Contents

Global foreword 4
The new age of tailoring by bank regulators 7
Governance frameworks remain in focus 11
Shift to nonfinancial risk 14
Optimizing across three lines of defense: New paradigms for risk and compliance management 17
Operational resilience 20
Cybersecurity and privacy 23
Third-party risk management 25
Technology: Modernizing and innovating 26
Data capabilities in banking: The journey continues 28
Navigating the changing financial crime compliance landscape 32
Structural optimization 33
Credit 35
CECL: Investors want a clear story; will CFOs be prepared to tell it? 36
LIBOR transition: Time is running out 38
Volcker 2.0 40
FBO industry landscape in year four of Enhanced Prudential Standards 42
Other important regulatory topics 46
Staying ahead 47
Leadership 47
This publication is part of the Deloitte Center for Regulatory Strategy, Americas’ cross-industry series on the year’s top regulatory trends. This annual series provides a forward look at some of the regulatory issues we anticipate will have a significant impact on the market and our clients’ businesses in 2020. The issues outlined in each of the reports provide a starting point for an important dialogue about future regulatory challenges and opportunities to help executives stay ahead of evolving requirements and trends. For 2020, we provide our regulatory perspectives on the following industries and sectors: banking; capital markets; insurance; investment management; energy, resources, & industrials; life sciences; and health care. For a view of the other trends that affect insurance in 2020, we encourage you to read the Deloitte Center for Financial Services companion paper.

We hope you find this document to be helpful as you plan for 2020 and the regulatory changes it may bring. Please feel free to contact us with questions and feedback at CenterRegulatoryStrategyAmericas@deloitte.com.
Global foreword

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

Economic outlook

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

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

Meanwhile in China, growth has continued to slow and gross debt surged from 171% of Gross Domestic Product in 2008 to 299% in 2018. High debt levels could become unsustainable if growth slows further.

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

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

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

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

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

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

**The fraying international consensus**

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

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

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

**More accountability for senior individuals**

In contrast, regulators are increasingly holding senior individuals to account for the compliance, professional standards and culture of their firms. Following the introduction of the UK’s Senior Managers and Certification Regime, similar regimes have emerged, or are emerging, in several other jurisdictions, including Ireland, Australia, Hong Kong Special Administrative Region, Singapore and South Africa. Other jurisdictions are driving increased accountability through different mechanisms. The US Federal Reserve Board has proposed guidance which seeks to delineate the roles, responsibilities and accountabilities of senior management and the board better. The Belgian Parliament recently announced the introduction of a “Banker’s Oath” similar to that which the Netherlands introduced in 2015. In response to these initiatives, firms will need to foster a culture of accountability through measures such as balanced incentive plans; strong governance and controls; and appropriate monitoring, reporting, escalation and disciplinary action.

**Regulating technological innovation**

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

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

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

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

Regulators and supervisors will also need to accelerate their own digital transformation. Well-resourced regulatory data science and analytics capabilities will be essential to understand and supervise a financial sector characterised by an increasingly blurred regulatory perimeter and greater technological complexity. Part of the solution may be for financial, security and data protection authorities to share resources, capabilities and insights more effectively. We see efforts in this direction, but more work is needed before regulators and firms can reap the benefits. Progress will more likely be achieved at national than at international level, mainly because of the absence of cross-sectoral global standard-setting bodies.
Responding to social concerns
Environmental sustainability is a rising social concern, and in Europe and Asia, a major focus for financial services regulators. In the US, it is not—at least not at federal level. However, even where regulators do not introduce specific requirements, firms will need to consider how climate change and unsustainable business models will affect their asset and liability exposures, as well as the new opportunities that may arise from the increasing customer demand for “green” products, including green investment funds.

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

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

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

The recent final rule by the FRB that tailored the Enhanced Prudential Standards (EPS) for domestic and foreign holding companies marks a significant new stage in the evolution of tailoring by bank regulators—a trend that intensified under the current administration. As designed, the EPS tailoring rule fine-tunes requirements for capital, stress testing, liquidity, large exposures, and reporting based on financial metrics that serve as a proxy for a firm’s size, complexity, interconnectedness, and systemic importance.

Although the FRB used its discretion in establishing the tailoring metrics, the rule is largely consistent with the asset size thresholds laid out in the EGRRCPA.¹ In some cases, it provides tailoring relief beyond that of the legislation, which gave the FRB more discretion to tailor or eliminate EPS requirements. In a complementary rulemaking, the FRB and Federal Deposit Insurance Corporate (FDIC) also tailored requirements related to resolution plans (aka “living wills”) in a similar manner. Moreover, the banking agencies are working to finalize their related EPS and other rules at the insured depository level.

Efforts to tailor the postcrisis reform standards reflect concern that initial efforts had gone too far and did not adequately balance the tradeoff between safety and soundness and burden, especially for smaller, less complex firms. Much of the tailoring reflects the experience of the industry and regulators in implementing and enforcing the latest rules and guidance. To date, the largest systemic firms have only been granted very modest relief, while smaller firms have received modest to substantial relief.

New tailoring criteria
A combination of elements determines where a firm lies on the spectrum of EPS tailoring categories (and their corresponding financial and risk management expectations). Most of the criteria were chosen to be simple, intuitive, and transparent, yet still correlated with the risk posed by an institution’s operations. The key criteria are shown in figure 1, and a detailed view of how the criteria are combined to create categories—and how requirements change by category. The key criteria are shown in figure 1.

Other tailoring efforts resulting in regulation changes
Over the past year, many banking agencies have also proposed or finalized other rulemakings consistent with EGRRCPA mandates and their own efforts to ease the burden, especially on regional and community banking organizations. Final rules include:

- Volcker Rule tailoring requirement based on size of trading assets and exemption of community banks²
- Simplifying reporting requirements for qualifying community banks³
- Simplifying capital requirements for qualifying community banks⁴
- Lengthening of exam cycles for smaller banks and branches and agencies⁵
- Raising the asset threshold that defines small bank holding companies subject to lesser requirements⁶

Tailoring supervision versus regulation
Over the past decade, the banking agencies have stated that their supervision and regulation of financial institutions is “commensurate with the size, complexity and risk profile” of banking organizations.⁷ In prior decades, tailoring of supervision and regulation largely focused on bank asset size, foreign exposure, legal entity type, and size of trading assets. Regulations and guidance were applied on these simple measures regarding capital rules and risk management expectations.

For supervision, examiners continue to exercise a great deal of latitude in interpreting how well an institution is adhering to rules or guidance based on their own judgments about the firm’s quality of management relative to its complexity and risk. That is unlikely to change, although expectations will be better delineated by category of company. At present, supervision programs continue to categorize firms as systemic banks, large regionals, foreign entities, or community organizations, and these supervision groupings might be more fully defined and segregated based on the new thresholds.

Currently, examination procedures and supervisory strategies are geared toward the broader institution types. Systemic firms and large regional firms receive horizontal supervisory reviews that allow supervisors to compare practices across firms and establish...
Global forward Leadership

Banking regulatory outlook 2020

The new age of tailoring by bank regulators

Risk and complexity indicators

These criteria were chosen as risk indicators for complexity and risk, with a goal of achieving simplicity and transparency of view.

All numbers are in billions.

<table>
<thead>
<tr>
<th>Entity type</th>
<th>&gt;&gt;$700</th>
<th>&lt;$700 &amp; &gt;=$250</th>
<th>&lt;$250 &amp; &gt;=$100</th>
<th>&lt;$100 &amp; &gt;=$50</th>
<th>&gt;&gt;$100</th>
</tr>
</thead>
<tbody>
<tr>
<td>US bank holding company (BHC)</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>Intermediate holding company (IHC)</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>N/A</td>
</tr>
<tr>
<td>Combined US operations (CUSO)</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>N/A</td>
</tr>
<tr>
<td>Global foreign banking Organizations (FBOs)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>√</td>
</tr>
</tbody>
</table>

“√” – Applicability for the asset threshold

“√” – Categories where corresponding requirement is applicable

G-SIB designation

If a firm is designated as a global systemically important bank (G-SIB) as defined in a separate rule, they are designated as a Category 1 firm for tailoring and face the most stringent requirements. The “G-SIB” designation criteria are determined on a more complex weighting of criteria, measuring size, interconnectedness, market preeminence, and other factors to identify the systemic risk posed by the US bank holding companies to the financial stability of the US. The rule was approved by the FRB in 2015.2
a consistent bar regarding what is considered a safe and sound practice. The topics and intensity of reviews are, of course, different depending on the portfolio type. For example, in the FRB’s most recent supervision and regulation report, they indicate their priority will be on topics such as operational and cyber resilience, while for community banks, the focus continues to be on asset concentrations.

It is important to note that, while there has been relief in the rules applied to institutions, the intensity of examiner scrutiny and level of expectations appear to have lightened only modestly and may have increased in some areas for some systemic firms. Regardless of which new tailoring category a firm may find itself in, examiner scrutiny of the basic blocking and tackling of risk management and related capabilities is unlikely to lighten appreciably in the near future.

Implications for institutions
Threshold management
As a result of increased tailoring, the number and complexity of thresholds that drive requirements and expectations for bank supervision and regulation will be more challenging than ever to navigate. Going forward, as firms grow (organically or through acquisition), change their funding strategies, diversify their operations through nonbank acquisitions, or diversify their product offerings, they may find that they have crossed an important threshold.

A threshold crossing can have a range of consequences, from minor to significant. For example, a firm that crosses over the $100 billion threshold will need to establish the ability to annually submit capital plans to the FRB. A firm with $200 billion in assets that has grown its nonbank activities beyond $75 billion will find its operations subject to the publication of company-run stress tests, as well as the FRB’s comprehensive capital analysis and review (CCAR) and FRB stress tests, among other requirements. On the other hand, the tailoring rule provides opportunity to review the US footprint for large FBOs. For example, an FBO with IHC assets over the $100 billion threshold can leverage this opportunity to consider moving assets out of the IHC to its branches and be subject to less stringent capital and liquidity requirements.

Key to operating in this new environment is to be forward-looking, aware, and deliberate regarding thresholds. Some important actions firms should consider taking include:

- **Normalize threshold triggers into the operation.** Incorporate thresholds into strategic planning, change management, and compliance processes throughout the organization.
- **Perform cost/benefit analysis.** As the firm grows and is at risk of crossing a threshold, perform a high-level gap assessment and a cost/benefit analysis weighing the cost of implementing capabilities and adhering to stricter requirements versus an opportunity for growth and diversification.

**Take the best and leave the rest**

Many institutions received some degree of relief regarding requirements and expectations as a result of the tailoring rules. It might be tempting to abandon enhanced standards around a stress test, liquidity measure, or other risk management requirement. However, firms should keep in mind that regulators will still expect rigorous capital and liquidity frameworks as a safety and soundness matter, even though the approach is not bound by specific rules. It is important to unwind the programs in a methodical manner that retains risk management and other benefits while discarding portions that are unnecessarily bureaucratic and burdensome. Such an approach can help maintain credibility and with regulators over the long run. Institutions should ask themselves the following questions as they think about unwinding:

- Are there features of the current requirement that can be discarded while retaining their core benefits?
- To what extent is the requirement limiting our flexibility in achieving our strategic objectives?
- To what extent is the requirement helping our control functions manage risk-taking in a balanced way?
- Over the long run, will we need to reestablish this capability as we grow and pass into the higher thresholds?
- To what extent has the requirement become embedded in our risk appetite and strategic planning, and would this element be missed if discarded?

Improved tailoring of regulatory requirements across EPS, resolution planning, and basic compliance with regulation and the safety and soundness standards is a welcome innovation from Congress and regulators. However, institutions should ultimately complement these tailored regulatory expectations with their own North Star of what good looks like for a well-run and profitable organization.
Take the best and leave the rest

Many institutions received some degree of relief regarding requirements and expectations as a result of the tailoring rules. It might be tempting to abandon enhanced standards around a stress test, liquidity measure, or other risk management requirement. However, firms should keep in mind that regulators will still expect rigorous capital and liquidity frameworks as a safety and soundness matter, even though the approach is not bound by specific rules. It is important to unwind the programs in a methodical manner that retains risk management and other benefits while discarding portions that are unnecessarily bureaucratic and burdensome. Such an approach can help maintain credibility and with regulators over the long run. Institutions should ask themselves the following questions as they think about unwinding:

• Are there features of the current requirement that can be discarded while retaining their core benefits?
• To what extent is the requirement limiting our flexibility in achieving our strategic objectives?
• To what extent is the requirement helping our control functions manage risk-taking in a balanced way?
• Over the long run, will we need to reestablish this capability as we grow and pass into the higher thresholds? To what extent has the requirement become embedded in our risk appetite and strategic planning, and would this element be missed if discarded?

Improved tailoring of regulatory requirements across EPS, resolution planning, and basic compliance with regulation and the safety and soundness standards is a welcome innovation from Congress and regulators. However, institutions should ultimately complement these tailored regulatory expectations with their own North Star of what good looks like for a well-run and profitable organization.

1. The EGRRCPA was signed into law on May 24. It increased the asset threshold for a banking organization to be designated as a systemically important financial institution (“SIFI”) from $50 billion to $100 billion immediately after enactment, with a further increase 18 months after enactment.  
5. Ibid.  
7. Ibid.  
Governance frameworks remain in focus

Strong governance is required to deliver financial services in a safe and sound manner. As such, regulators continue to focus on governance frameworks during examination activities. In particular, regulators often identify a breakdown in governance and controls as one of the root causes when something goes wrong. All levels of the organization are being scrutinized—from the board and senior management to the business lines, independent risk management, and audit functions.

Since governance and controls are sure to remain a hot regulatory topic in 2020, we outline below the current state of regulatory expectations, including what has changed and what has not.

As we write this, the FRB proposals outlining supervisory expectations for the board of directors (BoD) (Board Effectiveness Guidance) and for senior management, business line management, and independent risk management and controls (Management Guidance) have not been finalized. However, FRB officials have indicated they expect these documents, first proposed in August 2017 and January 2018 respectively, to be finalized soon. Although the final versions might contain some modifications from the proposed versions, the broad expectations outlined in these two proposals are not expected to materially change.

In November 2018, the FRB finalized its new rating framework for large financial institutions. This revised system has three components: (1) Capital Planning and Positions, (2) Liquidity Risk Management and Positions, and (3) Governance and Controls. In order for a firm to be considered “well-managed” consistent with various statutes and regulations, it must be rated as “broadly meets expectations” or “conditionally meets expectations” for all three components. Governance has been placed on equal footing with the capital and liquidity components, which arguably received greater focus historically.

In July 2019, the Office of the Comptroller of the Currency (OCC) updated the Corporate and Risk Governance booklet of the Comptroller’s Handbook.1 While broadly consistent with the OCC’s Heightened Standards guidance for large banks, issued in September 2014, the booklet is intended to be used for national banks of all sizes, calling out Heightened Standards in separate text boxes.

The OCC handbook update and the FRB proposed guidance and statements both clarify the role of the BoD to better distinguish its responsibilities from the role of management with regard to providing overall direction and oversight. Additionally, the two agencies continue to review their policies and examination protocols to better define the responsibilities of both groups.

On October 18, 2019, the FDIC and FRB solicited comment on the Uniform Financial Institutions Rating System (UFIRS). The UFIRS is more commonly known as the CAMELS Rating System (Capital adequacy, Asset Quality, Management, Earnings, Liquidity, and Sensitivity to Market Risk). The request for comment asks industry participants how federal banking agencies use the system, their consistency, and the implications of the system on expanding business activities and enforcement actions.2

**Regulatory expectations for boards: FRB and OCC**

FRB and OCC expectations for boards are similar, but not identical. For example, the FRB Board Effectiveness proposed guidance3 specifies the following five elements:

- Set clear, aligned, and consistent direction regarding the bank’s strategy and risk tolerance
- Actively manage information flow and board discussions
- Hold senior management accountable
- Support the independence and stature of independent risk management and internal audit
- Maintain a capable board composition and governance structure

Meanwhile, the OCC’s Heightened Standards set forth the following requirements:

- Require an effective risk governance framework
- Provide active oversight of management
- Exercise independent judgment
- Include independent directors (for the bank under the holding company)
Global forward Leadership

Banking regulatory outlook 2020 | Governance frameworks remain in focus

• Provide ongoing training to all directors
• Conduct annual self-assessments

Going further, the July 2019 OCC Corporate and Risk Governance booklet outlines a more extensive and detailed list of board responsibilities:
• Provide effective oversight
• Exercise independent judgment
• Provide credible challenge to management
• Establish an appropriate corporate culture and set the “tone at the top”
• Understand the legal and regulatory framework applicable to the bank’s activities
• Comply with fiduciary duties and all applicable rules and laws
• Direct and oversee an effective compliance management system
• Set realistic strategic goals and objectives and oversee management’s implementation of those goals and objectives
• Confirm that the bank has a risk management system, including audit, suitable for the bank’s size and activities, and understand the bank’s material risks
• Confirm that the bank has an effective system of internal control
• Hold management accountable for implementing policies and operating within established standards and limits

• Monitor the bank’s operations, oversee the bank’s business performance, and stay informed about the bank’s operating and business environment
• Select, retain, and oversee a competent chief executive officer (CEO) and senior management team
• Oversee the compensation and benefits programs
• Set formal performance standards for senior management, oversee the talent management process, and approve a management succession policy for the CEO and other key executives
• Establish and maintain an appropriate board structure and perform board self-assessments
• Maintain appropriate affiliate and holding company relationships
• Monitor and support management’s efforts to serve the convenience and needs of the communities in which the bank is chartered and its assessment area(s), including the need for credit and deposit services
• Approve the bank’s Bank Secrecy Act (BSA)/anti-money laundering (AML) compliance program
• Confirm that management’s actions to correct material weaknesses, including those identified by the bank, its auditors, and regulators, are timely and effective

Although the latter list from the OCC is more extensive (and is intended for banks of all sizes), like the other two lists, it distinguishes the board’s oversight role from that of day-to-day management. This enhanced definition of roles in regulatory guidance is a welcome improvement. And while it does not in any way reduce the directors’ oversight responsibilities, it does make clear that the board is not responsible for daily management of bank operations.

Regulatory expectations for bank management: FRB and OCC

As with board expectations, the FRB and OCC outline expectations for management in a different style, but ultimately, the expectations are broadly similar. OCC Heightened Standards outlines specific roles and responsibilities for frontline units, independent risk management, and internal audit. The proposed Management Guidance from the FRB provides core principles for management of the business lines, independent risk management, and internal controls. For internal controls, the proposed guidance expands upon
the expectations outlined in SR 12-17.6 noting that a firm should identify its system of internal control and demonstrate that the system is commensurate with its size, scope, activities, risk profile, strategy, and risk tolerance. Notably, the proposed guidance does not expand the FRB’s expectations for internal audit; instead, it references existing guidance under SR 03-57 and SR 13-1.8.

**A word about culture**

No discussion of corporate governance would be complete without mentioning the need for a sound corporate culture. Every large organization has culture statements about shared mission, values, and beliefs, including “doing the right thing.” However, the way statements are actually implemented in day-to-day operations can vary widely. It is not possible to change the culture of a large, complex organization overnight, and no culture is perfect; however, there are several common-sense steps that boards and executive managers can consider as a starting point:

- Set a sound “tone at the top” (leading by example)
- Promote an environment where problems are surfaced, escalated, and resolved
- Hold individuals accountable for intentionally violating policies, standards, and controls
- Review incentive compensation programs regularly to make sure they are working as intended
- Analyze issues identified by regulators, auditors, and others to see if the root cause had a cultural component
- Investigate trends in customer complaints, whistleblower calls, and other information sources, such as “voice of the customer” and “voice of the employee,” to understand potential cultural breakdowns

**Key takeaways**

Executive management, subject to board oversight, should understand the regulatory governance guidance applicable to the firm and then identify and resolve any gaps. Some specific actions that can be taken include ensuring the focus of the board is on oversight, setting strategy, and ensuring accountability, not only on day-to-day operation of the bank; properly defining roles and responsibilities at all levels of the organization; holding the business lines accountable for managing the risks they create; and honestly assessing the soundness of the firm’s culture and taking positive steps to improve it.

---

Shift to nonfinancial risk

In board rooms around the world, financial services executives are focusing on driving business performance forward while taking appropriate action against measures of traditional financial risk (e.g., credit, market, and liquidity risk). Although these efforts need to be sustained, notable risk events related to nonfinancial risk (NFR), such as cybersecurity breaches, employee misconduct, and customer protection, are dominating headlines and causing executives to reconsider their organization’s risk management programs and priorities.

According to a 2019 consumer survey, the financial services industry is the least trusted industry. In recent years, much of the visible media coverage of financial institutions has been negative, often stemming from NFRs. Although such risks remain a secondary consideration, they can have large financial and reputational impacts.

To address the challenges of NFR, many firms are looking for ways to enhance the effectiveness of their NFR management practices and rationalize coverage between the first and second lines of defense while at the same time reducing the costs associated with identifying, assessing, monitoring, and mitigating a wide variety of NFRs, including compliance risk, operational risks, cybersecurity and privacy, third-party, and model.

Compliance risk

Differentiation of risk types does not matter when it comes to compliance risk, as regulatory requirements continue to warrant ongoing management and attention across both financial and nonfinancial risk.

While the OCC's Heightened Standards and the FRB’s SR 08-8 guidance on compliance risk management have long been the guideposts for regulatory compliance in financial services, the ever-increasing complexity of financial institutions creates the need for a thorough assessment of current capabilities and potential opportunities for enhancement. Coupled with the Consumer Financial Protection Bureau's (CFPB) renewed focus on consumer protection and the Department of Justice's (DOJ) 2019 federal sentencing guidelines on evaluating corporate compliance programs, financial institutions may face challenges in substantiating the adequacy of their compliance risk management frameworks if those frameworks do not address key NFRs. Also, multiple and different frameworks, varying oversight and execution approaches, and siloed lines of reporting can create unnecessary costs to the institution and make effective oversight more challenging.

Important focus areas and trends we are seeing in the area of compliance risk management include:

• Broader push toward digital product channel availability and adoption. As traditional physical channels, such as local branches, are supplemented or supplanted by mobile apps, call centers, websites, and other nontraditional channels, risk management is adapting to fit. Many organizations are deploying risk management capabilities in a purely digital construct (e.g., agile risk management) and are positioning compliance risk management professionals closer to the front lines. Also, they are using technology to analyze and monitor risks in digital data streams such as texts, calls, and social media. Meanwhile, many organizations are increasingly relying on an ecosystem of third-party providers and technology partners to manage risk in a more automated and integrated way.

• Operating model redesign. As noted in a recent Deloitte report titled “Managing operational risk and compliance: New paradigms for synergy,” NFRs have traditionally been managed across multiple functional silos, leading to redundancy, inefficiency, and knowledge or process gaps. Now, alternative operating and delivery models are emerging that are more global and integrated, with much closer ties between various parts of the organization that are tackling NFRs; increased use of outsourcing, offshoring, and near-shoring; harmonization and rationalization of the three lines of defense (3LOD); and deployment of centers of excellence (COEs) that improve efficiency, consistency, and effectiveness by optimizing and standardizing how things are done.

• Increased adoption of enabling technology. Organizations continue to expand their use of data analytics and robotic process automation (RPA) to streamline and automate labor-intensive manual processes, allowing compliance and risk management professionals to
focus on activities and challenges that are higher-value and more strategic. Also, many organizations are moving past automation and seeking to deploy cognitive technologies such as AI (e.g., chatbots for customer interaction), machine learning, and natural language processing.

• **Large-scale data remediation and use of data analytics.** In a digital world, data is king. Disparate data sets (e.g., complaint data and third-party data) are being pulled out of silos and normalized, cleansed, and consolidated into a central repository that is shared across the enterprise (including the 3LOD). Such repositories provide a single source of truth and are a fundamental enabler for data analytics and other advanced technologies.

• **New change techniques and risk mitigation activities to foster innovation.** Successful innovation requires risk management capabilities that can keep pace with modern development approaches based on rapid iteration. Organizations are deploying agile risk management frameworks and establishing COEs focused on innovation. Also, they are creating regulatory compliance “sandboxes” to test and scale enabling technology before deploying it more broadly across the organization.

• **Horizontal risk management programs with an integrated, end-to-end view of risk—including product and service risk.** The traditional, siloed approach to business and shared services governance makes it difficult to manage NFRs in a comprehensive way and to demonstrate to regulators that processes are operating as they should. In response, many organizations are now making large investments in end-to-end process modeling, mapping, and maintenance to illustrate the intersection between disparate business activities such as risk, compliance, and controls. Also, many organizations are embedding risk management in a rationalized way across the first and second lines of defense. Product and service risk—viewing risk end-to-end at the product or service level—has emerged as a major enhancement tactic.

• **Expansion of compliance risk law, rule, and regulation (LRR) inventories.** Most NFRs stem from the need to comply with specific regulations. In the past, LRR inventories primarily focused on the federal level. However, as state-level regulations become more impactful and numerous, the compliance challenge grows more complex, and LRR inventories need to be expanded to include a risk-prioritized set of state-level regulatory requirements as well.

**Steps to more effective NFR management**

To tackle the NFR compliance challenges head-on and increase the effectiveness and efficiency of NFR management, institutions should consider the following steps. Ideally, these should be taken together, as each step addresses a different aspect of today’s fragmented NFR programs.

• **Identify NFRs and perform a skills assessment.** Using a standard risk assessment approach or aggregation methodology, institutions can identify which NFRs should be prioritized and then compare those priority NFRs to existing employees’ skills and competencies. Managing NFRs requires a substantially different skillset than does managing traditional financial risks. While core risk management skills are necessary across both risk categories, NFRs typically require specialized knowledge for that particular risk type. This deep subject-matter expertise is often lacking in many financial institutions.

• **Standardize and enhance governance of NFRs.** To effectively and consistently manage NFRs, the concept of NFRs should be understood and considered across all lines of defense and product and service offerings. Regardless of how the lines of defense are structured at a financial institution, organizational separation between the lines is required. However, this separation is often blurry for shared services that manage a portion of NFRs, such as IT and operations. An effective risk management framework for NFRs should reflect an effective governance structure for the institution, the complexity of its operations, and the regulatory requirements it is subject to. The core pillars of the risk management framework for NFRs should create consistency in
identifying (i.e., regulatory change identification), assessing (i.e., standard risk assessment methodology), monitoring (i.e., standard control attributes), mitigating (i.e., issue and corrective action standards), and reporting of risk across the institution. Also, the risk management framework should enable each NFR type to “speak the same language” through a common taxonomy, and clearly defined reporting lines should enable effective board engagement and oversight.

- **Recruit, hire, and train employees specializing in NFRs.** When facing an NFR event and/or the results of a disappointing skills assessment, many institutions find they lack sufficient expertise in key NFRs and thus need to rapidly hire new employees or provide extensive training programs to their current workforce. Training and hiring plans for each NFR type should be developed and actively managed.

- **Deploy technology to modernize NFR management.** Although technological advances can create new NFRs—specifically in the areas of cybersecurity and privacy—they can also provide solutions to existing challenges in managing NFRs. As technology disruption propagates across the financial services industry, executives can find opportunities in NFR management that may be ripe for cost reduction and increased efficiency. Potential solutions include using big data coupled with advanced analytics to identify patterns in testing results, developing predictive scanners to identify emerging risks, and automating repetitive, manual tasks in priority risk management areas.

Regulators today are no longer satisfied with frameworks, documentation, and audit validation alone; they want tangible evidence, including end-to-end testing, as well as compliance program management that is baked into day-to-day operating processes. Taking the steps above, in conjunction with a broader assessment of existing NFR management, can set financial institutions on a path to better manage NFR and the ability to meet the unique regulatory expectations facing today’s financial services industry.

---

Let’s talk

**Thomas Nicolosi**
Principal
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
tnicolosi@deloitte.com

**Joanna Connor**
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
jconnor@deloitte.com

**Greg Healy**
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
ghealy@deloitte.com

**Shaun Nabil**
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
snabil@deloitte.com

---


Optimizing across three lines of defense: New paradigms for risk and compliance management

The global financial crisis prompted years of significant spending on remediation of identified regulatory issues (and, at times, internal audit and risk management issues as well). Institutions focused on building and enhancing organizational structures and operating models, including a 3LOD framework, to provide more effective governance and oversight. Since no one wants a repeat of the crisis, institutions have continued to build capabilities, often in silos, to address specific areas of concern. One example is the situation where independent risk and compliance functions (i.e., the second line of defense) may have created multiple functions, some of which perform the same or similar activities and in certain cases generate redundant requests to the lines of business (i.e., the first line of defense). While the ultimate goal is to create and execute on a strong 3LOD model, enhancements are likely needed in how the model is implemented.

With the global financial crisis behind us and automation technology continuing to advance, institutions now have an opportunity to re-examine their governance operating models and risk management responsibilities—the “who” and the “what”—and ensure an effective foundation exists. In this section, we share our perspective on what an optimal 3LOD framework might look like and explore the synergies that potentially exist among the independent risk and compliance disciplines.

Overall, the 3LOD is a governance system that works across the business, independent risk, and compliance functions and internal audit.

1. First line of defense (first LOD) refers to the business—the revenue producers and risk-takers. The business generates, owns, and controls risk by establishing written policies, practices, and processes (including monitoring and testing) pertinent to its portfolio while executing within the risk appetite and limits established by the first LOD. Further, the business aligns its strategic, capital, and financial operating plans to the risk management framework, which it adopts and implements.

2. Second line of defense (second LOD) refers to the independent risk and compliance functions, which provide oversight to the first LOD and create, design, and implement the risk management framework, which includes among other things the risk assessment methodology, measurement, aggregation, reporting, processes and tools as well as defining risk appetite framework. The second LOD should provide effective challenge to the first LOD and influence incentive compensation systems (e.g., risk-reward objectives).

3. Third line of defense (third LOD) typically refers to internal audit, but may also include the credit review function. Internal audit’s remit, which is derived from the board, is to process-audit the first and second LODs. This includes assessing the design and effectiveness of the institution’s risk management program.

Ideally, a 3LOD model is supported by clear roles, responsibilities, and accountabilities, as well as reporting, escalation, and information flow between the 3LOD and across the institution (including the board and senior management). Although the 3LOD governance model has been around for a while, institutions can potentially enhance it by looking at three areas: roles and responsibilities; activities and processes; and data and automation. These optimization opportunities can help address key challenges that many organizations are facing as they transform their risk management processes (see sidebar on next page).

Potential optimization opportunities in the 3LOD model

One potential enhancement opportunity is to clarify the roles and responsibilities between the business and independent risk and compliance functions regarding who generates, owns, and manages the risks. Often there can be confusion in the business over who is responsible, since the necessary skills may reside in the second line or duplication of activities may exist between LODs (e.g., credit underwriting and approval decisions; onboarding or know-your-customer analysis). Another common issue is having an essential capability that is missing or inadequate in one line of defense but present in a different line. For example, if the business (first LOD) does not have testing capabilities, the risk and/or
Risk management transformation

Institutions are looking to transform their risk management processes to address a number of specific challenges (see figure 1).

Figure 1. Some specific challenges for risk management transformation

- **Process and cost inefficiency**: Challenges arising from inefficiencies due to siloed risk management practices of the same or similar activities across various risk and compliance functions and business lines. These challenges may be the result of a historical tactical-versus-strategic response to regulatory remediation (with associated increases in head count).

- **Outdated technology**: Segmented data sources (possibly due to acquisitions) and historical underinvestment in disparate legacy systems can impede the capture, measurement, and reporting of data.

- **Inability to assess or quantify risk**: Challenges providing management and the board with data that translates into information and insight. Need for data that is reliable, concise, on point, timely, and comprehensive to support informed decision-making. Need for a single risk and compliance view (versus multiple views of the same or similar issue) so that remediation can be cost-effective.

Today’s risk functions need to be smarter, faster, more agile, and more effective in identifying and proactively managing emerging risks. At the same time, they need to reduce their operating costs, comply with regulations, and work more closely with other functions to support business decision-making to ensure the firm is safe and sound.
A third potential opportunity revolves around data, analytics, and automation. Many institutions still struggle with quality, accuracy, and timeliness of risk data. There continues to be a need for “better” information (timelier, more accurate, and more insightful—from one “golden source”) and for predictive data and analytics that can be used in decision-making by all 3LOD. Automation can be used to help improve efficiency and decision-making to drive business growth.

**Looking ahead**

With the global financial crisis in the rearview mirror, financial institutions can now take the time to revisit their organizational constructs and required capabilities across the first, second, and third LODs. This can uncover valuable optimization opportunities in the 3LOD governance model—optimizations that can boost efficiency, transparency, and business value going forward.

---

**Figure 2. Deloitte’s 3LOD framework**

Deloitte’s 3LOD framework includes five key components to help enhance the 3LOD governance structure and drive business value.

1. Clarify roles and responsibilities by focusing vertically on “who” is performing “what”
2. Establish an end-to-end process view by focusing horizontally on key processes and controls (e.g., risk assessments, testing, issues management)
3. Determine where synergies among risk and compliance disciplines can be found to achieve simplification of processes, cost savings, and efficiencies that help the business make better, more informed decisions
4. Define a governance and operating model that sets the tone and structure for effective oversight and influences the design and effectiveness of the model
5. Implement enablers and measurement to support the model’s successful implementation and measure its effectiveness

---

**Let’s talk**

*Michele Crish*
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
mcrish@deloitte.com

*Peter Reynolds*
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
pereynolds@deloitte.com
Operational resilience

Operational resilience is the ability for organizations to proactively respond to (and recover from) operational disruptions to the business, industry, and customers. It is a foundational component of an organization’s operational risk management framework and aims to provide a common set of processes and governance across various domains such as cybersecurity, business continuity, disaster recovery, and crisis management.

In a recent Deloitte & Touche LLP survey of more than 500 financial services executives—the 2019 Future of Cyber survey—respondents cited loss of revenue due to operational disruption as the biggest impact to their organizations from a cyber perspective (figure 1). With rapid technology growth driving businesses in an increasingly interconnected world, it is imperative for organizations to build operational resilience frameworks to ensure they can meet ever-increasing customer expectations.

**Regulatory actions and guidance**

Digital transformation plays an increasingly pivotal role in providing modern financial services. Regulators and financial industry watchdogs in the United Kingdom and European Union have indicated a shifting focus toward technology and business resilience to help ensure firms are doing enough to make themselves more operationally resilient.

Over the past year, IT failures across financial institutions have prompted increased regulatory and supervisory attention on the risks that technology change can pose to the operational resilience of the financial services sector. The volume, velocity, and complexity of change present a significant challenge to many financial institutions, and often it is during change programs that disruptions arise.

In December 2019, the BOE, Financial Conduct Authority (FCA), and Prudential Regulation Authority (PRA) and FCA published a number of consultations on operational resiliency, refining the approach first set out in their July 2018 joint discussion paper. The consultations

---

**Figure 1. Biggest impacts of cyber incidents or breaches on organizations**

<table>
<thead>
<tr>
<th>Impact</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of revenue due to operational disruption</td>
<td>21%</td>
</tr>
<tr>
<td>Loss of customer trust</td>
<td>21%</td>
</tr>
<tr>
<td>Charge in leadership</td>
<td>17%</td>
</tr>
<tr>
<td>Reputational loss</td>
<td>16%</td>
</tr>
<tr>
<td>Regulatory fines</td>
<td>14%</td>
</tr>
<tr>
<td>Drop in share price</td>
<td>12%</td>
</tr>
</tbody>
</table>
included some of the following implications: i) dual-regulated firms may have to set two different impact tolerances for the same important business service, and ii) Boards and Senior Management will need to be actively involved in a number of aspects related to operational resilience, such as making prioritization and investment decisions. The agencies have said that changes to legacy systems must be managed carefully, as they present a heightened risk of operational disruption. The PRA and FCA further point out that failure to address obsolescent technology can weaken operational resilience.

The European Banking Authority (EBA) has published final guidance on information and communications technology (ICT) and security risk management, which will be applicable starting June 30, 2020. In their current form, the guidelines would require firms to manage changes to their IT systems carefully and have robust procedures in place in the event of disruptions.

The BoE and the PRA have released an operational resilience discussion paper centered around the need for banking and financial institutions to shore up their resilience capabilities to withstand disruptions.

In the United States, the FRB is conducting horizontal examinations to evaluate financial services organizations’ ability to stay resilient and recover from operational disruptions and failures. Sheltered Harbor is another evolving industry initiative centered on protecting the financial market infrastructure.

### Figure 2. An operational resilience framework

<table>
<thead>
<tr>
<th>Suppliers</th>
<th>Technology</th>
<th>Cyber</th>
<th>People</th>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Governance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a single, accountable body at an appropriate level for operational resilience</td>
<td>Minimum requirements are clearly documented and communicated (e.g., operations, functions, external suppliers)</td>
<td>Compliance with minimum requirements is assessed and exceptions escalated</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Planning and response</strong></td>
<td>During normal business conditions</td>
<td>During a major event</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anticipate &amp; assess</td>
<td>Protect &amp; control</td>
<td>Plan &amp; prepare</td>
<td>Respond &amp; recover</td>
<td></td>
</tr>
<tr>
<td>Critical services are identified and endorsed by senior management</td>
<td>Design standards for resilience are defined and communicated to the business, supporting functions, and third parties</td>
<td>Impact tolerances in the event of disruption are defined and communicated to all parties to set the context and direction for planning</td>
<td>Organizational crisis and function specific incident response arrangements, including escalation protocols, are aligned</td>
<td></td>
</tr>
<tr>
<td>Operational dependencies required for the end-to-end delivery of critical services are identified (e.g., systems, people, locations, suppliers)</td>
<td>Preventative measures are in place and documented to strengthen defenses and reduce the likelihood of disruption</td>
<td>Continuity or contingency strategies are in place to recover and/or operate critical services in line with strategic business objectives</td>
<td>Rapid and agile command, coordination, and communication (C3) established, and customer focus achieved</td>
<td></td>
</tr>
<tr>
<td>High risk scenarios are identified and active “risk sensing” is in place to provide “early warning” of emerging or imminent issue, incident, or crisis</td>
<td>Contingency and recovery plans are validated through testing and exercising. Key staff are trained for their role</td>
<td>Lessons are learned through post event reviews on major incidents, crises, and near misses</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Culture</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational resilience is a key consideration through change management and decision making</td>
<td>Changes to the risk environment are identified and pro-actively managed</td>
<td>A culture of continuous improvement exists through the review of adverse events and near misses, learning from the experience and adapting accordingly</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Taking action

According to a 2019 operational risk horizon survey conducted by ORX, a global operational risk management benchmarking organization, the top five risks, as chosen by respondents, are:

- Digital disruption and disintermediation risk
- Information security (including cyber) risk
- Geopolitical and macroeconomic risk
- Compliance risk
- Third-party risk

Digital disruption remains the top emerging risk; however, all risks are evolving as technologies and marketplaces mature.

Operational resilience programs need to be forward-looking and adaptable to the ever-growing threat landscape. Such programs should include a resilient framework that extends beyond traditional disaster recovery and business continuity practices by incorporating “designed-in” resiliency to restore critical business services.

More broadly, based on risk and regulatory drivers across the financial services industry, several common imperatives are emerging that need to be factored in while establishing operational resilience programs:

- Understand core mission-critical business services and processes
- Develop impact categories and establishing realistic recovery metrics
- Establish impact tolerances based on business strategies
- Establish a framework for coordination and communication
- Conduct scenario-based testing exercises

Let’s talk

Vikram Bhat
Principal
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
vbhat@deloitte.com

Damian Walch
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
dwalch@deloitte.com

Vaishnav Vijaykumar
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
vvijaykumar@deloitte.com

Cybersecurity and privacy

Banks are focusing more resources and attention than ever on cybersecurity. However, cybersecurity issues continue to grow, fueled by determined, well-funded, sophisticated adversaries—and by a world that is increasingly interconnected and digital.

According to a recent industry survey conducted by Deloitte & Touche LLP (in collaboration with FS-ISAC), responding financial services institutions on average spend 10.1 percent of their IT budget on cybersecurity. Yet the number of data breaches in the first six months of 2019 increased by 54 percent over the same period in 2018.

From a regulatory perspective, cybersecurity continues to be a key focus area, both in the United States and around the world. Issues coming under increased scrutiny and supervision from regulators include cybersecurity governance (board or leadership involvement), privacy, data security, cyber resilience, and outsourcing risks.

In response to these rising risks and regulatory expectations, banking institutions across the globe are continuing to strengthen their technology, risk, and compliance programs.

Regulatory activity related to cybersecurity and data privacy

OCC
The OCC’s Semiannual Risk Perspective (December 2019) identified cybersecurity and operational resiliency as priorities, with emphasis on threat vulnerability and detection, access controls and data management, and managing third-party connections. Examiner focus will include information technology risk management evaluation and information technology systems maintenance.

FRB
Cyber-related risks are among the supervisory priorities for the FRB for Large Institution Supervision Coordinating Committee (LISCC) firms, large and foreign banking organizations (LFBOs), and community banking organizations (CBOs).

FDIC
Enhancing oversight of banks’ cybersecurity risks is a top area of focus for the FDIC. As part of its Community Banking Initiative, the FDIC is adding to its cybersecurity awareness resources for financial institutions. This includes adding two new Cyber Challenge vignettes focused on cybersecurity and operational resilience.

US state regulations
More than 30 states enacted cybersecurity-related legislation as of December 2019. California’s Consumer Privacy Act (CCPA) has prompted new calls for comprehensive data privacy and security laws across the nation. Other states, such as New York and Nevada, are introducing similar privacy bills.

European Union
The European Council adopted the EU Cybersecurity Act in April 2019. The Act permanently designates the European Union Agency for Network and Information Security (ENISA) as Europe’s Cybersecurity...
Agency and establishes an EU cybersecurity certification framework. Separately, European Supervisory Authorities (ESAs) published a Joint Advice on the costs and benefits of establishing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector. In addition, General Data Protection Regulation (GDPR) and Payment Services Directive 2 (PSD2) requirements are driving closer regulatory scrutiny regarding the use of consumer data.

**Key focus areas**

Cybersecurity governance. The responsibilities and expectations for boards have evolved from just having a high-level understanding of cybersecurity to having an in-depth understanding of the cyber risks to which their organization is exposed, understanding the organization’s strategy for tackling those risks, and ensuring the strategy is being executed with enough rigor and accountability.

**Cyber resilience**

Cyber resilience is a focus for financial institutions globally, with an emphasis on building holistic, enterprise-wide cyber resilience programs. Lack of such programs can lead to extended disruption of critical functions, reduced confidence in firms and markets, and an inability to recover operations.

**Privacy and data security**

Businesses globally need to increase their focus and efforts in this critical area as various jurisdictions ratchet up their privacy and data protection laws (e.g., GDPR, CCPA). Many countries are also focusing on cloud-related data residency requirements, limiting data movement beyond borders.

**Outsourcing risks.** Regulators are concerned about the risks stemming from financial institutions’ increasing reliance on third-party service providers to support much of their critical infrastructure. Regulators are also concerned about too many financial institutions using the same providers and the widespread use of cloud.

Although regulatory scrutiny and pressure might be a key driver for cybersecurity programs, continued investment to strengthen cybersecurity programs is now a fundamental business need that should be utilized to help companies grow and prosper in this evolving and challenging digital environment.

---

Third-party risk management

Third-party risk management (TPRM) remains a basic regulatory expectation, with no significant updates to existing guidance published by the OCC and the FRB. Leading industry practices include considerations for important risk domain areas, such as cybersecurity, data privacy and data use, business continuity, financial health, and antibribery and anticorruption. In addition, as a basic expectation, third-party risk is included indirectly as an assessment topic in regulatory examinations (i.e., not via an examination of the TPRM program).

To effectively gauge and monitor risks in these domains, TPRM programs are expected to be at a level of maturity that includes (1) fully standardized processes integrated with tools and data and (2) proactive decision-making capabilities using analytics. Operating models should, at a minimum, include the ability to:

- Provide an accurate inventory of third-party relationships and associated inherent risk
- Create aggregated reporting that includes visibility into levels of risk (and associated processes in place to monitor such risks)
- Report on the overall health of the TPRM program through key performance indicators and consolidated data sources
- Demonstrate that first-line stakeholders are adhering to policy and program requirements

Operating model design should consider operating model efficiencies, as well as improved, streamlined processes to incorporate input and feedback from all stakeholders across various enterprise risk areas.

Operational resiliency (the ability to deal with operational risks) remains a key focus for regulatory reviews, particularly in banking. Dependency on third parties for both core and noncore functions dictates the need for formal assessments of resiliency and the impact of dependent relationships where exit strategies are required. The focus on resiliency is shifting to consider all types of financial infrastructure relationships and is likely to expand to financial market utilities (FMUs). A related focus area is oversight of payment networks, including correspondent and agent banking relationships. Regulators have been taking the perspective that regulatory oversight of an institution does not preclude it from assessment or oversight by other institutions.

As more third-party relationships include some level of dependency on cloud providers, adequate control reviews and understanding of interdependencies should be considered. Whether the third party provides business process as a service (BPaaS), software (SaaS), a platform (PaaS), or infrastructure (IaaS), cloud can affect multiple data-driven functions within a bank. Cloud providers and cloud infrastructure vary according to service type and technical architecture; as such, assessments of third parties utilizing the cloud should be commensurate with the risk identified and ongoing monitoring should be aligned accordingly.

Lastly, the complexity of fourth-party relationships remains a challenge. Lack of appropriate oversight over subcontractors and affiliates, in concert with third-party concentration risk, poses challenges to current TPRM programs. Leading organizations are starting to address the blind spots through “illumination” initiatives to discover and understand these networks within networks. Once a company understands who its vendors’ subcontractors are, the next step is to understand what assurance its third parties are obtaining about these fourth (and fifth) parties. This assurance needs to be supported by evidence. Some institutions are tackling the challenge by using risk intelligence tools to understand critical fourth-party control environments (including financial solvency).

Let’s talk

**Kevin Gallagher**
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
kevgallagher@deloitte.com

**Suzanne Denton**
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
sudenton@deloitte.com
Technology: Modernizing and innovating

Most large banks have a technology infrastructure problem: They are saddled with legacy core banking systems that date back to the 1960s. These systems have become inefficient, costly, and difficult to maintain. New technologies, such as the cloud and application programming interfaces (APIs), have emerged that offer a potential solution. However, the road from here to there is not easy.

Yet firms that stick with the status quo will likely find themselves in an increasingly weak competitive position. Financial innovation is going to continue, and it is important that large banks position themselves to take advantage.

Many banks have partnered with or acquired financial technology (fintech) firms to help modernize their operations. Such partnerships can bring advantages to both sides. Fintechs gain the stability of large banks, while banks gain potentially more agility and support for legacy system modernization.

Originally built decades ago, banks’ legacy mainframe systems were not designed for the modern world. Most were written in common business-oriented language (COBOL), are often highly customized, and in many cases are no longer supported by the vendor. The pool of COBOL programmers is dwindling fast, and the systems themselves are frequently not well documented, forcing banks to use a number of pre- and post-processors to maintain functionality. COBOL is inefficient compared to modern programming languages and techniques, and the mainframe model is becoming increasingly expensive compared to cloud.

Banks can continue to shore up their legacy core applications with interfaces that provide the functionality expected in today’s financial world, such as real-time responses, analysis, and reporting. However, this strategy is merely delaying the inevitable and is not a desirable long-term approach. That said, large complex firms cannot replace their core systems at once, so this tactic will continue for some time at most banks.

For systems so outdated that total replacement is the only real long-term solution, there are two broad options. The first is to maintain the core system as-is while building a new system and then to do a big-bang replacement at the end. The second is to move critical capabilities from the core system to the new system incrementally over time. Although the first option might be advantageous in some cases, the benefits of the second will likely make it the preferred approach. Those benefits include earlier realization of efficiencies, cost savings, and capabilities, as well as reduction of integration complexities.

Fintech firms can do more than help banks drive financial product innovation; they can bring capabilities and ideas to the relationship that help accelerate modernization of bank technology systems. Differences in corporate culture can sometimes be a problem, with fintechs wanting to move fast and banks exerting a more cautious approach. However, there are great benefits in achieving the right balance between encouraging innovation and adequately managing risk and compliance.

All US financial regulators have been actively supportive of financial innovation, setting up Offices of Innovation, holding financial innovation symposiums, and making speeches that advocate innovative methods for delivering financial services. On October 24, 2019, the OCC, CFTC, FDIC and the SEC announced that they would be joining the Global Financial Innovation Network (GFN). These US financial regulators have taken proactive steps in recent
years to enhance regulatory clarity and understanding for all stakeholders and promote early identification of emerging regulatory opportunities, challenges, and risks. Participation in the GFIN furthers these objectives and enhances the agencies' abilities to encourage responsible innovation in the financial services industry in the United States and abroad.  

Regulators have generally expressed support for regulatory “sandboxes” that provide a safe harbor for product development and experimentation. In particular, the CFPB in September 2019 announced three new policies to promote innovation, including a Compliance Assistance Sandbox (CAS) Policy. In its announcement, the CFPB summarized the policy as follows: "The CAS Policy enables testing of a financial product or service where there is regulatory uncertainty. After the Bureau evaluates the product or service for compliance with relevant law, an approved applicant that complies in good faith with the terms of the approval will have a “safe harbor” from liability for specified conduct during the testing period. Approvals under the CAS Policy will provide protection from liability under the Truth in Lending Act, the Electronic Fund Transfer Act, and the Equal Credit Opportunity Act."

In making the announcement, the CFPB stated that financial innovation can reduce customer costs, provide improved services, and expand financial options. Similar statements have been made by the other financial regulators, who realize that regulatory frameworks can stand in the way of financial innovation.

Banks and their regulators both understand that innovative financial services, supported by modern technology infrastructures, are critical in today’s digital, real-time world. But for many large firms, the road to modernization is long. To get there, firms need a well-thought-out, long-term plan for data infrastructure transformation, supported by appropriate and realistic funding. The plan should be updated regularly as technology evolves, reflecting advances such as improved cyber detection tools. Also, to set the right priorities, the plan should consider both the risks of continuing to maintain core legacy systems, as well as the projected efficiencies and cost savings of migrating those legacy systems to a modern platform. Finally, firms should consider phasing the migration of their core systems to capture incremental benefits and reduce the integration risk of a big-bang approach.

---

Data capabilities in banking: The journey continues

Effective data management and data quality remain high priorities for the banking industry and its regulators. There continues to be an increasing emphasis on how systemically important firms, foreign banking organizations, and other large banks are managing and integrating the data used for risk, regulatory, and financial reporting. And while the industry has made strides in improving quality for the most critical and impactful data, continuous improvement is necessary so that all the quality of data is fit for purpose across the firm. The goal is to create a dynamic data environment where the processes and infrastructure can quickly adapt to changing needs for financial, nonfinancial, and risk data.

Improved data capabilities are needed to meet current requirements, as well as regulators’ increasing requirements for data that is more granular and collected more frequently (e.g., daily) on an accelerated schedule (e.g., T+1). The new data requirements are creating greater regulatory risk (i.e., new regulatory constraints), as well as reputational risk from having to restate publicly disclosed data.

Much of the regulatory focus related to data and reporting stems from historical challenges. Through the horizontal examination process, regulatory expectations have been communicated firm-by-firm. These expectations create minimum standards that raise the bar on data quality and the associated control environment.

**Industry trends**

As the banking industry responds to these data-related challenges, several important practices are emerging regarding centralizing data activities, enhancing the control environment, and effectively prioritizing data remediation.

**Central data offices**

To contend with the large volume of data they possess—and the legacy data infrastructure that exists—many firms have started the cultural transformation of treating data as a firmwide asset. At many firms, the chief data officer (CDO) is playing an increasingly critical role as a standard-setter and second line of defense for data quality. Effective data programs established by CDOs and central data offices include:

- Setting data quality standards for the firm
- Monitoring data quality across the firm
- Developing models for firmwide data infrastructure that create authorized data sources and allow data sharing across the firm
Creating a centralized approach to data management has allowed firms to clearly articulate responsibility and accountability for data across the different data roles (e.g., data owners, report owners, data stewards). To be clear, data owners continue to be responsible for data quality, even when a central data office is implemented. Although data program maturity varies widely between firms, the integration of firmwide data programs with reporting processes and operating models is an emerging standard and regulatory expectation.

**Data lineage**

Firms continue to face significant challenges in documenting data lineage. A key role for data lineage is to identify the original sources of the data that is used for reporting and decision-making. In large, complex organizations, the sheer number of legacy systems and data repositories makes data lineage a daunting task. Firms that have tried to conduct full-attribute data lineage exercises have learned this can be a never-ending effort that requires a significant amount of resources, with results that are often out-of-date the moment they are complete. As such, the industry continues to consider how much lineage is sufficient to effectively manage data quality and data controls in a sustainable manner.

A scaled-down approach to data lineage is emerging that traces the inputs to reports and aggregations by mapping system flows and business processes. This allows data to be traced back to the original source where quality needs to be maintained. It also allows a comprehensive understanding of all the data transformations that occur in the reporting process and helps ensure the proper level of controls is in place for those transformations and related business processes.

Another emerging practice is tracing the lineage of data only as far back as the American Depository Shares (ADS). This can be effective if (1) there are criteria for the level of controls necessary to ensure the quality of data that is sourced into the ADS (including documenting the original sources of data), and (2) a governance structure exists where senior management approves an ADS and use of the ADS is monitored.

**Critical data elements**

The enormous task of maintaining high-quality, fit-for-purpose data for risk, financial, and regulatory reporting remains an elusive goal, especially for complex organizations. As such, remediating data quality issues and creating an effective data infrastructure requires careful prioritization. When prioritizing data quality efforts, many large firms have either begun to or have established critical data elements (CDEs). The definition and number of CDEs varies widely from firm to firm. This is appropriate, as CDEs are determined by a firm’s business model and risk profile. To correctly identify CDEs, firms should conduct an analysis of data attributes and then determine the impact those attributes have on managing risk, meeting regulatory requirements, and preparing management reports. Many firms identify CDEs at two levels: corporate and business line. This is an acceptable practice; however, it is important that the criteria for determining a CDE be consistent across the firm in order to avoid conflicts in the handling of data quality for CDEs.

Once CDEs are identified, the firm needs to decide what being a CDE means. Having CDEs for the sake of having them is of little value and may produce a negative impact. CDEs should be used to:

- Develop remediation plans
- Apply enhanced controls
- Determine the level of lineage

Remediation of data quality issues is resource-intensive, both in terms of human capital and technology spend. CDEs can aid in determining
where resources should be allocated. However, the identification of CDEs does not mean the quality of non-CDEs can be ignored. Rather, there should be a base set of data controls for all data, with CDEs having enhanced controls. The enhanced controls can take the form of additional business rules, management reviews, or more detailed reconciliations. Note that CDE remediation often has a halo effect, where improvements to CDEs also improve the processes and technology for non-CDEs. Also, CDEs are an important input to annual planning by the Internal Audit and Quality Assurance functions. CDEs should be used when determining the level of lineage needed. While a firm should understand system flows and end-to-end processes for all data, CDEs may require a deeper lineage at the attribute level. This includes maintaining detailed metadata in a central repository.

Risk and data assessments
CDEs—and the materiality of a data element’s impact—are not the only factors in determining where to focus efforts to enhance data quality and controls. Equally important is assessing the risk of poor data quality, especially for related business processes and data infrastructure. Independent risk assessments should occur regularly and consider:

- The number of transformations that occur from data source to report production
- The effectiveness of business processes, including the control environment for those processes
- The number of manual adjustments and end-user computing tools for report production

The risk assessment should be overlaid with the CDEs and materiality policies to determine where enhanced controls should be applied, prioritize data remediation efforts, and inform quality assurance programs. The internal audit function should do an independent risk assessment to develop its audit plans.

In addition to a risk assessment, conducting an overall assessment of the data environment and reporting processes is an effective practice to help firms understand where data gaps may exist and where controls should be strengthened to prevent material data errors. Some firms conduct self-assessments of data quality and the associated control environment. However, since there are often differing views about what constitutes good, fit-for-purpose data quality, an independent validation of these assessments should also be done. A logical place for end-to-end assessments and validation to occur is the central data office. In addition, an internal audit review of the processes for conducting a data assessment can ensure the proper level of quality is maintained and help identify significant data gaps.

Materiality and risk assessment

<table>
<thead>
<tr>
<th>High materiality /high risk</th>
<th>Low materiality /high risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test during annual current cycle</td>
<td>Testing occurs over the program cycle (e.g. once every three years)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>High materiality /low risk</th>
<th>Low materiality /low risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Testing occurs over the program cycle (e.g. once every three years)</td>
<td>Testing occurs over the program cycle if resources are available</td>
</tr>
</tbody>
</table>

Attestations and accountability

The use of attestations to ensure data quality continues to grow. After the initial round of CFO attestations for the FR Y-14, firms have started changing the attestation process to limit sub-attestation to only senior data owners, creating clearer accountability at the data-owner level.

Another emerging practice is an evidence-based approach. With the submission of business-line or data-owner attestation, the business line includes the evidence upon which the attestation is based. The overall attester (e.g., the CFO) then provides a challenge function before attesting to the quality of the data.

The most transformational change that is occurring is owner accountability. Firms are developing measures to monitor data quality and escalating material data issues. Also, firms are strengthening their accountability policies by creating more meaningful incentives.
for maintaining data quality. One such practice is to include in data owners’ annual performance evaluations an assessment of the data quality they own. Of course, an effective evaluation process requires clear measures of data quality.

Looking ahead
The maturity of data management practices varies widely, and the banking industry continues to develop effective ways to identify the needed data and improve data quality. These practices are helping to meet regulatory expectations and mitigate the risk of misstatement. However, the complexity of data requirements and the data content of new approaches to mitigating data risks—along with adoption of demonstrated approaches and methodologies.
Navigating the changing financial crime compliance landscape

There is growing consensus that the BSA/AML regime needs reform to better support law enforcement’s efforts to deter and disrupt global financial crime, money laundering, and terrorist financing. In the United States, this has resulted in several initial steps by the regulatory community that signal an openness to new approaches and innovation. US authorities are also considering how to best enhance risk-based BSA/AML supervision to align risk exposures with supervision resource allocation and institutional controls.

At the same time, financial crime risks continue to proliferate and evolve at ever-increasing speed. For example, sanctions compliance remains an ongoing challenge, given the frequency of changes to sanctions programs and rising expectations about banks’ ability to detect sanctions evasion.

Given these trends, in 2020, banks will need the agility to respond effectively to a rapidly evolving risk, regulatory, and enforcement landscape. Specific issues that should be actively considered include:

- Focusing AML programs on providing more useful output to law enforcement around high-priority risk and threats
- Addressing rapidly changing sanctions requirements and the importance of detecting potential sanctions evasion in BSA/AML controls
- Leveraging more data, as well as new approaches and technologies, to improve detection and reporting of suspicious activity with increased effectiveness and efficiency
- Understanding how money laundering, fraud, and cyber risks are connected and exploring ways to leverage intelligence across domains to better detect financial crime and protect the institution
- Participating in established and emerging efforts to promote private-private and private-public information-sharing partnerships

Many large institutions have started to address each of these areas in some fashion. And while the election cycle in 2020 is likely to affect the issuance of new guidance and regulations, it is probably still wise for banks to formulate strategy in anticipation of such changes, given the growing consensus around these topics among regulators, law enforcement, and industry.

That said, banks will need to decide how heavily to invest in addressing the expected changes before they come to fruition. They will also need to decide how aggressively to pursue efficiencies in their current programs to free up resources to focus on activities of higher risk management value.

Specifically, institutions should be considering how to (1) demonstrate an effective focus on new and emerging financial crime risks, (2) leverage new approaches and technologies to drive efficiency and to focus resources on the highest value areas, and (3) promote agility in AML monitoring and sanctions screening programs and controls in order to more effectively identify and manage risk.

Let’s talk

Fred Curry  
Principal  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
fcurry@deloitte.com

Satish Lalchand  
Principal  
Deloitte Risk & Financial Advisory  
Deloitte Transactions and Business Analytics LLP  
slalchand@deloitte.com

Clint Stinger  
Principal  
Deloitte Risk & Financial Advisory  
Deloitte Transactions and Business Analytics LLP  
cstinger@deloitte.com

John Wagner  
Managing Director  
Deloitte Risk & Financial Advisory  
Deloitte Transactions and Business Analytics LLP  
johnwagner@deloitte.com
Structural optimization

In the past, banks and other financial services firms started with market imperatives to determine their size, shape, and business model, then worked forward from there to adhere to the regulatory landscape in which they found themselves. However, today’s regulatory landscape demands that organizations begin with an integrated view that includes both regulatory and business dimensions, then tailor their regulatory profile and organizational structure to serve their long-term strategic interests.

Structural optimization is the effort to optimize, simplify, and adapt a bank’s business model—and implicitly, its use of legal entities across jurisdictions—to further grow and rationalize its US and global footprint. This is an increasing focus for US banks due to three factors: US corporate tax reform, a period of relative regulatory stability, and an overall focus on finding ways to grow the business and improve profitability.

**Key trends shaping structural optimization**

Regulatory changes are driving new efficiency plays. Also, technology disruption is bringing new players into the market and forcing existing players to review and enhance their approaches and delivery models.

**Fintech adaptation**

Fintech companies are uncovering new ways to carve out segments of the banking market and to provide value propositions for underserved consumers. These organizations are prepared to navigate the regulatory and strategic hurdles that accompany the maturation cycle of expanding into new market segments or adopting a more full-service business model. Over the past year, there have been several announcements of fintech companies that have filed with regulators to enter the banking business, either through de novo formation or via acquisition. Fintechs have been particularly encouraged by the expressed willingness of regulators such as the OCC, FDIC, and CFPB to work with them in pursuing bank charters.

**Optimization and simplification**

In a convergence of regulatory and business strategy, banks and other financial services entities continue to look for opportunities to optimize their booking models, product alignment, and legal entity structures. As an organization changes its business strategy, expands through acquisition of new companies, and/or encounters new regulatory requirements, its legal entity and operational structures become more complex and costly. Controls and governance that support the organization’s booking model and legal entity structure can help it manage toward its strategy and desired footprint, often unlocking valuable efficiencies.

**Growth**

Financial institutions are looking to increase their market presence and performance via new customers, new products, and/or enhanced interaction with existing customers through digital banking innovation. In some cases, banks are also pursuing growth through M&As.

All these trends are occurring against a backdrop where regulators are increasingly focused on the need for firms to demonstrate that what is booked and managed within the borders of a country or legal entity is well controlled and well managed centrally and across jurisdictions.

**Current and future impact**

Organizations need to consider where, how, and why they are doing business. That process includes continuously assessing their internal controls and the guardrails that are in place to monitor and govern booking models and product strategies. In cases where banks have fallen short of the expected regulatory standards related to booking models, we have seen remedial actions in the form of detailed data requests and continuous interventions from regulators. A clear and transparent booking model, combined with a legal entity governance model supported by controls, helps ensure regulatory expectations can be met and provides evidence that the business strategy is supported operationally. In the long run, this can serve to help organizations remain competitive and answer long-term strategic questions.

New technologies such as digital banking and payment services are redefining who engages in the broader banking community (and where), as well as how entities can take advantage of banking capabilities such as raising deposits. This leads organizations to
ask questions such as “What bank charter or legal entity option is right for my business strategy?” and “What is the right business model to execute my strategy?”

Fintechs are working to identify where and how they wish to enter and operate in the US market. This requires thinking about whether to buy (acquire an existing bank to gain capabilities), build (gain approvals and then design and construct a new bank), or partner (pursue relationships with established banking entities).

**Taking action**

Banks should review their options and determine what can be done to optimize, simplify, or further adapt their business models. This involves:

- Understanding the current strategy and overall positioning relative to peers, including legal entity structure and booking model
- Reviewing options based on the business model
- Defining a target state model that is grounded in meeting regulatory expectations

---

**Let’s talk**

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

Richard Rosenthal  
Senior Manager  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
rrosenthal@deloitte.com
Credit

The current state of credit quality in the banking system is strong when measured using traditional performance metrics, such as delinquencies, nonperforming loans, problem loans, and credit losses. So why are many experienced credit professionals, including regulators, sounding mild alarm bells? Most likely it is because they have seen this movie before and know that after a long period of expansion, competition and recent credit success encourage the booking of credits with more inherent risk.

Indeed, in a recent OCC semiannual risk perspective (December 2019), the agency warns that credit risk is building in the system from years of incremental easing in underwriting, risk layering, and in some cases, building of concentrations. Similar to the OCC, the FRB’s Supervision and Regulation Report (December 2019) states that the FRB identified firm-specific weaknesses in credit underwriting practices, particularly around policy exceptions, financial covenants, financial analysis, guarantor support. Finally, in a recent FRB Senior Loan Officer Opinion Survey on Bank Lending Practices (October 2019), banks reported tightening standards on CRE loans, credit card loans, and auto loans.

Regulators, especially the OCC, have also noted weak structures and uncertain repayment capacity in many of the leveraged loans currently being originated. They acknowledge that most of the credit risk associated with leveraged loans is being booked outside of the banking system. Because of the volume of leveraged and other elevated-risk loans being booked outside of the banking system, regulators are cautioning banks to understand their direct and indirect exposure to these nonbank lenders, including the potential general economic effects. For example, the OCC notes that bank lending to nondepository financial firms (NDFI) grew 20 percent in 2018. The agency advises banks with significant NDFI exposures to properly manage it. Additionally, the OCC states that banks should evaluate whether their borrowers have critical suppliers or vendors that could adversely affect their operations.

Often, we hear banks indicate that they are holding the line on terms but competing on price. Unfortunately, we also heard this in 2006, 1987, and other prerecession periods. As a senior regulator mentioned to us recently: “Isn’t properly pricing for risk a part of sound risk management?”

We certainly do not want anyone to take these comments the wrong way—after all, serving customers by making sound loans and thriving are what banks are supposed to do. Also, regulators continue to assess the state of bank credit underwriting as sound overall. However, credit cycle turns are hard to see in advance and loss content can be surprisingly high when such a downturn occurs. So, this is just a gentle reminder to remember the lessons of past downturns; continue to extend credit on your own terms, not terms driven by competition, and stay aware of the potentially large effects that gradual easing of underwriting standards can have over a long period of time.

Let’s talk

Michele Crish
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
mcrish@deloitte.com

Jeff Curry
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
jeffcurry@deloitte.com

Ray Gonzalez
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
rgonzalez@deloitte.com

Dave Wilson
Independent senior adviser to
Deloitte & Touche LLP
daviwilson@deloitte.com

3. Ibid.
CECL: Investors want a clear story; will CFOs be prepared to tell it?

Financial institutions are closing in on the adoption of the Financial Accounting Standards Board’s (FASB) Current Expected Credit Loss (CECL) standard that will be reflected in the first quarter of 2020 for many public companies. The new standard requires companies to measure expected credit losses over the estimated life of a loan using reasonable and supportable economic forecasts, representing a substantial departure from current allowance for loan and lease losses (ALLL) practices. However, measuring CECL’s estimated credit losses, while difficult, may pale in comparison to the difficulty in communicating to investors a financial institution’s methodology and its impacts to the financial statements.

FASB requires that CECL disclosures enable financial statement users to understand the credit risk inherent in the portfolio, how credit quality is monitored, the methodology used for estimates, and period-over-period changes in the estimation of CECL. However, if investors can’t understand key components of CECL, it becomes significantly more difficult to understand individual company results and industry comparability. And if investors are left to model CECL estimates through guesswork, it could result in a variety of challenges for investors.

Ultimately, it will be critical for chief financial officers (CFOs) to develop the right disclosure approach to help communicate effectively with investors. There are several ways CFOs can better prepare themselves to help deliver their organization’s CECL story effectively.

Grab hold of the disclosure reins
CFOs have led their organization’s CECL implementation process using traditional change management techniques. Now is the time for the CFO to take the reins and drive the disclosure phase from the top down. Running your disclosure review process like you would the disclosure process for a large merger or balance sheet restructuring can help drive that laser-like focus that stands to benefit your disclosure development. Further, active CFO engagement can help surface both strategic issues as well as some critical “in-the-weeds” issues earlier.

CFOs can drive the in-depth conversation using some probing questions, including the following:

- **What “Goldilocks” level of disclosure will best communicate the critical aspects of CECL?** Create an internal disclosure “control group” to provide independent feedback from an investor’s perspective.

- **What linkage should exist between credit quality indicators and portfolio allowance calculations?** Consider whether linking these two FASB disclosures would help provide transparency to CECL results.

- **Do we have the right information available to support the required period-over-period change disclosures?** Review the information the institution will utilize to support the “describe-and-discuss,” narrative disclosures.

- **Do any qualitative adjustments impact disclosures to our investors?** Review the qualitative adjustments to the CECL model results, including any adjustment for “forecast variability.”
Assess the US Securities and Exchange Commission’s (SEC) critical accounting estimate sensitivity disclosure requirements

Sensitivity analyses can help provide a better understanding of CECL among investors. While CECL sensitivity disclosures could be complicated, disclosures that provide insights to the impact of future changes in CECL estimates could be very useful to investors. For example, disclosing sensitivity information around changing economic forecasts and credit quality indicators should provide investors useful information to demystify the CECL estimate.

Actively engage your investor relations group

Investor Relations (IR) needs to have a big seat at the disclosure table. Their job is to build upon the fundamental Generally Accepted Accounting Principles (GAAP) and SEC disclosures to create a clear and simple investor message. Investor questions will likely fall into two categories: How does your CECL process work, and how do you project your future CECL provision expense? A few ways your IR group can help include:

• **Create the IR binder section for CECL.** Develop a comprehensive, pyramid disclosure prep package for CFO and CEO.

• **Develop the investor “tough questions” list for CECL.** As with quarterly earnings release preparation, both identifying the questions and the company’s responses will prove valuable.

• **Conduct mock earnings release calls focused on CECL methodology and results.** For something this important and complicated, there is no substitute for mock investor dialogue.

• **Draft a mock sell-side review of your CECL GAAP/SEC disclosures.** Use an independent internal control group, or bring a sell-side analyst over the wall, to review your draft disclosures to help you assess if investors “heard” your message, including their ability to predict future CECL provisions.

Developing the right CECL disclosure approach will likely be one of the most difficult financial disclosure decisions CFOs will face in their careers. CECL's required credit loss forecasting will bring a new level of uncertainty to the most closely analyzed number in banks’ financial statements. Clearly laying out and aligning all the credit and allowance disclosures could pay big transparency dividends for institutions and investors—something which could be invaluable whenever the current credit cycle ends.
LIBOR transition: Time is running out

The pressure is on as the 2021 deadline approaches for the global London Interbank Offered Rate (LIBOR) transition. Regulators around the world have been working feverishly over the past year to find replacement rates and build out working groups. To support the transition, they continue to publish guidance and collective expectations for the industry, including the “Practical Implementation Checklist for Secured Overnight Financing Rate (SOFR) Adoption.”

In the United States, efforts by the Alternative Reference Rates Committee (ARRC) have brought greater clarity to the transition. The SOFR, the proposed replacement rate for US dollar LIBOR, has been increasingly gaining acceptance. For instance, debt issuances—as well as trading volumes of exchange-traded futures and swaps that are tied to SOFR—continue to increase. SOFR futures volume on the Chicago Mercantile Exchange (CME) crossed $1 trillion in 2019. However, recent liquidity challenges in the US repo market have raised new questions about the stability of SOFR as an alternative, driving the daily volatility in SOFR to record levels (although the impact on the 90-day average, which will be the basis for most transactions, was negligible).

The ARRC has held extensive consultations with industry groups, including the International Swaps and Derivatives Association (ISDA), the Structured Finance Association (SFA, formerly SFIG), and the Loan Syndications and Trading Association (LSTA). Also, in 2019, the ARRC published fallback provisions for floating-rate notes, bilateral loans, securitizations, syndicated commercial loans, and adjustable rate mortgages (ARMs). Fallback language for other products are in progress.

Meanwhile, the Financial Accounting Standards Board (FASB) has convened a project to address accounting issues that could arise from the transition, and has designated SOFR as an accepted benchmark for hedge accounting.

Other jurisdictions have made progress as well. In the United Kingdom, over US $30 billion in floating-rate notes tied to the Sterling Overnight Index Average (SONIA) were issued in the first half of 2019. In Europe, the Euro Short Term Rate (ESTR) began publication in October 2019. Elsewhere, countries such as Switzerland and Japan have also made progress on identifying a replacement rate.
Although much progress has been made over the past year, more work is needed. Initial assessments have been performed, and banks have a better understanding of their exposure to transition away from LIBOR. Many banks have begun to realize that the transition away from LIBOR will have a widespread impact, requiring changes to front-to-back processes and supporting systems, a product replacement strategy, ongoing client communications, active management of conduct risks, and adjustments to contract language for existing and future exposure. To accelerate implementation, modernizing such processes and systems and executing on a well-thought-out transition plan should be considered a priority. Banks should be proactively working with their corporate and buy-side clients to help ensure a smooth transition process.

5. FASB Accounting Standards Update No. 2018-16, Derivatives and Hedging (Topic 815): Inclusion of the Secured Overnight Financing Rate (SOFR) Overnight Index Swap (OIS) Rate as a Benchmark Interest Rate for Hedge Accounting Purposes.
Volcker 2.0

The original Volcker Rule was finalized in December 2013 (the 2013 Rule) to prevent banks from engaging in impermissible proprietary trading and to prohibit them from owning hedge funds or private equity funds. The FDIC, OCC, FRB, Commodity Futures Trading Commission (CFTC), and SEC (collectively, the Agencies) jointly released proposed amendments to the 2013 Rule in July 2018. However, strident opposition and industry feedback led to a revised version of the proposed amendments, which were subsequently published on August 20, 2019. All five implementing Agencies have now formally approved the Final Rule, which becomes effective on January 1, 2020. Banking entities will have until January 1, 2021 to comply, but they can adopt (in part or in full) the provisions of the Final Rule any time after January 1, 2020.

Key considerations for banking entities with regard to the Final Rule include:

- **Tailored regulatory impact.** The Agencies created a three-tiered approach to apply the compliance program to banking entities based on the size of their trading assets and liabilities. The Final Rule increased the threshold for “significant” trading activity from $10 billion to $20 billion based on the average gross sum of trading assets and liabilities over the previous consecutive four quarters as measured on the last day of quarter-end. Banking entities generally know which tier they fall into; however, firms that are close to one of the thresholds should carefully evaluate their trading assets and liabilities to ensure they fall below the applicable thresholds.

- **Resource and process optimization.** Now that the Final Rule has been formally adopted by all implementing Agencies, banking entities need to understand where they fall within the scope of applicability and what the requirements are across the simplified and six-pillar compliance programs. Given the reduced compliance requirements, banking entities—especially those that are under the $1 billion “limited” trading threshold—can shift their focus toward reorganizing their resources. However, banking entities with “moderate” or “significant” trading assets and liabilities could benefit from an assessment of their existing compliance programs and processes to identify maintenance needs and potential modifications.

- **RENTD requirements and limits.** It is important to note that the core requirements and limits related to “Reasonably Expected Near-term Demands of Clients, Customers and Counterparties” (RENTD) remain in effect and that regulators will be scrutinizing these limits as part of the ongoing exam process. As discussed in our previous publications on RENTD and limit setting, the process of calculating RENTD and then translating it into defensible limits that can be used to establish the presumption of compliance will remain a critical exercise for most banking entities in the significant and moderate categories. For derivatives, there are potential areas of relief related to market making and risk management inventory constructs; trading desks focused on derivatives should evaluate these new requirements to determine if their RENTD analysis and limit-setting processes need to be updated.
• **Metrics reporting.** The Final Rule makes several meaningful changes to the metrics reporting requirements. Although some of the changes offer relief (e.g., elimination of certain metrics, and extension of the submission timeline), the addition of new metrics, such as transaction volume and positions, will require assessment and development of new data flows and reporting capabilities. The Final Rule’s overall alignment with how most covered banking entities view and manage risk will likely mitigate these impacts; however, banking entities should undertake a formal assessment of the requirements and identify any gaps that need to be addressed.

• **FBO considerations.** The trading by a foreign banking entity outside the United States (TOTUS) and solely outside of the United States (SOTUS) exemptions have been modified to make it easier for FBOs to qualify covered activities related to proprietary trading and covered funds.

• **Deferrals and additional rulemaking.** Looking ahead, the agencies intend to issue further rulemaking on fund-related issues, such as the definition and applicability of “covered funds” and “banking entity” (and their potential exclusions).
FBO industry landscape in year four of Enhanced Prudential Standards

More than three years after the implementation date of the EPS Regulation YY, FBOs are continuing to make progress transforming their operations into more self-sufficient regional organizations. However, many are still experiencing growing pains. Whether the challenge is to increase the maturity of risk management and governance or to rationalize organizational structures and business operations across the IHC or branch network of their CUSO, FBOs are likely experiencing a journey that is far more challenging than that encountered by other parts of their global organizations.

Subsequent to this implementation, the FRB finalized the EPS tailoring rule on October 10, 2019, granting some institutions with lower risk profiles relief from the more burdensome aspects of capital, stress testing, liquidity, and other requirements. However, the core expectation of achieving a self-sufficient, regionally focused organization remains, as does the requirement for FBOs with US nonbranch assets above $50 billion to form IHCs. Moreover, while the hard-and-fast rules for EPS (as well as resolution planning) may have been relaxed for many organizations, supervisors appear to be maintaining a clear, consistent, and strong focus on risk management fundamentals and governance over US operations.

Key considerations for FBOs in 2020—and beyond

Now that regulatory expectations for FBOs are more settled and stable (although still somewhat in transition as a result of tailoring), FBOs might want to reevaluate their business models and operations, taking a fresh look at where they are best positioned to succeed in the US marketplace and to capitalize on their unique ability to serve clients as part of a global network. This includes evaluating how the current regulatory and market landscape might call for certain businesses to be de-emphasized or cast off in favor of other areas that offer greater competitive advantage and the ability to successfully meet regulatory expectations for safety and soundness and being “well-managed.”

A refreshed business strategy goes hand in hand with the ongoing work to achieve a sustainably transformed regional operation that meets regulatory expectations while achieving business goals. When EPS took effect in July 2016, Deloitte noted that the go-live date was not a “finish line,” but rather that FBOs and their IHCs should see it as mile 13 of a marathon. We also noted that large FBOs would need to demonstrate the ability to govern and manage risk for their CUSO on a self-sufficient and sustainable basis and that success would come down to how US management and the US IHC BoD work through issues and decisions such as budget approvals, capital planning, and crisis management—as well as how they navigate shareholders, the parent organization, and the parameters between global consolidated efficiency and a regional legal entity focus.

Now, in year four of EPS, several ongoing challenges continue to require attention from IHC boards and senior management as FBOs strive to meet expectations and transform their business and operating models efficiently and effectively. Here are several key considerations FBOs should be mindful of in 2020 and beyond.

Regulatory focus areas for FBOs.
Supervisory reports from FRB and OCC highlight issues and forward-looking supervisory concerns across FBOs. According to a May 2019 FRB report,¹ “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 firms after a hypothetical severe global recession would remain above regulatory minimums.”

Although the FRB appears satisfied with institutions’ financial condition, the agenda for ensuring that governance and risk management are satisfactory is wide-ranging. In 2019, the focus across

Banking regulatory outlook 2020 | FBO industry landscape in year four of Enhanced Prudential Standards
Global foreward Leadership

Banking regulatory outlook 2020

Banking regulatory outlook 2020

The portfolios comprised four supervisory pillars: capital, liquidity, governance and controls, and recovery and resolution planning. The key supervisory priorities are:

- Liquidity buffer and contingency funding plan
- Operational & cyber resilience
- Risk reporting
- Use of AI for fraud and BSA/AML detection
- Compliance metrics
- Loss estimation methodologies and governance for residential mortgage and commercial real estate portfolios
- Governance of the capital planning process
- Recovery and resolution planning

Assessing and unwinding in a controlled manner. Institutions receiving relief due to tailoring need to evaluate how changes in standards should be factored into medium-term strategies for US operations. These firms should unwind their related supporting regulatory infrastructure in a measured manner and then only if the underlying capability is not additive as part of good governance or risk management or to ensure that fundamental risk management that intersects with these areas is not unintentionally degraded and that unnecessary rework is avoided. It is important to note that despite relief in the rules applied to institutions, the intensity of examiner scrutiny and level of expectations appears to have lightened only modestly and may have increased in some areas for some more systemic firms. Regardless of which new tailoring category a firm might find itself in, examiner scrutiny of the basic blocking and tackling of risk management and related capabilities is unlikely to lighten appreciably soon.

Cautious optimism—understanding the tailoring rule and navigating the web of thresholds. Institutions will need to understand the thresholds that apply to their FBOs and monitor them holistically going forward, not only as part of business as usual, but also as part of new business or new product analysis (as appropriate) and as part of overall strategy for CUSOs. Substantial training and awareness will likely be needed on an ongoing basis for US and parent-level executives. Transition timetables will need to be monitored carefully. Regular reporting capabilities will need to be leveraged at regulatory reporting (to report on the underlying data); they also will be needed for internal monitoring. Monitoring of thresholds will need to coincide with business and risk metrics on an ongoing basis.

Branch liquidity rules—impact to be determined. The FRB deferred the decision, but requested comments on whether standardized liquidity requirements should be imposed on US branches and agencies of FBOs, and what approaches to use. For years, the FRB has discussed addressing this risk by proposing the application of standardized liquidity requirements to the branches and agencies of foreign banks, which would reduce the incentive to shift assets to branches from IHCs. Since the IHC requirements were put in place, branch assets have actually grown as a percentage of foreign bank activities in the United States, and the US branches and agencies of foreign banks are now roughly twice as reliant on short-term wholesale funding as are the US IHCs.

Increase in transparency. Both FRB Vice Chairman for Supervision Randal Quarles and Comptroller Joseph Otting have stated their goals of increasing transparency within the regulatory system. This represents another step for regulators to strengthen transparency in regulation and supervision, which could provide a forward look into focus areas for supervision and examination.

Global and US operating model. Firms need to strike a balance between global and CUSO, with offshoring, nearshoring, remote booking, and centralizing all creating challenges for a CUSO-enabled governance and operating model. Many FBOs are struggling with parent dynamics to safeguard that the United States is not used only as a “booking point” within larger global cost and efficiency plays. Also, many FBOs are still having difficulty meeting governance expectations, as regulators look at outcomes—risk management failures, controls weaknesses, trading mishaps, compliance violations and issues, and quality of regulatory reporting—as measures of the effectiveness of the governance and control environment.

Booking model and US-managed view. Many institutions are wrestling with the issue of transparent business strategy within a US-managed view—defining what is originated, booked, or risk-managed—with risk limits and triggers and financials that can be explained across CUSO or IHC. There is sensitivity to booking choices between US branches and operating subsidiaries (particularly under BHC or IHC).

Another issue is transparency to parent boards, US risk committees, and senior management regarding how the business operating model, transfer pricing, and service level agreements affect risk and financials. In addition, many FBOs that are part of G-SIBs feel the pressure of home- and host-country regulator requests and expectations in responding to questions on US and cross-border booking practices and governance.
Operational risk and issue management. Firms need to sustain regional management capabilities for self-identifying, remediating, and monitoring risk and operational issues within the 3LOD model. They also need the ability to build a sustainable self-improvement process to prioritize operational breaks, operational issues, and risks across all three lines. A key focus area is management of controls and rationalization across different risk parameters and implementation of GRC tools to manage risk assessments and controls. Another key focus area is operational risk and identification of CUSO-related themes that are holistic across and within business units and controls functions. Institutions need to calibrate and prioritize outstanding remediation efforts to demonstrate that appropriate governance and oversight is provided by the board and CUSO management regarding escalation to the parent.

There is also a need for focused remediation that is not delayed or cut by parent-only views; institutions need CUSO governance and escalation to drive discussions with the parent. Finally, FBOs will need to demonstrate strong outcomes or prove their structure was not an impediment to strong governance and risk management.

CUSO management reporting transparency. Institutions need consistent and flexible management information systems (MIS) and reporting views emphasizing CUSO, IHC, and branch dimensions, along with sustainability of existing regulatory reporting processes for branch-to-branch and branch-to-subsidiary within an overall data governance model and approach.

US regulatory compliance. With significant pressure on regulatory change and broader change processes, firms need to continue building awareness and knowledge of the existing regulatory requirements related to operating model, staffing, systems, and processes. Institutions need the ability to maintain a sustainable end-to-end compliance program within CUSO as part of a broader parent approach.

BSA and AML compliance implementation has resurfaced as a significant challenge for businesses attempting to scale their operations while meeting requirements. More broadly, a key issue is evaluating controls on an end-to-end basis, not only from a first and second line distinction, but also across preventative and detective controls for compliance and operational issues.

TPRM and vendor risk management. First and foremost, firms need to maintain a CUSO view related to outsourcing risk, with a focus on whether a firm’s due diligence covers how well vendors manage their own risks. This “fourth-party” risk (particularly cyber risk), is an emerging focus area, although supervisory expectations are still in the early stages of debate and development.

Evaluation of NFRs is of near-term concern for US regulators, given changes in the business operating model and formation of service companies, as well as changes driven by cost efficiency concerns. For outsourcing risk, the definition of “vendor” is intended to be broad and to span the full range of service providers. Inventorying vendors and conducting vendor risk assessments is essential and drives monitoring, intensity of due diligence, and controls testing.

MIS/regulatory reporting and data governance. Institutions need the capability to meet regulatory reporting expectations for access to source information and underlying data. FBOs have generally relied upon their parent risk data aggregation (BCBS 239) programs for data governance. There is continued and sustained pressure on US and FBO LISCCs and large financial institutions to improve their data quality for management and regulatory reporting, with a greater focus on infrastructure and transparency of enterprise-wide data and legal-entity views. Institutions face challenges in reacting to information requests that are CUSO-wide while information is legal entity- or business-aligned. Challenges have been typically linked to the absence of:

- Governance structure that enforces accountability, measures data quality, and allocates resources to address data and financial-reporting challenges
- Accountability of data owners (i.e., business lines)
- Firmwide data integrity and quality assurance programs that include requirements related to MIS, financial reporting, and regulatory compliance
- Effective change management infrastructure
- Firmwide data programs that include policies for creating and maintaining standard data and account definitions
- Firmwide integrated accounting, risk, and data repositories

Governance and 3LOD effectiveness. Firms need to understand and balance expectations highlighted in finalized and proposed guidance for a new rating system for large financial institutions (finalized November 2018); board effectiveness (proposed August 2017); and risk management and 3LOD (proposed January 2018). Also, there is a resurgence of questions related to global and matrix reporting, decision rights, and the balance between parent and US influence—particularly as global operating models change, new
Global forward  

Leadership

Businesses are launched, and parent directives influence US operations. Key issues include accountability of IHC board or risk committee and escalation to the parent, accountability impact on individual performance evaluations and compensation, and confirmation of risk management and governance capabilities.

Operational and business resiliency. Institutions need the ability to understand and support the linkages across recovery, business continuity, and crisis management, with a governance overlay by the board (parent and IHC board). Cybersecurity and the ability to recover from cyberattacks or breaches is currently a supervisory topic across regulatory agencies. Remediation activities coming out of the horizontal examinations will need to keep pace with emerging risk across all regulators.

Institutions will need the ability to incorporate lessons learned from current incidents and refine parent and CUSO protocols. Key focus areas include building improved CUSO resiliency through informed technology and infrastructure decision-making, linking parent and CUSO leads and committees for technology, resiliency, business continuity, cybersecurity, and information security.

Resolution planning. There is a need to maintain momentum on resolution plans and the related mandates for operational continuity through resolution. Going concern, operational continuity, and crisis management efforts can be leveraged further for this effort in complying with regulatory timelines and mandates.

Setting priorities
Each firm should evaluate its focus areas and prioritize its improvement and sustainability efforts based on which areas are likely to have the biggest impact on its risk and operating profile. In the years ahead, prioritizing those high-impact efforts can lead to smoother expansion and refinement with fewer regulatory constraints.

Let’s talk

Craig Brown  
Managing director  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
cbrown@deloitte.com

Michele Crish  
Managing director  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
mcrish@deloitte.com

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

Aaron Bhardwaj  
Senior manager  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
aarbhardwaj@deloitte.com

Joanna Connor  
Senior manager  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
jconnor@deloitte.com

Richard Rosenthal  
Senior manager Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
rirosenthal@deloitte.com

4. Ibid.
6. Board of Governors of the Federal Reserve System, Supervision and Regulation Report, November 2019,  
Other important regulatory topics

Firms should stay apprised to the following regulatory topics and their developments in 2020:

Community Reinvestment Act (CRA). On December 12, 2019 the FDIC and the OCC announced a proposal to modernize the agencies’ regulations under the Community Reinvestment Act (CRA) that have not been substantively updated for nearly 25 years. The proposed rules are intended to improve the current CRA regulatory framework and promote increased lending and investment consistent with stakeholder feedback. The agencies propose to make changes in four key areas:

- Clarifying and expanding what qualifies for CRA credit;
- Expanding where CRA activity counts;
- Providing an objective method to measure CRA activity; and
- Revising data collection, recordkeeping, and reporting.

At the time of this update, the FRB has not decided on how to proceed.

BHC control

On April 23, 2019, the FRB invited public comment on a proposal that would simplify and increase the transparency of the FRB rules for determining control of a banking organization. If a company has control over a banking organization, the company generally becomes subject to the FRB rules and regulations.

The proposal laid out factors and thresholds that the FRB will use to determine if a company has control over a bank. The key factors include:

- the company’s total voting and non-voting equity investment in the bank;
- director, officer, and employee overlaps between the company and the bank; and,
- the scope of business relationships between the company and the bank.

The proposal clearly what combination of those factors would and would not trigger control.

Climate change and sustainability

In 2019, the US Congress and domestic and international regulators began to identify financial risk as a result of climate change as a potential risk to financial stability. In July 2019, the US House Committee on Financial Services, Subcommittee on Investor Protection, Entrepreneurship, and Capital Markets held a hearing titled “Building a Sustainable and Competitive Economy: An Examination of Proposals to Improve Environmental, Social and Governance Disclosures.” The hearing focused on reporting requirements for US public companies in response to increasing interest in the investor community for enhanced ESG disclosures and uniform reporting standards, the growing importance of ESG in the larger investment and regulatory landscape, and various proposals to improve ESG disclosures to build a sustainable and competitive economy.

In November 2019, FRB Governor Lael Brainard made a speech at the Federal Reserve Bank of San Francisco’s conference on climate change stating "Although there is substantial uncertainty surrounding how or when shifts in asset valuations might occur, the Federal Reserve can begin to identify the factors that could propagate losses from natural disasters, energy disruptions, and sudden shifts in the value of climate-exposed properties.

In addition, regulators are also considering adding climate change financial risks as an input to bank stress tests. The European Central Bank is developing an analytical framework for carrying out a climate risk stress test analysis, and the US Senate introduced legislation requiring the same from the FRB.

Staying ahead

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

Leadership

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

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

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

Irena Gecas-McCarthy
FSI Director, Deloitte Center for Regulatory Strategy, Americas
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
igecasmccarthy@deloitte.com
About the Center
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends. Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media, including thought leadership, research, forums, webcasts, and events.

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

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

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