesses are expected to understand their compliance risks and to take ownership and responsibility for mitigating those risks. Half of the insurers surveyed indicated that business units view themselves as primarily responsible for their compliance risks (see Figure 6). This highlights the changing times and a general shift in business units' view of compliance, from a potential impediment to an obligation they have to their customers. Among those surveyed, the business units with the strongest compliance functions tend to be from organizations that are overseen by federal regulators, such as affiliated banks, broker-dealer groups and asset management firms.

A strong enterprise compliance program is essential to an effective second line of defense. The second line of defense has the responsibility to establish base standards and policies for risk management activities that include the reporting, escalation and remediation of issues. The second line also has the responsibility to aggregate the applicable risk across the enterprise and ensure senior management and the board have the information required to provide guidance and oversight. The compliance function advises and validates the business units' compliance activities through oversight, establishing and enforcing a consistent approach to the identification and assessment of compliance risks, and testing activities.

The third line of defense is the internal audit function. Internal audit is responsible for providing the independent assurance to the audit committee and the board on the design and operating effectiveness of the enterprise compliance framework. Internal audit works with compliance to perform audits of key compliance functions and policies, such as anti-money laundering, privacy or the compliance testing unit. Additionally, internal audit works with compliance to ensure that compliance issues identified during audits are reported and escalated as appropriate, and may consult with compliance professionals before conducting specific business audits where compliance issues may exist.

As central as the compliance function is to managing regulatory risk, it must work effectively with the enterprise risk management, internal audit and legal functions to provide a comprehensive and efficient governance framework for managing all sources of risk to the organization. Most of the CCOs surveyed have some form of regular meetings with these three functions, either through a formal risk committee or informal touch points (see Figure 7). Even with regular interaction, insurers noted the level of integration could be improved. Also, much of the interaction focuses on past events, such as sharing of results, rather than planning for future events, such as developing an integrated plan to conduct assessments and testing.

Additionally, 44% of the CCOs indicated that the compliance function itself was subjected to internal audits (see Figure 8). However, an additional 37% indicated that internal audit did review key components of the compliance program ("Varies"), such as anti-money laundering programs and Office of Foreign Assets Control sanctions programs.

Figure 6. Business unit ownership of compliance

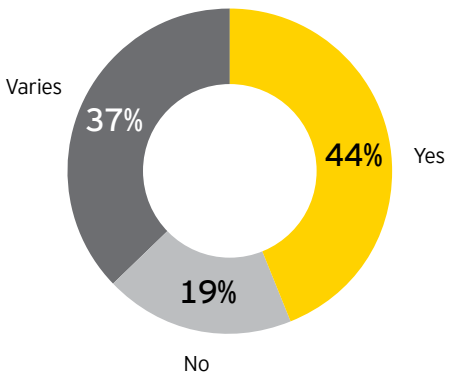


Figure 7. Type of interactions between compliance, ERM, legal and IA

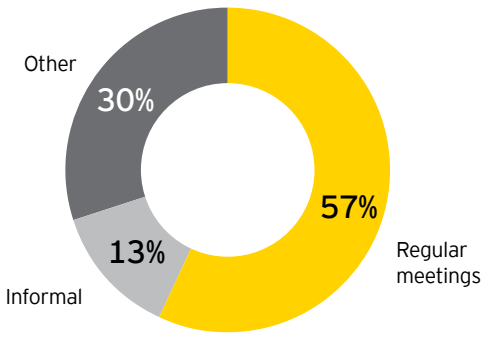
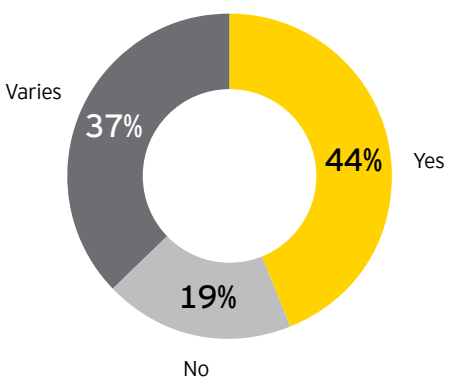


Figure 8. Audits of the compliance function

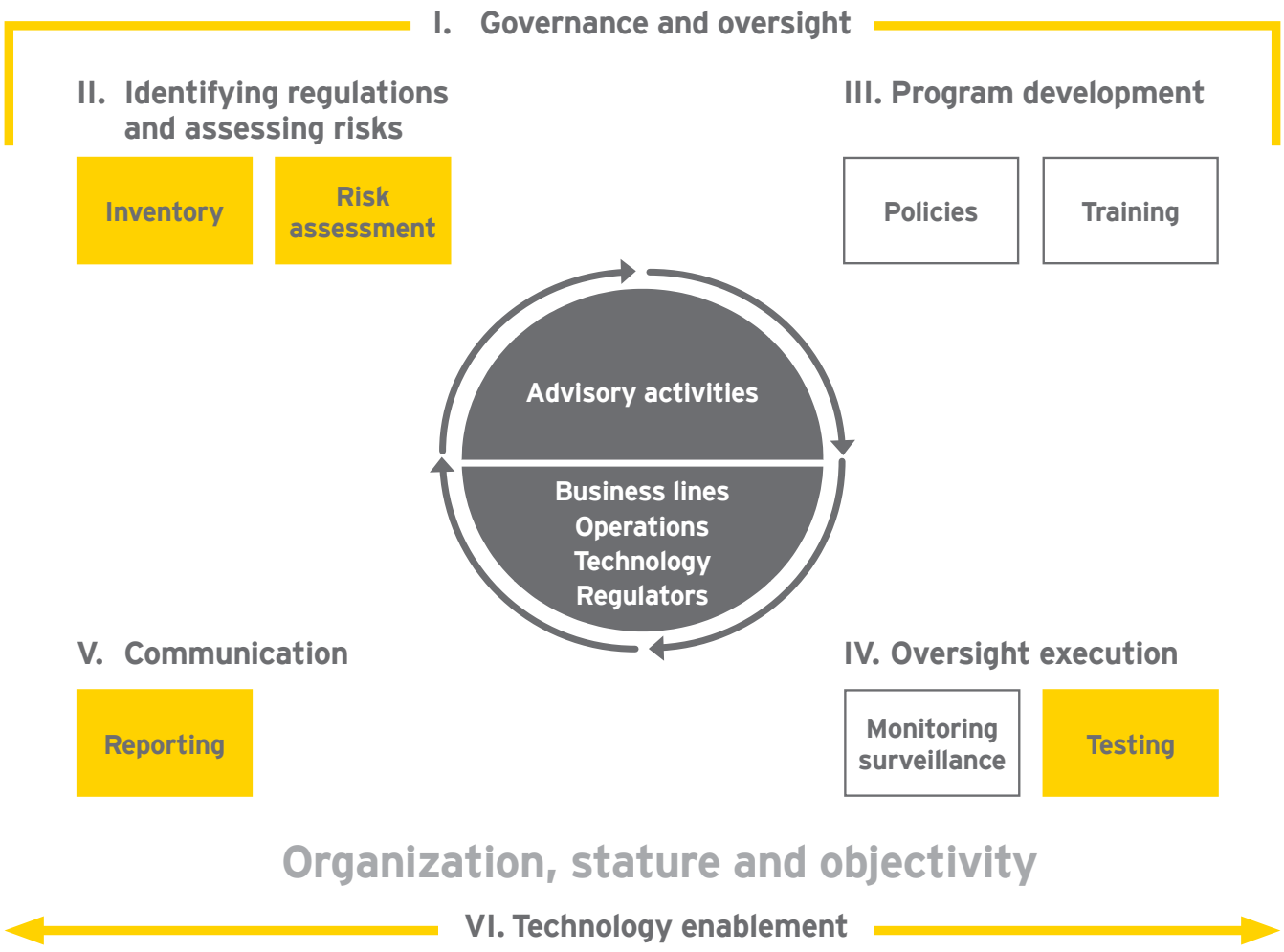


Core compliance program activities

The compliance life cycle lays out the key activities and responsibilities expected of a compliance program. The highlighted areas in the life cycle shown in Figure 9 identify areas covered in this survey.

This compliance life cycle is used with the financial services industry and provides a general framework for supporting a robust compliance function.

Figure 9. Compliance life cycle



Inventory of laws and regulations

One of the cornerstones of a robust compliance program is an inventory of the key laws and regulations with which the organization must comply. This is an expected practice in the banking industry, but traditionally, insurers have not been held to the same standard. According to our survey, such an inventory is uncommon in the insurance industry (see Figure 10). Only 31% of CCOs indicated they have such an inventory. Several other CCOs indicated each business unit maintains an inventory of regulations that apply to their operations but a master inventory at the enterprise level does not exist.

Even though only a few insurers have a master inventory, every insurer indicated that they do track new and amended laws and regulations. The activity varies from being a business unit responsibility to being performed by a centralized enterprise group. Regulatory information is gathered from myriad information sources, ranging from third-party providers to internal dedicated state counsels.

Compliance risk assessments

The compliance risk assessment identifies risks arising from the requirements in the inventory of laws and regulations, ranks those risks according to impact and likelihood of an occurrence, identifies relevant controls and assigns an effectiveness score to the control. The outcome is an overall or "residual" risk score. These scores are then used to prioritize compliance activities, identify controls needed to mitigate risks and allocate resources.

Most CCOs surveyed, 81%, indicated their organizations perform some level of compliance risk assessment, but often as part of a broader enterprise risk assessment (see Figure 11). These assessments tend to be concerned with big buckets of risk, such as fraud and privacy. They generally do not assess risk at the process or product level, nor do they attempt to quantify risks and evaluate controls.

Figure 10. Inventories applicable laws and regulations

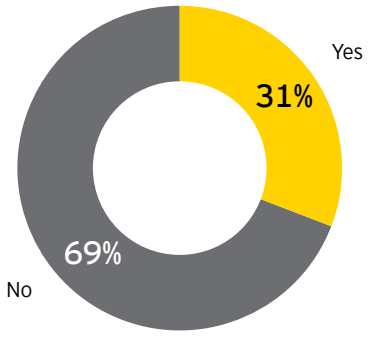
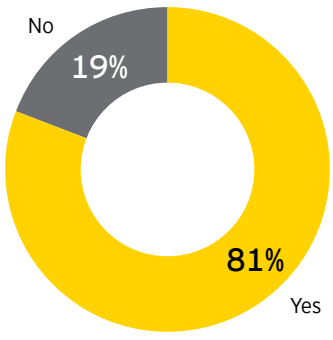


Figure 11. Conducts compliance risk assessments



Compliance testing

Ideally, compliance testing follows the proverb, "Trust, but verify." A comprehensive testing program helps provide this verification by confirming related policy, conformance to the process, and the existence and reliability of controls. The compliance risk assessment is a critical input into compliance testing, as it helps to identify the controls that are key to mitigating the compliance risk. The controls should be tested to ensure they operate as intended and are effective at mitigating the associated compliance risk.

Certain regulators emphasize compliance testing, seeing it as integral to the compliance program. Testing results should feed back into risk assessments and help shape the annual compliance plan by identifying areas that may need attention. In our survey, 62% of the CCOs indicated their organizations perform some level of compliance testing (see Figure 12). Some may have a dedicated compliance testing function, while others indicated that internal audit touches on compliance in its audits of the rest of the organization but compliance is not the sole purpose of those audits. Internal audit prepares by consulting with compliance before an audit of a business unit to identify where to focus their efforts.

One notable point relates to insurers who also maintain an affiliated bank, broker-dealer organization or asset management function. The regulations that govern these businesses often specify testing that must occur. Surveyed insurers with one of these specialty groups often maintain a separate compliance function for oversight and testing, but in general limited testing is performed other than what is mandated by regulation.

Compliance reporting

Eighty-seven percent of insurers surveyed indicated they report on compliance to keep the CCO, and ultimately senior management, informed about the status of the compliance program and key compliance issues resulting from regulatory requirements (see Figure 13). Responses to our survey indicated that reporting is primarily informal and consists of business unit compliance staff reporting issues and key events to the CCO, such as compliance violations and upcoming and completed exams. Centralized enterprise compliance functions then aggregate these reports into a single report that is regularly shared with senior management and often with the audit committee (or similar committee) as well.

Although identifying and reporting compliance violations are critical to an insurer, compliance reports are more valuable when they consist of more than just incidents. Compliance reporting should provide compliance leadership, senior management, the board and the audit committee with information that enables them to challenge whether the compliance program is operating as intended.

To be effective, enterprise compliance reporting should also provide information about the status of the annual compliance plan, such as the status of training and progress in risk assessments and testing; help to identify trends through analysis of complaints, violations and fines; identify changes to existing risks and identify emerging risks; and provide updates on the regulatory landscape. Standardized compliance reports and established metrics help to reveal trends and bring potential issues to light.

Use of technology

Information technology can bring the same benefits to the compliance function as it already brings to most other areas of an organization:

- Reduced costs
- Streamlined reporting
- Greater consistency in the execution of the program
- Insight to support sound business decisions

The vast majority of surveyed CCOs, 88%, do use technology for basic functions, such as tracking new and amended laws and tracking action

Figure 12. Conducts compliance testing

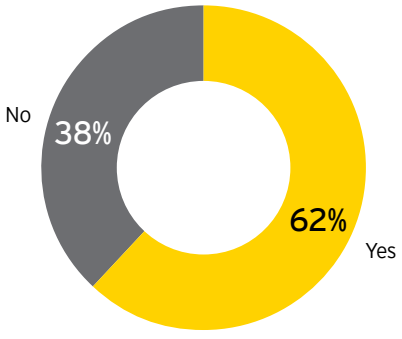


Figure 13. Reports on compliance performance

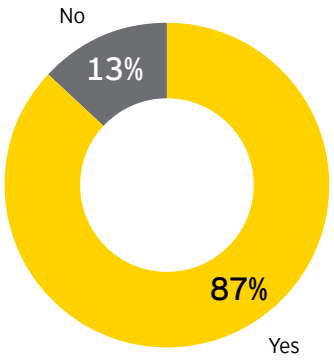
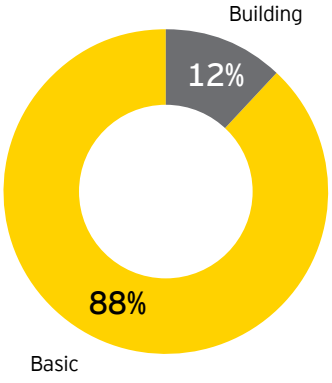


Figure 14. Use of technology



plans (see Figure 14). However, not a single compliance function operated with an advanced, integrated technology solution designed to meet its specific needs, although some of the CCOs are in the process of building such a solution. An advanced solution has the potential to deliver a more holistic view of compliance risk within the organization, provide a single set of tools to support compliance activities, automate monitoring and reporting, maintain a warehouse of compliance information and reach across geographies and entities.

CCO outlook on the insurance industry

Our survey also asked CCOs how they thought the industry would change in the next three to five years. The most common theme in their answers was that the regulatory pressures will continue to increase; however, most also felt that the size of their compliance functions will stay about the same.

With more regulations likely to be put in place, CCOs will have an enormous challenge in building and maintaining an effective compliance function. To meet this challenge, CCOs will need a strong grasp of the compliance risks throughout their organizations to prioritize resources and develop processes that address the organizations' highest risks. Technology will be an important tool in improving the management and monitoring of compliance risk, increasing an organization's awareness and helping to coordinate efforts while working with limited resources.

Conclusion

The regulatory change that is coming to the insurance industry is likely to call for a more robust compliance function than insurers have needed in the past and many have in place now. Many insurers are not only in the insurance business, but also oversee affiliated banks, brokerages and investment advisors. Each of these activities represents a significant compliance challenge by itself, let alone in combination with other change on the way.

Our survey indicates that the compliance functions of many insurers may not yet be ready for the extent of change expected, but they do appear to be making steps to prepare. Among all of the regulatory change ahead, one thing is for certain: the effectiveness of the compliance function will play a key role in enabling insurers to successfully navigate the path to regulatory readiness and enhance the policyholder experience. ■

EY would like to thank the following 16 insurers that participated in the survey.

Aegon USA (Transamerica Financial Life Company)

American International Group

Allianz Life Insurance Company of North America

The Allstate Corporation

CNA Financial Corporation

Country Financial

Lincoln Financial Group

Massachusetts Mutual Life Insurance Company

Metropolitan Life Insurance Company

Northwestern Mutual

Prudential Financial

QBE Insurance Group

State Farm Insurance

The Travelers Companies

Westfield Insurance Company

Zurich Insurance Group

For more information about the survey and findings, please contact:

Thomas P. Ward
Partner
Ernst & Young LLP
tom.ward@ey.com
+1 312 879 2234

Andrew Chenoweth
Manager
Ernst & Young LLP
andrew.chenoweth@ey.com
+1 312 879 3853

EY | Assurance | Tax | Transactions | Advisory

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.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

EY is a leader in serving the global financial services marketplace
Nearly 43,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Office today includes more than 6,900 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

SCORE No. CK0773
1402-1205721 NY
ED 0115

ey.com