



Charting the evolving role and authority of the CRO

2016 North American
insurance CRO survey
Findings and key themes



EY

Building a better
working world

About the survey

EY's sixth annual Chief Risk Officer (CRO) survey was designed to chart the evolving role and authority of North American insurance CROs, as well as the development of enterprise risk management (ERM) capabilities generally. EY has a clear perspective of these developments, having conducted annual CRO surveys since 2010.

This year's group of survey participants is larger than previous years, with a larger number of participating organizations and more diversity among them.

The survey also featured a broader set of questions this year, with increased focus on insurers' experience with cybersecurity issues, as well as the first round of Own Risk and Solvency Assessment (ORSA) submissions, required by a number of state regulators in 2015.

EY sincerely thanks the CROs and companies that shared their time and insights for this year's survey.

Sector

- ▶ Property and casualty (P&C): 55%
- ▶ Life: 35%
- ▶ Composite: 10%

Size

Ranging from large global organizations with multiple regulatory regimes (including US Federal Reserve Board oversight) to mid-sized national carriers with only US state regulators

Geography

Including Canadian and Bermudian insurers for the first time and the US operations of global insurers and reinsurers

- ▶ US-headquartered: 60%
- ▶ Foreign-headquartered: 40%

Executive summary: CRO influence expands as ERM matures rapidly, although late adopters remain

Results from EY's sixth annual survey of North American insurance CROs provide an overview of current ERM capabilities, practices and organizations. They also provide a view into the variety of ERM frameworks across the insurance sector. This year's survey revealed a spectrum of maturity levels of ERM programs – with some very impressive frameworks that are integral to and influential in how the business is run, to others that are limited in scope and formality. To a degree, this variety reflects the inclusion of a broader and more diverse group of participants in the 2016 survey compared with past years.

The survey also clarifies the role that companies expect CROs to perform. Where ERM structures are advanced, CROs are very senior officers and participate in decision-making at the highest levels of the organization. At the other end of the continuum, the survey included several insurers that do not have a single, titled CRO role, though there may be an officer leading ERM efforts. More robust ERM programs have typically been in place for a few years and are now fully embedded as part of routine business operations, while late adopters struggle to define the ideal role, structure and prominence of their risk teams.

Interestingly, despite the varying levels of sophistication and formality, all survey respondents felt their organizations have adequate processes to manage the risks to their business. In some cases, EY analysis reveals a degree of complacency where risk management capabilities do not seem sufficiently developed. There are just as many examples, however, where risks are very effectively monitored, controlled and mitigated without the recognizable or formalized superstructure that is often associated with "modern" ERM.

Key themes

The 2016 CRO survey results show clear trends toward expanding ERM scope and maturity, rising CRO influence and increasing “operationalization.” Clearly, ERM is advancing toward a “business as usual” status. The key themes that emerged from this year’s results are the following:

- 1 **Regulatory backdrop:** gradually increasing clarity despite lingering uncertainty 4
- 2 **Roles, responsibilities and reporting lines:** what CROs do now, with whom they work and how governance works..... 7
- 3 **ORSA:** one year in, a sense of limited value and learning curves for both insurers and regulators 10
- 4 **Risk appetite:** “build-out” work continues, with a focus on corresponding limits..... 13
- 5 **Extent of risk quantification:** increased stress testing and modeling via a wide range of practices 16
- 6 **Model risk management (MRM) and model governance:** greater adoption, but varying formality and model maturity..... 19
- 7 **Cybersecurity:** rising CRO involvement and a recognition that more must be done..... 21



Key theme 1

1 **Regulatory backdrop:** gradually increasing clarity despite lingering uncertainty



What CROs say about the current regulatory landscape:

“From talking with Fed-regulated companies, I know the lengths to which they’ve been driven. We see that as costly bureaucracy that would not add value.”

“It is tough to meet the challenges of more regulation, but in the end we are not doing anything beyond what is good business practice for ERM.”

Regulatory issues remain atop the agenda for many insurance CROs. It is no surprise that the ORSA requirement from the National Association of Insurance Commissioners (NAIC) was the most frequently cited regulatory concern, with every participant required to submit an ORSA summary report to state regulators for the first time in 2015 (see page 10 for more detailed survey results).

However, respondents cited a broad range of topics on their regulatory agendas, from Federal Reserve Board (FRB or Fed) oversight to evolving NAIC standards for cybersecurity.

(Regulatory backdrop cont.)

Beyond ORSA, the urgency in relation to regulatory issues depends on the nature of the insurer:

- ▶ The largest insurers, including those subject to federal regulation, are focused on developments from the FRB.
- ▶ Overseas regulation and global International Association of Insurance Supervisors (IAIS) developments are a higher priority for insurers with international operations.
- ▶ Insurers that distribute qualified investment products are evaluating the potentially significant impacts from the U.S. Department of Labor (DOL) ruling regarding fiduciary responsibilities.
- ▶ Interestingly, most respondents – including those from companies not likely to be regulated by the Fed – report paying close attention to FRB actions, given the likelihood that federal standards will inform and influence those imposed by state regulators.

Against the backdrop of expanding regulation and intensifying requirements, the landscape is becoming somewhat clearer thanks to announcements and publications during the last 12 months (see Figure 1).

Still, the considerable uncertainty that remains defines the climate in which US CROs must operate.

For companies under Fed regulation or subject to overseas mandate (e.g., US subsidiaries of parents subject to Solvency II), CROs find their agenda frequently set by regulators, either directly or indirectly. In contrast, CROs at companies under state regulation can chart their own course for ERM.



Figure 1: Top areas of regulatory change affecting CROs

	Applies to	Key developments	Uncertainties
NAIC – ORSA	All US insurers with gross written premium > \$500m or part of group with gross written premium > \$1b	A majority of US states required insurers to file ORSA summary reports for the first time during 2015	How much state regulators demand of ORSAs and the annual improvements expected
NAIC – other regulations	All US insurers	Ongoing development of new group capital calculation New insurance data security model law being developed by NAIC's cybersecurity task force	Interaction with developing FRB and IAIS group capital calculations Operational impact of new cybersecurity regulation
FRB regulation	Insurance groups designated by the Financial Stability Oversight Council as systemically important financial institutions (SIFIs) Insurance groups that own insured depository institutions (i.e., insurance savings and loan holding companies (SLHC))	Two proposed standards released in June 2016 for industry comments: ▶ Notice of proposed rulemaking (NPR) on Enhanced Prudential Standards for SIFIs, covering corporate governance and risk management and liquidity risk management ▶ Advance notice of proposed rulemaking (ANPR) on capital requirements for SIFIs and SLHCs	Final content and requirements of FRB rules Timeline for implementation "Trickle-down" effect of capital standards for insurers not regulated by the FRB Industry reaction to final rules after initial welcoming attitude Interaction with developing NAIC and IAIS group capital calculations
Overseas regulation (e.g., Solvency II, Bermuda, Australia)	US insurers with significant overseas operations Foreign-owned insurers	Solvency II officially came into effect 1 January 2016, though several areas are not fully resolved	Future developments in overseas jurisdictions Solvency II equivalency, including covered agreement negotiations Impact of Brexit
IAIS International Capital Standards/ ComFrame	Internationally active insurance groups (IAIGs)	Second round of ICS field testing and consultation takes place during 2016	Influence of IAIS standards on US-domiciled insurance companies Fed and NAIC rejection of internationally developed standards
DOL fiduciary rule	US life insurers and financial advisors	Final DOL rule requiring application of a fiduciary standard to a broader range of investment advice activities comes into effect in April 2017	Impact on insurers distributing investment products Level of market disruption

Key theme 2

Roles, responsibilities and reporting lines: what CROs do now, with whom they work and how governance works



One of the objectives of the 2016 survey was to assess the current roles and responsibilities of CROs. The general trend is toward larger roles and increasing responsibility, much of it occurring at the senior management level and with a broader range of stakeholders across the business. The results also reveal the most prevalent organizational structures, along with interesting variety in the shapes and sizes of risk teams.

Governance structure

Most CROs report directly to either the CFO or the CEO (see Figure 2). In a few cases, the CRO reports through another position, such as the chief actuary or COO. The independence of CROs has been a frequent topic of discussion in recent years. Most CROs have full access to the board and attend quarterly risk committee meetings. Many also attend board subcommittee meetings, such as the audit committee. In organizations where the CRO reports to the CFO, the independence of the risk management function is less clear.

Three lines of defense

The “three-lines-of-defense” model has become the norm for most of the financial services industry, and more than three-quarters of survey respondents reported its formal adoption at their organizations (see Figure 3).

Many of the organizations that have not implemented the model indicated that it is unnecessary, too bureaucratic and/or too costly. These organizations were also unlikely to adopt the model in the near future and were not subject to regulatory requirements to adopt it.

Organizations that aspire to adopt the model report challenges in demarcating the three lines, particularly where first-line and second-line responsibilities reside with the same officer. Some survey participants seemed slightly complacent when compared with peers who have made strides in governance to achieve proper independence for the risk management function.

(Three lines of defense cont.)

A few survey participants reported that their companies see more extensive and formal ERM as dangerous because it releases responsibility for risk from company officers in the first line. This was a minority view; many more participants reported that ERM is being used to enhance the value of the business.

Size of risk team

CROs report growing organizations, with higher numbers of direct and indirect reports than in previous years. Only 29% of CROs surveyed have more than five direct reports. However, 56% had more than 10 indirect reports. Some participants have risk teams numbering hundreds of personnel (see Figure 4).

The variation in size reflects the variety of insurers that participated in this year’s survey (which included more smaller companies than in past years), differing maturity levels of risk functions and the unique capabilities included in risk functions at different companies. For example, there is considerable inconsistency in the reporting lines for actuarial capabilities. At some companies, they are integrated in the risk function; at others, they reside exclusively outside it.

Some risk teams number only two or three people. In some cases, small risk teams reflect a minimalist approach; in others, small risk teams act solely as coordinators for the collation of risk reporting, with risk measurements received from actuarial, finance, asset managers and other groups. (Indeed, one participant argued that such an approach promotes wider corporate responsibility for risk.)

Survey results confirm that larger risk teams are needed when companies have more detailed risk appetite and limits or more extensive and frequent risk reporting requirements.

At some firms, risk quantification models are not currently owned by the risk team or CROs, though there is a trend toward risk models sitting under risk. The survey also found considerable variety in terms of responsibility for reinsurance management, regulatory affairs, compliance and second-line oversight of underwriting or technical provisions.

This diversity of the CRO portfolio leads to a corresponding variety in the size of risk teams and overall headcount designated to risk.

Figure 2: Reporting lines and board access

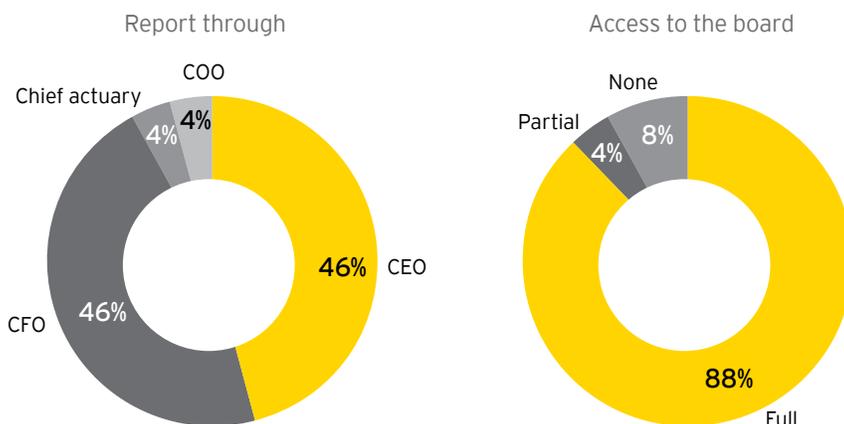


Figure 3: Formal adoption of a three-lines-of-defense model

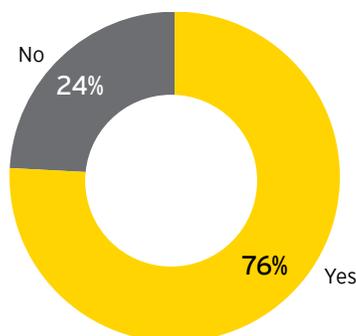
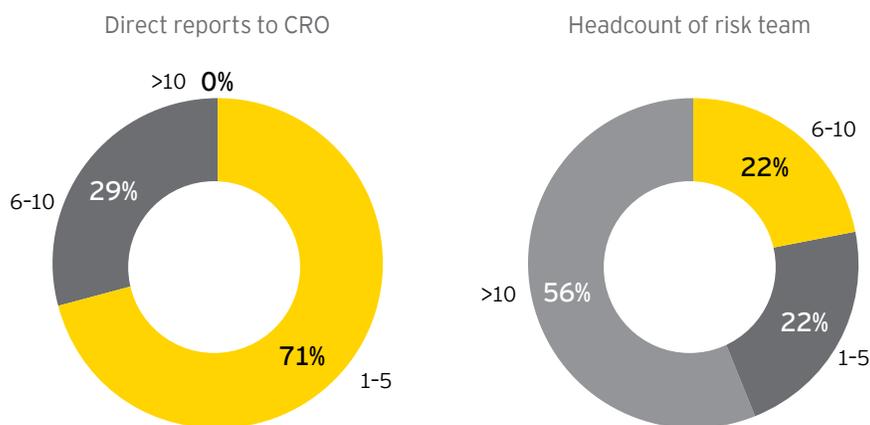


Figure 4: Size of risk team

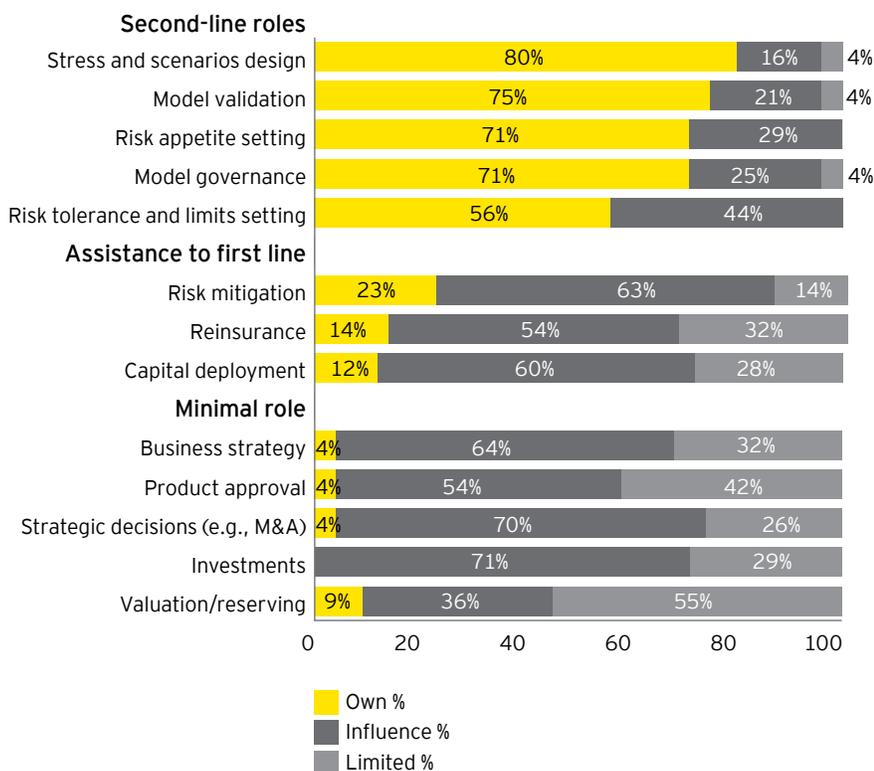


CRO roles and responsibilities

Half of CROs reported that they have been given new responsibilities in the previous 12 months, with some expecting to take on more within the next few years. In terms of CRO responsibilities, there are varying degrees of influence across a range of activities. It is somewhat surprising that not all second-line roles (such as model validation and risk appetite setting) are fully owned by CROs (see Figure 5).

For capital deployment, strategy, product approval, reinsurance, risk mitigation and reserving, most CROs have influence, but not ownership. This finding aligns with the second line of defense's increasing role as an "effective challenge" to decisions made by the first line.

Figure 5: Role of the risk function



What CROs say about their roles, responsibilities and organizations:

"We have adopted three lines of defense, but in a limited fashion. We believe risk is everyone's responsibility."

"We have not taken on new or additional responsibilities, but would like to be involved in more decision-making."

"We have begun to help the business units do advanced analytics leveraging their own risk tools."

"Stress testing results were a wake-up call for our board. More than any other activity, this gave them an understanding of the risk team's purpose."

"Too much of our modeling sits exclusively with the actuaries. There is insufficient independence even in the model reviews that have been completed."

Key theme 3

3 ORSA: one year in, a sense of limited value and learning curves for both insurers and regulators



In late 2015 and early 2016, many insurers submitted their ORSA filings to their state regulators for the first time. As such, the survey results hint at how state regulators are working with insurers with their ORSA submissions. The coverage included participants submitting ORSAs to 12 different state regulators, including Connecticut, Delaware, Illinois, Massachusetts, New York, Ohio, Pennsylvania and Wisconsin.

ORSA's value

Most respondents saw reasonable value in completing their first mandatory submission, although for many the value was limited (see Figure 6).

Notably, firms that had completed ORSA pilots in previous years perceived more value from the process, likely because ORSA was now embedded into regular operations and more parts of the business.

A few respondents viewed ORSA purely as a compliance exercise or reported that it did not bring value, although this was a minority view. The combined percentage of these naysayers and those CROs who remain in the “unsure” and “too early to say” category (currently more than half of CROs, according to survey results) bears watching in the future.

Comments from survey participants suggest the range of ways ORSA can produce current or future value. For instance, one CRO commented that having the ORSA report as a reference significantly shortened state-level audit procedures this year. For some insurers, ORSA highlighted gaps in risk management processes and capabilities, and clarified opportunities to refine governance and committee structures. One respondent commented that the “internalization” of stress and scenario impacts allowed more proactive thought about management responses.

All companies involved their boards in the ORSA process, in alignment with the NAIC's guidelines, and some CROs reported their board's satisfaction with the report. Other firms used ORSA as a source for employee education or as a single, centralized source for risk information.

(ORSA's value cont.)

Some survey participants did not regard the arrival of the ORSA requirement as so significant in that it gives rise to a report on general ERM activities that companies were taking anyway, before there was any regulatory compulsion. Other respondents described plans for streamlining the ORSA process in the future, implying that less laborious efforts could yield more value. This was particularly the case among those firms that were submitting multiple ORSAs (e.g., for different entities, different states or international operations).

Impact and effort

Only one-third of organizations reported major changes in their ORSA in 2015 (see Figure 7).

In particular, companies that participated in ORSA pilots in 2013-14 generally invested less time and fewer resources in producing their first official reports.

The level of effort and amount of resources necessary to produce the report varied greatly (see Figure 8).

This finding is a reflection of the diversity in the size and complexity of this year's participating insurers, as well as the different approaches to completing the exercise. Some companies have full-time resources dedicated to ORSA, while others have people doing "a little work often" alongside their other roles. Generally speaking, the larger and more complex organizations expended greater effort and resources for ORSA. But there is also considerable disparity between similar insurers, with very different interpretations of what the NAIC ORSA model law required for risk quantification and measurement.

Figure 6: Value obtained reflects the work required to produce the ORSA

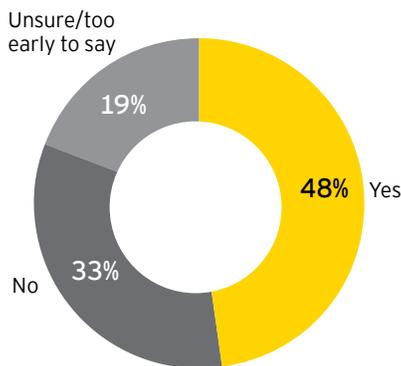
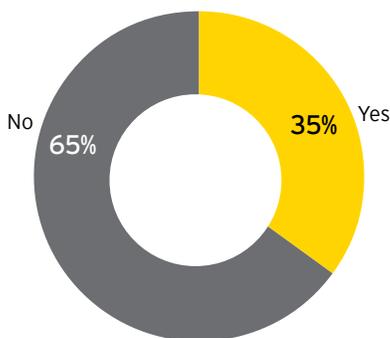


Figure 7: Major changes in this year's ORSA process



ORSA and the regulators

At the time of the survey, not all participants had received feedback from regulators on their ORSA submission. Those who had feedback indicated the following areas as needing enhancement:

- ▶ Clearer linkages between risk appetite and stress testing
- ▶ Increased focus on risk identification
- ▶ More detail on stress and scenario testing
- ▶ Reverse stress testing to determine what it would take for company to default
- ▶ Validation of results
- ▶ Inclusion in ORSA of M&A activity
- ▶ Clarity over unique ORSA features at mutual insurers

The survey results and comments from participants indicate that regulators are also coming to terms with ORSA – no surprise given that this was the first official year for submissions. One respondent described a “learning curve” for regulators in determining the best way to use the content of the reports and determining an effective review process. But it was a majority view that ORSA improved overall regulator understanding of current risk management practices (see Figure 9).

Figure 8: Level of effort to produce ORSA (FTE months)

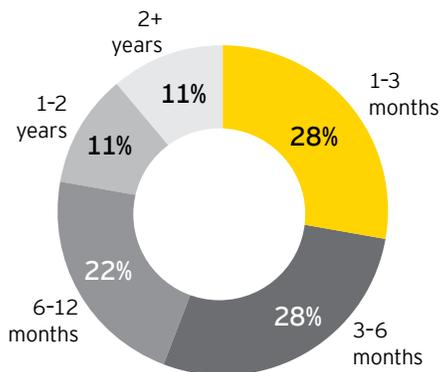
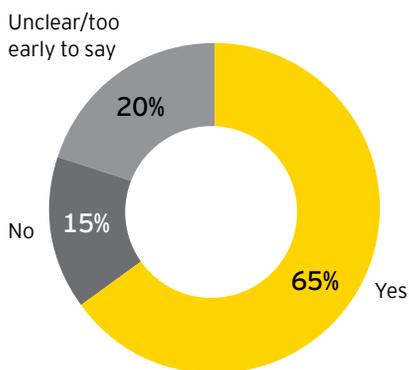


Figure 9: Better regulator understanding of your risk management practices as a result of the ORSA report



What CROs say about ORSA:

“Did ORSA add value? Yes, but not massively so.”

“There was value in educating regulators, which helped with reviews.”

“ORSA was mainly about putting into words what we do already.”

“The board loved reading the report!”

Key theme 4

4 Risk appetite: “build-out” work continues, with a focus on corresponding limits



Risk appetite is an area CROs are still working to build out by incorporating both quantitative and qualitative factors. CROs' focus on risk appetite is not surprising given that nearly three-quarters of survey respondents own the process (see key theme 2: Roles, responsibilities and reporting lines).

Risk appetite metrics

Virtually all respondents commented that their company's risk appetite references both “economic” internal views of capital and regulatory requirements (see Figure 10).

There was considerable variation in the internal view being used, with “economic capital” being defined in various ways by different companies. Strictly defined, market-consistent economic approaches are not common: the survey found fully developed market-consistent balance sheets, with corresponding risk metrics, at only a few of the companies surveyed.

External credit ratings are the third most common metric referenced by risk appetites. This is particularly important in situations where insurers' potential customers (especially large corporate customers through broker channels) place their business largely based on the rating of the carrier.

Profitability measures are becoming more common within risk appetites. These can be as simple as stating some fixed probability (or zero probability) of the business incurring a loss. Various companies use operating, total or “economic” profit. A number of respondents described active projects to develop greater use of profitability measures within risk appetites.

Quantitative views and qualitative issues

Most insurers have implemented quantitative risk limits regarding insurance risks, as well as market, interest rate and credit risks (see Figure 11).

Approximately half of respondents commented that they have quantitative limits relating to operational risk, with more saying they intend to build this out. Liquidity risk is a more emerging area for setting quantitative risk limits. Certain insurers reported the use of risk limits in relation to other metrics, such as the outputs from stress testing and measures of earnings volatility.

Respondents also cited a number of qualitative areas that are subject to risk limits (see Figure 12).

Risk limits

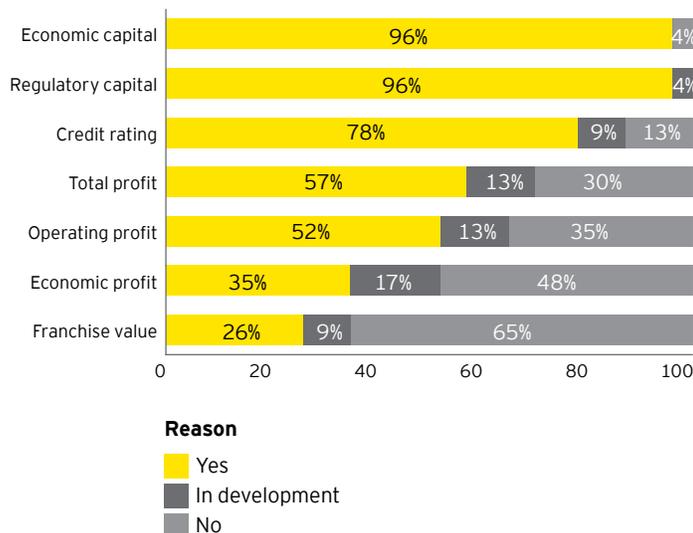
The 2016 survey probed deeper into companies' risk limits, particularly the relationship between risk limits and risk appetite. Many participants reported that their risk limits predated the introduction of a comprehensive risk appetite. Thus, companies face the challenge of extending risk limits to cover all risk types, so as to make sure the full sweep of risk limits is effective in keeping the organization within its risk appetite.

The starting point varies by company type. Life companies focus their risk limits on asset constraints to control interest rate risk and market risk. At P&C companies on the liabilities side, the traditional focus for limits applies to exposures, retention levels and PMLs (probable maximum losses) for natural and man-made catastrophes.

Top-to-bottom consistency

Most CROs reported that more work is required so bottom-up risk limits are fully aligned with risk appetite statements. In many cases, the top-down risk appetites were only two or three years old and had not been fully cascaded down into new or amended risk limits. Only 16% of respondents reported having full consistency between bottom-up and top-down measures. A higher percentage (56%) reported achieving full consistency only for some risks (see Figure 13).

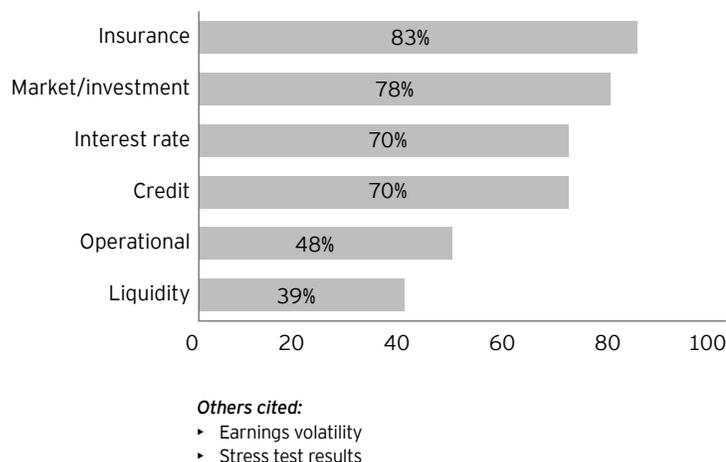
Figure 10: Metrics used in setting the corporate risk appetite



Others cited:

- Probability of making a loss/losing one year profit
- Return on risk-adjusted capital (RORAC)
- Managing catastrophe exposures
- Changes in market value of assets
- Leverage
- Reputational risk
- Legal and regulatory risks
- Strategic risks

Figure 11: Risks for which you have set quantitative limits



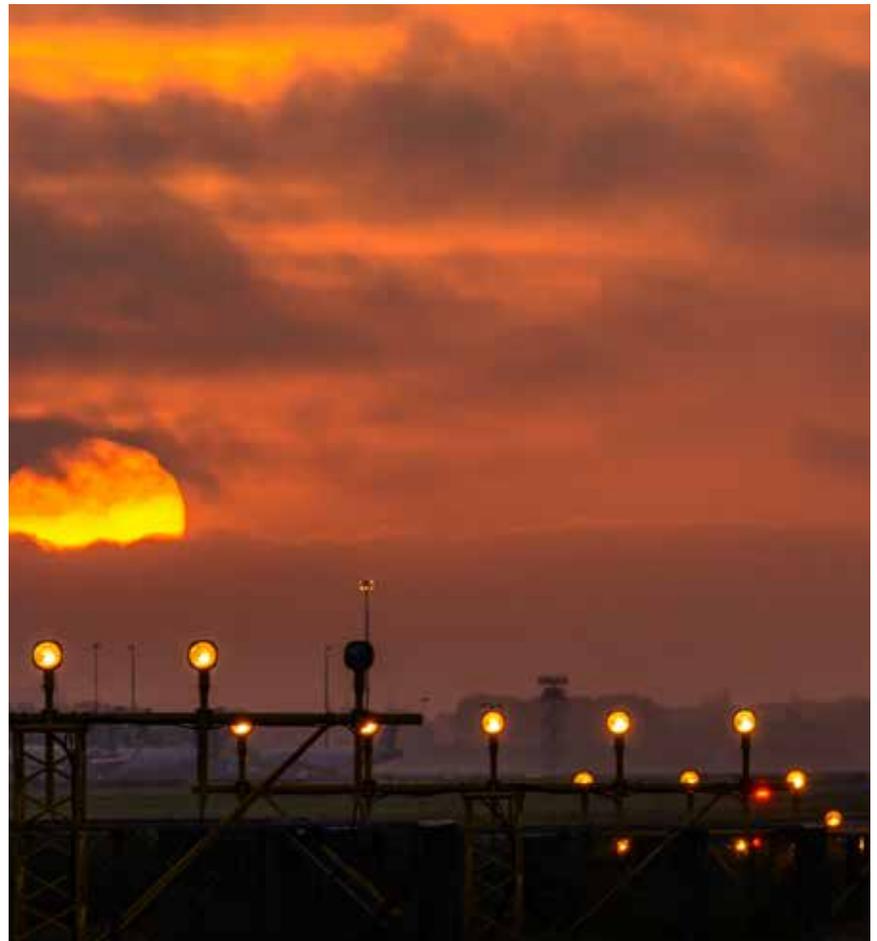
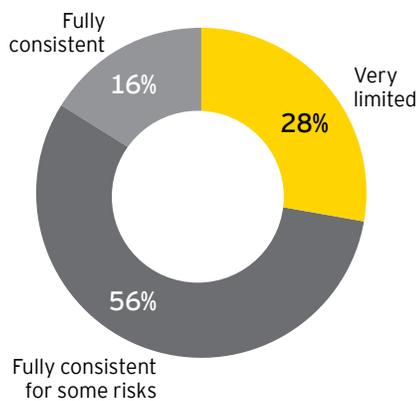
Others cited:

- Earnings volatility
- Stress test results

Figure 12: Qualitative issues affecting the setting of risk appetite (comments)

- ▶ Emerging risks
- ▶ Reputational risk
- ▶ Regulatory risk
- ▶ Competitive and rating agency
- ▶ Stakeholder obligations
- ▶ Alternative investments
- ▶ Service quality
- ▶ Employee engagement and satisfaction
- ▶ Strength of business partnerships

Figure 13: Consistency between bottom-up risk limits and top-down risk appetite/ tolerance statements



What CROs say about risk appetite:

“The board was unenthusiastic in the first year. But the annual review of appetite is now an important date on the board’s calendar and prompts vigorous debate.”

“I’m frustrated that I don’t think we’ll have risk appetite and limits fully in step until the 2017 planning cycle.”

Key theme 5

5 **Extent of risk quantification:** increased stress testing and modeling via a wide range of practices



Overall trends from earlier CRO surveys held, as companies expanded the scope and extent of their stress testing and continued to refine their capital models. However, there is a wide range of practices for risk quantification. Some larger companies (most notably groups with European operations) have comprehensive stochastic economic capital models that include all material risks.

Among companies with cruder risk measurements, ORSA requirements have not yet driven significant enhancements to quantification practices. Where some survey participants described taking a minimalist approach to risk quantification in their ORSA submissions, there is little evidence as yet that state regulators will demand better quantification. However, some companies had yet to receive state regulator feedback on submitted ORSAs. Many CROs felt regulators will demand more – seeing it as a question of “when,” not “if.”

Aside from the regulatory influence on risk quantification, increased senior management and board awareness of stress testing and model outputs has led to demands for enhanced quantification. Several CROs highlighted that greater board attention meant stress tests and models needed to be more reliable – which in turn required much better governance over methodology and assumptions.

CROs cited other associated activities, including better, more frequent and more transparent reporting. Because outputs need to be accessible to non-modelers outside the risk teams, “education” of boards and senior management is required, according to some CROs. Finally, CROs reported that board attention was driving the need for more documentation and validation for more complex models.

Business use of stress testing and modeling

A full 78% of participants cited organizational use of stress testing and modeling in business planning processes. Several CROs planned to include management in the setting of risk tolerances and limits (see Figure 14).

This finding provides encouraging evidence of strong links between ERM processes and core business planning. However, it is surprising to see fewer organizations (44%) stating that their risk quantification is included in their ORSA. It seems contradictory to have involvement with business planning and not report it as part of the ORSA report.

After business planning and ORSA, capital management was the next most frequent application of stress testing and modeling, cited by 44% of surveyed CROs. Participants also mentioned various downstream applications of risk quantification for liquidity management, reinsurance program optimization (both life and P&C), asset-liability matching, equity allocation and return on equity (ROE) reporting.

It appears that CROs' plans to invest more resources and attention to risk quantification – a top area of focus, according to the 2015 survey – have come to fruition. CROs are increasingly able to bring risk quantification and analysis to support more decisions across the business.

Governance over stress testing and modeling

The survey asked participants to list the areas of their company involved in setting assumptions and stresses for risk quantification. Half reported some form of centralized role in these activities, such as an enterprise-level risk committee, chaired by the CRO, with representatives from all the first-line functions in the company (see Figure 15).

Outside of this centralized function, participants reported finance (cited by 29% of participants), risk owners (29%) and actuarial (14%) as the other areas with direct involvement in setting

Figure 14: Use of stress testing

Setting level of risk tolerance, business planning	78%
Capital management (e.g., determine own view of how much capital to hold)	44%
ORSA	44%
Liquidity management	33%

Figure 15: Areas of the company involved in developing scenarios for analysis

Risk management/ risk committee	50%
Finance	29%
Risk owners*	29%
Actuarial	14%

*(underwriting, reserving, investments, credit, IT, legal/compliance)

(Governance over stress testing and modeling cont.)

assumptions or generating stress tests. Compared to previous surveys, more parts of the business are involved in generating scenarios, a clear manifestation of the advancement and maturation of ERM.

Survey respondents generally expressed a strong desire to expand stress testing and modeling capabilities in the future. It is clear that, despite significant advances, CROs still see an opportunity to apply risk quantification more broadly as a highly effective risk management tool.

Intended improvement to risk quantification

The most commonly cited areas of improvement were as follows:

- ▶ Increased granularity in stress testing and modeling
- ▶ Additional stress tests or scenarios for less-important risks
- ▶ The calculation of risk measures at different confidence levels
- ▶ Closer integration into business planning processes
- ▶ Acceleration of risk calculations to provide risk metrics soon after financial close dates
- ▶ Increased frequency (e.g., from annually to semiannually or quarterly)

What CROs say about risk quantification and stress testing:

“We use stress testing for everything: determining our overall capital, asking ourselves if we’re comfortable with the risks we are taking, and whether our risk profile is increasing or decreasing.”

“Our parent company plays a key role in that they require scenarios that are relevant to all subsidiaries. Within our company, risk management takes the lead with counsel and feedback from the executive management committee and the board.”

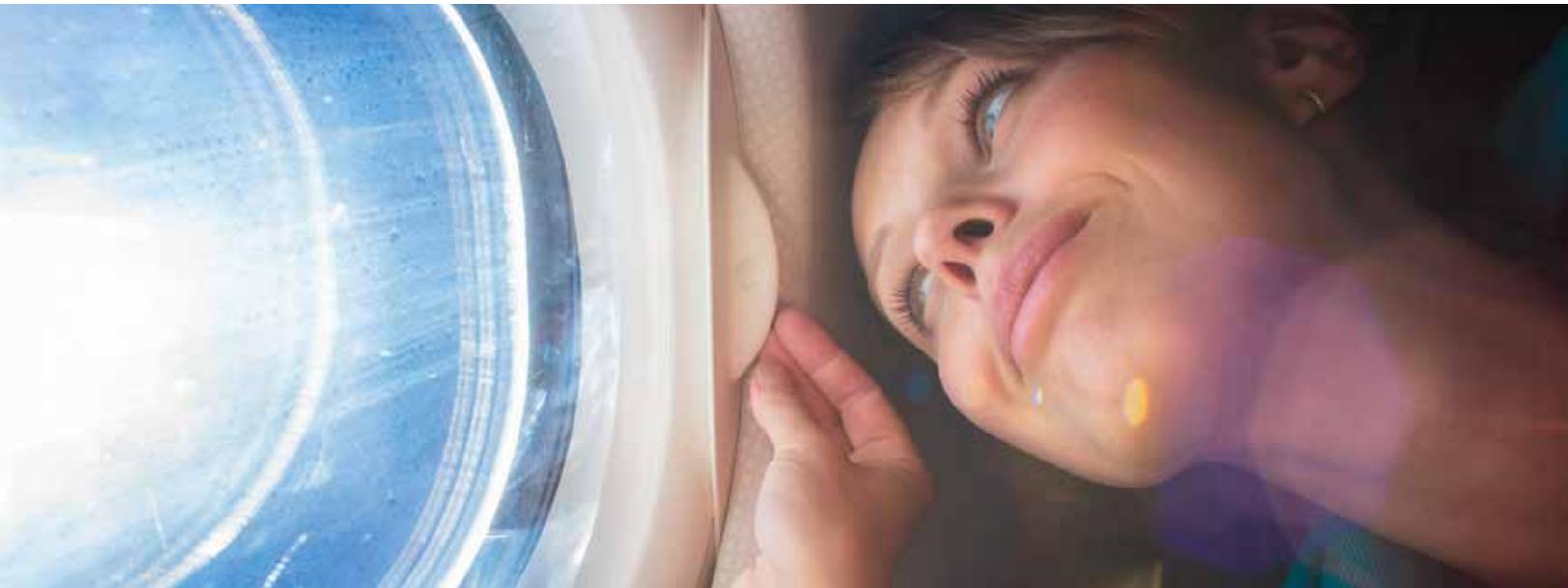
“Reporting of our economic capital position as it changes between quarters has drawn much more senior attention to our risk profile and how the profile changes due to external developments and internal business decisions.”

“Risk reporting is still viewed with suspicion in some parts of our business. We need it to become more stable to gain wider acceptance.”

6

Key theme 6

Model risk management (MRM) and model governance: greater adoption, but varying formality and maturity



The 2016 CRO survey results show significant advances in the area of MRM when compared with 2015 survey results. A full 73% of CROs reported that formal MRM programs are in place, up from 50% in 2015 (see Figure 16).

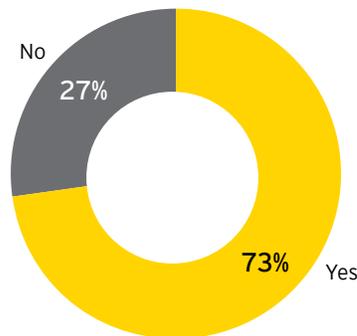
However, there is considerable disparity in the implementation approaches among different insurers. In general, greater formality is found at companies that are Fed-regulated (by virtue of their status as SIFIs or SLHCs), where MRM is mandatory and scrutinized by the Fed. At the other end of the spectrum, a few survey participants reported having no formal MRM.

MRM ownership

Some CROs surveyed are designated as responsible for MRM policies and protocols (see Figure 17).

In these cases, the structure for MRM generally follows a three-lines-of-defense model – with clearly identified “model owners” sitting in the first line, while CROs and their risk teams are responsible for model validation as part of the second line. However, the results include exceptions to this pattern, particularly where the risk team itself owns models for risk monitoring or internal capital reporting. In those cases, companies nonetheless attempt to have separation between model builders and owners and the parties performing the validation.

Figure 16: Formal model risk management (MRM) program in place



Independent validation

Most respondents (59%) indicated that their model risk management framework now requires independent model validation, a continuation of trends identified in previous surveys (see Figure 18).

High-priority models are often validated through the use of outside consultants or by internal resources from the second or third lines of defense who are deemed to be sufficiently independent from the model owner and are qualified to validate the model.

Several CROs highlighted further practical challenges in implementing successful MRM programs. For instance, some CROs and risk teams are involved in the first line of defense, meaning there is no fully independent second line. In other cases, CROs recognized that some validation remained incomplete or that the organization lacked the internal resources with the technical skills required for rigorous model validation, given that validation cannot be performed by the same personnel who originally designed or built the models.

MRM resources

As to the number of resources, 32% of respondents had more than five members of their MRM team in the second line. However, 27% reported having no dedicated team for MRM. As with the number of resources on the risk teams, these differences reflect both the varying size of the companies and the maturity of the MRM frameworks (see Figure 19).

As regulators, senior management and boards continue to increase their scrutiny of the accuracy and reliability of model outputs used in business decision-making, MRM will remain an area of sharp focus for CROs.

Figure 17: Primary responsibility for the MRM program

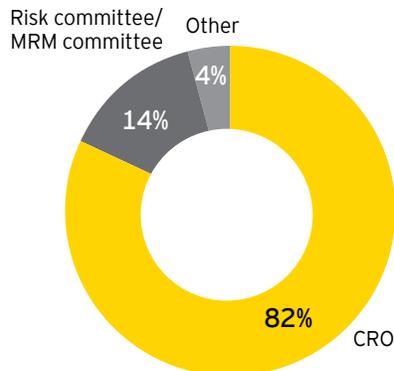


Figure 18: Company requirement for independent model validation

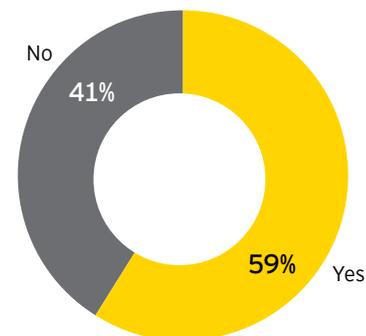
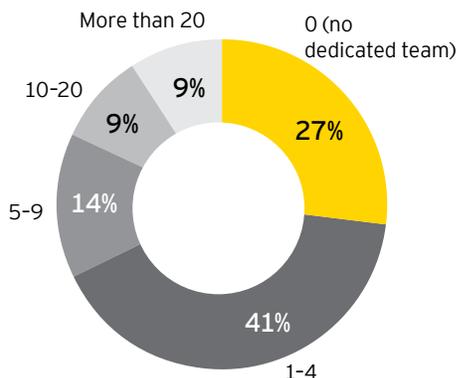


Figure 19: Size of model risk management team in the second line



What CROs say about MRM and model governance:

“Risk management validates inputs developed by the business. Models (capital, reserving and pricing) are categorized as high, medium or low risk. Risk management puts together the validation approach, budget and resource plan.”

“We don’t currently require a model owner independent from the validator, but we will starting next year.”

“We have model validation, but it would satisfy neither the Fed nor Solvency II.”

Key theme 7

7 **Cybersecurity:** rising CRO involvement and a recognition that more must be done



What CROs say about cyber:

“We are spending a lot on what could be called cyber risk management, although it is not identifiably under the risk management function.”

“Although we manage down the risk, we regard a cyber breach as inevitable, and we’re preparing to minimize the damage caused.”

Most CROs participating in the 2016 survey reported that their companies faced a real risk of suffering a serious cyber attack or data breach. The quantity and personalized nature of the data that insurers hold make them highly attractive targets for hackers and cyber thieves.

In regard to cyber threats, some CROs currently serve as liaisons to IT divisions, which typically own these risks. However, several respondents believe more must be done. One CRO already had a clearly designated role for cyber, with a direct reporting line to the CEO and risk committee designed to guarantee independence from IT.

The business potential

A second type of cyber risk involves insurance liabilities, especially casualty lines. Interestingly, many survey participants observed that casualty providers were underwriting cyber risks either consciously or unwittingly. Therefore, it is no surprise that some P&C CROs reported that they are involved in review of existing contract language to assess whether and which types of cyber risks have already been underwritten (knowingly or otherwise). P&C CROs spoke of seeking the right balance between seizing the profit potential of those risks and exposing the company to an unacceptable level of risk.

From the survey responses, there is reason to believe that CRO involvement in cybersecurity will increase. As boards and CEOs have greater visibility into the issue, it seems inevitable that they will ask CROs to engage in the evaluation and decision-making processes, even if CIOs and IT groups continue to own them. In some cases, CEOs have already requested that CROs serve as an independent check (or second line of defense) relative to cyber issues.



Outlook for the future: defining success as CROs expand their roles and responsibilities

CROs spoke of their aspirations for greater involvement in strategy development and business planning over the next three to five years. Such involvement will go beyond the typical “rear-view mirror” perspectives or baseline questions, such as, “How do we ensure that we remain in business over the next 12 months?” to incorporate more forward-looking and business-enabling views of risk.

As such, survey respondents spoke of broader perspectives and decision-making processes that incorporate the following:

- ▶ Risks to the “franchise” (i.e., shareholders) and those that threaten policyholder security overall
- ▶ Risks of “omission” – risks associated with not taking on new initiatives and/or change programs
- ▶ Risk-reward considerations in determining where the company should invest its next dollar

- ▶ Disruptive forces, such as major shifts in distribution channels and demographics
- ▶ Technology-driven changes, such as the impact of driverless cars (on auto lines), medical advance (on life insurance) and “digital-only” distribution channels
- ▶ Increased risk analysis and involvement in product development, pricing and underwriting
- ▶ Risk quantifications and the costs of risk (e.g., cost of capital, risk-adjusted profitability metrics, ROE)

There is an awareness of what these more forward-looking roles require, such as the ability to project accurately risk metrics across three- to five-year time horizons. It is clear that CROs believe the increasing maturation and sophistication of ERM capabilities present a compelling business case to the entire enterprise.

What CROs say about the future:

“I want to have influence on decisions to do new things.”

“Success in the future would mean a culture where business leaders tend to say ‘What, you haven’t told the CRO about this yet?’ when making key decisions or evaluating their options.”

Conclusion: CROs lead insurers forward on the ERM journey

The influence of ERM programs, CROs and the risk teams they lead continued to grow in the 12 months since the 2015 EY survey. Survey participants reported incremental gains across a variety of areas: size of risk teams, access to senior management and boards, risk appetite setting, impact of ORSA, quantification via stress testing and capital modeling, and risk reporting.

CROs keep a wary eye on regulatory developments. However, the survey found a variety of concerns – with understandable variation between US state regulation, Fed regulation or international influences. These matters influence the day-to-day practicalities of risk management programs generally and CROs’ agendas particularly.

While 2015 brought required ORSA submissions for most survey participants, the process proved to be less of a hurdle than might have been expected. Many companies had already “upped their games” through the ORSA pilots of preceding years. Furthermore, survey participants saw little evidence of strong challenges from state regulators receiving the first round of ORSA submissions.

The cumulative results of the survey show that, in the absence of regulatory drivers, the increasing influence of ERM is being earned on its own merits – which seems, in conclusion, a very good place for industry CROs to find themselves.

Contacts

US

Richard Marx
Principal
Ernst & Young LLP
+1 212 773 6770
rick.marx@ey.com

Chad Runchey
Principal
Ernst & Young LLP
+1 212 773 1015
chad.runchey@ey.com

Douglas French
Principal
Ernst & Young LLP
+1 212 773 4120
doug.french@ey.com

David Paul
Executive Director
Ernst & Young LLP
+1 212 773 8904
david.paul1@ey.com

.....

Global

UK
Graham Handy
Partner
Ernst & Young LLP
+44 7876 877 083
ghandy@uk.ey.com

Australia
Kent Wong
Director
Ernst & Young
Australia
+61 2 9248 4176
kent.wong@au.ey.com

Asia-Pacific

Sumit Narayanan
Partner
Ernst & Young Advisory Pte Ltd
+65 6309 6452
sumit.narayanan@sg.ey.com

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.

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 Organization 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 Wealth & 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.

© 2016 EYGM Limited.
All Rights Reserved.

EYG no. 03230-161Gbl
1608-2014562 BDFSO
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