Deloitte.

Leading in times of change

Banking 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 banking 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

Shift in focus to regulatory review and refinement

In the aftermath of the financial crisis and enactment of the D*odd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank)* in 2010, regulators put forth a substantial number of new or strengthened regulations and guidance documents. Now, after a period of real-world experience with these expanded requirements, some lawmakers and regulators appear to be stepping back to evaluate what is and isn't working, and make adjustments as necessary.

These themes are playing out both at a legislative level and at the banking regulatory agencies, which have substantial authority to adjust regulations within the confines of existing law. Actions being taken or contemplated include "right-sizing" regulatory requirements (e.g., adjusting obligations for banks under $250 billion), amending requirements perceived overly burdensome in practice (e.g., Volcker regulations), and refining expectations communicated to banks by regulators (e.g., the Federal Reserve Boards's [FRBs] board governance proposal).

Here, we discuss several of these shifting initiatives and how they might affect your bank.

At the legislative level, Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA)[1] was signed into law in May 2018. The law raises the "systemically important financial institution" (SIFI) threshold for banks from $50 billion to $250 billion. However, in terms of timing, the law immediately raised the threshold to $100 billion, while giving the FRB 18 months to tailor the SIFI requirements for banks between $100 billion and $250 billion.

In addition, the law eliminates the company-run stress test requirement for banks under $250 billion (with an 18-month off-ramp for banks from $100 billion to $250 billion). It also eliminates the annual Dodd-Frank supervisory stress testing requirement for bank holding companies (BHCs) with less than $250 billion in assets, although requiring periodic supervisory stress tests for firms from $100 billion to $250 billion.

The law contains a number of other provisions, such as a less restrictive definition of "high volatility commercial real estate" (HVCRE), and adjustments to the leverage ratio for custodial banks. Small institutions receive relief in a number of areas including: residential mortgage lending requirements, Volcker Rule exemption, home mortgage disclosure act (HMDA) exemption, and an increase in the threshold to qualify for an 18-month examination requirement.

EGRRCPA does not directly or immediately amend regulations written by the banking regulatory agencies; therefore, banks should remain aware of the content—including timing—of such regulations as they are rewritten going forward. Also, even though company-run stress-testing requirements have been eliminated, regulators will likely still expect banks to conduct stress tests as a part of their overall risk-management framework, including the sizing of risk appetites.

As we look forward to the 2019 legislative agenda now that the 2018 midterm elections are over, the Democratic Party leadership has indicated that the House Financial Services Committee will broadly focus its efforts toward protecting consumers and investors, preserving financial sector stability, and encouraging responsible innovation in financial technology. Meanwhile, we expect that the Republican-controlled Senate Banking Committee will continue to focus its legislative agenda on remaining refinements not already addressed in the EGRRCPA 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, banking organizations should continue to drive effectiveness and efficiencies across their risk and compliance programs so they can meet applicable laws, regulations, and supervisory expectations.

For 2019, how future legislation, rules, and guidance will be tailored in practice will be an evolving story. A key case in point is the US final rule to establish single-counterparty credit limits (SCCL) for large US BHCs and foreign banking organizations (FBOs) that was issued in June 2018.[2] The final rule represented the first instance where the FRB has applied the new thresholds based on the EGRRCPA and acted as a precedent for FRB applications of the threshold.

In a more direct response to EGRRCPA mandates, the FRB in October 2019 proposed tailoring the Enhanced Prudential Standards (EPS) framework for large, domestic banking institutions.[3] The proposed framework, which applies to all domestic BHCs and non-insurance, non-commercial savings and loan holding companies (SLHCs) with more than $100 billion in total assets, includes two proposals: One issued exclusively by the FRB, and another issued jointly with the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC). The proposals assign large banking organizations to one of four categories (I, II, III, IV) each with its own set of tailored requirements and goes beyond the EGRRCPA by tailoring standards for banks between $250 to $700 billion. In addition, the proposals modified the applicability of EPS by not just measuring size, but also including additional indicators such as status as a

global systemically important bank (G-SIB), cross-jurisdictional activity, weighted short-term wholesale funding, nonbank assets, and off-balance sheet exposures. Banks in the lowest category—generally domestic institutions between $100 billion to $250 billion in total assets—would no longer be subject to liquidity requirements and would have fewer regulatory mandates for stress testing.[4] Specifically, banks between $100-250 billion in total assets will be exempt from company run stress tests (Dodd-Frank Act Stress Tests, or "DFAST") and Comprehensive Capital Analysis and Review (CCAR) qualitative reviews, and will complete CCAR quantitative reviews on a two-year cycle.

Apart from changes mandated by statute, there are a number of other important initiatives and proposals coming from the banking regulatory agencies. These include:

Volcker Rule. In addition to the statutory changes highlighted above, banking agencies (plus the US Securities and Exchange Commission [SEC] and US Commodity Futures Trading Commission [CFTC]) have issued proposals to simplify and tailor the Volcker Rule to reduce the burden and uncertainty of its application. Among other things, the proposals would eliminate the 60-day presumption and simplify the market-making and underwriting exemption requirements.

Community Reinvestment Act (CRA). Passed in 1977, the CRA statue could not have anticipated internet banks, mobile banking apps, and other innovations that have affected how banks serve their communities. Recently, the OCC was the first banking agency to issue an advance notice of proposed rulemaking (ANPR) with the intent of modernizing implementation of the regulation while preserving the statute's original intent.[5] The ANPR focuses on three major areas:

- Revising the assessment area from a focus on brick-and-mortar locations to where a bank's "business operations are located";
- Increasing transparency of the evaluation by providing "clear and transparent metrics for what banks need to do to achieve a certain CRA rating";
- Increasing the type of activities that would receive CRE "credit," such as small business lending, credit cards, auto lending, and affordable "small-dollar loans."

Resolution planning

Consistent with broader regulatory trends, US regulators appear to be tailoring their approach to resolution planning. Deadlines are being pushed back,[6] and the number of institutions required to prepare and submit recovery plans is in the process of being reduced.[7] In their bank-specific feedback for the G-SIBs that submitted 2017 resolution plans, the FRB and FDIC concluded that none of the plans were deficient.[8] This recognizes substantial progress by banks on enhancing resolvability in recent years, since five of the eight plans were deemed to have deficiencies by the agencies in the 2016 submission.

At the same time, however, regulators are expanding their requirements in selected areas, and offering more specific guidance about what is expected from US G-SIBs. In particular, additional requirements are proposed in two key areas:[9]

- Booking practices, monitoring, and reporting related to derivatives and trading (DER)
- Operational capabilities related to payment, clearing, and settlement (PCS)

For the largest FBOs, the FRB and FDIC are currently reviewing their July 2018 submissions against SR-14 as this was incorporated into the FBO guidance released in 2017.

BSA/AML. The Bank Secrecy Act was passed in 1970, but because of changing technologies and shifting areas of anti–money laundering (AML) focus, banks have found AML compliance to be problematic over the years. Recently, there have been legislative and regulatory proposals to reform AML programs; however, nothing concrete has yet happened. Ideas that could simplify compliance, while adhering to the intent of AML regulations, include:

- Raising the $10,000 threshold for filing Currency Transaction Reports and the $5,000 threshold for filing BSA/AML-related Suspicious Activity Reports;
- Facilitating and encouraging increased AML–related information sharing among financial firms;
- Improving communication and feedback from government agency recipients to the filing institutions.

Small-dollar lending. With new leadership, the OCC and the Consumer Financial Protection Bureau (CFPB) have become more supportive of small-dollar lending programs. In May 2018, the OCC issued its Core Lending Principles for Short-Term, Small-Dollar Installment Lending,[10] which encourages banks to offer responsible short-term, small-dollar installment loans. The agency had previously rescinded guidance on deposit advance products. The CFPB has stated that it intends to engage in a rulemaking process to reconsider the Payday Rule, and the OCC plans to work with the agency to ensure that OCC-supervised banks can offer responsible lending products, including those now covered by the Payday Rule.

Board governance. The FRB has issued a proposal to clarify expectations for boards of directors, and to better separate expectations for board governance from those for bank managers. The proposal outlines five attributes for an effective board: (1) set clear, aligned, and consistent direction regarding the bank's strategy and risk tolerance; (2) actively manage information flow and board discussions; (3) hold senior management accountable; (4) support the independence and stature of independent risk management and internal audit; and (5) maintain a capable board composition and governance structure.[11]

As a part of this initiative, the FRB is reviewing and revising existing guidance when it does not align to the core responsibilities of boards. The OCC has also articulated to examiners that reports of examination and other communications should distinguish between the responsibilities of the board and those of management, including their roles in addressing supervisory issues.

LIBOR replacement. The clock is ticking on replacing LIBOR as the reference rate in financial contracts. The Financial Conduct Authority has set a deadline of year-end 2021 to discontinue LIBOR, and has pledged to stop compelling banks to provide estimates at that time. (LIBOR will likely continue to be quoted beyond 2021; however, the usefulness of the index will probably be greatly diminished). In the United States, the Alternative Reference Rates Committee has settled on the "Secured Overnight Financing Rate" (SOFR) as the replacement rate. It is important that banks start planning for LIBOR's replacement now. One key step is to make sure that longer-dated financial contracts contain fallback language in case LIBOR stops being quoted. It is also advisable to begin educating customers, as SOFR rates will likely be lower than the LIBOR rate, meaning that spreads will need to be higher to achieve the same return for the bank.

What does all of this change mean? One important takeaway is that the long-awaited "pendulum swing" is now occurring, albeit in a very measured way. Another is that tailoring of bank supervision is back in style, both from a statutory perspective and in the way regulators conduct their supervision. Although these generally appear to be positive developments, banks can take further advantage of this moderate regulatory relief by maintaining sound risk frameworks and continuing to embrace tools such as stress testing to calibrate risk.

Optimizing across the three lines of defense

Nearly 10 years after the financial crisis—and eight years after the passage of Dodd Frank—many banks have completed or nearly completed their build of new risk management systems and they are now ready to get back to business-as-usual. However, while the hardest work has been completed, much has changed with regard to their customers, marketplace, technology, and regulatory environment since the blueprint of those systems was initially conceived. The FRB's inaugural version of a banking supervision and regulation report stated that "over half of the supervisory findings issued in the past five years were related to governance and risk management control issues."[12]

In the period leading up to the financial crisis, risk and compliance systems were heavily siloed, and the operating environment was characterized by highly manual processes, ineffective controls, and a "check the box" mentality. Afterward, given the heightened expectations of Dodd-Frank reform and regulators' low tolerance for missed deadlines and weak solutions, systems were built quickly and with a focus on sturdiness, not efficiency. However, now that banks have experience in operating these systems under business-as-usual circumstances, the redundancies and design compromises that resulted in sturdiness at the expense of efficiency have become clearer. As such, these newly built systems—which span the "three lines of defense" (e.g., business line; independent risk and control functions; and internal audit)—are ready for a refresh to improve efficiency while maintaining alignment with regulatory expectations.

Banks are now looking to optimize their risk-management approaches and systems to be more automated, more flexible, more capable of near real-time risk reporting, and more closely linked to bank strategy and risk appetite—harnessing the technology and business innovations occurring inside and outside of the bank.

The first step in optimizing the three lines of defense is to revisit the operating model. This includes deciding whether the current roles and responsibilities are appropriately allocated across the bank. Banks are starting to acknowledge that there are unproductive redundancies in certain areas, and that controls are not always located in the right place to be both effective and efficient. For example, some banks are now moving selected testing and monitoring activities up to the first line of defense, with the goal of improving detection, prevention, and accountability. This move enables the second and third lines to conduct a more strategic review, while also freeing up resources for advanced data analytics, risk aggregation, and targeted testing to better evaluate risk.

Challenging the current operating model

At a detailed level, banks are evaluating their current operating models across several key dimensions:

Structure

- **Location of resources.** Are the roles and responsibilities of each line appropriate, or do some roles need to be relocated closer to the origin of risk for faster and more effective detection and remediation?
- **Balance of resources.** Does the balance of resources—particularly between the first and second lines of defense—promote accountability and address fundamental needs at the origin of risk?

Alternative service delivery models

- **Leveraging subject matter experts (centers of excellence).** How can subject matter experts for key areas—such as capital and resolution planning, vendor management, and cyber—be leveraged to help inform both first- and second-line efforts in a manner that fosters consistency and quality?
- **Cosourcing a portion of risk roles (managed risk services).** How might the use of third parties and/or offshoring produce better risk management at lower cost, particularly in areas where specialized talent is hard to recruit, or where repetitive tasks might enable an outside provider to achieve greater economies of scale?
- **Joint ventures (industry utilities).** How might joint ventures with other banking organizations enable costs to be shared across the industry for common activities, such as conducting annual due diligence for third-party vendors used by multiple banks?

Rationalizing controls and linking to risk appetite

In conjunction with rethinking their operating models, many banks are looking at rationalizing their controls and linking them more tightly to the bank's risk appetite. The first step is to take an end-to-end view of a business process for a particular product or offering, searching for ways to reengineer the process to simplify and strengthen delivery.

The next step is to see how controls could be rationalized for the reengineered process in order to reduce costs and improve effectiveness. This involves assessing, analyzing, and prioritizing risks relative to the firm's risk appetite, then identifying control areas that can be simplified, strengthened, eliminated, or reused—with the goal of creating a more streamlined and effective control environment.

The final step is to rethink controls testing with the idea of moving toward targeted risk-based and redundant controls testing

that focuses on effectiveness against the key risks. Rebalancing the mix of tests with continuous monitoring of key risk control indicators is an essential complement to testing. This continuous monitoring program can be further enhanced through user-customizable data analytics that are either pushed to end users or event-driven.

Enabling operating model and controls rationalization and enhancement

As part of the reengineering process, banks should assess whether they have the right tools to enable transformation and allow their key employees to imagine and execute the "art of the possible." Today, there are existing and emerging technologies that can greatly aid in the transformation effort—helping to automate workflows, enhance platforms, generate advanced data analytics, and automate repetitive tasks.

Tools such as robotic process automation (RPA) and natural language processing (NLP) can help banks eliminate essential but repetitive and mundane tasks, creating economies of scale and freeing up resources for higher-value analysis. Advanced data analytics and reporting allow users to leverage the same data across the three lines of defense without creating redundancies, while at the same time enabling customizable views that fit the role and needs of each line.

As banks move up the digital continuum, they are able to create a more effective risk and compliance framework that is increasingly frictionless, agile, intelligent, automated, and actionable. Also, by digitizing their processes and controls, banks can enhance their suite of risk and compliance capabilities. For example, banks can use digital technologies to develop predictive modeling that answers the question "What happens next?" They can create randomized testing that answers the question "What happens if we try this?" And they can perform statistical analysis to answer the question "Why is this happening?" In addition, they can create alerts that answer the question "What actions are needed?"—as well as ad hoc reports that tell them "How many, how often, and where."

Although advanced capabilities such as these might seem beyond reach, many are already in use today at several of the industry's largest institutions. Figure 1 highlights opportunity areas actively being tapped by banks that have challenged their operating models and asked themselves "What might be possible?"

Figure 1. Risk management of future/areas of opportunity

RISK MANAGEMENT

Risk assessment/RCSA results—Deploy text analytics within the risk assessment data

Testing/monitoring automation—Automated data collection and execution of rules based test steps, sampling continuous monitoring routines, control testing and validation, surveillance

Complaints analysis—Capture real-time complaint feedback and reporting, sentiment and trend analysis

Risk sensing—Predictive risk identification, social media scanning, new product launch

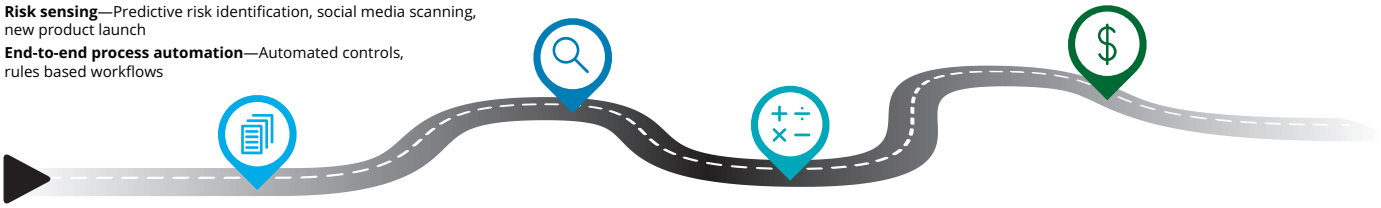
End-to-end process automation—Automated controls, rules based workflows

CREDIT RISK

Operational services—Reference data sourcing, portfolio ops, collateral management

Analytical services—Risk analysis, model management, reporting

Policy and control—Approval underwriting QA, credit risk control, portfolio management



COMPLIANCE/OPERATIONAL RISK

AML/KYC/client on-boarding—Transaction monitoring, due diligence, alert management, SAR reporting population

Legal inventory—Law, regulation and guidance extraction, automated control language generation/development

Regulatory change—Identification of change, case management routing, tracking and reporting

Policy maintenance—Update of documentation, central tracking and governance

Rule monitoring—Automated checks or reconciliations for various internal/external thresholds (e.g., Marketing, HMDA, SCRA)

Vendor management—NLP-based contract reviews to extract terms to feed vendor risk analysis, contract remediation

RISK REPORTING

Regulatory reporting—Automated data gathering, aggregation and template population with software logs for reference, Control testing, reconciliations and data quality reviews

Client reporting—Standard client reports/template population (bolt on commentary generation)

Management reporting—Rapid data extraction and report generation (bolt on generation of narratives), aggregation of results and automated visualization tool development

KRIs/KPIs—Rule and threshold monitoring, automated calculation of risk metrics, trend analysis, data aggregation, visualization

ADDITIONAL USE CASES

Fraud detection and prevention—Credit card fraudulent transaction analysis, identity and access management

Internal audit—Generation of reports, data aggregation, population testing, predictive risk identification, audit assessment

Finance/Treasury—Transaction processing, close, consolidate and report, management reporting, CCAR reporting, transfer pricing, contract term capture and review

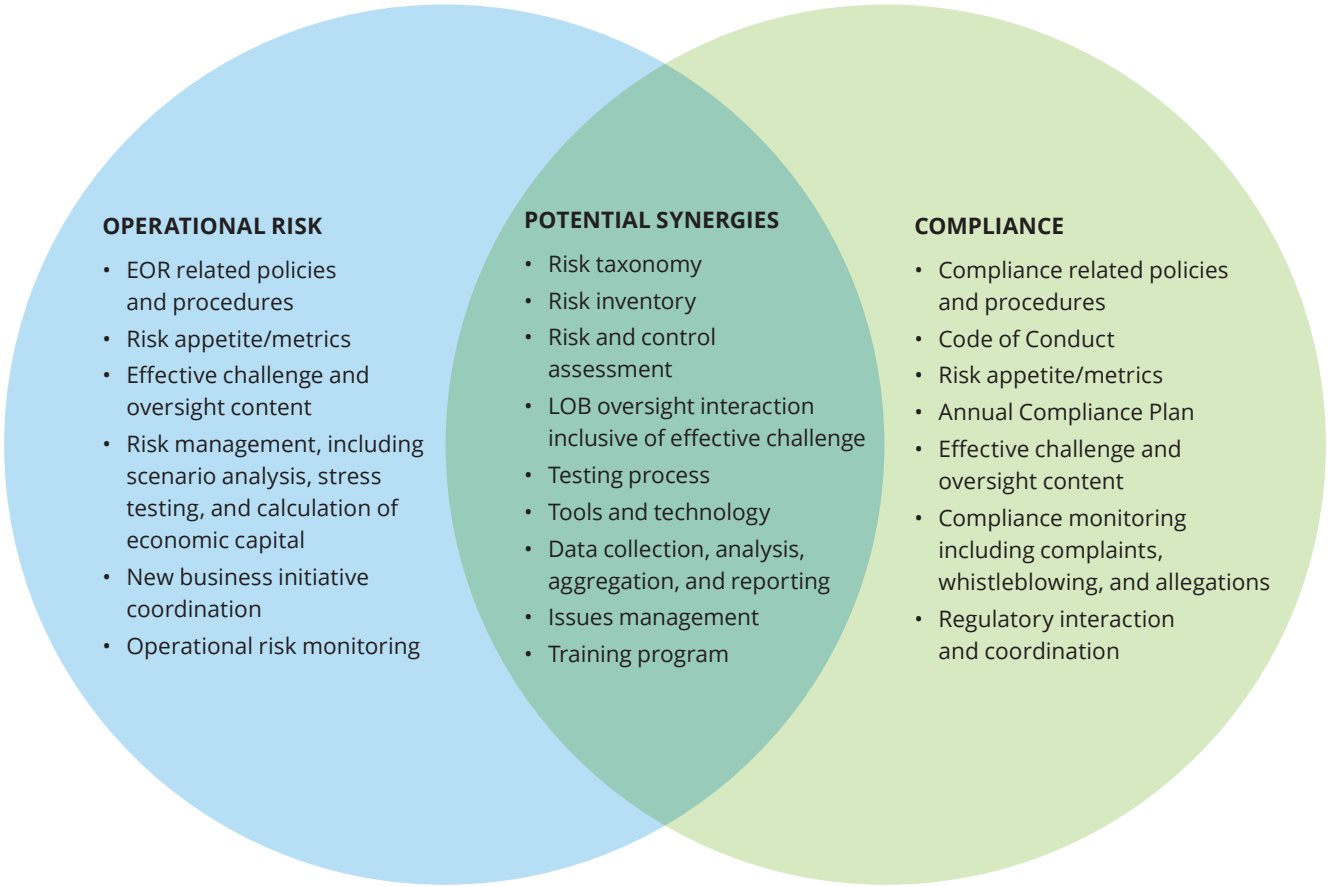
When deciding how to move forward, banks need to consider whether investing time, energy, and money to optimize their three lines of defense model and capabilities—while possibly raising costs in the short term—will be worth the future payoff of achieving better, more sustainable risk management performance at lower cost in the longer term. Of course, they also need to consider that the alternative might be making endless minor tweaks to inefficient systems that may or may not meet internal and regulatory expectations—and that may ultimately require a more expensive and distracting overhaul down the road.

Integrated risk and compliance

Operational risk and compliance both have a shared mandate to provide second-line-of-defense oversight and challenge, but sometimes that may create conflicts (e.g., activities such as discrete testing for each function can create overlap in time, resources, and outcomes). Financial institutions are facing challenges in the execution of such activities and continue to explore ways to optimize, differentiate, and streamline risk-management activities and where possible, reduce costs.

Given a strong correlation between operational risk and compliance risk exposures (e.g., compliance violations may translate into operational losses and other process failures), increased stakeholders expectations from the first line of defense, and executive management and the board for clarity and transparency, institutions may identify synergies and consider centralization of certain activities (e.g., issue management, risk aggregation and reporting) with careful consideration and prioritization.

Figure 2. Operational risk/potential synergies/compliance



A common and consistent taxonomy (e.g., for five critical elements: risks, controls, processes, policies, and obligations) is foundational for effective risk measurement and realization of opportunities for synergies. Figure 2 highlights other key areas of opportunity where potential synergies and touchpoints between operational risk and compliance can be realized.

However, careful consideration and prioritization are required before trying to implement any kind of synergies such as ensuring processes of each respective discipline will align along with objectives. Banks are exploring different ways to realize these synergies, for example developing a shared services model (e.g., centers of excellence), singular ownership for identified activities for both disciplines, or coordination among the two discrete disciplines.

There is also high potential of automation tools and emerging technologies (such as big data, artificial intelligence, machine learning, predictive analytics, etc.) to help improve the risk-management effectiveness. Innovation is at the cusp of financial services, and banks are taking advantage of these automation tools, emerging technologies, and proof of concepts to improve the effectiveness of operational risk and compliance management processes to predict and mitigate risk.

Regulatory divergence

Overall, the global regulatory landscape for banking looks set to become increasingly divergent and fragmented—a trend that, if left unchecked, could have significant implications for banks with substantial operations in multiple jurisdictions. The potential impact is particularly great for current efforts to create a regulatory, risk, and compliance infrastructure that's more streamlined and sustainable. As decision makers grapple with feeling like they have "too many regulators to manage," they should adopt new approaches and invest in tools and strategies that can help them efficiently navigate the new complexity. Otherwise, they could face strategic paralysis as the cumulative impact of regulatory complexity—and the resulting binding constraints on how a bank operates—becomes harder to understand.

For more information, read our whitepaper:

"Dealing with divergence: A strategic response to growing complexity in global banking rules"

Cybersecurity and 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. According to a 2018 study, the global cost of cybercrime in 2017 was a staggering $600 billion.[13] A study[14] by Deloitte Advisory revealed that the business impact of a cyberattack extends beyond the traditional costs attributed to a cyber incident and range from regulatory and legal action to long-term loss of trust, customer relationships, and brand value. Financial institutions are at the forefront of bearing the brunt of cybercrimes. The US Treasury Department has named cyberattacks as one of the top risks facing the US financial sector.

As the 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."[15]

The current administration in the United States has placed renewed emphasis on improving the coordination between federal agencies and state member organizations to improve the reliability and security of the financial sector infrastructure through the Financial and Banking Information Infrastructure Committee.[16]

Specific trends in banking—such as increased use of outsourcing to reduce costs and largescale adoption of innovations such as cloud computing—have increased the exposure to cyber risks. Further, exponential increase in data-processing capabilities because of mainstream adoption of RPA and use of machine learning has increased the ability to correlate large volumes of data sets and introduce decision making that can infringe upon the privacy and rights of individuals.

Legislators are working to keep pace by introducing new privacy and cybersecurity laws. A selection of key legislative and regulatory developments is presented below to provide insights into the nature of issues that legislators are requiring banks to address.

EU General Data Protection Regulation (GDPR)

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 banks 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) take effect in May 2018, providing two years of adoption. 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.[17]

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).

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 drastic as a ban on data processing, as well as fines of up to 4 percent of annual global turnover.

California Consumer Privacy Act (CCPA)

In the United States, California enacted the California Consumer Privacy Act of 2018 (CCPA), a significant legislation 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."[18]

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 the Gramm-Leach-Bliley Act (GLBA).

New York State Department of Financial Services cybersecurity regulation

The New York State Department of Financial Services (NYDFS) regulation took effect on March 1, 2017, with a phase-in period concluding on March 1, 2019. The regulation requires banks to establish and maintain a risk-based cybersecurity program and supporting capabilities.

The two-year phase-in provides a glide path toward compliance. Banks 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, the board of directors need to be involved in the creation of standards and should 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 cyber security 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.

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, etcetera.
- 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.

Banks today should consider investments in revisiting and validating their TPRM programs to formalize the program scope, enhance inventory processes, and optimize 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.

SEC disclosure guidance

The SEC issued disclosure guidance to public companies in early 2018.[19] 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. CEO and 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.[20] Banks 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.

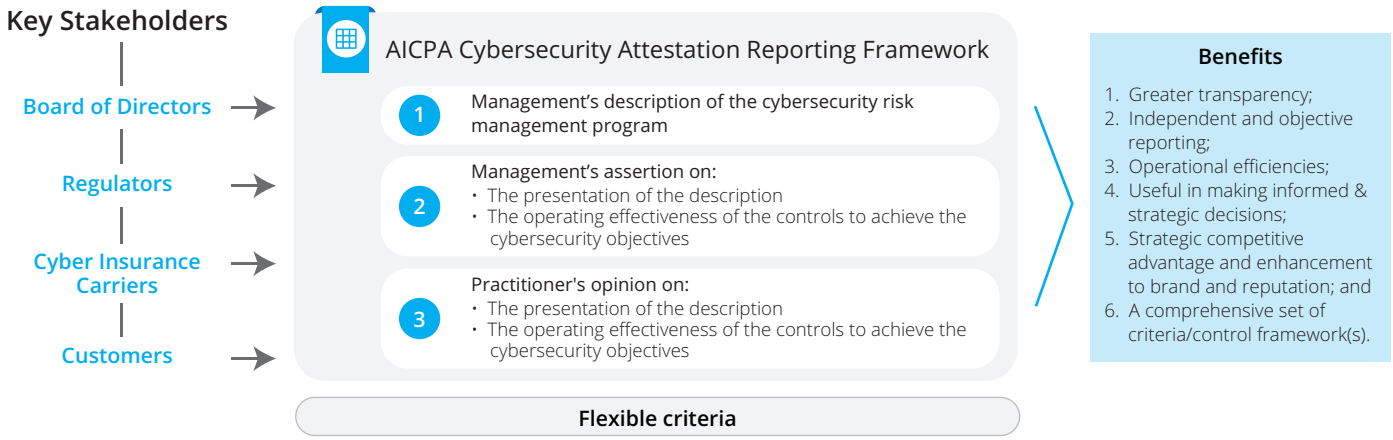
The SOC for Cybersecurity consists of three sections:

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 of 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
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 banks planning to embark on an attestation, a leading practice to consider might be the AICPA Cybersecurity Attestation Reporting Framework (figure 3).

Figure 3: 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

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[21] that significantly provides for significant rights and protections to personal information. The law is widely touted as being very similar to GDPR. Banks have 18 months to comply.
- **United Kingdom** issued its Data Protection Act 2018[22] that implements the GDPR provisions and imposes as well as implements additional requirements, such as on matters related to national security and immigration.
- **Singapore** passed the Cybersecurity Act in March 2018,[23] subjecting banks 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[24] that obligate financial credit institutions to notify individuals whose personal information is involved in a data breach that may cause harm.

Future outlook related to cybersecurity and data privacy continues to indicate strong regulatory developments, with several countries either implementing or enhancing existing regulatory requirements. Within the United States, banks 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,[25] as well as continued efforts towards harmonization of data privacy and cybersecurity laws and regulations.

Fintech

After a period when fintech companies were sprouting up rapidly, the rate of new fintech startups began to decline in 2015. However, new dollar investment in fintech firms remains strong and the number of acquisitions is rising. This reflects a maturing market where traditional banks and fintech firms are increasingly teaming up to offer innovative services.

Two important developments in the fintech regulatory landscape occurred in late July 2018 when the Treasury department issued a report entitled *"A financial system that creates economic opportunities: Nonbank financials, fintech, and innovation,"*[26] which outlined core principles and recommendations for a fintech regulatory framework. One recommendation was for the OCC to move forward with the national fintech charter. Hours later, the OCC announced it would begin accepting applications for special-purpose bank charters for fintech firms that offer bank products and services.

Here is a look at the current banking fintech landscape, recent regulatory developments, and the implications for traditional banks.

In a recent report, Deloitte outlined the changing landscape in the fintech industry.[27] The report found that the number of new fintech startups rose from 177 in 2008 to 668 in 2014. However, in 2015, the rate of fintech formations began to decline, and was down to only 41 startups in the first nine months of 2017. In the banking and capital markets fintech category, the peak of 281 startups occurred two years earlier in 2012, declining steadily to only 10 in the first nine months of 2017. However, at the time of the report, more than 2,000 firms existed in the areas of banking operations, capital raising, financial management, deposits and lending, and payments.

Despite the decline in new startups, new fintech funding remains strong, with a shift toward later-stage investment in a maturing market. Meanwhile, acquisition activity is on the rise, with about 50 acquisitions occurring in the banking and capital markets category during the first nine months of 2017.

For traditional banks, fintech companies can represent either a competitive threat or an opportunity to offer better services and improved processes through strategic partnering. Many banks have embraced the latter, partnering with or acquiring fintech companies to modernize their own operations and services.

For fintech companies that are not acquired by traditional banks, the regulatory environment remains a bit fragmented. Currently, most fintech companies are licensed and regulated by the states, often under existing laws for money service businesses. Some states have adopted statutes specifically for fintech; others have not. And despite efforts to build a more unified licensing regime between the states, inconsistencies and varying requirements still exist. Indeed,

one of the major themes in the Treasury report recommendations was "aligning the regulatory framework to combat unnecessary regulatory fragmentation, and account for new business models enabled by financial technologies."

As part of the effort to encourage innovation, US financial regulators have opened offices of innovation to understand fast-moving industry developments and provide information to the growing financial technology community of how regulators may be responding to these developments. The OCC, CFTC, SEC, and CFPB have all established Offices of Innovation, and the FDIC and the US Treasury's Financial Crimes Enforcement Network (FinCEN) have indicated that their offices are in development.

To foster innovation, the development of regulatory "sandboxes" has been discussed in concept by Treasury and regulators to provide a safe haven for product development and experimentation. In particular, in December 2018, the CFPB drafted a proposal for a revised "No-Action" policy, which would give startups greater protections from agency enforcement. Companies that receive No-Action letters would not have to share data with the agency. The proposal would also create a "Product Sandbox" that would be open to a broader pool of businesses than typical regulatory sandboxes, and participating firms would be required to share data with the agency.[28]

For fintech companies wishing to enter the banking industry directly and to gain greater regulatory certainty, the OCC fintech charter has garnered quite a bit of attention as one of several banking entry options. Fintech companies may wish to apply for such a charter from the OCC, especially if they are operating in multiple states. However, the promise of greater consistency in regulation could come with downsides, depending on a fintech's business model. These downsides could include more burdensome regulatory requirements, and initially, a legal challenge from the states, many of which oppose the OCC's fintech charter.

The OCC defines a *special-purpose national bank* (SPNB) as a "national bank that engages in a limited range of banking or fiduciary activities, targets a limited customer base, incorporates nontraditional elements, or has a narrowly targeted business plan." The OCC fintech charter is a subset of that. Chartered fintech companies can engage in the core banking activities of paying checks and/or lending money, but cannot take deposits and will not be insured by the FDIC.

The OCC's licensing process for fintech companies is essentially the same as the process for other charter applications, and includes four phases: prefiling, filing, review, and decision. The prefiling phase is especially important for fintech firms that are considering a national charter. In this phase, applicants meet with the OCC to discuss the proposal, the chartering process, and the application requirements. This is an opportunity for the OCC to understand a firm's business model, and to point out any special requirements and/or potential impediments. It is also an opportunity for the fintech firm to understand the requirements and process involved in obtaining a national charter, providing the firm with valuable information to help it decide whether to move forward with the application. Prospective applicants should also weigh developments at the state licensing level, since those requirements might become more stringent as states beef up their fintech statutes. Conversely, efforts to standardize state licensing requirements could improve consistency in state-to-state regulation in the future.

A more complete discussion of chartering options for FinTechs is provided in our publication: "So you want to be a bank."

While the OCC SPNB option is new, some fintech companies are considering other previously existing charter options such as becoming or establishing a full-service commercial bank or an industrial loan company. Both have the advantage of offering FDIC insured deposits, and the latter's parent company, if any, would be exempt from the FRB supervision.

While there are many options for becoming a bank, for many fintech companies, the current bank parterning model of has the advantage of capitalizing on each entity's unique advantages and capabilities. Combining strengths has the potential to create more value than either business could produce on its own.

Banks and fintech companies should seek to understand each other's capabilities and needs by attending industry forums and roundtables that bring traditional banks and fintech firms together. They should also stay abreast of regulatory developments related to fintech firms and partnership arrangements, constantly looking for ways to enhance their services by partnering, or possibly merging. Fintechs that provide payments and/or lending services should also explore their licensing options in order to choose the option that best fits their business model.

Data quality and availability

Data quality and data availability are growing concerns across all aspects of risk management and regulatory compliance. In order to address these concerns, data management and data quality can no longer be the sole responsibility of the corporate functions or specific executives such as the chief financial officers (CFO), chief risk officer (CRO), or chief data officer (CDO). Rather, it needs to be an enterprise activity with shared responsibilities and accountability across all three lines of defense.

Data owners within a bank should be asking: Is the quality of the data fit for purpose? Are the origins of the data clear and well documented? Are data definitions and standards established and consistent across the enterprise?

Recently, some reporting requirements have been reduced through regulators' burden reduction efforts, regulatory relief legislation, and tailoring of data requirements. However, these reductions do not change regulators' expectations for managing data. In fact, some of the reductions in reporting have been offset by new data requirements, particularly for large complex banks, and there is a general trend toward requiring more granular, product-level data and with more frequent availability. This trend underscores the need for strong enterprise data management practices and accountability.

Regulatory expectations for a bank's data environment focus on three areas:

- Strengthening governance and oversight
- Building data competencies across the bank
- Establishing an integrated approach to data

However, this framework is applicable not only to regulatory reporting, but to all data initiatives, including public reporting, liquidity management, risk management, and management reporting.

Strengthening governance and oversight

The banking industry is shifting and developing its approach to data-related governance and oversight. As practices mature, leading banks are assessing how their data management processes align with their organization's operating model. The objective of a governance and oversight framework is to develop, communicate, and monitor effective data standards and policies. These standards and policies are foundations for implementing an effective data environment. A critical element of the standards is having consistent data definitions and data quality standards. Another important element is having a methodology for determining "Critical Data Elements" (CDEs). The process of determining CDEs requires a bank to understand the origins of data, all downstream uses of the data, and the impact on all data users (including external parties).

In many cases, the biggest challenge banks face in this area is the need for a culture shift. Successful bank-wide data programs require support from senior management and the board. Without a culture shift and top-level support, the key components of the governance process—and accountability of key stakeholders, including business lines—likely will not be achieved.

Effective oversight and accountability require a measurement and monitoring function armed with quantitative measures of data quality. These measures can be used to rationalize and enforce accountability at the data owner/business line level. The monitoring function should also be responsible for aggregating and tracking data issues related to both quality and availability—ideally managed through a single, centralized issue-tracking system. Data issues should be reviewed from a bank-wide perspective to identify any systemic issues and to escalate issues based on their associated risk. In addition, the monitoring function should ensure there is a comprehensive remediation plan for addressing data issues, and if the remediation plan is not executed on time, ensure proper escalation within the bank's management structure.

Data quality controls

Part of an effective data governance structure is having controls in place to ensure the integrity of data. A significant number of such controls originate from data quality programs.

Data quality programs are not a single responsibility or action. Effective data quality programs include an independent quality assurance function that conducts detailed, end-to-end testing. This testing is conducted on a multiyear planning schedule that considers the impact of CDEs overlaid with a risk assessment. Effective data quality programs also include cross-dataset reconciliations. These reconciliations are a valuable tool for identifying systemic data issues and ensuring data completeness.

Transaction testing and reconciliation are ex-post activities that occur after data have been submitted. Data quality programs need controls that are conducted contemporaneously. These controls should include the application of quantitative business rules to data at the point of origin, and at every point where data are transformed or modified. In addition,

qualitative analysis should be conducted to ensure the results make sense in the context of the data definition and the bank's business model. Outcomes of all analysis conducted under the data quality program should be documented and shared across the organization.

Building data competencies across the bank

With the heightened attention to data quality—and the increased need for granular product-level data—a data owner's (usually residing in a business line) responsibility for data quality has intensified. To meet regulatory expectations, business lines, the finance function, and other data aggregators need to have expertise in data management and data analytics.

In many cases, data owners understand their data as it relates to their specific business, but have a limited understanding of how their data affects other users across the bank. Thus, the first step for business lines is to gain awareness of the bank's existing data standards and data programs. Formal awareness training is important for senior management and for all staff involved in providing data to the rest of the bank. Awareness training—which varies by role—helps data owners understand how their data are being used by others in the bank. This knowledge helps data owners to ensure the appropriate level of data quality controls at the data attribute level. Regulators expect this awareness training to be implemented as part of a bank's accountability policy.

As data requirements become more complex, there is increased need for specialists who can properly interpret how regulatory requirements relate to a bank's products and transactions. To address this issue, data owners and report owners (i.e., the functions responsible for reporting) need access to a pool of talent that understands capital requirements, liquidity management, and broad regulatory definitions.

Establishing an integrated approach to data

Historically, business lines have typically each maintained their own separate and unconnected data and IT architectures. However, this siloed approach is no longer sufficient to meet regulatory expectations or the data needs of today's businesses. Sustaining a highly effective data program requires an integrated approach that includes finance, regulatory, risk, and capital data. BCBS 239[29] makes clear that such an approach is necessary for risk aggregation:

"Principle 2: Data architecture and IT infrastructure—A bank should design, build and maintain data architecture and IT infrastructure which fully supports its risk data aggregation capabilities and risk reporting practices not only in normal times but also during times of stress or crisis, while still meeting other Principles."

In our view, however, the concept of integration should be applied to all data, not just risk data.

As data requirements continue moving toward more granular, complex data elements, the need for an integrated approach to data increases—as does the need for tools to analyze and validate the data. Integration improves access to data across the bank. It also makes it easier to apply data analytics and artificial intelligence technologies to data sets, enhancing the bank's data capabilities and process efficiencies. This is particularly important for product and transaction data with a large number of data attributes.

The shift to an integrated data environment should be supported by a bank-wide data stewardship program that spans business lines, products, and legal entities. This requires expertise in data management practices and subject matter knowledge of data requirements. An effective data program also includes creating a data repository to capture information at data attribute level on data definitions, uses, and quality. The bank-wide standards for this should be outlined, communicated, and monitored as part of the governance process.

What's next?

The evolution of data practices in banking will continue to be influenced by the growing need for granular product-level data. Banks planning or conducting data remediation efforts—or those facing new data requirements (e.g., SCCL reporting, Volcker metrics, current expected credit loss [CECL], FDIC Rule 370)—should consider migrating to more mature practices that can improve data quality, integrity, and availability.

Financial crimes risk

The national security objectives embedded within financial crimes compliance—as well as the need to preserve the integrity of the financial system, both domestically and across the globe—have sustained the US government's concentrated focus in this area.

The new leadership at the Federal Banking Agencies (FBAs) and FinCEN have created new initiatives regarding the efficiency and effectiveness of the AML and sanctions supervision. Their public pronouncements include: a commitment to greater clarity of regulatory expectations; and increased transparency, efficiency, and simplicity in their supervisory oversight of AML/sanctions. In November 2018, the United States Senate Committee on Banking, Housing, and Urban Development held a hearing on regulator's points of view on BSA reform and changes that would affect both banks' and the regulators' efficiency and effectiveness. Both Congress and the regulators are still discussing opportunities to further tailor AML oversight and clarify risk-based expectations and alleviate current burdens, particularly on smaller financial institutions.

Examples of initial steps taken by the FBAs and FinCEN include: (1) recent interagency guidance publications (e.g., FinCEN's *Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions; Interagency Statement Clarifying the Role of Supervisory Guidance*; and *Interagency Statement on Sharing BSA Resources*), and (2) notice of a proposed rule change expanding the number of banks eligible for the 18-month examination cycle. This change in examination cycle criteria will not only further amplify risk-based supervision, but also free up examination resources to focus on other agency priorities, including perceived riskier areas and institutions. Over the past few years, the number of AML-related civil and criminal enforcement actions has increased across the globe. Domestically, there was a relative increase in enforcement actions against individuals. This continues a trend where actions against individuals are not isolated or rare, but rather are common enforcement tools available and used by regulators. Financial Action Task Force's (FATF) jurisdiction mutual evaluation assessments are having an impact as well. There appears to be an increase in enforcement actions around the time of mutual evaluations, adding to the number of actions taken globally. Overall, enforcement and other actions across the globe related to AML/sanctions appear to be increasing in frequency.

Sanctions programs and designations from the Office of Foreign Assets Control (OFAC) continue to expand. The United States' withdrawal from the Joint Comprehensive Plan of Action (JCPOA) reinstituted sanctions and secondary sanctions related to Iran; however, non-US signers and Iran are trying to maintain the agreement. This divergence of interests—along with the possible imposition of secondary sanctions on any foreign entity doing business with both the United States and Iran—greatly complicates a wide range of areas, including compliance; new and ongoing client relationships and transactions; international financial flows; and risk exposures. Risk and compliance management related to the imposition of secondary sanctions creates a need to engage the first line of defense's local jurisdiction and customer knowledge. Also, it places additional emphasis on customer due diligence information—both at account opening and throughout the life of the relationship.

In 2018, two new substantive regulatory requirements were implemented: (1) FinCEN's *Customer Due Diligence Rule (CDD)*, which includes beneficial ownership data collection for legal entities; and (2) the NYDFS *Rule 504* requirements and certification. Both of these requirements (greater transparency within the financial system through specific customer due diligence/beneficial ownership regulation requirements; and increasing rigor of suspicious activity and sanctions-monitoring processes) are key areas of regulatory focus.

Law enforcement authorities and regulators have long advocated for additional transparency within legal entities due to the threat that they pose. The CDD requirement will address the transparency issues and also define—within a regulatory framework—the monitoring requirements and expectations related to customer due diligence and suspicious activity.

Operationalizing CDD/beneficial ownership requirements—which include adjustments and enhancements across all three lines of defense (business unit management, risk and compliance, and internal audit)—continues to be challenging for many banks. The NYDFS transaction-monitoring and sanctions-filtering requirements have focused the industry on ensuring thoroughness in three key areas: (1) data integrity; (2) risk-impacted selections of filtering scenarios; and (3) sound, documented alert-tuning methodologies. Both the NYDFS and FBAs have publicly stated that overall industry implementation of these new requirements has gone relatively well. Also, thus far there have not been any public enforcement actions tied to these new requirements.

Despite an evolving regulatory environment, specific actions can be taken to strengthen AML/sanctions compliance programs:

- Strengthening board and senior management governance of AML/sanctions can help ensure the necessary resources, expertise, and controls are in place to appropriately manage an institution's unique risks. Regulators continue to focus their attention on compliance in this area. Also, continued integration of financial crimes compliance within the overall risk-management framework remains a regulatory focus. Board and senior management monitoring of AML/sanction program performance is essential for proper governance.
- Augmenting and strengthening OFAC/sanctions compliance expertise, technology, and processes continues to be key to effective risk management and compliance. With sanctions programs and designations accelerating—and additional secondary sanctions taking effect—thorough monitoring of risk exposures and sanction program performance is crucial. Regulators frequently use NYDFS 504 requirements and *Interagency Guidance on Model Risk Management* to assess and confirm the robustness of design and implementation for these critical AML/sanction controls.
- A comprehensive and documented risk assessment process is essential for the design and implementation of an institution's control environment. Also, it can be an effective document for defending implemented control levels and risk decisions. Regulators consistently focus on the risk assessment methodology and results. In particular, they expect a consistent, repeatable risk assessment process with: quantified risk exposures (enterprise-wide, by department, and, if necessary, at the business unit level); documented mitigating controls; and identified residual risks.
- Expertise and advanced technologies are, at times, underappreciated assets within an AML/sanctions program. Expertise in key areas—AML/sanctions requirements; institution operations/customers; analytics; and technology—is considered one of the most critical levers for operating, maintaining, and sustaining an effective program. This expertise can help insulate the institution from regulatory criticism and potential enforcement actions. However, competition for well-seasoned and deep-knowledge experts continues unabated. Active recruitment strategies focusing on leadership and financial-crimes middle management can give an AML/sanctions compliance risk-management program an advantage in both operational efficiency and effectiveness. In addition, advanced analytics technologies can help identify criminal schemes/threats, as well as identify ways to improve efficiency. Additional operational efficiencies can be achieved through (1) strategic deployment of technology by centralizing customer due diligence and (2) advances in systems for suspicious activity monitoring and reporting.
- Progress is being made—albeit more slowly than anticipated—in the use of innovative technologies to boost productivity and reduce costs. Although they are still maturing, innovative technologies can provide measurable efficiency improvements, particularly in the processes for suspicious activity investigation and customer on-boarding. RPA and cognitive automation technologies are also maturing, and over time can increasingly improve operational efficiencies and productivity—with the goal of eventually reversing the escalating cost of compliance.

In 2019, OFAC sanctions will continue to be actively used, and will remain a vital part of US National Security and Foreign Policy objectives. Institutions should monitor and, where necessary, raise the profile of sanctions controls and compliance to manage this important risk area. The various AML/sanction stakeholders in the United States (law enforcement, FinCEN, FBAs, OFAC, and the Treasury Department) are expected to increasingly focus on this critical compliance and risk-management discipline, and so likely will foreign governments. Institutions—particularly those with ambitious growth plans and relatively high-risk profiles—should continue to prioritize compliance program performance, expertise, and use of innovative technologies in this area as a possible source of strategic advantage.

Finishing the CECL journey

CECL methodology is the Financial Accounting Standards Board's (FASB) new standard for estimating allowances for credit losses. It applies to all companies that make loans, and will have a major impact on everything from governance and financial reporting to investor communications, risk modeling, and capital. The new standard takes effect for most companies on January 1, 2020, and while discussions within the industry are ongoing, including the recent industry proposed alternative accounting model (the other comprehensive income [OCI] approach), it is important to stay focused on existing timelines and requirements.

Many companies planned to complete the build phase in late 2018 or early 2019 and then run their new CECL systems and processes in parallel with their current operations through the adoption date. However, CECL's complexities and evolving interpretations may cause some companies to slip and thus companies may struggle to stay on track. Below are three areas that can be focused on now:

Know where you are and where you are going

The CECL journey in 2019 will likely have many twists and turns. To get to the destination on time, you need to know where you are now—and how you plan to reach the end.

Doing a deep dive assessment, and then adjusting your plan accordingly, can give you confidence that your company can meet the adoption date without costly and avoidable last-minute fire drills. Specific steps include:

- Assessing the status of your program management capabilities
- Conducting a deep dive "program readiness assessment" similar to merger conversions
- Assessing whether you have sufficient "contingency" time in your plan
- Making sure roles are well defined in your program and your new CECL processes

Since pushing the adoption date back is not possible, it is essential to have a robust plan with sufficient contingency time to allow for unexpected problems.

Make sure your parallel phase is sufficient

As companies are challenged to finish their build phase, they will likely be tempted to cut back on the amount of time allocated for the parallel phase. However, in many cases a better option might be to reaccelerate the CECL effort by tapping resources from other projects that have more flexible timelines. This can help ensure sufficient time to operate the new and existing systems and processes side by side.

The parallel phase should include a full-dress rehearsal that covers everything from generating the new CECL data to creating mock-up reports and communications for investors. This comprehensive, end-to-end rehearsal not only gives a bank the opportunity to confirm its systems and processes are up to the task, but it also provides a valuable opportunity to refine and hone all aspects of the CECL transition, operations, and communications.

Develop an effective investor communications strategy

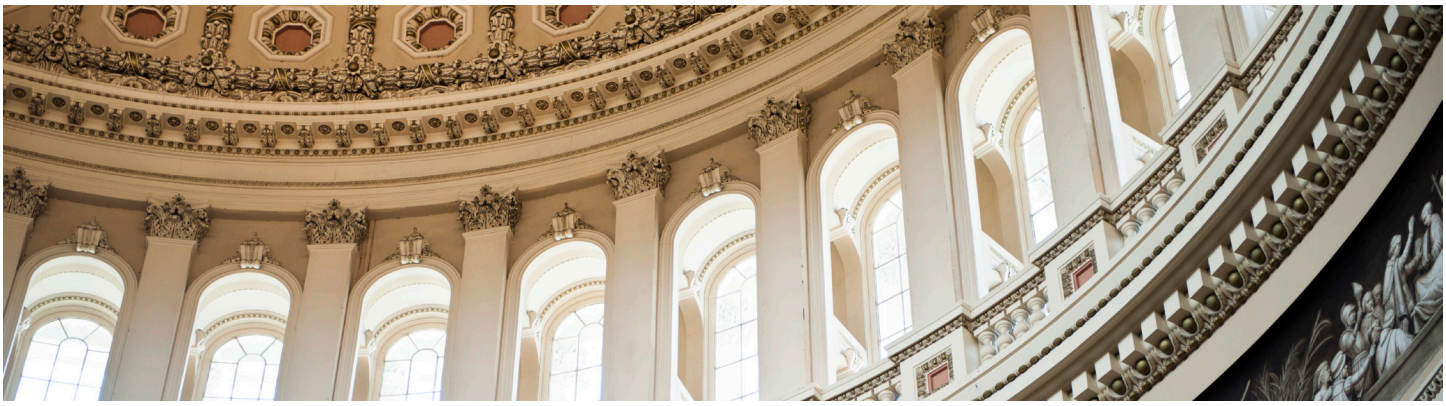
Establishing an effective strategy and capabilities for communicating with investors about CECL should be a top priority in the months ahead. From a communications perspective, CECL presents a "perfect storm"—it is a principles-based standard that allows significant room for judgment and interpretation; it hinges on complex processes and forecasts; and its disclosure regime is very flexible.

For CFOs and investor relations groups, getting the right balance of qualitative and quantitative information to tell a complicated story about a highly judgmental estimate that has a significant impact on an institution's market valuation will likely be the biggest disclosure challenge since communicating about credit quality during the last recession.

CFOs will be expected to craft a thoughtful, transparent CECL communication strategy from SAB 74 through adoption and beyond. These activities will require significant time and effort, so banks should consider getting started soon. However, too often the task of developing the communication and disclosure strategy is positioned toward the end of CECL programs, minimizing the time the CECL team can iterate and refine its financial statement disclosures and investor messaging.

Investors will be busy with CECL in 2019 as well. Investors should be researching the fundamentals of CECL accounting and measurement and developing their own CECL readiness preparations. Providing useful SAB 74 numeric disclosures with appropriate context will be an important step for institutions in aiding investor preparations. Further, institutions may reduce investor adoption confusion significantly by conducting pre-adoption education sessions with investors.

A new age for governance



In recent years, regulators, investors, and institutions have increasingly been focusing on the adequacy of governance at all levels of an organization—from the board and senior management to the business lines and independent risk and control functions. Given the significant challenges of managing a bank of significant size and scale, strong governance is the linchpin for ensuring a business is operating as intended and in the best interests of employees, shareholders, and the broader community.

We expect regulatory scrutiny of governance to remain a primary focus for 2019 as past issue remediation is scrutinized, and as proposed guidance issued by the FRB in August 2017[30] and January 2018[31] is finalized.

The current body of banking agency guidance has generally included expectations for board and senior management governance. The OCC issued its Heightened Standards[32] to better describe the expectation for board and risk governance across the three lines of defense. As noted, over the past year and a half, the FRB issued its own series of governance guidance focused on (1) board effectiveness and (2) core principles for senior management, business lines, and independent risk-management and control functions. This proposed guidance[33] is designed to both clarify expectations and assist examiners in rating governance and controls. The FRB's new framework for rating large financial systems, finalized as of November 2, 2018,[34] has three components, placing *Governance & Controls* on equal footing with the Fed's past focus on *Capital* and *Liquidity*.[35]

Board effectiveness

Proposed in August 2017, the FRB's guidance would significantly revise its expectations or boards of directors by specifying the five key attributes of an effective board. By rescinding or revising past guidance and rules, the proposal would set in motion efforts to better delineate the oles, responsibilities, and accountabilities between senior management and the board.

This significant rebalancing of board expectations emerged from the FRB's multiyear post-crisis reviews on board effectiveness at the largest banking organizations, combined with a better understanding from industry of the unintended consequences triggered by past guidance and rules. A key finding by the FRB was that many board requirements in existing guidance and rules had contributed to blurring the lines between boards and senior management, diluting accountability.

Another finding was that boards were devoting significant time to satisfying supervisory expectations at the expense of focusing on their core responsibilities (such as setting strategic direction and articulating risk tolerance). In addition, the Fed found challenges in the flow of information.

The FRB guidance highlights five specific attributes of effective boards:[36]

1. "Set clear, aligned, and consistent direction regarding the bank's strategy and risk tolerance."
2. "Actively manage information flow and board discussions."
3. "Hold senior management accountable."
4. "Support the independence and stature of independent risk management and internal audit."
5. "Maintain a capable board composition and governance structure."

By focusing on specific attributes, the Fed seems to be shifting away from a process-oriented view of board responsibilities. The Fed says it will evaluate banks against these five attributes through its supervisory process; however, it also says larger banks can perform self-assessments for their own improvement, which can be shared with the Fed.

The new board effectiveness guidance should be welcomed by the industry, as should the efforts to revise past guidance and rules in ways that better distinguish the roles, responsibilities, and accountabilities of boards and senior management. However, as this and other guidance and rules are revised and finalized, boards need to recognize that their responsibilities have not diminished. On the one hand, the Fed is removing certain review- and process-oriented expectations that are not core to a board's responsibilities. On the other hand, the Fed is now more clearly specifying how an effective board operates, and will be directing its examiners to consider the five key attributes when rating a board's effectiveness.

Core principles for senior management, business lines, and independent risk and control functions

To help supervisors more broadly rate and set expectations for governance and controls beyond the board of directors, the Fed also proposed guidance with core principles outlining supervisory expectations for senior management, business line management, and the independent risk-management (IRM) and controls functions.

The principles seem broadly consistent with longstanding supervisory expectations from past guidance and supervisory feedback, and do not appear to establish new requirements. Rather, they consolidate and clarify risk-management expectations by better describing and delineating the key elements of governance and controls that the Fed believes are most critical for a bank to be well managed. With regard to managing business lines, the emphasis is on accountability and management of conduct risk— including a focus on detection, prevention, and remediation of risk and compliance issues.

As principles, the guidance gives line supervisors a great deal of discretion to interpret whether institutions are meeting the spirit and substance of the guidance.[37]

Implications for institutions

With some institutions experiencing unexpected losses, harm to customers, and reputational damage (in part due to poor management), investors, regulators, and customers are pressuring boards and management across the three lines of defense to upgrade their bank's practices. Ultimately, regulators are seeking to reinforce sound risk governance principles, and to prompt upgrades over past practices based on industry lessons learned and a better understanding of how the governance process reinforces accountability within the operating model, given the challenges of overseeing and managing a large, diversified institution.

Banks generally recognize that the current economic expansion and relatively benign global business conditions will not last forever. Preparing now for the next business cycle (or potential unexpected event) by establishing a strong governance framework can improve resiliency and lay the foundation for sustainable growth with a competitive edge.

What should institutions have in place?

As banks consider the supervisory guidance and adjusting their frameworks to more explicitly consider their views, there are a number of key elements required for success, including:

- Comprehensive understanding of entity and organization structure
- Documentation of governance at legal entity and business level
- Consistent definition and understanding of materiality
- Concise management information flows
- Policy governance framework
- Clarity of roles and responsibilities

In addition, banks that are further along the path will likely be expected to have in place:

- Internal governance resources
- Effective subsidiary boards
- Internal testing
- Technology enabled processes

Taking action

Banking groups should be realistic about what they expect to achieve. In some cases, there may be substantive governance challenges requiring significant overhauls of the governance operating model—challenges that could take several years to work through, particularly if they involve significant cultural changes to how groups operate. In other cases, governance efforts will focus on existing challenges, but with a renewed focus and clarity on the key issues (rather than treating them as an afterthought of broader structural change, or worse, being forced to act by regulatory intervention that places constraints on the business). A top-down review that considers variations in group practices can help banks identify opportunities to improve their practices and reduce duplication, while relieving some of the pressures of steering highly complex banks through an economic, political, and regulatory environment that is constantly evolving. A more thorough discussion for optimizing the three lines of defense is presented in the "Optimizing across the three lines of defense."

FBO peer landscape for year three of enhanced prudential standards and launch of intermediate holding companies

The key milestone for FBOs to establish US intermediate holding companies (IHCs and to implement the EPS established by the FRB is more than two years past. Much progress has been made across the impacted institutions and capabilities and processes put in place are to be business as usual. Some face challenges in targeted areas, as the focus is now to run the combined US operations and the IHCs within the current global/parent operating model.

Key regulatory developments for FBOs

As noted earlier, the FRB proposed tailoring the EPS for large, domestic banking institutions. The FRB stated that it would release a similar tailoring proposal for FBOs, even though FBOs were not originally included in the financial regulation relief law.

In November 2018, the FRB issued its inaugural Supervision and Regulation Summary,[38] targeting semi-annual distribution. The report highlights issues and forward looking supervisory concerns across institutions it supervises—including the large banking organization portfolio and the Large Institution Supervision Coordinating Committee (LISCC portfolio across US bank holding companies, US banks, and FBOs. Feedback for the FBOs is reported across the LISCC feedback and the LBO feedback. "Large financial institutions are in sound financial condition. Capital levels are strong and much higher than before the financial crisis. Recent stress test results show that the capital levels of large banks after a hypothetical severe global recession would remain above regulatory minimums." Focus for 2019 across the portfolios remains under the banner of the four supervisory pillars: capital, liquidity, governance and controls, and recovery and resolution planning.

Challenges going forward and select IHC-related focus areas

FBOs are moving into year three of their IHC sustainability efforts against a backdrop of external regulatory reform and internal sustainability efforts.

Global/US operating model. Calibrating the right balance between global/parent and combined US operations (CUSO) priorities and considerations when developing a US-focused and—enabled governance and operating model—factoring in opportunities for offshoring, nearshoring, and centralizing of operations across global businesses. The regulators' expectations are that the United States will not be utilized solely as a "booking point."

US managed view. Developing a transparent business strategy within a United States managed view—defining what is originated, booked, or risk managed—with risk limits, triggers, and financials that can be explained across the CUSO and IHC.

CUSO management reporting transparency. Enhancing consistency and flexibility in Management Information Systems (MIS)/reporting views, emphasizing CUSO/IHC/branch dimensions and sustainability of existing regulatory reporting processes for branch to IHC within an overall data governance model and approach.

US regulatory compliance. Continuing to build awareness and knowledge of the existing regulatory requirements and their potential impact on operating models, staffing, systems, and processes. There is currently significant pressure on regulatory change and broader change processes, particularly as management appointments change over time.

FBO focus areas and action items

To achieve business as usual and move toward sustainability, there are a number of focus areas that IHC boards and senior executives can focus on for FBOs (and their CUSOs and IHCs) regarding EPS compliance for 2018/2019:

Business strategy and booking models. Reassess the sustainability and global impact of the US business strategy and booking models across IHC/branches. Identify markets and business lines in US operations that should continue to be profitable to support the IHC. Evaluate business models linked to strategic planning and the linkage to parent bank plans for US operations. Evolve booking practices for IHC activities and branch activities.

Governance and three lines of defense. Demonstrate the ability to operate autonomously in the United States, with clear delegation of authority from parent. Fine-tune the operating model for the IHC board, CUSO management, business line management, and the three lines of defense, with clearly outlined roles and responsibilities across business lines,

control functions, compliance, and internal audit (across Regulation YY[39] and related safety and soundness requirements).

Regulatory change and portfolio management. Connect the dots across regulatory change (e.g., understand expectations for capabilities across the four supervisory areas—capital, liquidity, governance and controls, and resolution planning). Monitor the regulatory landscape and the impact of the current legislative landscape and changes as a result of regulatory agency focus areas including tailoring, proposed rulemaking and supervisory guidance.

Internal MIS and regulatory reporting effectiveness. Review internal reporting/MIS on an end-to-end basis to support the governance model for issue escalation, risk monitoring, challenge, and review. Implement data governance and close data quality gaps within the FBO/parent approach within overall parent bank context across internal and regulatory reporting.

Sustainable training and awareness across parent, affiliates and CUSO. Continue awareness and training regarding the US regulatory environment over the long term, and ensure new processes align with parent perspectives and changes.

Integration of capital planning process into CUSO process. Work through lessons learned and year three improvements; also, calibrate top-down versus bottom-up business planning. Advance toward sustainability of the attestation/certification framework, data and controls, CCAR "business as usual" operating model, and modeling and validation processes across the three lines of defense.

Liquidity planning and stress testing. Focus on operational sustainability for end-to-end liquidity processes that link business-as-usual, stress, recovery, and resolution frameworks with appropriate infrastructure upgrades for flexibility in data, controls, reporting, and governance.

Resolution planning in the spotlight. Calibrate resolution strategy to FBO guidance for alignment by July 1, 2018. Align the IHC board and CUSO governance processes. Implement operational capabilities that were outlined in March 2017 guidance across financials, collateral, risk management, reporting, and monitoring guidance provided to the US BHCs.[40]

Strategic remediation and issue identification. Build end-to-end remediation that is strategic, holistic, and positions the organization for future growth and sustainability.

Implementation of a risk management framework within a parent model. Drive challenge and decision rights for the US CRO in implementing the CUSO Risk Management Framework within a global model (risk governance, strategy, decisions rights, escalation, and risk tolerances across the risk hierarchy).

Other important regulatory topics

A recent risk perspective from the OCC reports that capital and liquidity are at or near historic highs, and that asset quality is sound as measured by traditional metrics. Earnings, aided by low loan losses and tax law changes, continue to improve. Additionally, the OCC reports "incremental improvement in banks' overall risk management practices."

However, after a long period of economic expansion, rising concerns exist in some areas. Here are a few additional topics bank risk managers should have on their radar.

Rising interest rates

Although recent rate increases have thus far generally been a good thing for most banks, there are also potential downsides. Since the recession, deposits have increased as a share of banks' liabilities and the ratio of nonmaturity deposits to total deposits has also increased. When interest rates were near zero, acquiring deposits, including nonmaturity deposits, was easier since customers had little incentive to look elsewhere. Even when rates started moving up in late 2015/early 2016, deposit betas (change in deposit interest rates relative to the change in market interest rates) remained initially low.

However, as rates have continued to move up, competition from money market funds and other short-term investments has returned. Deposit betas (the relative speed at which deposit rates move relative to market rates) are increasing and banks' ability to grow deposits is becoming more difficult. Large banks with liquidity coverage ratio (LCR) requirements also provide competition. Asset/liability managers should closely monitor deposit beta trends and recalibrate models accordingly. They should also carefully plan appropriate funding and liquidity management strategies in the face of increasing deposit competition. Rising market interest rates also raise concerns in the credit area. See the credit comments below for more detail.

Capital and CCAR

CCAR continues to be the annual report card for large financial institutions, while the FRB has also made efforts to enhance the transparency surrounding CCAR and stress testing procedures. The 2018 CCAR results did not raise a quantitative objection for any bank despite three banks falling below minimum capital requirements under stress, and several banks showed deficiencies in areas including internal controls, stress loss forecasting, and trading strategy vulnerabilities.[41]

In April 2018, the FRB issued a proposal to more closely align capital requirements and the Comprehensive Capital Analysis and Review (CCAR).[42] The proposed changes would create a *stress capital buffe*r (SCB) that would be calculated based on the decrease in capital a bank experiences under the hypothetical "severely adverse scenario" in its annual CCAR. In addition, in July 2018, the federal banking agencies issued a joint statement on the implementation of EGRRCPA, the agencies extended the deadline for company run stress tests by 18 months for all insured depositories below $100 billion, effectively eliminating the requirement immediately.[43]

In recent speeches, FRB Vice Chair Quarles has suggested making the following changes to the stress testing regime:[44]

Adopt SCB and re-propose certain elements. The FRB will soon issue a final rule to adopt the SCB, but will re-propose certain elements of the SCB framework:

- **Dampen volatility of stress test results:** The FRB is considering ways of preserving the dynamism of stress testing while reducing its volatility. Currently, a highly variable capital requirement from year to year presents a management challenge. In addition, the FRB is exploring ways to incorporate multiple market shocks in its stress test (rather than a single market shock) to fully capture the risk in banks' trading books.
- **Reorder capital planning sequence:** The FRB is evaluating adjusting the operation of the capital planning rule so that a bank knows its SCB before it decides on its planned distributions for the coming year. This change would effectively eliminate the pass/fail aspect of CCAR and capital planning. The FRB would continue to test a bank's ability to predict its stress losses and incorporate those losses into its capital planning through the supervisory process.
- **Include share repurchases in SCB:** The FRB is reconsidering the requirement that the SCB include four quarters of dividends. The FRB is looking for ways to encourage greater reliance on share repurchases, which the FRB assumes are easier than dividends for a bank to cancel in times of stress.
- **Remove stress leverage buffer:** The FRB is considering removing the stress leverage buffer that the Federal Reserve proposed along with the SCB in the April 2018 proposal. Leverage requirements are not intended to be risk-sensitive, and determining requirements based off risk-sensitive post stress estimates runs counter to that definition. The FRB would retain "static" leverage ratios, including the enhanced Supplementary Leverage Ratio, in the regulatory capital regime.

- **Adjust operation of capital buffers:** The banking agencies may seek to change the current operation of capital buffers, which limit a bank's capital distributions and discretionary bonus payments to a percentage of "eligible retained income" when the bank dips into its buffer. In a strong economic cycle, when banks distribute all or nearly all of their income for the year, their eligible retained income could be zero or near zero. As a result, dipping into a capital buffer—by even a small amount—results in an immediate cessation of all capital distributions. The FRB is considering making the rules "more consistent with the graduated intent."

With these adjustments, the SCB would not go into effect before 2020. The FRB will also consider whether any elements of the April 2018 proposal can be implemented in the 2019 CCAR exercise, such as relaxation of assumptions related to balance sheet growth.

- **Increase transparency:** The FRB is evaluating the following changes to increase the transparency involved with the stress testing process:
- **Governing principles for supervisory stress testing:** The FRB will soon issue a policy statement describing the governing principles around the supervisory stress testing process, including detail about models and results, and publishing portfolios of hypothetical loans and associated loss rates.
- **Public input on scenario design:** The FRB is considering gathering the public's input on scenarios and salient risks facing the banking system each year.

Qualitative objection. The FRB is considering eliminating the qualitative objection in CCAR for the banks that remain subject to it, while continuing to evaluate a bank's stress testing processes through normal supervision.

Regardless of these changes, regulators will still expect banks to maintain sound capital planning frameworks. Thus, even for banks with fewer stress testing mandates, stress testing will still be required to calibrate risk appetites and to properly size capital levels. The difference is that banks will be able to incorporate stress testing into planning processes with more control over tailoring, and without being bound by a regulatory calendar.

Consumer compliance

Despite a change in tone at the CFPB—along with softening views on the permissibility of certain products such as small-dollar loans—the fair and responsible treatment of consumers remains as important as ever. And unlike the more esoteric compliance issues in institutional and wholesale products, unfair or illegal breaches in the consumer area are well understood by the general public. As such, they can rapidly create major reputational issues through social and other media, and quickly grab the attention of regulators.

A recent "Supervisory Highlights" published by the CFPB[45] summarizes the following issues found in recent examinations:

- Deceptive billing practices on auto loans after application of insurance proceeds from a total vehicle loss;
- Repossessing vehicles after the repossession was supposed to be cancelled, an unfair practice;
- For credit cards, and contrary to Regulation Z,[46] (a) failed to reevaluate all eligible accounts, (b) failed to consider the appropriate factors when reevaluating eligible accounts, or (c) failed to appropriately reduce the rates of accounts eligible for rate reduction;
- Debt collectors that failed to obtain and mail debt verifications before engaging in further collection activities pursuant to Fair Debt Collection Practices Act (FDCPA);
- Residential mortgage servicers that inappropriately delayed processing the permanent modification after the consumer successfully completed the trial modification;
- Mortgage servicers that charged consumers unauthorized amounts;
- Mortgage servicers who initiated foreclosure after the borrower had properly accepted a loss mitigation offer.

Many of these issues appear to be a result of operational breakdowns stemming from improper process design and/or implementation. Specific actions that can be taken to build a robust compliance framework include:

- Inventory all compliance management processes and conduct an end-to-end review for each process
- Implement a robust process to aggregate, categorize, and analyze customer complaints, whistleblower comments, fraud investigations, social media comments, and other "voice of the customer" channels
- Monitor regulatory publications (e.g., the CFPB's "Supervisory Highlights" and the OCC's "Semiannual Risk Perspective"[47] to understand issues occurring in the industry, in order to identify if similar issues exist at your bank
- Consider RPA to improve compliance outcomes and drive effectiveness and efficiency

Credit

Traditional credit metrics at most banks appear to be in good shape, as has been the case for some time now. However, risk managers with long memories will tell you that times like these are when you should become concerned. When the good times are rolling and credit portfolios are in great shape, the focus turns to loan growth and competition heats up. As a result, pricing becomes tighter, underwriting gets looser, and policy exceptions increase.

Although a recent FRB survey seemed to indicate[48] some focused tightening, the general trend over the past several years in both FRB and OCC surveys is one of loosening underwriting standards. And though the OCC in a recent "Semiannual Risk Perspective" indicated that the majority of banks operate with a moderate credit risk appetite, it also articulated some concerns in credit underwriting. Of note was a recent increase in outstanding matters requiring attention (MRA) concerns related to commercial credit underwriting. The OCC listed these examples of underwriting issues: "Diminished protective financial covenants, generous cash flow adjustments, limited or no guarantees, longer amortization periods, extended interest-only terms, and higher loan-to-value ratios or advance rates." The OCC also noted an increased risk appetite in credit cards and auto lending, which has resulted in increasing delinquencies. In addition, the FRB recently issued its October senior loan officer survey. The survey found that loan standards are easing due to falling demand.[49]

Rising interest rates will also likely put a strain on certain types of credit. Portfolios that probably will be affected include leveraged lending, some commercial real estate credits, and highly leveraged consumer borrowers.

Don't get us wrong; making loans and thriving is what banks are supposed to do. But past credit downturns have not been visible very far in advance. When they do occur, they sometimes are more severe than anticipated, with loss content higher than expected. That's why, when times are good, it is important to maintain a level of credit discipline that is informed by experiences from past downturns.

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, https://www.congress.gov/bill/115th-congress/senate-bill/2155, accessed December 6, 2018.
2. Federal Register, "Single-Counterparty Credit Limits for Bank Holding Companies and Foreign Banking Organizations," https://www.federalregister.gov/documents/2018/08/06/2018-16133/single-counterparty-credit-limits-for-bank-holding-companies-and-foreign-banking-organizations, accessed December 6, 2018.
3. Board of Governors of the Federal Reserve System, "Notices of proposed rulemaking to tailor prudential standards," https://www.federalreserve.gov/aboutthefed/boardmeetings/files/board-memo-20181031.pdf, accessed December 6, 2018.
4. Board of Governors of the Federal Reserve System, "Prudential Standards for Large Bank Holding Companies and Savings and Loan Holding Companies," https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20181031a2.pdf, accessed October 31, 2018; and Office of the Comptroller of the Currency, "Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Proposed Changes to Applicability Thresholds for Regulatory Capital and Liquidity Requirements," https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20181031a1.pdf, accessed October 31, 2018. The OCC adopted the Interagency Proposal on October 31, 2018.
5. Office of the Comptroller of the Currency, "OCC seeks comments on modernizing Community Reinvestment Act regulations," https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-87.html, accessed December 6, 2018.
6. Board of Governors of the Federal Reserve, "Agencies extend deadline for certain resolution plan submissions," https://www.federalreserve.gov/newsevents/pressreleases/bcreg20180830a.htm, accessed December 6, 2018.
7. Government Printing Office, "OCC guidelines establishing standards for recovery planning by certain large insured national banks, insured federal savings associations, and insured federal branches; technical amendments," https://www.gpo.gov/fdsys/pkg/FR-2018-09-19/pdf/2018-20166.pdf, accessed December 6, 2018.
8. Deloitte, "FRB, FDIC issue proposed additional and consolidated guidance for 2019 GSIB resolution plans," https://www2.deloitte.com/us/en/pages/regulatory/articles/frb-fdic-issue-proposed-additional-and-consolidated-guidance-for-2019-g-sib-resolution-plans.html, accessed December 6, 2018.
9. Ibid.
10. Office of the Comptroller of the Currency, "Core lending principles for short-term, small-dollar installment lending," https://www.occ.gov/news-issuances/bulletins/2018/bulletin-2018-14.html, accessed December 6, 2018.
11. Federal Register, "Proposed guidance on supervisory expectation for boards of directors," https://www.federalregister.gov/documents/2017/08/09/2017-16735/proposed-guidance-on-supervisory-expectation-for-boards-of-directors, accessed December 6, 2018.
12. Board of Governors of the Federal Reserve System, "Supervision and Regulation Report," https://www.federalreserve.gov/publications/2018-november-supervision-and-regulation-report-preface.htm, accessed December 6, 2018.
13. Jame Lewis/McAfee, "Economic impact of cybercrime—No slowing down," https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf, accessed December 6, 2018.
14. Deloitte, "Beneath the surface of a cyberattack," https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html, accessed December 6, 2018.
15. Securities and Exchange Commission, "Commission statement and guidance on public company cybersecurity disclosures," 17 CFR Parts 229 and 249, February 26, 2018.
16. US Department of the Treasury, "A financial system that creates economic opportunities: Banks and credit unions," https://www.treasury.gov/press-center/press-releases/Documents/A%20Financial%20System.pdf, accessed December 6, 2018.
17. 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, accessed December 6, 2018.
18. "The California Consumer Privacy Act of 2018,"Assembly Bill 375, Chapter 55, State of California, June 29, 2018
19. Securities and Exchange Commission, "Commission statement and guidance on public company cybersecurity disclosures," 17 CFR Parts 229 and 249, February 26, 2018.
20. American Institute of Certified Public Accountants, "System and Organization Controls (SOC) for Cybersecurity," https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html, accessed December 6, 2018.

21. Brazil's General Data Protection Law.
22. Information Commissioner's Office, "Data Protection Act 2018," https://ico.org.uk/for-organisations/data-protection-act-2018/, accessed December 6, 2018.
23. Cyber Security Agency of Singapore, "Cybersecurity Act," https://www.csa.gov.sg/legislation/cybersecurity-act, accessed December 6, 2018.
24. Office of the Australian Information Commissioner, "Privacy Act," https://www.oaic.gov.au/privacy-law/privacy-act/, accessed December 6, 2018.
25. US Department of the Treasury, "Core principles," https://home.treasury.gov/policy-issues/top-priorities/regulatory-reform, accessed December 6, 2018.
26. US Department of the Treasury, "A financial system that creates economic opportunities: Nonbank financials, fintech, and innovation," https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf, accessed December 6, 2018.
27. Deloitte, "Fintech by the numbers: Incumbents, startups, investors adapt to maturing ecosystem" (2017), https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/financial-services/dcfs-fintech-by-the-numbers.pdf, accessed December 6, 2018.
28. Consumer Financial Protection Bureau, "Policy on No-Action Letters and the CFPB Product Sandbox," http://src.bna.com/DOC, accessed December December 12, 2018.
29. Basel Committee on Banking Supervision, "Principles for effective risk data aggregation and risk reporting," https://www.bis.org/publ/bcbs239.pdf.
30. Deloitte, "A new age for governance," https://www2.deloitte.com/us/en/pages/regulatory/articles/frb-proposed-guidance-board-effectiveness.html, accessed December 6, 2018.
31. Deloitte, "FRB proposes new supervisory expectations for management," https://www2.deloitte.com/us/en/pages/regulatory/articles/frb-proposed-guidance-supervisory-expectations.html, accessed December 6, 2018.
32. Office of the Comptroller of the Currency, "OCC finalizes its heightened standards for large financial institutions" https://www.occ.treas.gov/news-issuances/news-releases/2014/nr-occ-2014-117.html, accessed December 6, 2018.
33. Deloitte, "FRB proposes new supervisory expectations for management" https://www2.deloitte.com/us/en/pages/regulatory/articles/frb-proposed-guidance-supervisory-expectations.htmll, accessed December 6, 2018.
34. Deloitte, "New rating system for large financial institutions" https://www2.deloitte.com/us/en/pages/regulatory/articles/federal-reserve-board-rating-system-large-financial-institutions.html, accessed December 6, 2018.
35. The new rating system would apply to bank holding companies (BHCs) and non-insurance, non-commercial savings and loan holding companies (SLHCs) with more than $50 billion in total assets, as well as intermediate holding companies (IHCs) of foreign banking organizations.
36. Deloitte, "A new age for governance," https://www2.deloitte.com/us/en/pages/regulatory/articles/frb-proposed-guidance-board-effectiveness.html, accessed December 6, 2018.
37. Deloitte, "FRB proposes new supervisory expectations for management," https://www2.deloitte.com/us/en/pages/regulatory/articles/frb-proposed-guidance-supervisory-expectations.html, accessed December 6, 2018.
38. Board of Governors of the Federal Reserve System. "Supervision and Regulation Report November 2018," https://www.federalreserve.gov/publications/files/201811-supervision-and-regulation-report.pdf, accessed December 6, 2018.
39. Federal Reserve Board, "Regulation YY Foreign Banking Organizations Requests," https://www.federalreserve.gov/supervisionreg/regulation-yy-foreign-banking-organization-requests.htm, accessed December 6, 2018.
40. Federal Deposit Insurance Corporation, Federal Reserve Board, "Living Wills," https://www.federalreserve.gov/supervisionreg/resolution-plans.htm, accessed December 6, 2018.
41. Board of Governors of the Federal Reserve System, "Federal Reserve releases results of Comprehensive Capital Analysis and Review (CCAR)," https://www.federalreserve.gov/newsevents/pressreleases/bcreg20180628a.htm, accessed December 6, 2018.
42. Federal Reserve Board, "Federal Reserve Board seeks comment on proposal to simplify its capital rules for large banks while preserving strong capital levels that would maintain their ability to lend under stressful conditions," https://www.federalreserve.gov/newsevents/pressreleases/bcreg20180410a.htm, accessed December 6, 2018.
43. Federal Reserve Board, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation, "Interagency statement regarding the impact of the Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA)," https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20180706a1.pdf, accessed December 6, 2018.

44. Federal Reserve Board, "A New Chapter in Stress Testing," https://www.federalreserve.gov/newsevents/speech/quarles20181109a.htm, accessed December 6, 2018; and Federal Reserve Board, "Beginning Stress Testing's New Chapter," available at https://www.federalreserve.gov/newsevents/speech/quarles20181116a.htm, accessed December 6, 2018.

45. Consumer Financial Protection Bureau, "Supervisory Highlights, Issue 17, Summer 2018," https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/bcfp_supervisory-highlights_issue-17_2018-09.pdf, accessed December 6, 2018.

46. Consumer Financial Protection Bureau, "12 CFR Part 1026 – Truth in Lending (Regulation Z)," https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1026/, accessed December 6, 2018.

47. Office of the Comptroller of the Currency, "Semiannual Risk Perspective," https://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/index-semiannual-risk-perspective.html, accessed December 6, 2018.

48. Federal Reserve Board, "Senior Loan Officer Opinion Survey on Bank Lending Practices," https://www.federalreserve.gov/data/sloos.htm, accessed December 6, 2018.

49. Federal Reserve Board, "Senior Loan Officer Opinion Survey on Bank Lending Practices," https://www.federalreserve.gov/data/sloos/sloos-201810.htm, accessed December 6, 2018.

Contacts

Leadership

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

Vik Bhat
Advisory Banking & Capital Markets Leader
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
vbhat@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

John Corston
Independent Senior Advisor to Deloitte & Touche LLP
jcorston@deloitte.com

Irena Gecas-Mccarthy
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
igecasmccarthy@deloitte.com

Corey Goldblum
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
cgoldblum@deloitte.com

Marlo Karp
Americas Regulatory Risk Leader
Partner | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
mkarp@deloitte.com

Satish Lalchand
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
slalchand@deloitte.com

Ken Lamar
Independent Senior Advisor to Deloitte & Touche LLP
kelamar@deloitte.com

Gregory Norwood
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
grnorwood@deloitte.com

Jonathan Prejean
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
jprejean@deloitte.com

Gina Primeaux
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
gprimeaux@deloitte.com

Peter Reynolds
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
pereynolds@deloitte.com

John Wagner
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
johnwagner@deloitte.com

Dave Wilson
Independent Senior Advisor to Deloitte & Touche LLP
daviwilson@deloitte.com

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

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

Nitin Pandey, Senior Manager| Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Richard Rosenthal, Senior Manager| Deloitte Risk and Financial Advisory, Deloitte & Touche LLP

CENTER *for*
REGULATORY STRATEGY
AMERICAS

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

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

Deloitte.