# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global foreword</td>
<td>4</td>
</tr>
<tr>
<td>Introduction</td>
<td>7</td>
</tr>
<tr>
<td>Privacy compliance with data management upgrades</td>
<td>8</td>
</tr>
<tr>
<td>Best interest industry sales standards</td>
<td>10</td>
</tr>
<tr>
<td>Market conduct</td>
<td>12</td>
</tr>
<tr>
<td>Fraud</td>
<td>14</td>
</tr>
<tr>
<td>Conduct risk</td>
<td>17</td>
</tr>
<tr>
<td>Development of capital standards for US insurers</td>
<td>20</td>
</tr>
<tr>
<td>Impact of international regulatory trends on US regulations</td>
<td>22</td>
</tr>
<tr>
<td>Third-party risk management</td>
<td>23</td>
</tr>
<tr>
<td>Staying ahead</td>
<td>27</td>
</tr>
<tr>
<td>Leadership</td>
<td>27</td>
</tr>
</tbody>
</table>
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 2020. 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 2020, 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 that affect insurance in 2020, 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 2020 and the regulatory changes it may bring. Please feel free to contact us with questions and feedback at CenterRegulatoryStrategyAmericas@deloitte.com.
Global foreword

After a decade of global regulatory reforms defined by the financial crisis and misconduct issues, the regulatory environment is now changing profoundly. The international consensus on regulatory reform is fraying. Political appetite for globalisation is retreating, and trade tensions are mounting. Technological change and social concerns, including environmental sustainability, are rising on regulators’ agendas. Financial services firms need to be prepared to respond to these trends.

Economic outlook

We may see weak growth in a number of regions in 2020, with significant downside risks.1 Regulators’ and supervisors’ work programmes are likely to be heavily influenced by their assessment of the economic conditions under which firms will be operating. Increased trade tensions, especially between the US and China, are likely to fragment markets further, dampen growth and create a harsher business environment for financial services firms.

In the United States, the yield curve on Treasury bonds was inverted until recently, which has in the past been a harbinger of recession. Equity valuations are high due, in large part, to monetary easing: The US equity market is more overvalued on some measures than at any point since the dotcom bubble.

Meanwhile in China, growth has continued to slow and gross debt surged from 171% of Gross Domestic Product in 2008 to 299% in 2018.2 High debt levels could become unsustainable if growth slows further.

In our view, the risk of a recession is highest in Europe. Growth in Germany is expected to be as low as 0.5% in 2019, partly due to its manufacturing sector’s vulnerability to poor export markets, although some recovery is expected in 2020.3 Italy is facing political uncertainty, economic stagnation and resurfing financial turbulence, while servicing high public debt.4 And the UK faces an uncertain outlook, in part due to Brexit. Therefore, while growth for the Eurozone in 2020 is projected at 1.4%, which is similar to its postcrisis trend rate, significant downside risks remain.5

Central bankers are likely to respond with further monetary easing, with the US Federal Reserve Board and the European Central Bank having already cut rates further and renewed their asset purchase programmes. However, with interest rates at an unprecedented low, and with a record amount of sovereign and even corporate bonds trading at negative nominal rates, the effectiveness of such measures in isolation is debatable.6 Authorities may consider using macroprudential measures, such as allowing banks to run down countercyclical buffers. Governments are also likely to face pressure to increase spending to stimulate growth, especially given the backlog of infrastructure spending in some countries.

These macroeconomic trends and conditions will put even more pressure on financial services firms’ business models, at a time when competition from new entrants and major digital players is also increasing. We expect supervisors to have a heightened focus on business model resilience, through stress testing, and on the quality of risk governance and oversight.

Banks may struggle to regain profitability, and even to maintain margins, through their traditional business model in a low, or negative, interest rate environment. For example, Japan has had a zero or negative interest rate policy for nearly two decades. Japanese banks have struggled with low interest margins and face increasing supervisory scrutiny on business model sustainability.7 A reduction in cross-border financial flows as risk appetites reduce may also narrow banks’ growth opportunities. Banks will need to redouble their efforts to control costs and refocus on more profitable business lines. However, they will need to be mindful of conduct risk. Supervisory focus on credit risk is also likely to intensify. For example, the Bank of England estimates that global banks retain exposures to over half of the leveraged loan market, and that the global stock of leveraged loans has reached an all-time high.8

Insurers, particularly those providing long-term guarantees, are also likely to find it harder to be profitable in a persistently low interest rate environment. In Asia, however, the potential for the insurance market to grow in China may help insurers to generate more off-setting revenue.9

Investment managers too will likely struggle to perform well in an environment characterised by high asset prices and low growth potential. The increasing scrutiny by investors and regulators of the value generated by active management is likely to drive a continued...
“search for yield” and encourage investment in more exotic and less liquid markets. We expect supervisors to focus increasingly on how investment managers and distributors satisfy themselves that funds holding higher risk assets meet the needs and risk appetite of their target market.

The fraying international consensus
With the postcrisis reforms near completion and the political environment becoming less supportive of international cooperation, global standard-setting bodies—particularly the Basel Committee on Banking Supervision and the Financial Stability Board—have less ambitious plans to introduce new standards than in previous years. Work to implement the remaining aspects of the G20 financial regulatory reforms has slowed, with many jurisdictions behind in implementing Basel III (“Basel IV” to industry).10

Given the current economic conditions, political concerns will grow if regulation is seen to impede competition, new lending or investment. We are already seeing a deregulatory stance from the US authorities, including a limited relaxation of the Volcker Rule.11 Other countries may follow, and we might even see competitive deregulation.

While deregulation might reduce some compliance costs, global firms will face more complexities and expenditure as regulatory standards across jurisdictions diverge in timing and substance. The G20 highlighted market fragmentation was an area of concern in 2019, and the Financial Stability Board has an ongoing work programme in this area.12 It is unlikely that global standard-setters will be able to reverse fragmentation that has already happened, but their efforts could reduce future divergence.

More accountability for senior individuals
In contrast, regulators are increasingly holding senior individuals to account for the compliance, professional standards and culture of their firms. Following the introduction of the UK’s Senior Managers and Certification Regime, similar regimes have emerged, or are emerging, in several other jurisdictions, including Ireland, Australia, Hong Kong Special Administrative Region, Singapore and South Africa. Other jurisdictions are driving increased accountability through different mechanisms. The US Federal Reserve Board has proposed guidance which seeks to delineate the roles, responsibilities and accountabilities of senior management and the board better.13 The Belgian Parliament recently announced the introduction of a “Banker’s Oath” similar to that which the Netherlands introduced in 2015.14 In response to these initiatives, firms will need to foster a culture of accountability through measures such as balanced incentive plans; strong governance and controls; and appropriate monitoring, reporting, escalation and disciplinary action.

Regulating technological innovation
Policymakers and regulators will continue to be challenged by the need to respond to the pace and scale of technological change. The financial services regulatory debate will be characterised by issues such as whether to expand the regulatory perimeter, risks associated with increasing use of artificial intelligence, the impact of innovation on operational resilience and cybersecurity, and digital ethics. These are global issues, but a lack of political will and adequate international bodies in some policy domains will likely hinder efforts to align regulatory approaches.

Cross-sector policies will increasingly affect financial services firms, although these will differ across regions. For example, in relation to data protection, the EU is taking a stricter stance on individuals’ right to access and control personal data than the US and China.15 Globally, the emergence of tighter data localisation requirements will also introduce additional obstacles to cross-border data flows.

The growing evidence that ineffective implementation of technological change can increase cyber and operational risk is also attracting regulatory scrutiny. International standard-setters will likely try to establish baseline common approaches for operational resilience, but we expect progress on cyber-resilience to be made mostly at the G7 and European levels.

These trends will affect firms’ ability to use and share data to innovate, enhance their cross-border resilience, and deliver value and security to their clients.

Regulators and supervisors will also need to accelerate their own digital transformation. Well-resourced regulatory data science and analytics capabilities will be essential to understand and supervise a financial sector characterised by an increasingly blurred regulatory perimeter and greater technological complexity. Part of the solution may be for financial, security and data protection authorities to share resources, capabilities and insights more effectively. We see efforts in this direction, but more work is needed before regulators and firms can reap the benefits. Progress will more likely be achieved at national than at international level, mainly because of the absence of cross-sectoral global standard-setting bodies.
Responding to social concerns

Environmental sustainability is a rising social concern, and in Europe and Asia, a major focus for financial services regulators. In the US, it is not—at least not at federal level. However, even where regulators do not introduce specific requirements, firms will need to consider how climate change and unsustainable business models will affect their asset and liability exposures, as well as the new opportunities that may arise from the increasing customer demand for “green” products, including green investment funds.

Financial inclusion is another area of focus globally. The World Bank Group estimates that in 2017 there were still 1.7 billion adults without a basic transaction account, primarily in Asia and Africa. It has a goal for all adults to have access to an account to store money and make payments by 2020. In developed countries, regulators are focused on barriers to financial inclusion such as overly complex processes and lack of accessibility for “nonstandard” customers, including the elderly or people with disabilities. Firms should expect to be challenged by regulators if their services are unduly hard for certain groups to access.

Conclusion

Although the postcrisis wave of regulatory change is subsiding, there is much to attract regulatory and supervisory attention in 2020, and firms should not expect scrutiny to abate. Against a darkening economic background, there will be increased focus on firms’ financial and operational resilience, how they adapt to technological change and innovation, and how they respond to political and social pressures in areas such as sustainability and financial inclusion. In an environment where boards and individual senior managers are increasingly being held to account for their actions, financial services firms will need to ensure they have the foresight, governance, skills and operational capabilities to adapt and respond effectively.

1. International Monetary Fund, *World Economic Outlook*, October 2019
3. International Monetary Fund, *World Economic Outlook*
5. International Monetary Fund, *World Economic Outlook*
7. Japan Financial Services Agency (JFSA), *Publication of summary points from JFSA policy assessment and strategic priorities 2019, August 2019*
13. Federal Reserve Board, “Federal Reserve Board invites public comment on two proposals: corporate governance and rating system for large financial institutions,” August 2017
15. The EU General Data Protection Regulation introduced rules on the collection and use of personal data, including, for example, the obligation to limit the amount of data held to that which is necessary for the stated purpose, and the right of individuals to have their personal data erased in certain circumstances.
16. In the EU, the European Commission has adopted an action plan on financing sustainable growth. In Asia, regulators in several countries (including Australia, Hong Kong Special Administrative Region, Japan and Singapore) have also released goals to promote sustainability in financial services. In Singapore and Hong Kong Special Administrative Region, this includes developing ESG reporting guidelines for financial services firms.
Introduction

With the increasing prevalence and effectiveness of technology around the globe, the status quo is no longer an option. To keep up with the pace of change, the insurance industry should continue evolving its approach to keep up with the myriad of challenges that it is facing, and more importantly, the opportunities that it can take advantage of in this fourth industrial revolution. Regulatory, legal, and compliance functions are being asked to do more with less while grappling with new and emerging challenges that stem from the near-ubiquitous use of advanced technologies to meet the increasing cost pressures and need to deliver value beyond limitations with traditional approaches to testing, monitoring, analysis, and supervision.

In this digital world, new threats are emerging along with new laws and regulations to help protect consumers and the markets. Regulators, both domestic and foreign, are focused on data privacy protections to mitigate the risks that result from improper collection, handling, storage, and use of data. Cyber threats continue to become more sophisticated and more damaging, putting even more urgency around developing protections from bad actors, both external and internal.

Against this backdrop, insurance companies should continue to modernize and rationalize their regulatory, legal, and compliance functions and their practices. Insurance companies that take a holistic view of regulatory risk management may find efficiencies that can lead to streamlined and rationalized programs. A modernized compliance function can help insurance companies achieve compliance as efficiently and effectively as possible by “thinking forward” and then harnessing the leading available compliance practices and technologies to comply with current and future regulatory requirements. Some companies are even looking at their regulatory and compliance risk management programs as a competitive differentiator that enables them to be more nimble in the market place.

Regardless of how the changes promulgated by lawmakers and regulators affect insurance companies, it is imperative that they continue to modernize and rationalize their regulatory, legal, and compliance risk management programs so that they can meet applicable laws, regulations, and oversight and monitoring expectations in a sustainable, proactive, and cost-effective way.
Privacy compliance with data management upgrades

Insurers have spent a lot of time and money preparing to comply with the European Union’s General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). But have they done enough?

The immediate concern, particularly for those subject to the new CCPA once enacted, is implementation and execution of compliance plans. Have insurers done enough to meet the new standards and avoid potential stiff penalties and reputational damage, or are there elements they have overlooked? What course corrections still need to be made?

Looking ahead, insurers need to brace themselves for additional regulatory initiatives. For example, New York is debating its own stringent privacy rule that goes further than either GDPR or CCPA by establishing insurers and other data collectors as information fiduciaries and allowing private causes of action.¹

The good news for organizations with a global footprint is that much of the effort that has gone into GDPR compliance overlaps with what needs to be done for CCPA (see figure 1). Also, the European Court of Justice recently ruled that the GDPR’s “right to be forgotten,” which allows individuals to ask that their personal information be removed from websites, news articles, and databases, cannot be applied outside the European Union.² In essence, this means such a right will not exist in the United States without federal or state laws mandating it, easing the burden on insurers with US operations.

---

**Figure 1: Insurers can leverage GDPR preparedness for CCPA**

**GDPR**
- Mandatory breach notification (covered under other California laws)
- Data Protection Impact Assessment (DPIA)
- Governance specific requirements (e.g., policies, procedures)
- Privacy by Design (PbD)
- Supervisory/regulatory authority authorization for certain types of processing
- Mandatory Data Protection Officer (DPO)
- Requirements specific to data processors
- Cross-border transfer requirements
- Processing bans
- Supervisory authority right to audit
- Restrictions specific to automated decision making

**CCPA**
- Right to limit the sale of PI
- Unable to discriminate the services or products provided based on opting out of the sale of PI

*Although required by both the CCPA and GDPR, there are specific requirements to demonstrate compliance with the CCPA.

Source: Deloitte Development, LLC
Tackling privacy and data management in 2020

Many insurers are struggling to meet the new regulatory requirements because their siloed legacy systems lack integration. The overwhelming volume of data being maintained can also be a problem. Insurers should consider establishing a more comprehensive information governance program that addresses these and other data management and privacy challenges, not just to meet compliance standards, but also to enable better business decisions and actions.

One potentially helpful approach is data minimization, which involves setting protocols to automatically flush superfluous information on a regular basis. Insurers are learning that one of the leading ways to protect sensitive information from a breach is to carefully and legally discard that information when it is no longer needed for legal or business reasons.

Insurers should also realize that regulatory compliance is only half the story. From a business perspective, insurance companies should consider increasing their engagement with customers to better utilize all the new data at their disposal—for the mutual benefit of the company and the customer. Treating data as a tradable asset that consumers knowingly and willingly exchange for something of value could be turned into a competitive advantage.3

Key questions to ask

Insurers need to know exactly what and where data about specific consumers is being stored, how complete and accurate it is, and how it is being used and protected. They should also ask themselves:

- Do we have the appropriate leadership, structure, capabilities, resources, collaboration, and support to manage data privacy risks in the context of our business model and goals?
- Have we organized our compliance and privacy functions to best provide support for—and oversight of—our business and operations?
- How do our information governance programs and capabilities stack up against industry standards and our industry peers?
- What new uses and technologies for data are planned, and how might we engage with customers more effectively to access data in return for added value?
- Does our chief privacy officer have the skills and stature to coordinate privacy and data governance efforts across the organization—and to positively affect the customer experience?

The answers to these questions can help insurance organizations understand where they stand and determine the right path forward to developing an effective privacy compliance program. For more information on what organizations can do, we encourage you to read our recent paper Data privacy as a strategic priority: Enabling growth and innovating by using information governance to effectively manage data privacy risk.

Let’s talk

Jay Cohen  
Managing director  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
jaycohen@deloitte.com

Tim Cercelle  
Managing director  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
tcercelle@deloitte.com

Best interest industry sales standards

The insurance industry is facing transformative changes to its sales conduct standards, driven by important new federal securities and state insurance regulations. While these regulations vary considerably in scope (affected sales professionals and products, disclosure obligations, etc.), they all reflect an ongoing trend towards acting in the client’s best interest and requiring heightened standards that go beyond existing suitability obligations when providing advice and recommendations to clients.

On June 5, 2019, the US Securities and Exchange Commission (SEC) voted to adopt new principles-based rules and interpretations in its “Regulation Best Interest package, including Form CRS Relationship Summary and other interpretations (Reg BI).” Reg BI requires broker-dealers (including insurance-affiliated broker-dealers) and their registered representatives to act in the “best interest” of their clients when providing securities transaction and/or investment strategy recommendations, including those related to variable life and annuity products. The compliance date for Reg BI is June 30, 2020.

Reg BI requires broker-dealers to satisfy four important obligations:

• Care obligation
• Disclosure obligation
• Conflicts of interest obligation
• Compliance obligation

The SEC has also clarified certain aspects of the fiduciary duty that investment advisers owe to their clients. The Investment Advisers Act of 1940 specifies a duty of care and loyalty that at all times requires an adviser to “serve the best interest of its client and not subordinate its client’s interest to its own.”

Similarly, although different in scope and approach, the New York Department of Financial Services’ (NYDFS) Regulation 187 – Suitability and Best Interests in Life Insurance and Annuity Transactions (Reg 187) sets forth important requirements for insurers and producers (i.e., insurance agents/registered representatives) who provide recommendations for the purchase of annuity products (effective August 1, 2019). It also sets forth requirements for life insurance products (effective February 1, 2020). Reg 187 covers policies and contracts delivered or issued for delivery in the state of New York. Importantly, the scope of Reg 187 includes noninvestment life and annuity insurance products, as well as variable insurance products. Some of the regulation’s other requirements relate to preventing financial exploitation and abuse, producer training, producer titles, and an effective system of supervision.

Overall, the regulatory landscape is becoming hazier as multiple states introduce legislation focused on different requirements for investment and financial advisers, such as fiduciary duties, conflicts of
interest disclosures, best interest standards, and fee transparency.

At their core, all of the various requirements are intended to address the inherent conflicts of interest associated with recommendations by producers. Affected professionals are expected to be unbiased and not place their own financial interest above their clients’ when providing recommendations. Note that the standards do not require firms and advisers to recommend the lowest-cost product, but more aptly recognize that there are a variety of available products that may meet a client’s needs and objectives, as well as a variety of compensation models—fee-based and commission-based—that may align with a client’s best interest.

Firms will likely face significant strategic and operational decisions as they analyze the various regulations and implement measures to meet the requirements. Impacts will likely span a wide range of areas, including product offerings; conflicts analysis; producer compensation and incentives; various client disclosures; documentation to support producer recommendations; and supervisory and compliance policies, procedures, monitoring mechanisms, and recordkeeping.

Effective planning and implementation to meet the various requirements will require strong governance, as well as integrated planning and decision-making across multiple workstreams. It will also require significant involvement from the IT function.

Let’s talk

George Hanley
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
ghanley@deloitte.com

Mike Ruiz
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
miruiz@deloitte.com


Market conduct

Market conduct exams continue to be a hot topic in the insurance industry. Recently, regulators have been increasing their use of examinations to ensure consumers are protected and to verify that insurers are complying with statutes and regulations and adhering to their filings.

This uptick in exam activity shows how serious regulators are about ensuring compliance, as do recent multimillion-dollar fines and remediation activities that required insurers to go back several years in order to make consumers whole.

In addition to rising fines, the costs of compliance and remediation are also rising to a point that the mere thought of a market conduct exam can cause some insurers to cringe at the time and expense required to respond.

**Key areas of regulatory scrutiny**

Data analytics are gaining importance as regulators analyze Market Conduct Annual Statement (MCAS) peer data looking for outliers. Data calls are another tool regulators are using to increase their vigilance and industry monitoring. Activities likely to attract regulatory scrutiny include increases in complaint ratio, large increases or decreases in premium volume, significant changes in a company’s book of business, rapid expansion in a new state or states, and heavy reliance on third parties for key business functions. Market conduct exams can cover a variety of areas, with regulators focusing on just one area or multiple areas. If issues are found in one area, examiners will often expand their examination to include additional areas. This expanded scope can cost an insurer significant time and money.

Typical examination areas include sales practices, claims, underwriting, forms, sales materials, complaints, policy issuance, new business and/or renewals, policy administration, customer service, suitability, replacements and surrenders, fees and charges, and agent licensing.

In addition to typical market conduct exams, the NYDFS has begun to conduct a cybersecurity regulatory examination process. According to superintendent Linda A. Lacewell, “As technology changes the financial services industry, regulation must evolve, and [NYDFS] is evolving to meet the challenges and opportunities of the new landscape, to protect consumers, safeguard the industry, and encourage innovation.”

Meanwhile, Financial Industry Regulatory Authority (FINRA) continues to actively examine insurance companies that include broker-dealers, scrutinizing conduct in key areas such as insider trading, money laundering, improper use of funds/forgery, quality of markets, best execution, reporting/provision of information, sales practices, recordkeeping, compliance procedures, sales practices and suitability, communication with the public, disclosure of conflicts of interest, net capital requirements, and supervision.

At the National Association of Insurance Commissioners (NAIC), the Big Data Working Group continues to focus on data algorithms and models, particularly those using data from third parties, since many of those external vendors are not regulated entities and their data could contain inaccuracies and inherent biases. Regulators are educating themselves on these sophisticated data models—including how the models operate and the potential impacts of their components—so they can effectively assess the models’ appropriateness in the marketplace.
Getting ahead of the curve

Insurers can take steps to prepare for or mitigate potential market conduct activity by proactively monitoring compliance with policies, procedures, statutes, and regulations. Helpful tools include self-assessments, mock market conduct exams, self-analysis of MCAS data to look for significant year-to-year variances, and use of data analytics to identify outliers or points of noncompliance that might attract the attention of regulators. Insurers should also closely monitor their rate compliance to ensure the rates they charge consumers comply with what has been filed and approved. A firmly established three-lines-of-defense model for risk mitigation can help monitor risk and noncompliance throughout an organization.

Innovative technologies such as robotic process automation (RPA), combined with natural language processing (NLP), higher-order cognitive technologies, and artificial intelligence (AI), can help enable end-to-end product oversight, as well as monitoring of market reactions and regulatory actions. These technologies can also be enablers for a talent transformation, freeing up people in the compliance function to focus on high-value work beyond reporting. Insurers not yet exploring such technologies might find it useful to create a framework that can help them appropriately leverage talent and technology to cope with a world of increased market conduct oversight.

Let’s talk

Jay Cohen
Managing Director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
jaycohen@deloitte.com

Fraud

Many insurers continue to struggle identifying and reducing both hard and soft insurance fraud within their companies, a problem that costs the industry $80 billion annually. Fraud is perpetrated by different parties involved in the insurance transaction life cycle, including applicants for insurance, policyholders, third-party claimants, internal employees, and professionals who provide services and equipment to claimants.

Fraud activity is up 62% year-over-year, often driven by the extensive theft of personal data and the continued digitization of insurers. Recent studies reveal a number of customer soft fraud incentives—belief they can get away with it, belief that insurance costs too much, desire to recover the deductible, and poor customer service—all of which motivate retribution.

During the Anti-Fraud Taskforce session of the most recent NAIC Summer Meeting, there were discussions about how to make the process more efficient for companies to submit antifraud plans to the states and also how to consolidate state-specific requirements for the antifraud plans. The Coalition Against Insurance Fraud noted that 174 antifraud bills have been introduced into legislation within the states, so the fraud epidemic is clearly on the minds of regulators and legislators.

Also, in July 2019, the National Council of Insurance Legislators amended the Insurance Fraud Model Act, which had last been updated in 1998. The major changes included increasing authority for prosecutors, streamlining the proof of intent to defraud and how the intent to defraud is identified, and eliminating multiple-proof requirements in many areas to allow for greater prosecution.

Most states require insurers to document and submit their antifraud plan to the state’s department of insurance. These antifraud plans outline the company’s procedures (appropriate to the type of insurance provided by the company) to prevent, detect, and investigate fraud in applications for insurance, renewal documents, rating of insurance policies, claims fraud, and security of the company’s data processing systems.

Although companies have documented antifraud plans, do they know how effective they are? How are they measured?

Types of fraud
Insurers should manage against several different types of fraud threats, both internal and external, including:

- **Adverse selection.** Withholding information from an insurer (e.g., not disclosing poor health status on an application).

- **Agent fraud and/or sales risk.** Commission theft via falsified sales (e.g., fictitious policy, misclassified type of sale to meet a sales goal or contest) or fraud against the customer (e.g., theft of account value, unsuitable sale).

- **Cyber risk.** An attack on an organization’s IT system targeting sensitive client data (e.g., hacking or phishing), often resulting in financial and/or reputational losses.

- **Employee theft.** Misuse of an employer’s assets (e.g., embezzlement, insider threat, intellectual property theft, conspiring with outside actors) often enabled by insufficient segregation of duties and controls.
Known-party account takeover or impersonation. A known-to-you party, such as an agent or family member, pretending to be someone else in order to gain access to an account and take or misdirect cash value, premium, payments, etc.

False claims or information. Submitting false claims or information for injuries or damage that never occurred, services never rendered, equipment never delivered or owned, attributing a prior condition to the current event, or providing an incorrect loss date to bring a claim into the coverage period.

Third-party account takeover or impersonation. A third party pretending to be someone else in order to gain access to an account and take or misdirect cash value, premium, investment contribution, payments, loans, etc.

Underwriting misrepresentation. Misrepresenting facts on an insurance application (e.g., falsely claiming not to smoke).

Traditional fraud management typically handles business risks in silos: a fake customer account here, a padded claim there. It’s an inefficient model that is not able to quickly counter evolving fraud schemes and behaviors. Thus, insurers keep suffering loss—and constantly seem one or two steps behind—despite experience that indicates that enhanced analytics yields a favorable return on investment through increased prevention and recovery.

Three core principles
Many companies are beginning to break down those silos by assessing their Enterprise Fraud Management Risk across three high-level core principles: govern, manage, and operate.

Govern
• Enterprise strategy that defines the antifraud function role and fraud program objectives and establishes a forward-looking strategic roadmap
• Organizational and governance components for an effective fraud program that include roles and responsibilities, goals and objectives, policies and procedures, transparency, and culture/awareness in order to manage fraud risks across various businesses

Manage
• Policies, standards, and procedures defining fraud, activities across the antifraud life cycle, and integration points between functions to improve consistency and quality in program activities
• Coordinated communication channels and programs to educate stakeholders about their responsibilities at all stages of the fraud program life cycle

Operate
• Due diligence and ongoing oversight that an organization should consider exercising throughout the fraud program life cycle, including a fraud risk assessment that aligns risks and controls and that measures residual risks
• Aligned technologies to support fraud prevention and detection; use of advanced analytics, behavioral economics, and adaptive behaviors
• Metrics and reports that provide a comprehensive view of enterprise fraud risk to the relevant stakeholders across the organization, including cost/benefit analysis considerations

Don’t operate in a digital future with an antifraud strategy from the analog past.
Traditional fraud detection depends on rules, which requires fairly specific knowledge of previous fraudulent behaviors. It is also labor-intensive, since it requires subject-matter experts to write, apply, and continuously modify the rules. A modernized approach using advanced analytics—whether through real-time, near-term dynamic, and longer-term scanning/emerging threats—can help a company respond to gaps in current processes and/or improve controls and monitoring for fraud. Key capabilities include:

• Anomaly detection. Identifying patterns inconsistent with “normal” activity through statistical profiling/outlier detection; might include data from external sources and social media.
• Machine learning. Detecting how issues relate to one or more other factors using patterns uncovered within historical data.
• Text/voice analytics. Unlocking patterns trapped in unstructured data and developing measurable data points to use for modeling.
• Network analytics. Discovering associations between similar and related entities to identify fraud networks and other collusive behavior.

By applying an updated approach to discovering and preventing risk across the modern digital enterprise, as well as leveraging tools that might already be in use somewhere in the business, companies can gain high-value risk insights. They can then use those insights to
dramatically improve operational and strategic decision-making.

Benefits of improved enterprise fraud management

The incentive to begin this work is quite powerful. A new approach to enterprise fraud management can provide organizations with many benefits, including:

• Substantial, concrete near-term return on investment resulting from the detection and resolution of current inappropriate business activities

• Strategically improved ability to predictively protect the business and the brand from a wide range of previously unidentifiable dangers—including internally and externally perpetrated fraud, nonmalicious employee errors, compliance failures, and cybersecurity issues.

• Enhanced credibility with compliance auditors resulting from the differentiated level of diligence, as demonstrated by the adoption of innovative self-policing.

• Better long-term business performance through reduced financial leakage, optimized brand value, and more secure lifetime relationships with customers, vendors, and other stakeholders.

Moving forward, the industry (including regulators) should continue looking for ways to educate consumers about the products available in the marketplace, their purpose, and the components of the policy (including deductibles). Educating consumers about insurance products—and fraud in general—can affect their behavior patterns. Consumers need to understand the impact of fraud on the industry—and that fraud is a major crime that does more than cost companies money. These nudges can have a significant impact on consumer behavior and reduce the perception of insurance fraud as a normal cost of doing business.

1. https://www.insurancefraud.org/statistics.html#1
Conduct risk

The mitigation of conduct risk continues to be a key area of focus for insurance companies globally. The heightened regulatory scrutiny over the way insurers and their employees and agents interact with customers and markets has persisted and, in some cases, increased. There is also increased regulatory focus in certain new jurisdictions. In addition, the behavior of customers is now being carefully considered in the overall conduct ecosystem, since various forms of fraud are widely perpetrated on all insurers, driving up product rates and overall expenses.

While insurance companies have been addressing these requirements through enhanced control environments, global regulators have similarly been investing in their oversight capabilities and have developed increasingly sophisticated tools and techniques to identify potential insurer misconduct. With this, we continue to observe conduct-related incidents that result in substantial fines, penalties, and potential reputational damage for insurers and other financial services firms.

Regulatory guidance with respect to conduct risk has to date been primarily principle-based rather than rule-based. This principle-based guidance has led the industry to adopt a variety of different approaches. However, there is now increasingly broad consensus among insurers that any effective solution to these areas will involve companies making intelligent use of technology and advanced analytical tools.

Technology can enable insurers to work with large datasets to detect misconduct by identifying trends and anomalies dynamically rather than trying to codify static use cases and thresholds that are much harder to calibrate and easier to manipulate. Similarly, technology is also playing a key role in designing solutions that link compensation to conduct in a more consistent and transparent fashion. Concurrently, insurers have begun to explore and leverage nudging techniques and other methods from behavioral economics to guide the behavior of employees, distributors, business partners, and customers.

Detecting and preventing misconduct

Insurers should manage against numerous types of misconduct, both internal and external to the organization.

External misconduct
One characteristic that makes the insurance business unique is the significant level of risk stemming from external fraud and other misconduct by customers and third parties. Common types of external misconduct can be found in the fraud topic that preceded this.

Traditional fraud management typically handles such risks in silos: an omitted disclosure here, a padded claim there. However, this inefficient model is unable to quickly counter evolving fraud schemes and behaviors. As a result, insurers keep suffering losses and constantly seem one or two steps behind the fraudsters.

Internal misconduct

In recent years, many insurance companies have made significant investments in ramping up their misconduct detection capabilities within the first and second lines of defense. These efforts have been driven by regulatory impetus globally and by the advent of more sophisticated tools and technology that allow for advanced monitoring and surveillance. The Market Abuse Regulation framework that took effect in mid-2016 is a prime example of the regulatory focus on further strengthening the market abuse framework and expanding the scope of behaviors that insurers and other financial services firms are expected to detect and monitor. However, a large portion of the industry continues to struggle with significant gaps in coverage across regions and products, as well as with developing a holistic framework that can adapt to new and evolving risks. Common pitfalls we observe in the industry include:

- Gaps and inconsistencies in monitoring and surveillance coverage across global regions. Typically, the focus has been on large operations in EMEA and North America, with more significant gaps existing in other regions and smaller countries.
- Inability to adapt monitoring and surveillance tools to identify newer patterns of behavior, as opposed to focusing on simple rule-based monitoring and surveillance that only looks for static thresholds
- Focusing on data sources in silos rather than linking various data sources together.
sources (e.g., the inability to link information from communication surveillance to information from product sales and suitability surveillance)

- Supervision framework inconsistencies that limit supervisors’ ability to generate meaningful insights from the monitoring and surveillance data that is presented to them
- Lack of high-quality data to monitor and surveil, especially for large global organizations with multiple sources of data across geographic and system boundaries

We believe that the use of more sophisticated analytical tools will be an important piece to solving the monitoring and surveillance puzzle. Increased industry adoption of cloud platforms can also further unlock powerful data analysis capabilities. As insurers refine their misconduct monitoring and detection capabilities, they should evaluate how to connect different types of data, including transaction data, communication data, and other employee and distributor indicators. Also, insurers should better define the risk prioritization criteria as they roll out monitoring and surveillance capabilities to various geographies and businesses. The risk prioritization should consider the inherent risk profile of the business and the maturity of other mitigating controls, as well as any other region- or country-specific risk or regulatory drivers.

Linking employee conduct with compensation to drive culture

While many insurance companies, as part of their conduct risk management programs, have made enhancements to their performance review processes, compensation continues to largely be based on financial metrics. Regulators globally have highlighted the need for insurers and other financial institutions to rethink their performance review processes and incorporate nonfinancial metrics into their performance management frameworks. The US Department of Justice 2019 Guidance Document on the Evaluation of Corporate Compliance Programs specifically calls out incentives as a “hallmark of effective implementation of a compliance program” to incentive compliance and ethical behavior.

Insurers should be considering how to take the financial and nonfinancial performance data collected as part of their conduct risk management program and apply it to year-end performance evaluations and determination of compensation. This would likely include providing managers with relevant metrics, scorecards, and summaries of various conduct and compliance infractions for their employees. Common pitfalls during implementation of such approaches include:

- Failing to apply meaningful reductions to compensation that truly reflect both the nature and severity of conduct and compliance infractions. Reductions in compensation should be large enough to provide an effective disincentive for future misbehavior. Furthermore, individual infractions should be made known to other employees in order to create a sentinel effect that discourages further misconduct elsewhere in the organization.
- Failing to clearly document the link between compensation adjustments and conduct and compliance infractions. Companies should be able to show the original proposed compensation and then any reductions arising from infractions, with the link explicitly documented and communicated to the employee.
- Failing to maintain adequate documentation and supporting rationale for decisions related to compensation adjustments. Companies should have a clear record of why adjustments were made (or not made) for conduct and compliance infractions.
- Considering conduct and compliance infractions only during financial compensation. Companies should also consider conduct and compliance infractions during promotion cycles and when doling out additional responsibilities.
Looking ahead
We believe this topic will likely be a key focus area for the industry in 2020 and that insurance companies should proactively use advanced technology and data analytics capabilities to detect and manage internal and external misconduct more effectively. Also, to drive the appropriate internal behaviors, companies should make conduct data available to managers and employees throughout the year as a central part of ongoing performance management discussions. A well-defined linkage between conduct and compensation can not only help insurers reinforce good conduct, but also serve as a key driver for lasting changes in employee behavior and the overall organizational culture.

Development of capital standards for US insurers

The United States will have a group insurance capital calculation/standard for the first time (in addition to the existing legal entity risk-based capital (RBC) requirements). However, various proposals are still being consulted upon, and currently it is not clear exactly how insurers will be affected. For example, one proposal includes a capital buffer that could be used to limit capital distributions and discretionary bonus payments should insufficient capital be held.

The 2008 financial crisis prompted a variety of regulatory activities related to capital standards. The NAIC launched its Solvency Modernization Initiative (SMI) to review many aspects of the US regulatory framework, including RBC. US legislators passed the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), which subjected a number of insurance companies to Fed supervision. Globally, the International Association of Insurance Supervisors (IAIS), of which US insurance supervisors are a part, was challenged by the Financial Stability Board (FSB) to develop insurance group capital measures that would enable comparison of insurers’ solvency across jurisdictions (the United States has traditionally had a legal entity–based approach to monitoring insurers’ capital positions). Additionally, the International Monetary Fund (IMF) conducted its Financial Sector Assessment Program (FSAP) of the US insurance supervisory process and found that no supervisory tool existed to monitor group solvency.

Partly due to these various events and resulting initiatives, multiple US-based capital standards options are now being developed by regulatory bodies such as the Federal Reserve Board (FRB), the US states (through the work of the NAIC), and internationally under the IAIS. The proposed capital standards/calculations, which at some point will likely affect US-based insurers, are currently in varying stages of development. However, the objectives of each are largely similar: provide a commonly accepted method across the industry that enables insurers to understand and communicate their capital positions against the regulatory requirements they face.

In October 2019, the FRB invited public comment on a proposal to establish capital requirements for certain insurance companies supervised by the FRB. The proposal builds on existing state-based insurance standards while also establishing minimum capital requirements that are specific to the insurance business. Under the proposed framework, known as the Building Block Approach...
(BBA), holding companies significantly engaged in insurance activities would be required to aggregate their state-based capital requirements into a consolidated requirement. The proposal would establish both minimum requirements and a potential buffer on top of the minimum.

At the state level, US regulators are developing a Group Capital Calculation (GCC), which is a supervisory tool and not a standard, to monitor solvency across insurers. According to NAIC, “the GCC will be an aggregation method for use with groups that include a US insurance company, and it is intended to provide additional analytical information to the lead state for use in assessing group risks and capital adequacy to complement the current holding company analysis in the US.”

On the global stage, the IAIS is pushing forward with design and implementation of a global insurance capital standard (ICS). The objective of the ICS is to provide a common language, along with comparable outcomes, for insurance company regulatory capital. The ICS version 2.0 was approved at the end of November 2019, with an initial five-year monitoring period during which it will not be a prescribed capital requirement (PCR) but will be used by supervisors to monitor performance.

Upon implementation, each of these proposed capital standards/calculations could have a significant impact on US-based insurers, which means the domestic insurance industry is likely approaching a pivotal point in this important regulatory area. Insurers should understand the various proposals and their potential impacts and, if necessary, take the opportunity to provide input into the regulatory consultation processes while there is still time.

---

Impact of international regulatory trends on US regulations

The IAIS published The IAIS Strategic Plan 2020–2024 in June 2019.¹ The strategic plan sets a new direction that is described as a pivot from working to implement past reforms toward emerging industry risks and trends. Going forward, the IAIS’ core functions are defined as follows:

- **Assessing and responding to market developments.** Monitoring and scanning key risks and opportunities by leveraging the membership base of more than 200 supervisors.
- **Standard setting.** The IAIS has spent many years developing and agreeing to supervisory standards and will continue to maintain this effort as needed. However, the focus will be on monitoring and assessing implementation of current standards. The IAIS will pilot a deep dive and conduct comprehensive member assessments to evaluate compliance and adoption of standards, which should help IAIS members understand how well they are meeting the minimum standards.
- **Supporting supervisory practices.** Supporting the implementation of supervisory material and helping supervisors adopt leading practices.
- **Supporting observance of standards.** Partnering to enhance supervisory capacity to improve the insurance market, and to enable supervisors to better supervise their local markets.
- **Effective operations and transparency.** Improving internal efficiency of the IAIS by creating a sustainable financial model that no longer relies on industry contributions.

IAIS activities will focus heavily on certain key themes over the term of the 2020–2024 strategic plan. Many of the IAIS key themes are areas of common interest with other standard-setting bodies, but with an insurance-specific perspective, including:

- **Technological innovation.** Financial technology (fintech) presents significant opportunities for financial inclusion and policyholder value, but also poses significant operational and underwriting risks. The rapid expansion of alternative data sources and advanced data analytics has the potential to disrupt the insurance market.
- **Cyber resilience.** Insurers are not only exposed to cyber risks, but also actively take on cyber risks through their cyber underwriting activities.
- **Climate risk.** Insurers are exposed to transition risk as institutional investors, as well as physical risk from natural disasters through their underwriting. They can also be key agents in the mitigation and management of climate risk.
- **Conduct and culture.** Technological changes to the insurance business model present new conduct challenges. A holistic approach to market conduct and prudential supervision is needed, recognizing that conduct and culture issues could lead to financial soundness and stability concerns.
- **Financial inclusion and sustainable economic development.** Insurance supervision has an important role to play both in the insurance market and in overall economic development. Policyholder protection and contributing to financial stability are fundamental to ensuring the insurance sector’s sustainable involvement in closing the protection gap.

The 2020–2024 strategic plan will also see the IAIS continue to support and implement existing standards that contribute to global financial stability, such as an ICS. The high-level goals and strategic themes of the plan can help IAIS members respond to the new risk environment and can help shape future regulatory trends in the United States.

Note: The strategic plan was approved by the entire IAIS membership at the time of the 2019 IAIS Global Seminar in June 2019.

The rise of third-party risk

According to Deloitte Touche Tohmatsu Limited’s Extended Enterprise Risk Management Global Survey, 1 83 percent of organizations experienced a third-party incident in the past three years. Of these, 11 percent experienced a severe impact on customer service, financial position, reputation, or regulatory compliance, and 35 percent experienced a moderate impact.

An uncertain economic and business outlook affects third-party risk management (TPRM) by forcing organizations to challenge TPRM budgets and investments, increase operational efficiency to reduce costs, and rethink their strategies on the activities for which to engage third parties.

Third-party cybersecurity risks are of particular concern. According to another study, 2 61 percent of US survey respondents experienced a data breach caused by one of their own third parties or other third parties in 2018, up from 56 percent in 2017. Using innovative and market-leading technology partners offers many benefits, but also introduces additional risks due to the inherent distributed architecture of cloud. As third- and fourth-party providers increasingly rely on cloud infrastructure to deliver best-in-class solutions, the requirements for shared responsibility and transparency will continue to grow.

Increased scrutiny of third-party risk is coming from two directions. Externally, regulators expect organizations to have compliance mechanisms in place. Internally, organizations have set up robust third-party risk management programs mirroring the scrutiny applied by regulators.

Emerging regulations

New federal and state regulations related to third-party risk management are emerging in all sectors of the financial services industry (FSI). Sector-specific developments are likely to affect or shape the regulatory environment in other sectors as well and should therefore be of interest to all FSI decision-makers.

State security and data protection laws affecting third parties

The NYDFS has enacted new regulations that apply to any person or entity required to operate under a license or registration under New York banking law, insurance law, or financial services law. These so-called “covered entities” include banks, insurance companies, and various other financial services institutions. The guiding principle of the regulations is that all covered entities must maintain a “robust” cybersecurity program designed to protect the confidentiality, integrity, and availability of its information systems.

As of March 1, 2019, all covered entities must have completed the following: implement third-party service provider security policies; complete identification and risk assessment of third-party service providers; identify minimum cybersecurity practices required by such providers to do business with the covered entity; enact due diligence processes to evaluate the third-party service providers’ cybersecurity policies and practices, including limitation of access controls, encryption of information, and notice procedures in the event of a cybersecurity event; and require periodic assessments of third-party service providers—both old and new—based on risk and continued adequacy of their cybersecurity practices.

Insurance

The NYDFS regulations are bringing industries and sectors into scope that previously were not scrutinized to the same degree as banks. Although the regulations largely focus on cyber risk, they are prompting insurance companies to examine—and in many cases improve—how they manage third-party risk in general. Insurers need to look at revenue-generating relationships from a risk angle. This includes performing additional risk assessments and adding controls to the management of such relationships.

The NYDFS regulations also apply to third parties that traditionally fell outside the boundaries of TPRM programs, such as brokers and agents, bringing them into scope. This has uncovered vulnerabilities that insurance companies have had to resolve at smaller, less sophisticated third parties with access to network and systems.
More broadly, the EU-US Insurance Project continues to regularly discuss insurer cybersecurity, the cyber insurance market, and big data issues. The insurer cybersecurity workstream, for example, is discussing the development of a template for a supervisor exercise to help improve cooperation and coordination of cross-border response in the event of an international cyber incident. One outcome of this workstream could be a cybersecurity exercise. The cyber insurance market workstream is examining nonaffirmative cyber exposure and the potential for catastrophic losses; the challenges of reinsuring cyber risk; and the availability of cyber insurance data, including lessons learned from cyber data reporting in the United States. It is also examining the potential for similar initiatives in the European Union. Meanwhile, the big data workstream is looking at third-party risk and other issues. The EU-US Insurance Project anticipates holding a seventh public event in Washington, D.C. in early 2020.

**Investment management**

The SEC has guidelines related to third-party resiliency, and third-party cyber continues to be a priority exam item. The SEC requires dealers that store information electronically to maintain a relationship with an independent third party that can access their records in the event of an audit or a request where the dealer is unable or unwilling to furnish the information. This is known as the Designated Third Party (D3P) rule.

Per the SEC guidelines, the following issues have been identified:

- **Misconfigured network storage solutions.** In some cases, firms did not adequately configure the security settings on their network storage solutions to protect against unauthorized access. In addition, some firms did not have policies and procedures addressing the security configuration of their network storage solutions. Often, misconfigured settings resulted from a lack of effective oversight when the storage solution was initially implemented.

- **Inadequate oversight of network storage solutions provided by a third party.** In some cases, firms did not ensure—through policies, procedures, contractual provisions, or otherwise—that the security settings on third party-provided network storage solutions were configured in accordance with the firm’s standards.

- **Insufficient data classification policies and procedures.** In some cases, firms’ policies and procedures did not identify the different types of data stored electronically by the firm and the appropriate controls for each type of data.

Compliance requirements under the SEC define rules around recordkeeping, preservation, and access. Known as SEC Rule 17a-4, these requirements and regulations require participating services firms (i.e., broker-dealers) to retain and make available all pertinent records related to the sale of securities—including prospectus content, communications, and transactional data—for purposes of satisfying investigations or audits related to regulatory actions or lawsuits.

**TPRM improvement opportunities**

Deloitte’s survey report extensively explores several key areas that are affecting the future of TPRM programs.

**Economic and operating environment**

To improve their processes, 53 percent of survey respondents said they seek, above all, a “more coordinated and consistent approach to TPRM across organizational functions.” The need to improve processes, technologies, and real-time management information for TPRM was ranked second (49 percent).

**Investment**

Half of respondents said they spend more than $1 million annually on TPRM operating costs, and the top 11 percent spend more than $10 million each and employ over 100 full-time equivalent staff. In specific risk domains, investment is skewed toward information security (68 percent of respondents); data privacy (62 percent); and cyber risk (58 percent). The survey also found many organizations underinvest in other domains, such as labor rights (18 percent), as well as geopolitical and concentration risk (both at 12 percent).

**Leadership**

Thirty-seven percent of survey respondents said better in-house coordination between leaders and risk domains, business units, and functions—such as procurement, legal, and internal audit—is a top TPRM priority.

**Subcontractor and affiliate risk**

Fifty percent of survey respondents said they do not understand the nature of their third parties’ relationships. Organizations also continue to lack clarity in their approach to monitoring and managing risks related to affiliates. Just 32 percent of respondents said their organizations apply the same rigor in evaluating and monitoring such risks as they do with third parties. Another 46 percent reported varying standards, including some degree of ambiguity or an ad hoc approach.
Digging deeper

The lack of appropriate oversight over subcontractors and affiliates to third parties makes it difficult for organizations to establish an effective strategy and approach for managing third-party risk. These risks are typically hidden in deeper layers of the third-party ecosystem, impairing a company’s ability to apply the appropriate discipline and rigor to managing third-party risk. This issue is particularly relevant in regulated industries, such as financial services, where systemic concentration risks are a significant cause for concern. However, recent legislation and regulation has extended the challenge to other industries as well by including requirements to manage relationships with fourth parties and beyond. These regulatory developments include the United Kingdom’s Modern Slavery Act and the European Union’s GDPR.

Leading organizations are starting to address the blind spots through “illumination” initiatives to discover and understand these networks within networks. Once a company understands who its critical subcontractors are, the next step is to understand what assurance its third parties are obtaining about these fourth parties. This assurance must be supported by evidence.

A number of organizations are going even further by forming combined inspection teams with their third parties to undertake assurance activities on fourth parties. Some are requesting the option to complete additional assurance activities themselves. Others are adopting a less invasive approach by using risk intelligence tools to understand critical fourth-party control environments (including financial solvency). In some cases, these organizations are insisting on the ability to veto subcontractors to the third party if they believe the subcontractors pose too much risk.

Tackling the challenges

System and organization controls (SOC) standards from the American Institute of Certified Public Accountants (AICPA) are evolving to address the need for better service organization oversight. Developments around SOC for cyber and SOC for supply chain are a direct response to the pressure service providers are feeling to satisfy these demands. Several changes have been made to the Trust Services Criteria, which will affect all service organizations that issue a SOC 2 report. Most significantly, control requirements have become more prescriptive in two areas: risk management and incident response. As a result, service organizations are now being pushed toward more standardized, robust, and mature processes—to the benefit of their customers.

Another new requirement helps SOC 2 report users understand the specific objectives that the service organization’s controls should be designed to achieve—for example, what security or processing integrity means in the context of the provided services and responsibilities of the service organization. The description of principal service commitments enables SOC 2 report users to better evaluate whether the service organization has implemented the right
controls. User organizations should review future reports to verify that principal service commitments are adequately described and that service organizations’ controls sufficiently address the new criteria.

From a technology perspective, TPRM capabilities can be viewed in three tiers:

• In tier 1, enterprise resource planning (ERP) or procurement platforms establish a common foundation and operational discipline for TPRM.

• In tier 2, there are two common approaches: TPRM-specific risk management packages tailored to an organization’s third-party management requirements or generic, integrated risk management solutions for TPRM use.

• Tier 3 supports the first two tiers by providing niche packages for specific TPRM processes or risks, providing feeds from specialized risk domains (such as financial viability, financial crime, contract management, sustainability, and cyber threats).

The implementation of a configuration management program that includes policies and procedures governing data classification, third-party oversight, and security features can help mitigate the risks incurred when implementing on-premise or cloud-based network storage solutions. During examinations, staff in the SEC’s Office of Compliance Inspections and Examinations (OCIE) have observed several features of effective configuration management programs, data classification procedures, and third-party management programs, including:

• Policies and procedures designed to support the initial installation, ongoing maintenance, and regular review of the network storage solution

• Guidelines for security controls and baseline security configuration standards to ensure that each network solution is configured properly

• Third-party management policies and procedures that include, among other things, regular implementation of software patches and hardware updates, followed by reviews to ensure those patches and updates did not unintentionally change, weaken, or otherwise modify the security configuration

Investments in managed services and shared assessments and utilities can drive efficiency by reducing the need for increased head count and dramatically reducing capital expenditures. Risk-sensing technology enables real-time evaluation and response, helping organizations keep up with the rapid pace of change. By engaging with external providers that offer both managed services and ongoing due diligence and monitoring of third parties (and the risks they pose), companies—especially those in FSI that have thousands of vendors—are able to transform from being reactive to proactive about managing third-party risk.

Let’s talk

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

Kevin Gallagher
Managing Director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
kjgallagher@deloitte.com

Jonathan Rizzo
Principal
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
jonrizzo@deloitte.com

John Hardwick
Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
jhardwick@deloitte.com

4. Deloitte, “All together now”
Staying ahead

The regulatory landscape is constantly shifting. Some changes are big enough to grab headlines. Others are nearly invisible but can have a big impact. For the latest regulatory updates and insights, please visit www.deloitte.com/us/InsuranceRegulatoryOutlook.

Leadership

**Alok Sinha**
Regulatory & Operations Risk Leader
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
asinha@deloitte.com

**Monica O’Reilly**
Advisory Financial Services Industry Leader
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
monoreilly@deloitte.com

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

This article contains general information only and Deloitte is not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser.

Deloitte shall not be responsible for any loss sustained by any person who relies on this article.

About Deloitte
As used in this document, “Deloitte” means Deloitte & Touche LLP, which provides audit, assurance, and risk and financial advisory services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2020 Deloitte Development LLC. All rights reserved.