Deloitte.

Navigating the year ahead

2018 insurance regulatory outlook

United States
December 2017

CENTER *for*
REGULATORY
STRATEGY
AMERICAS

This publication is part of the Deloitte Center for Regulatory Strategy, Americas' cross-industry series on the year's top regulatory trends. This annual series provides a forward look at some of the regulatory issues we anticipate will have a significant impact on the market and our clients' businesses in 2018. The issues outlined in each of the reports provide a starting point for an important dialogue about future regulatory challenges and opportunities to help executives stay ahead of evolving requirements and trends. For 2018, we provide our regulatory perspectives on the following industries and sectors: banking, securities, insurance, investment management, energy and resources, life sciences, and health care. For a view of the other trends impacting insurance in 2018, we encourage you to read the Deloitte Center for Financial Services companion paper.

We hope you find this document to be helpful as you plan for 2018 and the regulatory changes it may bring. Please feel free to contact us with questions and feedback at **CenterRegulatoryStrategyAmericas@deloitte.com**.

Contents

Global foreword

Another year has passed, so what has changed?

This time last year, we expected 2017 to be a period of uncertainty for financial services regulation. Financial services firms were challenged by the continuing lack of clarity over the final shape of post-crisis reforms, the implications of Brexit, and a new US political administration. We also saw significant pressures on the banking and life insurance sectors from sluggish economic growth and low interest rates in Europe and the US, as well as from competition from new entrants (particularly fintechs).

Looking ahead to 2018, most of these challenges and uncertainties remain.

Economic growth, but how robust?

Global growth prospects improved through 2017 and continue to be broadly positive, albeit more subdued than in the period before the financial crisis. China, Europe, and Japan have all been outperforming expectations, and although India's economy has slowed lately, the long-term outlook is upbeat. There are now signs that the extraordinary monetary easing of the last ten years is starting, slowly, to unwind in Europe and the US, although this stands in contrast to the situation in China and Japan.

There are reasons for caution. Asset markets and prices have seemed impervious to the prospect of tighter monetary conditions and geopolitical tensions. This has left many commentators worrying that markets are in the grips of a bout of irrational exuberance. There are also signs of price bubbles in commercial and residential property markets, as well as leveraged finance markets, and of elevated levels of consumer indebtedness, particularly in the advanced economies.

Supervisors across the globe are very alert to the financial stability risks posed by the political and economic climate, and we expect them to focus on the ability of financial institutions in all sectors to deal with the downside risks of an abrupt shift in market sentiment and any increase in asset price volatility, irrespective of the trigger. Boards are expected to keep their risk appetites under review and will also need to engage closely with stress testing, whether prompted by supervisors or carried out internally.

What does this mean for the regulatory agenda?

Last year we predicted that there would be no wholesale rolling back of the post-crisis regulatory framework, and this continues to be our view. The consensus in the US is that there will be some meaningful adjustments to the Dodd-Frank Act, but no large-scale repeal or rewrite. In the EU there remains a considerable volume of ongoing legislative work; and even where there is no new legislation, there is a great deal of "fine tuning" of existing rules. The Asia Pacific region faces a long tail of implementation work and must also deal with the impact of regulation from outside the region.

At the international level, the Financial Stability Board (FSB) has shifted its primary focus toward a post-implementation evaluation framework, which will be "progressively applied" in the coming years. This is part of a rebalancing away from introducing new rules and toward assessing the effectiveness of what has been done over the past decade. Boards will need to be ready to demonstrate to supervisors that they have embedded change and that this is leading to the desired outcomes.

One major area where a number of significant unanswered questions remains is bank capital requirements. Although the Basel Committee on Banking Supervision (BCBS) has until now been unable to complete the Basel III package, final agreement on the open issues seems within reach. We do not see any major economies as being in a hurry to introduce more legislation, and we also see those economies being more willing to depart from the letter of global standards where they conclude it is in their interest to do so.

As a consequence, financial services firms need to be prepared to deal with the challenges of diverging regulatory frameworks. At a minimum, they will need globally coordinated approaches to understand overlaps, incompatibilities, and potential synergies.

Supervisors are turning more attention to long-term structural issues

Technological innovation, aging populations, and climate change have all caught the attention of the regulatory and supervisory community as emerging risk areas. We expect some supervisors to begin to challenge boards, risk committees, and senior management to demonstrate that they understand the impact on their customer bases, business models, and risk profiles—and that they are set to take effective mitigating actions where needed.

- **Fintech:** While new technologies present opportunities, regulators want to understand the potential risks and the likely impact on incumbents' business models. The FSB has a clear interest in the subject. The European Commission is expected to deliver a fintech "action plan" in January. Similarly, US regulators are considering the implications of new technologies, including third-party relationships among fintechs and banks. They're even exploring special purpose bank charters for fintechs.
- **Climate change:** The FSB has taken the lead internationally with its Task Force on Climate-Related Financial Disclosures, which made its final recommendations in June 2017. Many regulators in the Asia Pacific region are instituting policies to encourage green finance. The Bank of England (BoE) is also researching climate change, and the EU recently proposed to integrate environmental risks into the mandates of the European Space Agency as part of its action plan on sustainable and green finance.
- **Aging populations:** Aging populations worldwide will create a widening pool of potentially vulnerable customers and influence demand for different types of financial services. They will also affect how financial institutions engage with their customers. At the international level, the International Organization of Securities Commissions (IOSCO) is taking forward work on aging populations.

Leadership changes

Finally, we note that by the end of 2018, the most senior leadership of many of the world's leading regulatory bodies will be starkly different from what it has been for the majority of the post-crisis regulatory reform era. Mark Carney's term as chairman of the FSB has been extended through December 2018, lending some additional continuity to reform efforts. But this will be his final year at the top of the FSB. We expect Stefan Ingves to stand down as chair of the BCBS in the near future. There's also a great deal of change in senior leadership across national and regional regulatory bodies, particularly in the USA. It remains to be seen how far new leaders will uphold the key tenets of the international supervisory agenda of the last decade, particularly its emphasis on cross-border coordination, or whether supervisory priorities will tilt more toward promoting the competitiveness of individual jurisdictions.

On balance, we think that these new leaders will emphasize practical supervisory initiatives over (new) rule making, as well as the need for firms to demonstrate that they're financially and operationally resilient to a range of threats, both old and new. New leaders will be keen to consolidate the outcomes and achievements of the prudential policy agenda that has dominated the last 10 years and focus their tenures on continuing structural challenges as well as emerging risks and issues.

Acting in the face of uncertainty

While we expect some greater clarity about the regulatory outlook to emerge in 2018, the overriding challenge for firms remains coping with uncertainty, including from the global impacts of Brexit and how markets in Europe and elsewhere will be reshaped by Markets in Financial Instruments Directive (MiFID) II. This will put a premium on firms maintaining strategic flexibility, while they also adopt new technologies to react to the threat from "challengers," improve their customer service and outcomes, better manage their risks, and help control costs. With yields, income levels, and return on capital still under severe pressure, cost control will continue to be extremely important. Even though interest rate rises are underway, they will be neither quick enough nor big enough to alleviate pressure on incumbents' business models.

David Strachan
Centre for Regulatory Strategy, EMEA
Deloitte UK

Kevin Nixon
Centre for Regulatory Strategy, APAC
Deloitte Australia

Chris Spoth
Center for Regulatory Strategy, Americas
Deloitte US

Introduction

Most insurers are moving ahead deliberately with their risk and compliance initiatives, even as certain areas pose regulatory uncertainty that will likely remain a significant and ongoing challenge. Even if lawmakers and regulators make certain definitive changes, insurance companies must continue to drive effectiveness and efficiency of their risk and compliance programs so they meet applicable laws, regulations, and supervisory expectations.

Many of the new state regulatory requirements are clear. But in other areas, such as the Department of Labor's (DOL) Fiduciary Rule (Rule), companies don't have the time or luxury of waiting to see how things will shake out. Therefore, they're planning implementation based on available guidance.

Overall, many of the changes insurance organizations are making to achieve compliance are useful improvements that are worth doing from a risk and business perspective.

Here's a look at the key regulatory trends insurers will likely need to monitor and address in 2018. By embracing regulatory complexity in 2018, organizations can accelerate performance and stay ahead of changes so they can better navigate the regulatory landscape.


HOME
INSURANCE
CAR
CONTENTS
INSURANCE
MEDICAL
INSURANCE

Cyber regulation

The insurance industry has seen a shift as the regulatory environment has driven organizations to take a serious yet fresh look at the state of their cybersecurity risk management programs. Institutions at both the state and federal levels remain committed to protecting insurance organizations from the influx of cyber threats and to raising the bar on cyber risk management and reporting. And all signs point to this behavior continuing for the foreseeable future.

A report by the New York State Department of Financial Services (DFS) noted that "[c]yber attacks against financial services institutions, including insurance companies, are becoming increasingly frequent and sophisticated. Insurance firms often possess large amounts of personally identifiable information (PII) and protected health information (PHI) … PII and PHI are becoming more valuable on the black market, which increases incentives for cyber attacks."[1]

DFS may have been among the earliest state insurance regulators to recognize and seek to address the problem with a cybersecurity regulation, but it's not alone. Numerous regulatory agencies at the federal level, as well as the National Association of Insurance Commissioners (NAIC), have moved or are moving to establish regulations governing the conduct of insurers with respect to this significant operational risk.

Major new cybersecurity regulations affecting many insurers include DFS's new regulation, which became effective on March 1, 2017, and the NAIC's Insurance Data Security Model Law, adopted on October 24, 2017. Although there are some differences between the two, the good news for insurers is that, because there are enough functional similarities, compliance with the New York regulation is considered prima facie evidence of compliance with the NAIC model.

The NAIC model requires an annual risk and safeguards assessment to be included in an insurer's annual report to regulators. Annual certification to regulators is required, and records supporting certification—or associated with any cybersecurity events—need to be retained for five years. Also, cybersecurity events must be reported within 72 hours to the appropriate domiciliary regulator and to any regulator where 250 or more consumers may be harmed (or where notice is provided to any other regulatory body). The NAIC will allow a one-year implementation window for information security programs.

The DFS regulation similarly requires a risk assessment and annual certification. Unique to the DFS regulation, firms must have a chief information security officer (CISO) and a written cybersecurity policy, and boards must receive reports and be involved in creating standards. Third-party risk must be managed consistent with internal risk management, and any non-public data must be encrypted and protected from alteration. Other requirements include periodic penetration testing and vulnerability assessment, as well as breach reporting. Audit trail data must be preserved, and entities must track and maintain data that enables the accurate reconstruction of all financial transactions, along with any accounting necessary to respond to a cybersecurity event for at least three years. Any information needed to reconstruct material financial transactions and obligations must be kept for five years. The system must also track and maintain data logging of all privileged authorized user access to critical systems.

One development that holds promise—especially for smaller companies that may not view data security as one of their core competencies—is the opportunity to outsource data tracking and maintenance to a qualified entity. DFS's regulation, for example, allows insurers to use a qualified outside service for their cyber program.

Demonstrated compliance with leading practices and cyber regulations may be useful for insurers with both consumer and investor stakeholders. To that end, the American Institute of Certified Public Accountants (AICPA) unveiled a cybersecurity risk management attestation reporting framework. The AICPA's framework strives to expand cyber risk reporting to address expectations of greater stakeholder transparency by providing a range of stakeholders, both internal and external, with information about an entity's cyber risk management program effectiveness.

What has become clear from evaluating the requirements from the DFS and NAIC, as well as the guidance from the AICPA, is that a comprehensive cyber risk management program needs active involvement and oversight from the board. Such involvement and oversight can hold the organization accountable and help shape and address expectations for improved cyber risk

reporting that's integral to the achievement of an organization's business objectives.

In an era where cyber criminals could be state-sponsored, part of a political cooperative, or just after the money, how can boards and senior executives assess the soundness of their cybersecurity programs? The banking network SWIFT articulated three overarching objectives:

- "Secure your Environment"
- "Know and Limit Access"
- "Detect and Respond"

These objectives translate to a focus on security, vigilance, and resilience as an approach to reduce an organization's vulnerability, while being prepared to respond quickly and resume normal business.

- Being **secure** means focusing protection around the risk-sensitive assets at the heart of the organization's mission.
- Being **vigilant** means establishing threat awareness throughout the organization and developing the capacity to detect patterns of behavior that may indicate, or even predict, compromise of critical assets.
- Being **resilient** means having the capacity to rapidly contain the damage from an attack and to mobilize the diverse resources necessary to reduce the broad impact—including direct costs and business disruption, as well as reputation and brand damage.

The number of cyberattacks—and the associated costs—will likely continue to rise, as will hackers' sophistication. Much of the new cyber regulation is designed to encourage insurers to implement the right level of security, vigilance, and resilience—along with sound governance—to form an effective defense.

Information management, governance, and security: Lessons from DFS 500.13

The DFS's newly effective cybersecurity regulation contains even more challenges for insurance companies than appear at first glance. Despite the title, these rules aren't only about cybersecurity. Compliance with these rules requires a commitment to strengthened information governance and records management, in addition to better information security.

DFS Section 500.13 requires that, as part of their cybersecurity programs, companies:

> **... shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information [as defined by these rules] that is no longer necessary for business operations or other legitimate business purposes, except where such information is required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.**

DFS isn't an outlier in this respect. The Insurance Data Security Model Law adopted by the NAIC provides that a company's information security program shall be designed to, among other things, "[d]efine and periodically reevaluate a schedule for the retention of Nonpublic Information and a mechanism for its destruction when no longer needed." The Model Law further defines an "Information Security Program" as "the administrative, technical and physical safeguards [a company] uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Nonpublic Information.

Emphassis Added

While the concept is straightforward, compliance with this section of NY DFS will neither be simple nor quick. The process by which a company locates all the relevant Nonpublic Information (NPI) it's keeping—as well as what it decides to do with that NPI—could require attention, project management, resources, and expertise beyond what the organization is devoting to the information security aspects of these rules. Industry experience suggests that adapting existing systems to enable systematic records destruction will be a major undertaking.

Organizations subject to the DFS regulations are likely to find that:

- The risk assessment will identify the volume of SSNs and other types of nonpublic information and the unlikely places where they're found.
- Knowledge of the company's records retention schedule by the application owners, as well as their use of and systematic destruction of records containing nonpublic information, are inconsistent.
- In the absence of dedicated resources, the assessment and remediation may well take far longer than anticipated.

Also, this isn't a project just for the CISO and IT. It requires a collective effort involving the business and corporate users of the data (as well as the legal, compliance, and risk management teams; records management staff; and information security) to find the NPI, assess the needs and risks for its retention, and take actions in response.

Compliance with these requirements cries out for information governance—an approach that brings all the disparate stakeholders together to provide the needed authority, knowledge, and responsibility to make the right choices and effectively manage the considerable risks at stake. The information governance model brings coordination and oversight to that effort.

In every organization—regardless of the state of its information governance—Section 500.13 compliance requires its own work stream, with dedicated resources supported by outside expertise, in addition to everything the organization is otherwise doing to comply with the DFS cybersecurity requirements. This work stream includes:

1. Identifying information systems and applications, as well as the data they contain
2. Finding the covered NPI in those systems and applications
3. Assessing the business value and legal need to retain that information
4. Determining if records retention schedules are being applied to the data
5. Developing retention decision criteria and justifications
6. Assuring the appropriate input from the right sources into retention decisions
7. Creating the road map for compliance
8. Executing the choices
9. Documenting the decisions and their justifications

Within an information governance framework, this work stream will be distinct—to make sure it gets done—but it won't be alone. Section 500.13 compliance will be an integral part of how an organization manages its critical information assets—from creation, storage, and use to protection and disposal.

What's next in the march toward best-interest standards?

The DOL's Fiduciary Rule has already significantly shifted the financial services industry to operate more in the best interest of the customer, specifically retirement account investors and policyholders. It has also prompted other regulatory agencies to develop or propose new regulations that are likely to be enacted (or enter the rule-making process) during 2018, thus creating a new patchwork of state and federal regulations that might not be completely aligned.

The US Securities and Exchange Commission (SEC) is considering its own fiduciary rule proposal that would require a fiduciary standard of care when delivering advice to retail investors. Also, at the time of this writing, four states, including Nevada, are planning to implement legislation related to providing advice to investors under a fiduciary standard that's expanding to include non-qualified as well as qualified accounts. Meanwhile, the NAIC is in the process of developing a "best interest" standard for initial presentation at its fall 2017 meeting in December, with an ambitious comment and adoption timeline that would allow the adoption of a model regulation applicable to state-regulated annuity products in 2018.

The DOL rule requires that investment advice given to qualified retirement investors (including rollovers) must be provided under a "fiduciary" standard. Conflicts of interest are prohibited unless an exemption is used—such as the Best Interest Contract Exemption (BICE) or Prohibited Transaction Exemption (PTE) 84-24 for annuities. Under scaled-back BICE compliance measures, effective June 2017, there are requirements to meet impartial conduct standards and provide limited disclosures. For other compliance measures, the DOL delayed the full applicably date from January 1, 2018 to July 1, 2019.

Deloitte's analysis and discussions have identified a number of important market implications (some of which were highlighted in a 2017 study that Deloitte facilitated for the Securities Industry and Financial Markets Association (SIFMA)) :[2]

NAIC best-interest standard. The revisions to the annuity suitability rule are expected to introduce new and uncertain regulatory requirements for insurance companies. This enhanced responsibility will present a number of challenges, including how to implement the rules and the need for increased information from independent agents to enable companies to fulfill this duty.

Reduction in product shelves and enhanced product due diligence. In response to the Rule, firms have reduced or consolidated product shelves—particularly related to mutual funds and annuities—as part of the effort to enhance product due diligence processes and compensation requirements. At the same time, new products have been launched in the market that are presumably less conflicted (e.g., clean shares and T shares mutual funds, fee-based annuities), but whose futures are highly dependent on the developments in fiduciary space.

Movement to fee-based accounts for retirement investors. The trend toward

fee-based accounts was accelerated by the Rule, along with other industry factors. Notably, this trend raises a concern that while fee accounts address perceived conflicts that might exist with commission product sales, they could also increase total client charges and reduce product access due to product or account minimums. Also, the regulatory risk of reverse churning can't be overlooked in this market shift.

Enhanced rollover and due-diligence processes. Virtually all SIFMA report participants indicated that they have revisited their firms' policies and processes related to the rollover of client assets from retirement accounts, resulting in enhancements to rollover review processes, including increasing the size of oversight teams and/or leveraging vendor rollover review tools that are evolving to meet industry needs.

Advisers' retention and incentive management. Advisers have been in a state of continuous flux over the past 18 months due to uncertainty around outcomes of the Rule and related changes firms are making to achieve compliance. Product-related changes—as well as widespread revisions to incentives programs (e.g., bonuses, sales contests) to minimize conflicts—have led advisers to search for better opportunities in the industry. This issue is more critical than ever as firms strive to retain their best talent while adhering to shifting compensation schemes and regulatory compliance requirements.

The Rule continues to serve as a catalyst for change across the financial services industry. Although implementation efforts to achieve compliance have slowed, the industry continues to migrate toward a fiduciary (or at least a "best interest") model for delivering advice to both retirement and non-retirement clients. This trend will likely further accelerate in 2018 under a number of emerging scenarios, such as the DOL's Rule progression, the SEC drafting of a rule, individual state legislation, and adoption of the NAIC model regulation by individual states.

The Rule continues to serve as a catalyst for change across the financial services industry.

Big data: Big issues, big potential rewards

The potential benefits of analytics are undeniable. In fact, one can reasonably argue that as the use of analytics rises—and as the analysis becomes increasingly precise and personal—insurers will be able to offer more effective, customized products to consumers with greater efficiency. The counterargument is that the increasing availability of data—and the increasingly sophisticated ability to analyze and manage it—could enable insurers to micro segment the market to a point where it undermines the fundamental concept of risk pooling. In addition, while such data and analytics (e.g., telematics) are currently used to offer lower prices, would regulators object if prices to some consumers were to rise as a disincentive to risky behavior?

Another issue is data ownership. If a company collects data on an insured person's driving, who owns that data? The company or the individual it insures? Should the data go into a central repository, as with credit ratings? And who should control it—the insurer who first collected the data, the central repository, or the insured? What about the third-party data used in predictive analytics? Who is responsible for its accuracy?

None of this would matter if the use of big data and analytics were not so filled with potential for the industry. On the property & casualty side, telematics already has begun to demonstrate the utility of big data. And the Internet of Things is poised to provide more data than ever before on habits both good and bad. Meanwhile, the emergence of autonomous vehicles is just one challenge facing the insurance structure for property & casualty insurers, and declining penetration remains an issue for life insurers.

In this environment, the ability to use data and predictive analytics to accelerate underwriting and reduce market friction could be both a competitive advantage and market expander. The question regulators—and the industry—face is where to draw the line. For example, the value and validity of genetic information is indisputable, but should it be usable? A 2017 Stanford University study found that an artificial intelligence (AI) algorithm could predict sexual orientation 81 percent of the time for men and 74 percent of the time for women simply by examining a photo. What if AI could determine with precision, simply by looking at a photo, the probability that a specific individual will develop a particular illness? Should that information be usable? How accurate does it need to be?

Regulators worldwide are moving to address the issue. The NAIC has created the Big Data Working Group to "[r]eview current regulatory frameworks used to oversee insurers' use of consumer and non-insurance data. If appropriate, recommend modifications to model laws/regulations regarding marketing, rating, underwriting and claims, regulation of data vendors and brokers, regulatory reporting

requirements, and consumer disclosure requirements."

Similarly, in the wake of some cyber breaches, Congress held hearings in late 2017 questioning the very business model of some third-party data accumulation services. Also, the DFS has extended its supervision to include credit reporting agencies providing data to insurers and others.

The EU's General Data Protection Regulation (GDPR) applies extraterritorially "not only to European companies, but also to foreign companies offering products and services to EU citizens, or monitoring their behavior. In other words, the same rules will apply to all companies operating in the EU regardless of where they come from .... Big Data analytics does not always involve personal data. But, when it does, it should comply with the rules and principles of data protection." The need to secure consumer consent and reinforcement of the "right to be forgotten" are among the salient requirements contained in the GDPR. This data protection travels with the data. Fines for breaches can run as high as 4 percent of annual global turnover or €20 million.

This is in addition to concerns about the accuracy of third-party data used in analytics. Regulators that were skittish about the use of credit reports in underwriting or dynamic pricing models might need to be convinced that the underlying data used in an insurer's predictive analytics are accurate. According to a recent study of the accuracy of data provided by commercial data brokers, "More than two-thirds of survey respondents stated that the third-party data about them was only 0 to 50 percent correct as a whole. One-third of respondents perceived the information to be 0 to 25 percent correct."

These challenges aren't necessarily an argument for caution but for rigorous preparation and risk management, including external review of data sources and usage, clear lines of accountability, and transparency. Involving regulators from the beginning in efforts to use advanced analytics is a basic requirement. Insurers should ask—and be prepared to answer—the following questions about their data and analytics, both for business reasons and to reassure regulators:

- Is it accurate?
- Is it useful?
- Is it discriminatory in effect?

Also, from a practical perspective, another question about data and analytics might be even more important:

- Can we explain and defend it on the evening news?

The cold, hard truth is that insurers have no real alternative to increasing their use of big data and analytics. Any overly restrictive regulation on or retreat from the use of data and advanced analytics by insurers only opens the door to external disruptors. What's more, if properly used, data and advanced analytics could reduce costs and provide better products for consumers, while expanding the universe of insurable risks for industry.

The cold, hard truth is that insurers have no real alternative to increasing their use of big data and analytics.

Enterprise risk management and Own Risk and Solvency Assessment (ORSA)

With the passing of the Risk Management Own Risk and Solvency Assessment Model Act #505, the NAIC paved the way for the formal requirement for insurance companies to have a risk management program and framework within their organizations. The ORSA requirement specifies a filing at least annually that sets out:

- The company's risk management framework
- A stress testing requirement for the risks the company faces
- A forward-looking projection of solvency

Although insurance companies are naturally in the business of managing risk, these new requirements have taken time and effort to formally adopt. And they will continue to do so for some time.

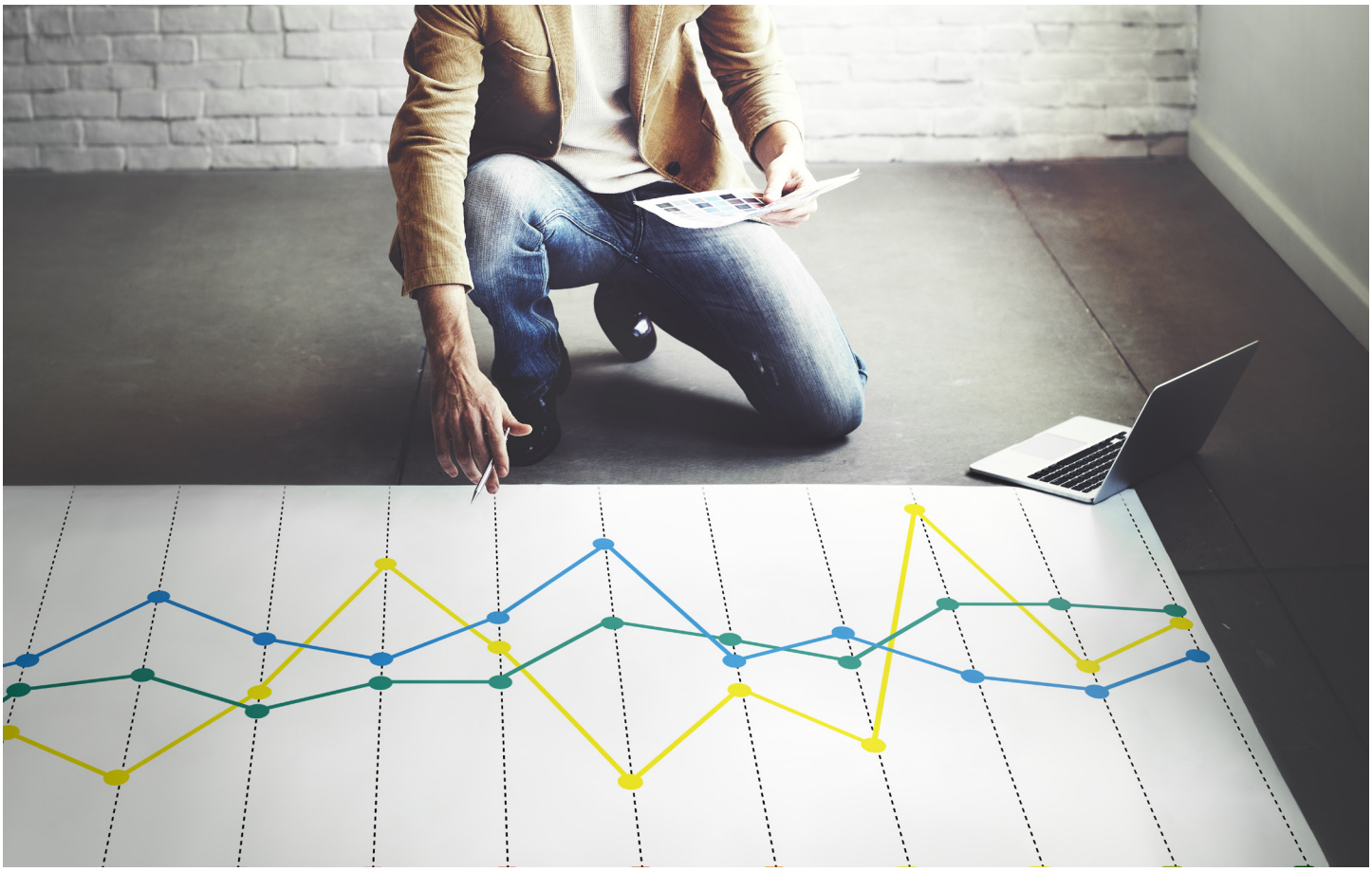
The reach of these ORSA requirements has been significant, spanning the life, property & casualty, and health insurance industries. The proportional nature of the requirements means that larger companies will be held to a higher standard than will smaller companies. At first, the ORSA was described as an evolution—not a revolution—but regulatory expectations have continued to grow. What's often described as a "first-year pass" for previous ORSA filings will now be tested and scored under the financial examination process, with regulators wanting to see that ORSA is more than just a filing and that risk management and the ORSA process are part of a company's business-as-usual practices and corporate governance framework.

The annual ORSA filing will be subject to review by the lead state of domicile. This review could take many months to complete since companies often file at the same time, creating a natural review backlog for regulators. In some cases, states have chosen to outsource their ORSA reviews to external third parties. Thus, in addition to receiving regulatory feedback in the form of a scorecard with areas noted for improvement, companies may also receive an invoice to pay for the cost of the review itself. At the time of passing, the ORSA requirements for a strict pass or fail weren't explicit, but it's clear that a company whose ORSA and underlying risk and capital management processes aren't adequate will have this fact communicated along with expectations for improvement. Also, the ORSA and how it's being applied within the business will be reviewed as part of the financial examination process, and the ORSA requirements have been written into the financial examiners handbook.

During the regulatory review process, a company might not be able to demonstrate that all the ORSA requirements are being met, but it can help its case by providing evidence that an effective ORSA process is in place. Key questions to consider include:

- Should the organization have a formal chief risk officer and a risk management function to manage the day-to-day risk management processes?
- Does the board need a stand-alone risk management committee, and how is risk management handled within the corporate governance framework?
- Are the three lines of defense clear within the organization, and does the company know where responsibility for risk management resides?
- How can a risk-based culture and risk-based decision making be demonstrated within the company's governance structure?
- While many companies now identify and prioritize their risks on both an inherent and residual basis, are the controls and mitigation strategies truly effective? And could they be used in a time of stress?
- How does the organization identify "unknown" risks and brainstorm about them to understand how well the business would respond if they were to occur?
- Through which lens does the organization view capital—and its capital requirements—and how robust is its approach to stress testing key risks?
- How is the company using the risk and capital management process to add value to the business? Is it allocating resources efficiently to focus on specific areas of risk and opportunity?

The first-year pass is becoming part of ORSA history, and regulatory expectations continue to rise as ORSA evolves. We expect regulators to start communicating their continued vision for ORSA, perhaps through an update to the NAIC's ORSA Guidance Manual. Although improving the regulatory assessment and examination outcome isn't always easy, taking a few practical steps can certainly help.



"Core Principles" Report: Treasury Department's recommendations

On October 26, 2017, the Treasury Department released the third of four reports pursuant to President Trump's executive order setting forth the Administration's "Core Principles for regulating the US financial system. The report covers the asset management and insurance industries, and offers recommendations across four broad categories: (1) systemic risk, stress testing, and solvency, (2) efficient regulation, (3) international engagement, and (4) promoting economic growth and informed choices.

Although the report provides President Trump's nominees a roadmap for enacting the Administration's policy priorities, it remains unclear which of the recommendations will be implemented, or how quickly. However, the recommendations—nearly all of which would be enacted without Congressional action—may inform the regulatory and supervisory agendas of federal and state insurance supervisors, and may also have significant implications for the FSOC's work going forward.

Below are several of the report's most significant recommendations:

Recommendations for Congress

- Clarify the "business of insurance" exception to ensure that the Consumer Financial Protection Bureau (CFPB) does not engage in the oversight of activities already monitored by state insurance regulators
- Pass a law setting forth requirements for insurer data security (if adoption and implementation of the Insurance Data Security Model Law by the states does not result in uniform data security regulation within five years)

Recommendations for federal regulatory agencies and states

- Move away from entity-based systemic risk evaluations of insurance companies, and focus on risks arising from products and activities
- Continue engagement in international forums, but promote the US insurance industry and the US regulatory framework
- Re-example the DOL fiduciary rule and delay full implementation until the relevant issues are evaluated and addressed
- Harmonize insurance capital initiatives by the NAIC, the states, and the FRB
- Eliminate or reduce the inconsistencies between existing data calls concerning terrorism risk insurance
- Adopt the NAIC Insurance Data Security Model Law
- Improve information sharing within the insurance industry

Prepare for corporate governance disclosure

Corporate governance disclosure may have been a quiet issue lately, but it's one that most insurers will need to begin addressing soon.

The NAIC's Corporate Governance Annual Disclosure (CGAD) Model Act and Regulation were adopted in 2014 to provide regulators with more details on insurers' corporate governance practices. Since then, states have steadily adopted its provisions. By July 2017, 18 states had adopted the model act and 11 states had adopted the model regulation.

This trend should continue to accelerate, as the act is expected to become an NAIC accreditation standard as early as 2020. While much of the recent regulatory focus has been on measures directly related to solvency, such as the ORSA, regulators regard the CGAD as integral to solvency modernization. Regulated entities not already reporting should begin preparing for the process now.

Under the model act, a new CGAD must be submitted by individual insurers no later than June 1 of each calendar year. However, if an insurer is part of a holding company system, the top-level holding company may submit a CGAD for the entire insurance group. Submissions must be made to the holding company system's lead state regulator as determined by the NAIC's Financial Analysis Handbook. But disclosures may be required at the ultimate controlling entity level, intermediate holding company level, and/or individual legal entity level. Unlike the ORSA, the CGAD does not have an exemption for smaller insurers.

All insurers, no matter their size, will be required to file an annual CGAD. Insurers that don't file may be subject to a penalty.

The CGAD must contain discussions of the following:

- The insurer's corporate governance framework and structure
- The policies and practices of its board of directors and significant committees, including information regarding board member qualifications and independence
- The policies and practices directing senior management, including information regarding significant compensation programs
- The processes by which the board of directors, its committees, and senior management ensure an appropriate level of oversight of the critical risk areas impacting the insurer's business activities

Insurers may for the first time be required to analyze and rationalize items that previously had been glossed over, such as the size, composition, and qualifications of the board of directors, as well as the standards for retaining key persons in control functions.

For public companies, a significant section of the required disclosures may already be included in their proxy statements and could be repurposed. However, some items, particularly those dealing with risk and oversight, might need to be created. For many insurers, preparation of these disclosures should include a review of their ORSAs—and should complement the ORSA process.

The model act requires detailed disclosure of the corporate governance procedures. To prepare, an insurer should evaluate:

- Its corporate governance framework, structure, and documentation
- Policies and practices of its board of directors, as well as any significant committees
- Board policies and practices that direct senior management
- Suitability standards used to select board members and the CEO
- Codes of conduct and ethics
- Performance evaluation and compensation practices
- Succession planning
- Processes by which the board of directors, its committees, and senior management conduct an appropriate level of oversight to the critical risk areas impacting the insurer's business activities

Insurers that haven't yet submitted their first CGAD should consider initiating a mock CGAD disclosure filing to:

- Identify any gaps in the corporate governance framework, structure, and oversight policies and procedures, so that they can be updated as needed; if not already in place, an annual policy and procedure review process should be implemented
- Identify key internal business contacts for all CGAD filing requirements, establishing process ownership for the gathering of materials for annual submission
- Complete a gap analysis on the communication process for critical risk areas that affect business activities, including all communication up to the board of directors and down from the board of directors to management
- Complete a gap analysis of policy, procedures, and suitability documentation for board members and implement updates as needed
- Review the suitability of current board members and provide any needed training
- Review all key conduct and ethics policies for thoroughness and applicability and establish an annual review process, if needed
- Review committee charters for the audit, risk, and compliance committees for completeness, clear scope of responsibilities, and authority

In light of these criteria—and given the lack of regulatory feedback in the early stages of this process—companies that have already submitted their first CGAD might wish to review and update their CGAD accordingly. While these actions might be difficult to take, ultimately the CGAD must be certified by the insurer and must be provided to the board of directors or an appropriate board subcommittee.

With such high visibility for the CGAD, it might be better for company management to err on the side of over- rather than under-compliance.

Insurers may for the first time be required to analyze and rationalize items that previously had been glossed over, such as the size, composition, and qualifications of the board of directors, as well as the standards for retaining key persons in control functions.

2018 market conduct environment

The NAIC and state Departments of Insurance (DOI) continue to focus considerable resources to market conduct exams and analysis. While many of the areas of focus aren't new (claims, underwriting, marketing material), some are more recent and gaining more attention (big data, cyber security, vendor/third-party administrator (TPA) management).

In addition, many insurers are experiencing more frequent examinations, driven in part by heavier reliance on market analysis data and greater activity on the part of state regulators as the federal government has limited authority and inclination to increase its presence. A recent analysis of publicly available data from the NAIC's Insurance Data Resources, Inc. (IDR) database suggests a noticeable rise in the amount of state-levied fines and penalties against insurers over the past five or more years.

Market conduct examinations and the underlying laws and regulations are less uniform when compared to the financial solvency examination. In addition, each state makes decisions regarding the allocation of resources and prioritization of insurers to be examined. This has resulted in some states reevaluating how they determine which companies to examine, the frequency of exams, and the extent to which examiners need to be on-site at the insurer's home office.

With continuing data breaches that impact customer PII, the NAIC and states are continuing to focus on appropriate measures and the controls insurers should have in place to protect sensitive policyholder information. Likewise, as carriers get more sophisticated in their use of big data, the states find themselves trying to determine what safeguards are required to protect against unfair and/or discriminatory behavior.

Areas of market conduct focus of the NAIC and industry trends

The NAIC continues to focus its attention on key market conduct issues being addressed by the NAIC's respective subcommittees, task forces, and working groups. Given the NAIC's processes for adopting new model laws and regulations, it's not unusual to see multiyear activity and evolving regulatory actions. The NAIC continues to focus on certain insurance products, including lender placed insurance, life insurance, and products primarily marketed to seniors such as long-term care. In addition, regulators continue to work with law enforcement agencies to grapple with the appropriate regulatory response to ensure sound cybersecurity practices and controls at insurers.

The industry continues a trend toward heavier reliance on outside vendors and/or TPAs to carry out a number of major operational areas traditionally handled by the carriers themselves. This has given rise to an increase in regulation and more focus on how insurers manage their vendor relationships.

As the industry continues to refine its use of big data and other tools to assist in underwriting, pricing, claims, and other areas, the NAIC and the DOI will be monitoring these developments and considering whether enhanced laws and regulations may be required.

Key focus areas from NAIC fall national meeting

The NAIC's agenda for the fall national meeting held in early December contained a number of key market conduct issues impacting insurers. The Innovation and Technology (EX) Task force received reports from a number of working groups, most notably those focusing on big data, cybersecurity, and speed to market. The Long-Term Care Subgroup continues to examine ways to break down regulatory barriers and find tangible solutions to allow the private insurance market to play a larger role in financing long-term care needs. The challenge for regulators is to find the right balance between allowing for more innovation, while concurrently protecting seniors who may be vulnerable to improper sales activities.

Likewise, the Senior Issues B Task Force continues to focus on issues relative to long-term care and Medicare supplement insurance, including applicable solvency concerns for writers of long-term care insurance and improvements to the related rate stabilization standards.

Voluntary market regulation certification program

NAIC's Market Regulation Certification (D) Working Group has been developing a formal certification program for market conduct examinations and oversight. The working group is focused on developing certification standards as well as a process designed to allow for state-by-state implementation of the program. In addition, the regulators are considering the proper process for gauging states' compliance with the standards and program. Finally, a process will be proposed that deals

with future changes to the standards and how to best help the various state DOIs achieve certification. The working group continues to review the pilot program in which approximately 14 states were tapped to be part of the certification program as it evolves.

Outlook on state insurance department market conduct capabilities

Recent analysis of NAIC's IDR database suggests that market conduct exams and related regulatory penalties are on the rise. We believe that one important driver of these trends is the enhancements that DOIs continue to make to their market conduct capabilities. Such enhancements include expanded use of market analysis, greater access to data and shared publications, and enhanced coordination between states. We're seeing the improved coordination evidenced through increased activity of the Market Actions Working Group (MAWG). In addition to multistate coordination, the NAIC has recently provided additional guidance promoting the expanded use of standardized data requests during examinations. Greater standardization is expected to improve the consistency and effectiveness of exams and analysis going forward. In general, we're seeing states move toward a more data-driven and analytical approach to market conduct, leveraging information from financial statements, rate and form filings, and information from other state and federal regulators. In addition, the Market Analysis Prioritization Tool (MAPT) continues to be used by states to narrow the focus to companies with potential issue areas by applying a scoring system that analyzes any complaints, regulatory actions, and exam histories, among other data points.

Summary

Insurers should continue to enhance their controls in key areas of market conduct exams with a focused review on regulatory areas that are still evolving, such as big data, cybersecurity, and vendor/TPA management. These new areas will be challenging for insurers as regulators further enhance their tools and expand their analysis of company data and use of specialized third-party examiners to focus on these and other areas. This will be a particular challenge with regard to protecting customer PII and PHI data and potential unfair trade practice abuses, including sales practices. Investments in enhanced compliance, analytics to proactively identify risks, and controls should pay off in the long term as insurers attempt to mitigate the increasing risk potential of fines, consent orders, and adverse publicity.

In general, we're seeing states move toward a more data-driven and analytical approach to market conduct, leveraging information from financial statements, rate and form filings, and information from other state and federal regulators.

International regulatory change

Regulatory change continues to pervade the insurance industry, and international regulatory change is no exception. The international regulatory environment is significant even for US-only industry participants because of the direct and trickle-down impacts of globally accepted changes. The International Association of Insurance Supervisors (IAIS), which is the standard-setting body for insurance supervision, comprises more than 140 different jurisdictions and 190 different insurance regulators. The IAIS not only supports standard setting for regulators themselves, but it also responds to the needs of governments through the G20 and the FSB.

Standards set by the IAIS take a number of forms. Establishment of the Insurance Core Principles (ICPs) and then implementation of those principles in local jurisdictions lead to a harmonization of supervisory standards across the globe. Also, implementation monitoring and peer review are performed. The work of the IAIS focuses on prudential standards of solvency; risk management and governance; and, increasingly, market conduct issues. The agenda and timeline for these existing and new proposed standards stretch out for many years, creating significant uncertainty in the industry.

Local country-based change is also creating uncertainty, with socio-economic and political change driving significant regulatory adjustments within individual countries. For example, the political shift within the UK to exit the European Union has direct implications for the regulatory landscape, driving companies to reconsider how their business operates and how it will be structured within the European Union. Also, the UK financial services regulators—the Prudential Regulatory Authority (PRA) and Financial Conduct Authority (FCA)—will need to revisit their rules and guidance in the context of being outside of European Union law.

Brexit is just one example of the many country- and region-specific changes that are currently taking place. European capital standards under Solvency II are currently being reviewed, with the review results due in 2018. At the same time, countries in Asia and Latin America are looking to enhance their current capital regimes. The development of the Insurance Capital Standard (ICS) by the IAIS is seen by some countries as a key input to their local capital standard considerations. Meanwhile, regulators continue to enhance their local regimes in both prudential and market conduct. Also under consideration are many emerging issues, such as:

- How insurance can respond to consumer needs
- How insurance can support in-country development, such as infrastructure projects
- How regulation should respond to emerging issues and trends, such as cybersecurity and fintech

Against this backdrop, both US domestic and international insurers would be well-advised to stay on top of global regulatory developments and continuously assess the potential impact on their business models.

Taking decisive action in uncertain times

Regulatory uncertainty remains a fact of life. But in most cases, waiting for absolute certainty isn't a viable option. Instead, insurance organizations need to keep moving forward as planned, with deliberate linkage between regulatory strategy; business strategy; and building infrastructure for governance, regulatory reporting, and risk management that scales and is flexible. Senior management will need to take decisive action while also paying close attention to emerging regulatory developments and staying as flexible as possible. The good news is that many of the changes insurance organizations are currently implementing make good sense from a business perspective—not just a regulatory perspective—and are worth doing no matter how the future unfolds.

Endnotes

1. New York State Department of Financial services, "Report on Cyber Security in the Insurance Sector," February 2015
2. https://www.sifma.org/resources/submissions/deloitte-study-on-the-dol-fiduciary-rule-august-2017/

Contacts

Leadership

Nicole Sandford
Regulatory & Operational Risk Leader
Partner | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
nsandford@deloitte.com

Alok Sinha
Deloitte Risk and Financial Advisory Financial Services Leader
Principal | Deloitte Advisory
Deloitte & Touche LLP
asinha@deloitte.com

Rich Godfrey
Deloitte Risk and Financial Insurance Leader
Principal | Deloitte Advisory
Deloitte & Touche LLP
monoreilly@deloitte.com

Chris Spoth
Executive Director, Center for Regulatory Strategy Americas
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
cspoth@deloitte.com

Authors

Steve Foster
Independent Senior Advisor to Deloitte & Touche LLP
sfoster@deloitteretired.com

George Hanley
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
ghanley@deloitte.com

Jordan Kuperschmid
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
jkuperschmid@deloitte.com

Andy Mais
Senior Manager | Center for Financial Services
Deloitte Services LP
amais@deloitte.com

Howard Mills
Howard Mills | Global Insurance Regulatory Leader
Deloitte Services LP
howmills@deloitte.com

Jeff Schaeffer
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
jschaeffer@deloitte.com

David Sherwood
Senior Manager | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
dsherwood@deloitte.com

David Vacca
Independent Senior Advisor to Deloitte & Touche LLP
dvacca@deloitte.com

The Center wishes to thank the following Deloitte professionals for their insights, contributions, and support for this report:

Najeh Adib, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Jared Bixler, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Zach Dressander, Senior Marketing Specialist, Deloitte Services LLP
Lara Hamilton, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Alex LePore, Senior Consultant | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Nitin Pandey, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
David Pompei, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Ryan Press, Senior Marketing Specialist, Deloitte Services LLP
Andrew Rafla, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP

CENTER *for*
REGULATORY STRATEGY
AMERICAS

About the Center
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends.

Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research ,forums, webcasts, and events.

Deloitte.