Deloitte.

Leading in times of change

Insurance regulatory outlook 2019

United States
December 2018

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 2019. 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 2019, we provide our regulatory perspectives on the following industries and sectors: banking; capital markets; insurance; investment management; energy, resources, & industrials; life sciences and health care. For a view of the other trends impacting insurance in 2019, 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 2019 and the regulatory changes it may bring. Please feel free to contact us with questions and feedback at **CenterRegulatoryStrategyAmericas@deloitte.com**.

Contents

Global foreword

Nearly 10 years after the financial crisis, the long shadow it has cast has started to fade. With the exception of one final component of Basel III, most post-crisis prudential policies have now been decided, and banks in particular are now much better capitalized and more liquid than before the crisis. Amid varied approaches and timetables to national implementation of agreed prudential reforms, attention is now more acutely focused on culture and governance; the challenges of new technology; and emerging economic, market, and operational risks. Firms need to be prepared to respond to this shifting focus and the new demands that it will place on them.

Lifting of accommodative monetary policy

Globally, monetary easing and low interest rates are slowly giving way to interest rate "normalization," although rates are expected to settle at levels significantly below historical norms. The United States has led the way with a series of rate rises and the Federal Reserve has begun to shrink its balance sheet. The Bank of England has tentatively begun to raise rates, and the European Central Bank is bringing an end to the expansion of its balance sheet. In Australia, interest rates remain on hold but are expected to begin rising. Japan is the major exception to this trend, with rates expected to remain low in the near future. Given the number of headwinds to the global economy (e.g., high levels of debt, elevated levels of geopolitical risk, and trade protectionism), the pace of any interest rate rises is likely to be slow.

Higher interest rates may be beneficial in net terms to certain firms: banks may enjoy higher net interest margins and insurers could benefit from rising asset yields. However, interest rate normalization may also lead to falls in some asset values and rising credit defaults as well as revealing structural weaknesses in both the global economy and individual firms. It is unclear what the overall effect of these opposing factors will be, especially at the level of individual firms and sectors.

An uncertain economic environment

Meanwhile, a period of accommodative monetary policy has contributed to a buildup of debt, with global debt levels now at $247 trillion,[1] significantly higher than their pre-crisis peak. In many commentators' eyes, this represents a key systemic vulnerability.[2] Low rates also contributed to a sustained search for yield that may have led many lenders and investors to move down the credit quality curve. Further, comparatively higher capital requirements for banks have paved the way for a rise in nonbank lending, which means that exposure to credit markets now extends to a much wider variety of firms. Both the leveraged loan and real estate markets are likely to be vulnerable to higher interest rates, while consumer credit expansion and the resulting high levels of personal debt may have left many consumers vulnerable to interest rate rises, especially after such a prolonged period of low rates.

[1] IIF, Global debt monitor, July 2018. https://www.iif.com/Publications
[2] IMF, Bringing down high debt, April 2018. https://blogs.imf.org/2018/04/18/bringing-down-high-debt/

Looking at the wider global economic picture, we see a mixed outlook. Economic growth continues to be strongest in parts of Asia, although Chinese growth has slowed, while the outlook for emerging and developing economies is uneven. Recoveries in both the United Kingdom and United States are now close to a decade long, while eurozone expansion—although weaker—is also well embedded. Historically, downturns or recessions have occurred at least once each decade, suggesting that such an event may be overdue.[3]

Some commentators[4] consider that the global economy has reached its "late cycle" phase, most evident in asset valuations that appear stretched on historic bases. In the European Union, close to €731 billion[5] of nonperforming loans continue to act as a major risk to some banks' resilience and profitability, while globally, increasing trade protectionism and political uncertainty also weigh heavily on the minds of many in the industry. Brexit continues to be a major geopolitical and regulatory uncertainty, and both regulators and politicians will attempt to mitigate its risks and effects throughout 2019. Nevertheless, if there is a disorderly Brexit, leading potentially to new political strategies and approaches, the implications for how a number of these regulatory predictions unfold in the United Kingdom could be profound.

Against this background, we expect regulators across sectors to remain highly vigilant to the risks of economic downturn and market shocks. They will likely want to use stress testing extensively to assess firm vulnerability and resilience, recognizing that during a period of unprecedentedly low interest rates some business models have grown up in relatively benign conditions and have yet to be tested in a sustained downturn.

A retreat from global coordination

The global regulatory approach is changing. The aftermath of the financial crisis saw a globally coordinated response to draw up a series of new regulations that would underpin a more robust and stable financial system. However, there is starting to be a move away from global policy making and a reduced appetite for cross-border regulatory cooperation. As a result there are increasing signs of regulatory divergence, including geographical and activity-based ring-fencing, as different regions and countries look to tailor regulations to their own needs. Global firms are, therefore, having not only to comply with these divergent rules in the different jurisdictions in which they operate, but also to optimize their local governance structures, operating models, legal entity structure, and booking models.

A shift to supervision

We do not expect regulators to embark on a path to wholesale unraveling or reversing the post-crisis reforms implemented since 2008. But it seems that, absent a significant unexpected event,

[3] Alex J. Pollock in the Financial Times, Financial crises occur about once every decade, March 2015. https://www.imf.org/en/News/Articles/2018/04/26/sp04272018-outlook-for-global-stability-a-bumpy-road-ahead
[4] International Monetary Fund, Outlook for Global Stability: A Bumpy Road Ahead, April 2018. https://www.imf.org/en/News/Articles/2018/04/26/sp04272018-outlook-for-global-stability-a-bumpy-road-ahead
[5] EBA, Risk Dashboard Data, Q2 2018.

there is little prospect of major new regulation, especially in relation to bank and insurance capital. Regulators' key priorities are to consolidate and safeguard and—in some jurisdictions—refine the reforms of the past decade. What we do expect is a sharp tilt away from a period of regulatory re-design and innovation, to one of operating and embedding the reformed supervisory system.

As a result, firms in many countries are seeing rising supervisory expectations, reflecting the growth of principles-based supervisory approaches that emphasize the importance of firms' governance, culture, and management approach and the outcomes, both prudential and conduct, these are delivering. Firms' conduct and the treatment of their customers are also receiving increased focus in numerous countries, driven by political and regulatory concern over the perceived poor conduct of firms across all financial sectors.[6]

Supervisors are also adopting more intrusive practices, including greater use of on-site supervisory visits. This reflects global leading practice and the increasing need for supervisors to engage directly with firms in order to understand their strategies and business models, risk profiles and appetites, and risk management frameworks and approaches, and to hold boards and senior management accountable for the outcomes these deliver.

New technologies

Firms, regulators, and their customers are considering the opportunities and risks associated with new technologies. For example, due to the rapid development of artificial intelligence, machine learning, and fintech solutions, once-new technologies are quickly becoming mainstream. The powerful impact these technologies will have should not be underestimated, not only on consumers, but also on regulation and supervision. The pace of technological change, therefore, demands deep thinking about the appropriate regulation of processes, products, and institutions to avoid regulatory gaps and to ensure financial stability and consumer protection.

These technology developments and disruption have triggered a debate around the perimeter of financial services regulation. Many incumbent firms worry that new technology-driven entrants offer services that lie outside the boundaries of existing financial services regulation and which incumbent firms find more costly to deliver because of a "compliance leakage" from the regulated activities that they are undertaking. We do not expect regulators to "come to the rescue" of incumbents, who will have to look to their own resources to rise to the challenge of competition. However, we expect that these level playing field concerns, along with worries about the role of technology in society more generally, will drive increasing interest in how fintech firms and crypto assets are regulated—or rather, at present, how they are not. We expect clarification of the regulatory treatment of crypto assets, especially in the areas of investment by retail consumers, money laundering, and prudential capital for banks.

[6] FCA, Transforming Culture in financial services Discussion Paper, March 2018. https://www.fca.org.uk/publication/discussion/dp18-02.pdf

Acting in the face of uncertainty

While the current regulatory environment appears more settled compared to the recent past, regulators across the world continue to set high expectations intended to maintain a strong, resilient financial sector through firms having robust financial and operational resilience, supported by strong risk management and compliance capabilities. In our view, this may provide an opportunity for leading financial firms to pivot from having to build frameworks to reflect a barrage of new regulations to optimizing through taking advantage of new technologies and operating models.

The world changes and regulation changes with it

The debates around the regulatory perimeter and potential fragmentation of the financial system mean that firms' operational resilience, as well as their susceptibility to cyber and financial crime, are becoming much greater issues for regulators. As part of this, we also expect a sharpening supervisory focus on how boards and senior management teams control the risks posed to them by their exposure to outsourced providers and other third parties.

The past decade has seen profound and lasting changes in the structure of the economy, employment, and society. The providers, consumers, and regulators of financial services are all changing. Aging populations and new Millennial consumers are demanding different types of financial services and products, distributed in different ways. This changing and challenging background makes it essential to consider the future of regulation holistically, rather than in a piecemeal manner. All sectors and stakeholders have an important role here, and we hope that this year's outlook from our Regulatory Centers will both inform and stimulate this discussion.

David Strachan
Centre for Regulatory Strategy, EMEA
Deloitte UK

Kevin Nixon
Centre for Regulatory Stategy, APAC
Deloitte Australia

Chris Spoth
Center for Regulatory Strategy, Americas
Deloitte US

Introduction

Compliance modernization helps companies pursue their core mission and achieve compliance as efficiently and effectively as possible by "thinking forward" and then harnessing the best available compliance practices and technologies to comply with current and future regulatory requirements. This is an ongoing need driven by never-ending technological advances and market expectations that are constantly rising. No matter how "modern" a company's existing compliance systems and processes might be, there is always room to improve.

This is especially true when changes in political leadership can lead to different areas of regulatory focus. Following the 2018 midterm election, the Democratic Party leadership has indicated that the House Financial Services Committee will broadly focus its legislative agenda toward protecting consumers and investors, preserving financial sector stability, and encouraging responsible innovation in financial technology. Meanwhile, the Republican-controlled Senate has indicated that it will continue to focus its legislative agenda on the remaining refinements not already addressed in the Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA)[1] passed in 2018. Beyond the divided Congress, we note that the regulatory agencies are now all led by President Trump appointees who have discretion, subject to congressional oversight, to calibrate their supervisory policies and programs.

Regardless of what definitive changes lawmakers and regulators might make, such as the Financial Stability and Oversight Council's recent de-designation of individual insurers as Systemically Important Financial Institutions, insurance organizations should continue to drive effectiveness and efficiencies across their risk and compliance programs so they can meet applicable laws, regulations, and supervisory expectations.

Cybersecurity and data privacy

In an age when hacking and data breaches have become so commonplace that they are almost expected, cybersecurity continues to dominate both the headlines and the regulatory agenda. This includes reporting on the cost of cybercrime (and on the investments organizations are making to enhance their cyber risk management programs), as well as a heightened focus on cybersecurity regulation and compliance.

As the US Securities and Exchange Commission (SEC) stated in its February 2018 guidance to companies on cybersecurity disclosure, "Cybersecurity risks pose grave threats to investors, our capital markets, and our country. . . . Today, the importance of data management and technology to business is analogous to the importance of electricity and other forms of power in the past century."[2]

For insurers to remain competitive, they need the ability to acquire and manage vast quantities of data to provide more relevant coverage for consumers. While marketplace innovations such as wearable computers and Internet of Things provide the ability to collect such data, having access to large volumes of contextual data introduces its own risk, related to unintended processing, loss, and theft. The risk is compounded because of changes in business models, such as adoption of cloud-based storage and computing, use of large-scale process automation, and increased adoption of data processors, to name a few.

US policy makers are keeping pace by introducing unprecedented privacy and cybersecurity laws. Governments outside the United States are also focusing on cloud and data residency requirements, limiting the movement of data across borders. A selection of key legislative and regulatory developments is presented below to provide insights into the nature of issues that lawmakers are asking organizations to address.

EU General Data Protection Regulation

Among all issues related to data, *privacy rights* and *ownership* have come to the fore. Widely reported data breaches may have been one of the initial causes for increased consumer and supervisor concerns about data privacy. However, those concerns were quickly supplanted by concerns about what companies do with data after a consumer clicks "accept" on a user agreement. For insurers reliant on data analysis in various forms, this raises fundamental questions. In particular, how do you use data that in some sense belong to your customer, without violating customer privacy or raising regulator concerns?

This year saw the European Union (EU) General Data Protection Regulation (GDPR)[3] take effect in May 2018, following a two-year post-adoption grace period. GDPR replaced the EU Data Protection Directive of 1995 and is the first and most globally publicized move to safeguard consumer privacy rights. As such, it may be indicative of what is to come elsewhere. The GDPR regulates the processing by an individual, a company, or an organization of personal data relating to individuals in the EU.[4]

Among numerous protections offered by GDPR, consumers need to be informed if their data are moved outside the EU; have the right to be "forgotten"; and must be given a chance to contest the use of automated algorithms. Other rights include the right to object to the use of one's data for marketing purposes, as well as the right to data portability (i.e., the ability to receive one's data in a machine-readable format and send it elsewhere, perhaps to another insurer competing for that consumer's business).

Insurers operating in the EU have numerous obligations under the GDPR—many of which are consistent with other data security regulations—including the obligation to appoint a data protection officer. Data transfers from the EU to the United States are covered by the EU-US privacy shield framework. Data transfers to other countries that the EU deems to have adequate protection may be conducted similarly to intra-EU transfers; however, transfers to countries not deemed adequate require other safeguards.
Violations can be costly. Individuals suffering material damage from a violation have the right to compensation. Also, in response to infringements, European data protection authorities can impose sanctions that can be as severe as a ban on data processing, as well as fines of up to 4 percent of annual global turnover.

California Consumer Privacy Act

In the United States, the State of California enacted the California Consumer Privacy Act of 2018 (CCPA),[5] that greatly expands data subject rights and introduces provisions for civil class action lawsuits based on statutory or actual damages. The law takes effect in July 2020.

Although there may still be amendments before the law takes effect, for now it provides California citizens with some similar protections to the GDPR. These include the right to access personal information (and to know how a company uses that information), as well as the right to have information removed in some circumstances.

Among other rights, the CCPA "authorizes a consumer to opt out of the sale of personal information by a business and prohibits the business from discriminating against the consumer for exercising this right, including by charging the consumer who opts out a different price or providing the consumer a different quality of goods or services, except if the difference is reasonably related to value provided by the consumer's data."

Consumers have a right to private action in response to uncorrected CCPA violations, and the state Attorney General is also empowered to pursue civil penalties. There are certain exemptions that are granted within the law for data that are subject to the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA).

New York Department of Financial Services cybersecurity regulation

For US insurers, the New York State Department of Financial Services (NYDFS) regulation[6] was the first of its kind—and the first to directly affect a significant number of insurers. It took effect on March 1, 2017, with a phase-in period concluding on March 1, 2019. The regulation requires nearly 2,000 insurers registered with the state to establish and maintain a risk-based cybersecurity program and supporting capabilities.

The two-year phase-in was intended to provide insurers a glide path toward compliance. Companies subject to the regulation should by now have satisfied most of its requirements, which include creation of a written cybersecurity policy; designation of a Chief Information Security Officer (CISO); periodic penetration testing and vulnerability assessment; data preservation that enables accurate reconstruction of all financial transactions; and necessary accounting to respond to a cybersecurity event for at least three years.

To achieve compliance, a company's board of directors must be involved in the creation of standards and must receive regular reports on cybersecurity. In addition, companies are required to file a risk and safeguards assessment in their annual report to regulators.

The next and final phase of the NYDFS regulation—to be completed by March 1, 2019—is the requirement that financial services organizations establish cybersecurity controls and protocols for third-party risk management (TPRM). This includes requirements related to developing and implementing a TPRM program, maintaining a third-party inventory for service providers that access nonpublic information (NPI) or information systems, and performing due diligence and ongoing monitoring.

It is important to note that the NYDFS regulation expands the scope of covered third parties beyond typical vendors to include all third parties with access to NPI. Given this broad purview, programmatic essentials such as governance, reporting, and broader end-to-end life cycle management are key for the sustainable management of an effective TPRM program.

In the United States,, the National Association of Insurance Commissioners' (NAIC) Insurance Data Security Model Law "requires insurers to implement an information security program and investigate and notify the state insurance commissioner of cybersecurity events."[7] The specified model bears many functional similarities to the New York regulation. As such, compliance with the New York regulation is considered sufficient to establish compliance with the NAIC model.

SEC disclosure guidance

The SEC issued disclosure guidance to public companies in early 2018.[8] The guidance stipulates that public companies are required to disclose material information in a timely manner, and, among other guidance, the SEC clarified the desired extent of disclosure related to cyber risks and cybersecurity. In some cases, this may include retroactive disclosure.

The SEC also clarified the need for board involvement in cybersecurity and cyber risk management. Chief Executive Officer (CFO) and Chief Financial Officer (CFO) certifications "should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. In addition, to the extent cybersecurity risks or incidents pose a risk to a company's ability to record, process, summarize, and report information that is required to be disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective."

To address the need for uniformity and transparency in cyber risk reporting, the American Institute of Certified Public Accountants (AICPA) released its cybersecurity attestation reporting framework—"System and Organization Controls (SOC) for Cybersecurity"—in 2017.[9] Organizations can use this framework to convey information about the effectiveness of their cybersecurity risk management programs in a common language, helping all stakeholders better understand the organization's cybersecurity risk management program.

The SOC for Cybersecurity consists of three sections:

1. A management-prepared narrative description of the entity's cybersecurity risk management program, designed to provide information about how the entity identifies its most sensitive information, the ways in which the entity manages its cybersecurity threats, and the key security policies and processes implemented and operated to protect the entity's information assets against those threats
2. Management assertion whether the description in the first section is presented in accordance with the description criteria, and whether the controls within the program were effective to achieve the entity's cybersecurity objectives based on the control criteria

Third-party risk management

TPRM may now be viewed as a basic regulatory expectation. Examples of leading industry practices for an effective TPRM program related to cybersecurity and data risk include:

- Adequate reporting and governance, along with training to facilitate accountability and oversight
- Streamlined processes for third-party management, including stakeholders from sourcing, legal, etc.
- Appropriate third-party termination practices that address retention and destruction of records

In addition, a comprehensive TPRM program should address broader risk and control management practices, including service level agreement (SLA) performance; exit strategy; financial viability; resiliency; reputational review; and regulatory compliance.

Organizations today should consider investments in revisiting and validating their TPRM programs to formalize the program scope, enhance inventory processes, and improve due diligence and assessment procedures—and to integrate contract management of their third-party landscape.

All of these components should be managed as part of a broader risk management and information governance effort that stretches beyond the CISO and IT. All data users—whether internal or external—are responsible for data security. However, it is the responsibility of the board and executive leadership to provide the required resources, authority, and accountability to ensure adequate data security across the enterprise. Also, it is critical for the board to lead by example, providing the necessary tone-at-the-top to convey the importance of properly managing this prime operational risk.

3. Practitioner's opinion, in which a certified public accountant (CPA) provides an opinion on the description, and on the effectiveness of controls within the program

The SOC framework provides a number of potential benefits, including helping to satisfy information and oversight requirements for the board and senior management (as well as regulators) and helping to reassure investors and customers.

For organizations planning to embark on an attestation, a leading practice to consider might be the AICPA Cybersecurity Attestation Reporting Framework (see figure 1).

NAIC Big Data Working Group

Even as the privacy debate pushes other data-related issues from the headlines, regulators in the United States continue their work. The NAIC created the Big Data Working Group to, among other things, "review current regulatory frameworks used to oversee insurers' use of consumer and non-insurance data" and "assess data needs and required tools for state insurance regulators to appropriately monitor the marketplace and evaluate underwriting, rating, claims and marketing practices."[10]

Big data concerns cited by the NAIC include the following:[11]

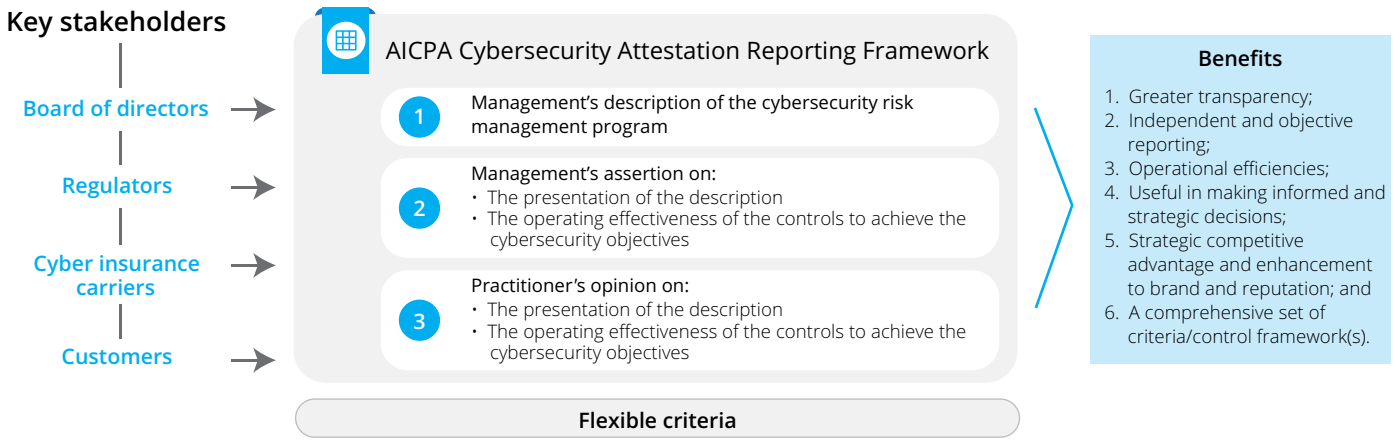
- Complexity and volume of data, which may present hurdles for smaller insurers
- Insurance regulatory resources for reviewing complex rate filings
- Lack of transparency and the potential for bias in algorithms used to synthesize big data
- Highly individualized rates that lose the benefit of risk pooling
- Collection of information that is sensitive to consumers' privacy (or potentially discriminatory)
- Cyber threats to stored data

Ongoing and future developments

Several other countries have continued to enhance their privacy and cybersecurity laws. Notable examples include:

- **Brazil** enacted its General Data Protection Law in July 2018[12] that significantly provides for significant rights and protections to personal information. The law is widely touted as being very similar to GDPR. Organizations have 18 months to comply.
- **United Kingdom** issued its Data Protection Act 2018[13] that implements the GDPR provisions as well as imposing additional requirements, such as on matters related to national security and immigration.
- **Singapore** passed the Cybersecurity Act in March 2018,[14] subjecting organizations to information sharing, reporting incidents, conducting cybersecurity audits, and participating in national cybersecurity exercises.
- **Australia** included mandatory data breach notification requirements within its Privacy Act[15] that obligate financial credit institutions to notify individuals whose personal information is involved in a data breach that may cause harm.

Figure 1: AICPA Cybersecurity Attestation Reporting Framework



Source: Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program, https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx

The outlook for cybersecurity and data privacy continues to indicate strong regulatory developments, with several countries either implementing or enhancing existing regulatory requirements. Within the United States, organizations can also expect to see continued attempts toward simplification of regulatory compliance requirements, such as those noted within the Core Principles report from the Treasury,[16] as well as continued efforts toward harmonization of data privacy and cybersecurity laws and regulations.

The life insurance business shifts to a customer best interest standard

As customer protection regulations for the financial services industry zigzag from the vacating of the Department of Labor's fiduciary rule to proposed new rules by the SEC in its Regulation Best Interest, the NYDFS has published its final version of Insurance Regulation 187.

Regulation 187[17] applies a "best interest" standard to annuity and life insurance product recommendations that becomes effective on August 1, 2019, for annuities, and on February 1, 2020, for life insurance products.

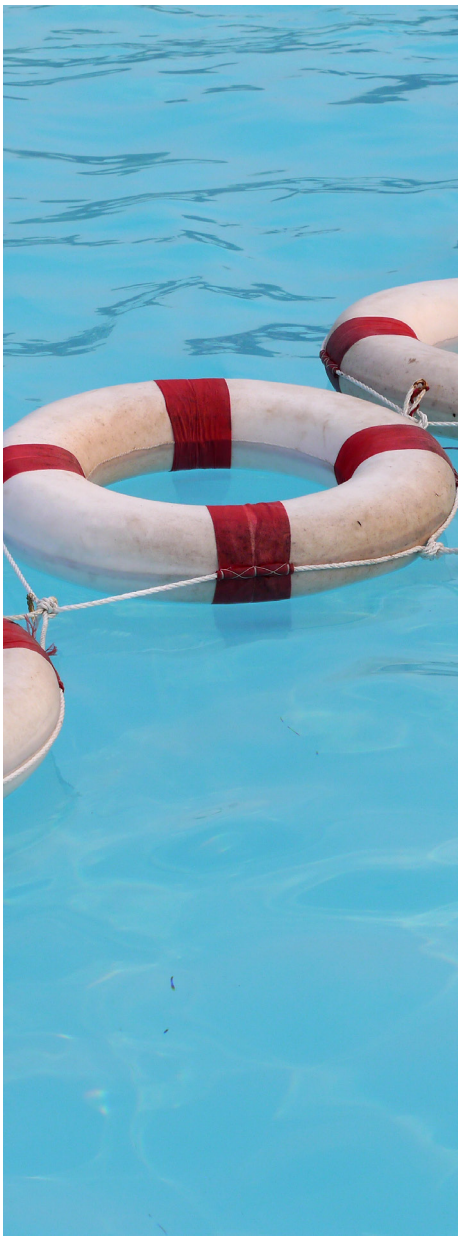
This regulation will have far-reaching impacts on insurers for a number of reasons, including (1) its scope of applicability and (2) its interconnected effects on agents/producers and insurers—particularly the obligation for insurers to supervise, monitor, and take corrective action for any consumer or other third party harmed by an agent/producer. In essence, insurers may potentially be responsible for paying when a consumer is affected by agents and producers failing to act in the consumer's best interest.

Scope of applicability:

- Includes insurers, producers, life insurance, annuities, and in-force policies/contracts
- Applies to policies and contracts delivered—or issued for delivery—in New York
- Applies to recommendations relating to entering into a policy, or to refraining from entering into any transaction
- Includes transactions for which recommendations are made at the point of sale for an insurance product, and post-sale during the servicing of the product for the consumer (e.g., election of a contractual provision)

Integrated end-to-end requirements:

- **Agents/producers.** Recommendations for the purchase, replacement, or retention of life and annuity products must meet a best interest standard of care or suitability obligation, must cover many disclosures, and must appropriately address consumer insurance needs and their financial objectives.
- **Supervision by insurers.** Insurers must establish and maintain a system of supervision—along with standards and procedures—reasonably designed to achieve insurer and producer compliance.
- **Oversight by insurers.** Insurers must establish a system of audit that is reasonably designed to achieve compliance with the insurer's and producer's responsibility.
- **Books and records.** Insurers must maintain all records, including appropriate information about a customer's financial situation and the complexity of the transaction, as well as documentation to support the agent/producer recommendation.



Regulation 187 may present significant challenges

The requirements of Regulation 187 come at a time when the life insurance industry is already facing difficult challenges to drive revenue and manage costs. For example, there is increased competition to grow and differentiate its products, increase agent retention, and expand margins. Digitization is expected to accelerate the ability for life insurance carriers and agents/distributors to provide consumers with a more interactive and informative discussion of product alternatives. Regulation 187 in New York is added complexity in an already-difficult business environment. Regulation 187 will require insurers to adapt their sales process, producer training, and home office supervisory and compliance operations. Aside from annuities, there is the added complexity of life insurance for which there are fewer solutions presently available. The confluence of these factors, along with uncertainty about whether other states might follow New York's lead, will present significant potential challenges in 2019 and into 2020.

Conduct risk

We continue to see global interest across jurisdictions in advancing a conduct and culture agenda. This suggests that conduct risk is an issue that is here to stay. Outside the United States, there has been a general shift from approaches that are pragmatic and principles-based to approaches that are more rules-based (such as Market Abuse Regulation[18] and Markets in Financial Instruments Directive [MiFID II][19]).

Within the United States, the Federal Reserve Bank (FRB) is most active around conduct in the capital markets space. The FRB Board of Governors is executing horizontal exams via its Large Institution Supervision Coordinating Committee (LISCC), with a focus on how firms are addressing business conduct and compliance risk, and on firms' capabilities related to detection and prevention of misconduct.[20]

As a concept, conduct risk has taken on greater meaning since the financial crisis. Ten years ago, "business practices" and "conduct" started becoming a more prominent topic. Five years ago, firms began establishing frameworks to identify, manage, and monitor conduct as a new dimension of risk. Today, numerous industries are coming to terms with how to proactively prevent employee misconduct and manage company culture.

Key trends

Enterprise view of conduct risk. Large US institutions are expected to have an enterprise-wide conduct risk management program and an enterprise-wide conduct risk function. The regulatory focus is on (1) continuous monitoring of conduct and improvement and (2) detection and prevention mechanisms to influence how strategic objectives are being achieved.

The traditional focus on employee conduct is converging with a newer focus on market conduct, business practices, and impact on clients and markets. Also, there is significant focus on development of internal controls, creating a need to rationalize activities in order to efficiently manage the program. This may lead to some realignment of supervisory/surveillance activities.

Analytics and predictive intelligence applied to conduct and culture. Firms are looking to generate meaningful insights on employee conduct for the board, senior management, and regulators. The ability to predict and prevent employee misconduct is a business imperative across institutional, retail, and wealth management sectors. Firms are looking to identify employees with poor conduct sooner; proactively identify the next population of at-risk employees and activities; and develop improved approaches for heightened supervision and targeted surveillance/monitoring.

Challenges and opportunities from emerging technologies. Technology continues to disrupt how firms engage, deliver, monitor, and interact with customers. As a disruptor, technology gives rise to new business practices that can lead to new or increased conduct risks and challenges (e.g., digital banking, robo-advisers, electronic/algorithmic trading, new products such as cryptocurrency). However, it also creates opportunities to implement and refine controls that support sound conduct risk management (e.g., harnessing the increased availability of data to better predict—or more quickly detect—employee misconduct).

Compensation and remuneration focus. This continues to be a significant area of attention for regulators. The FSB is planning to release recommendations on how firms can enhance their capacity to consider and monitor the effectiveness of compensation tools. The FSB's recommendations are also expected to highlight mechanisms for promoting good conduct and addressing misconduct risk. In Australia, the Banking Royal Commission reviewed a number of financial services institutions and identified remuneration as one of the root causes of misconduct.[21]

Market conduct

Market conduct has become a hot topic in insurance regulation recently, and its importance will likely continue to grow.

The financial crisis forced insurance supervisors worldwide to reexamine their approaches to regulation, and to evaluate the industry's potential systemic risk. In 2015, the International Association of Insurance Supervisors (IAIS) released an issues paper noting, "In the aftermath of the financial crisis, supervisors' immediate priorities were to focus on prudential regulatory issues, including strengthening capital. As the concept of conduct of business risk now gathers momentum globally, it is timely that the IAIS considers this form of risk in more detail within the context of supervision of the insurance sector."[22]

Today, efforts that incorporate new or changed approaches to solvency regulation are nearing completion, or have been completed. These include: the Solvency Modernization Initiative in the United States; Solvency II in Europe; and Common Framework for the Supervision of Internationally Active Insurance Groups (ComFrame), and the International Capital Standard at the global level. Regulators are now freer to focus on other aspects of insurance supervision, particularly market conduct regulation. This increased focus on market conduct may be aided by the increased availability of analytical and technological tools for regulators; insurers would do well to proactively review their own practices to help achieve compliance.

Trends in market conduct regulation

Market conduct has long been important to regulators. One recent newsworthy example was insurance departments across the country cracking down on insurers using the Social Security Death Master File to stop making certain kinds of payments, while not leveraging the same information to make life insurance payments. Although these actions may have been standard for the industry—and not necessarily contractual or legal violations—they likely tarnished the industry's reputation.

Insurance regulators around the world are looking more closely at market conduct. At the global level, when the IAIS announced the creation of its new five-year plan, it stated its intent to focus on a number of emerging issues, including market conduct. In the United States, member regulators of the NAIC have indicated an interest in the subject. Meanwhile, state regulators are considering the use of consultants for market conduct examinations and quality. This should help level the playing field nationally for analysis of market conduct issues.

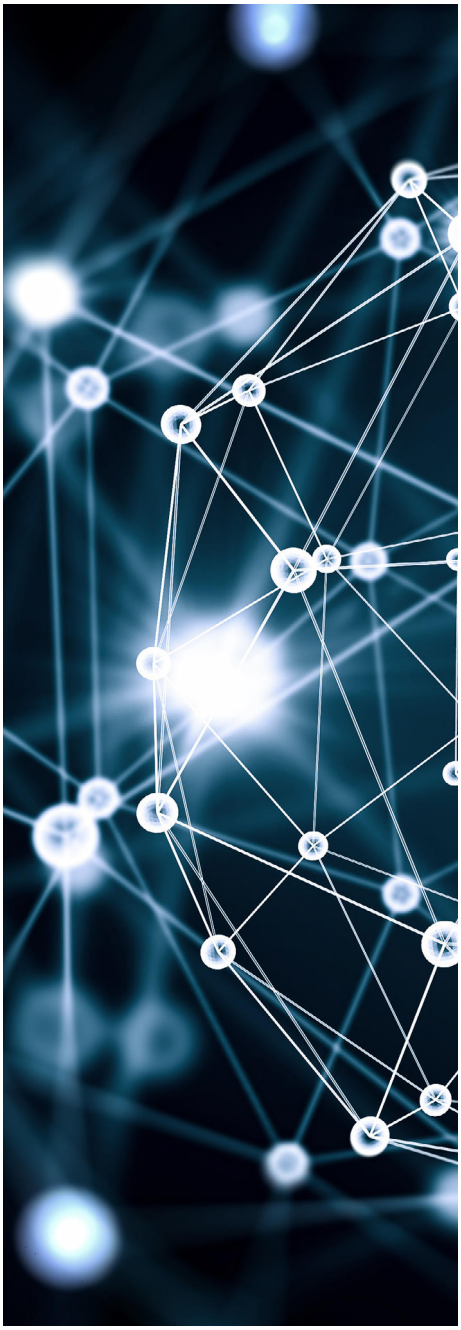
In addition, the state insurance regulator members of the NAIC recently adopted measures prohibiting the use of pre-dispute mandatory arbitration, as well as choice of law and choice of venue clauses in personal lines of insurance. These measures, which were adopted at their late summer 2018 meeting,[23] are widely seen as pro-consumer.

As noted elsewhere in this outlook, perhaps the single biggest discussion item related to market conduct thus far has been the possible creation of new, higher sales standards for annuity and life insurance. Regulators have been moving toward consensus that a "best interest" standard might be appropriate for annuity sales, and the state of New York has already issued regulations instituting such a standard both for life insurance and annuity sales. These standards may increase regulatory scrutiny throughout the sales process for both insurers and producers.

The technology factor

Technology could be the most significant difference maker for market conduct in the near future. The NAIC has embarked on its three-year State Ahead strategic plan,[24] with the goal to provide its member regulators with the talent and technology to support advanced analytics and oversight. For some insurers, this development might have the most direct impact on market conduct, giving regulators timely, deep, broad, and actionable insight into the market conduct performance of both product lines and insurers.

The good news for insurers is that similar regulatory technology is available to help them too. Innovative technologies ranging from robotics process automation to natural language processing, higher-order cognitive technologies, and artificial intelligence (AI) can help enable end-to-end product oversight while monitoring market reactions and regulatory actions. These technologies can also help enable a talent transformation, freeing up the compliance function and related talent for high-value work beyond reporting. Insurers not yet exploring such technologies may wish to consider creating a framework within which to appropriately leverage talent and technology to cope with a world of increased market conduct oversight.



The fraud epidemic

Insurance fraud continues to be a major issue for the insurance industry and consumers. While overall fraud is difficult to measure, an insurance industry coalition estimates it to be an $80 billion-a-year problem.[25] The insurance fraud epidemic affects the industry and consumers in many ways, including higher premiums for consumers from the costs of fraud being passed on, and reduced earnings for insurance companies that continue to pay fraudulent claims and allow rate evasion.

The problem can be divided into two main categories—hard fraud and soft fraud. Hard fraud is typically perpetrated by criminal organizations with the explicit intent to commit fraud, usually on a large scale.[26] Soft fraud is opportunistic and typically perpetrated by individuals through relatively benign acts such as exaggeration, embellishment, malingering of a claim, or misrepresentation of a previous condition.[27]

It is estimated that 3 to 5 percent of every claim dollar is lost to hard fraud—the kind committed by organized criminals—while 5 to 25 percent of every claim dollar is lost to soft fraud.[28] In addition, premium leakage is estimated to cost personal auto insurers $29 billion annually due to missing or erroneous underwriting information provided during the application process.[29]

In September 2018, Michigan Governor Rick Snyder formed a new anti-fraud unit within the state's Department of Insurance and Financial Services.[30] By adopting this executive order, Michigan effectively became the 42nd state to have a fraud bureau.[31] In addition to fraud bureaus, states have various ways to help identify and deter fraud: 43 states have mandatory fraud reporting statutes; 22 states require companies to have anti-fraud plans; and 15 states require companies to utilize special investigative units (SIU). According to the Coalition Against Insurance Fraud, which actively tracks and monitors state legislatures across the country, in the 2018 legislative session 30 anti-fraud bills have been enacted, and 26 bills are pending (as of September 20, 2018).[32]

Barriers to detecting and preventing insurance fraud

A recent study by the NAIC surveyed insurance fraud experts and identified several common barriers to fighting insurance fraud:[33]

- **Lack of political and judicial support.** Insurance fraud is not as visible or glamorous as other crimes, and often the punishment perpetrators receive is not enough of a deterrent. Also, the cost for insurance companies and government entities to detect, investigate, prosecute, and punish fraudsters can greatly outweigh the value of the fraud that is detected.
- **Financial barriers.** Many companies are under constant pressure to do more with less and may lack the necessary budget to aggressively fight fraud.
- **Fraud is difficult to identify and quantify.** There is no standard way for companies or the industry to identify and quantify fraud. Although most people recognize hard fraud when they see it, soft fraud tends to be more elusive—with many false positives in the fraud detection process. As such, soft fraud must be teased out of the insurance ecosystem using operational processes that are nonaccusatory and less confrontational.
- **Fraud is a social problem.** The public generally accepts insurance fraud as a normal cost of doing business. Lack of consumer education and inadequate business processes contribute to the problem, especially in key areas such as deductible fraud, premium leakage, claims embellishment, and employee misclassification.
- **Changes in claims staff.** According to the survey, many experienced claims adjusters have been moved into more of a claims processor role, leaving less skilled employees to handle claims adjustment and investigation.
- **Insurance companies can be their own worst enemies.** Many companies make the business decision to simply pay suspicious claims without a fight, since it can be cheaper in the short term to settle claims without incurring the additional costs of challenging them. Short-term profits often take priority over detection. Also, companies are often able to file for and obtain higher rates to compensate for the costs of fraud, and in many cases regulators have not required carriers to prove they are effectively combatting fraud before approving rate increases. On the front lines, many companies are increasingly hiring professionals without investigative experience, reducing their ability to fight fraud.

While detailed statistics for the volume of fraud, waste, and abuse that insurance companies detect and filter out are difficult to find, the actions insurers take to reduce

such leakage are analogous to how retailers work to prevent shrinkage in their business ecosystem. As an example, a retail company's processes to reduce shrinkage might yield a benefit of approximately 3 percent of annual sales. Equating that benefit to the Property and Casualty (P&C) industry's 2017 net written premium of $558.2 million,[34] for every 1 percent of fraud detected and prevented, the P&C industry could potentially realize billions in savings.

What are companies doing to mitigate insurance fraud?

Despite the barriers reported by the NAIC survey, a number of companies have taken steps to identify and reduce insurance fraud, waste, and abuse—with varying degrees of success. A recent study by the Coalition Against Insurance Fraud found that a growing number of insurers are embracing and expanding their use of technology to improve their anti-fraud capabilities.[35] Companies typically use automated red flags and/or business rules to identify insurance fraud; however, while such capabilities do add value, they are not sufficient to combat the more sophisticated fraud rings, or to detect many types of soft fraud.

More advanced analytics techniques include:

- **Data exploration.** Identifying trends, outliers, and circumstantial anomalies through exploratory data analysis.
- **Geospatial analysis.** Using geographic coordinates to identify spatial patterns and anomalies.
- **Social networking.** Visualizing and analyzing relationships to identify key players and uncover hidden patterns.
- **Machine learning.** Leveraging advanced modeling techniques such as neural networks, random forests, and regression to uncover subtle fraud patterns.

Advanced analytics techniques go beyond the traditional red flags and business rules, enabling companies to identify hidden fraud patterns that were previously undetectable. For example, with machine learning, companies can quickly and efficiently uncover situations where a person is fraudulently filing multiple claims with different insurance companies using slight modifications of their name (e.g., John Smith, J Smith, John Smyth). Another example might be where machine learning detects that subtle circumstances or data signals for a claim fall outside the boundaries of data normalcy across a broad population of past and current claims. Advanced capabilities such as these are rapidly improving, giving insurance companies new and powerful weapons to fight back against the fraud epidemic.

Capital standards

A decade ago, the survival of the world's financial system seemed at risk, prompting governments and regulators to undertake various actions to ensure the system's survival. In the aftermath of the crisis, legislators and regulators began work to minimize the possible systemic risk posed by various sectors of the financial services industry.

For insurers, the IAIS was charged by the G20 with developing measures[36] to manage systemic risk. Much of the work focused on macro-prudential regulatory measures, including the development of capital standards.

Internationally, the risk-based, global insurance capital standard (ICS) was created.[37] Insurers designated as "Internationally Active Insurance Groups" (IAIGs), as defined by ComFrame, will have to consider the application and impact of the ICS. According to the IAIS, there are a dozen insurers headquartered in North America that are potentially affected.

In the United States, the NAIC has been engaged in a similar effort to develop a group capital calculation (GCC) for US insurance groups.

At the IAIS, work on ComFrame[38]—including the adoption of ICS 2.0—is in its final stages. The next field testing is scheduled to begin in April 2019. One more consultation on ComFrame is then expected in mid-June 2019. Subsequently, in November 2019, the requirements are scheduled for adoption during the IAIS Annual General Meeting. A five-year confidential reporting and monitoring period will begin in 2020, during which the IAIS and group-wide supervisors will monitor the results. This could lead to further changes to the ICS; however, stability is generally expected, in contrast to the significant changes that typically occurred in the field testing period. During the monitoring period, the ICS will not be considered a prescribed capital requirement (PCR), and thus will not in and of itself trigger supervisory action.

US state insurance regulators at the NAIC have charged the Group Capital Calculation (E) Working Group with constructing "a US group capital calculation using a risk-based capital (RBC) aggregation methodology; liais(ing) as necessary with the ComFrame Development and Analysis (G) Working Group on international capital developments and consider(ing) group capital developments by the Federal Reserve Board, both of which may help inform the construction of a US group capital calculation."[39]

It is important to note that while the ICS is ultimately intended to be a prescribed capital requirement, the NAIC has insisted its GCC is just that—a calculated metric designed to help regulators assess the solvency of insurance groups; not a standard. The NAIC's working group has issued a number of drafts, each time revising its proposed calculation in response to stakeholder feedback. Field testing is expected to further inform development of the GCC.

InsurTech

InsurTech is the next wave of technology innovation in insurance, pushing the entire industry to be more customer-centric, data-driven, and platform-based. This trend is being fueled by the exponential growth of data, computation power, and connected devices—and by data democratization. It is also being fueled by an influx of capital, with more than $10 billion invested in InsurTech companies over the past five years.

InsurTechs are harnessing the power of the latest technologies, including mobile and apps, AI, algorithms and robo-advice, smart contracts, the Internet of Things (IoT), and blockchain/distributed ledger technology (DLT).

So far, InsurTechs have primarily affected the insurance industry by supporting and serving legacy insurers, as opposed to disrupting the established market. In many cases, legacy insurers have acquired technology from InsurTechs and incorporated it into their own ecosystems, or partnered with InsurTechs that provide software-as-a-service (SaaS) or licensing solutions.

Regulators may find it challenging to develop a comfort level with InsurTech innovations and their proposed uses. Also, they may have trouble monitoring and assessing the effect of InsurTech use. For example, while robo-advisers could enable insurance consumers to receive advice at lower price points, regulators need to make sure the provided advice essentially conforms to the same general principles that guide humans when offering similar advice.

Wearables and other biometric devices could potentially enable insurers to gather large amounts of data to perform no-lab underwriting. Also, the ability to track policyholder behaviors could enable insurers to offer health advice (both physical and mental), effectively merging the roles of life insurer and health insurer. Smart devices in homes, vehicles, industrial facilities, and elsewhere could enable insurers to better select, price, and prevent risks. However, for all these innovations, regulators need to be concerned about outcomes—including any possible discriminatory impacts.

Recognizing this need, the NAIC established an Innovation and Technology (EX) Task Force to monitor new InsurTech developments and help regulators stay informed. In a release issued after numerous regulators attended the InsurTech Connect conference in late 2018, NAIC CEO Mike Consedine said, "We're going to see more insurance innovation in the next 10 years than we've seen in the last 150. Regulators and innovators must work together to educate each other about the new technology, its impact on the marketplace and consumers in order to effectively regulate it."[40]

For regulators, significant concerns are likely to include privacy and transparency, and the level of consumer education in using new products and platforms. For insurers, a significant concern might be how well regulators understand the emerging technologies. Thus, as insurance companies employ more InsurTech, Consedine's call for regulators and innovators to educate each other might be of prime importance.

For now, the biggest issue may be that regulators will simply say "no" if they do not have sufficient information or expertise to analyze and understand InsurTech innovations. To address this issue, a key goal of the NAIC's State Ahead strategic initiative[41]—scheduled for completion in 2020—is to provide the resources for state regulators to effectively analyze and regulate new technologies and technology uses.

In the meantime, the best available option for insurers might be to inform and involve regulators early in the process of InsurTech adoption. InsurTech has the potential to transform the relationship between regulators and regulated by emphasizing the importance of working together from the beginning in order to get to "yes." This could help bring relevant, innovative products to market more quickly, which is something all stakeholders should find appealing.

All of these technology innovations have significant potential benefits for consumers; however, they also pose challenges that may trigger regulatory scrutiny.

Analytics and modeling in risk and compliance

The year 2018 appears to have been the turning point for insurers embracing the use of analytics and modeling to help manage their operational risk and regulatory compliance exposures. Chief Risk Officers and Chief Compliance Officers at insurance firms cite numerous examples where prior years' "science experiments" were replaced by defined resource investments and a deeper commitment to harnessing company and external data for risk and compliance analytics.

Many firms have added data scientists to their risk and compliance teams and are tapping into various data sources to support their analytics and modeling activities. As those efforts gain traction, 2019 may be the year when the industry accelerates its pace of using analytics and models to generate new insights and more effectively measure and predict risk exposure.

Although the industry's efforts are quite varied in terms of scope, approach, and rate of progress, several common themes and trends have emerged:

- Nearly all firms are discussing the potential of improved data analytics, and no firm wants to get left behind. This general trend applies to many parts of the business, including the risk and compliance functions, where many firms have hired dedicated scientists or analysts to drive their efforts.
- Firms may view regulators' use of data analytics as an emerging risk. Some firms already face questions from regulators about why they did not proactively identify certain agent conduct risks, given the volume of information they had.
- Risk and compliance leaders often have ambitious goals for analytics and modeling; however, those lofty aspirations face tactical challenges, including how to access and use internal and external data, and how best to architect the data for uncertain future uses. Similarly, the desire to show "quick wins" from improved insights can conflict with longer-term goals.
- Selecting the best short-term opportunities can be challenging; however, a number of high-priority areas are clear: emerging risks associated with regulatory market conduct exams; policy rate accuracy and related laws and regulations; sales practice misconduct; and the need to correlate data characteristics with improved modeling (such as risks cited in own risk and solvency assessment or ORSA reports).
- An important and frequently cited goal is to improve the portrayal both of business risks (insurance, investment, credit, and operational) and regulatory compliance risks through enhanced data visualization and reporting.

In 2019, we expect to see firms continuing to invest in dedicated resources and experiment with data in a more organized and effective manner. There will undoubtedly be some setbacks and frustrations, but also some important wins. Sharing leading practices and success stories can help inspire risk and compliance professionals to continue the journey into the world of analytics. This journey has very clearly started—although the final destination remains unclear. Firms should strive for meaningful progress in the year ahead, using periodic checkpoints to refine their goals; demonstrate progress, value, and ROI; manage internal expectations; and adjust course as needed.

2019 may be the year when the industry accelerates its pace of using analytics and models to generate new insights and more effectively measure and predict risk exposure.

Taking the lead in times of change

Today's regulatory environment is in the midst of significant and unpredictable change, driven by a variety of forces including political shifts, new social norms and behaviors, and technological innovation. To succeed in this challenging environment, companies need to actively look for ways to improve the effectiveness and efficiency of their compliance strategies and operations. Technology is likely to play an increasingly important role in this pursuit. Robotic process automation, for example, is being widely adopted by compliance-related functions to help them do more with less. At the same time, emerging technologies such as artificial intelligence and advanced analytics are making it possible to do things that have never been done before. Innovations like these can create business value no matter which way the regulatory winds might shift—enabling leaders to take action confidently and decisively in times of significant and ongoing change.

Endnotes

1. Economic Growth, Regulatory Relief, and Consumer Protection Act, available at https://www.congress.gov/bill/115th-congress/senate-bill/2155.
2. Securities and Exchange Commission, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," 17 CFR Parts 229 and 249, February 26, 2018.
3. European Union General Data Protection Regulation, available at https://eugdpr.org/.
4. European Commission, "What does the General Data Protection Regulation (GDPR) govern?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en.
5. The California Consumer Privacy Act of 2018, Assembly Bill 375, Chapter 55, State of California, June 29, 2018.
6. New York State Department of Financial Services, "Cybersecurity requirements for financial services companies," https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.
7. NAIC Center for Insurance Policy and Research, "Cybersecurity," July 11, 2018, https://www.naic.org/cipr_topics/topic_cyber_risk.htm.
8. Securities and Exchange Commission, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," 17 CFR Parts 229 and 249, February 26, 2018.
9. American Institute of Certified Public Accountants, "System and Organization Controls (SOC) for Cybersecurity," available at https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html.
10. NAIC Big Data (EX) Working Group, "2018 Charges," https://www.naic.org/cmte_ex_bdwg.htm.
11. NAIC Center for Insurance Policy and Research, "Big data," July 12, 2018, https://www.naic.org/cipr_topics/topic_big_data.htm.
12. Brazil's General Data Protection Law.
13. Information Commissioner's Office, Data Protection Act 2018, available at https://ico.org.uk/for-organisations/data-protection-act-2018/.
14. Cyber Security Agency of Singapore, "Cybersecurity Act," available at https://www.csa.gov.sg/legislation/cybersecurity-act.
15. Office of the Australian Information Commissioner, "Privacy Act," available at https://www.oaic.gov.au/privacy-law/privacy-act/.
16. US Department of the Treasury, "Core Principles," available at https://home.treasury.gov/policy-issues/top-priorities/regulatory-reform.
17. New York State Department of Financial Services, "First Amendment to 11 NYCRR 224 (Insurance Regulation 187)," available at https://www.dfs.ny.gov/insurance/r_finala/2018/rf187a1txt.pdf.
18. Financial Conduct Authority. Market Abuse Regulation. Available at https://www.fca.org.uk/markets/market-abuse/regulation.
19. European Securities and Markets Authority. MIFID II. https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir.
20. Board of Governors of the Federal Reserve System (Board), Proposed Supervisory Guidance, available at https://www.federalregister.gov/documents/2018/01/11/2018-00294/proposed-supervisory-guidance.
21. Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, "interim Report," available at https://financialservices.royalcommission.gov.au/Pages/interim-report.aspx.
22. International Association of Insurance Supervisors, "Issues paper on conduct of business risk and its management," November 2015.
23. Deloitte, NAIC update: Summer 2018, available at https://www2.deloitte.com/us/en/pages/financial-services/articles/naic-update.html.
24. National Association of Insurance Commissioners, State Ahead, available at https://www.naic.org/state_ahead.htm.
25. Coalition Against Insurance Fraud, Insurers: Victim impact statements, available at https://www.insurancefraud.org/the-impact-of-insurance-fraud.htm.
26. USLegal, Hard Fraud Law and Legal Definition, available at https://definitions.uslegal.com/h/hard-fraud/.
27. USLegal, Soft Fraud Law and Legal Definition, https://definitions.uslegal.com/s/soft-fraud/.

28. Insure.com, Padding insurance claims hits everyone's wallets, available at https://www.insure.com/car-insurance/padding-insurance-claims.html.

29. Verisk, Auto insurance premium leakage: A $29B problem for the industry, available at https://www.verisk.com/insurance/visualize/auto-insurance-premium-leakage-a-29b-problem-for-the-industry/?print=1&tmpl=component.

30. Insurance Journal, Michigan Insurance Department Getting New Anti-Fraud Unit, available at https://www.insurancejournal.com/news/midwest/2018/09/13/501100.htm.

31. Coalition Against Insurance Fraud, Statutes: State insurance fraud statutes, available at https://www.insurancefraud.org/statutes.htm.

32. Coalition Against Insurance Fraud, State legislation: Legislative scorecard, available at https://www.insurancefraud.org/state-legislation.htm.

33. National Association of Insurance Commissioners, Journal of Insurance Regulation, available at https://www.naic.org/documents/prod_serv_jir_JIR-ZA-33-04-EL.pdf?15.

34. Insurance Information Institute, Facts + Statistics: Industry overview, available at https://www.iii.org/fact-statistic/facts-statistics-industry-overview.

35. Coalition Against Insurance Fraud, *the state of insurance fraud technology, available at* http://www.insurancefraud.org/downloads/State_of_Insurance_Fraud_Technology2016.pdf.

36. International Association of Insurance Supervisors, Holistic Framework for Systemic Risk in the Insurance Sector, page 8, available at https://www.iaisweb.org/file/77862/holistic-framework-for-systemic-risk-consultation-document.

37. International Association of Insurance Supervisors, "Insurance Capital Standard," available at https://www.iaisweb.org/page/supervisory-material/insurance-capital-standard.

38. International Association of Insurance Supervisors, "Common Framework," https://www.iaisweb.org/page/supervisory-material/common-framework.

39. NAIC Group Capital Calculation (E) Working Group, "2018 Charge," https://www.naic.org/cmte_e_grp_capital_wg.html.

40. National Association of Insurance Commissioners, "Regulators connect with innovators at InsurTech conference," press release, October 3, 2018.

41. National Association of Insurance Commissioners, State Ahead, available at https://www.naic.org/state_ahead.htm.

Contacts

Leadership

Monica O'Reilly
Regulatory & Operations Risk Leader
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
monoreilly@deloitte.com

Rich Godfrey
National Advisory Insurance Leader
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
rgodfrey@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

Elia Alonso
Global Conduct Risk Leader
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
elalonso@deloitte.com

Bryan Berkowitz
Senior Manager | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
bberkowitz@deloitte.com

Julie Bernard
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
juliebernard@deloitte.com

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

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

John Lucker
Global Advanced Analytics Market Leader
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
jlucker@deloitte.com

Andrew Mais
Senior Manager
Deloitte Services LLP
amais@deloitte.com

Howard Mills
Global Insurance Regulatory Leader
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
howmills@deloitte.com

Nitin Pandey
Senior Manager | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
npandey@deloitte.com

Jeff Schaeffer
SOC for Cybersecurity Solution Leader
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
jschaeffer@deloitte.com

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

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.