

**Deloitte.**



2023 banking  
regulatory outlook

CENTER *for*  
**REGULATORY  
STRATEGY  
AMERICAS**

# Contents

'Still work to do' to meet core and emerging supervisory expectations	1
Responding to forces of innovation	4
Fortifying governance and controls as part of core safety and soundness	8
Data governance and reporting	
Cyber and information technology (IT) risk	
Bank Secrecy Act (BSA)/anti-money laundering (AML) and sanctions	
Consumer protection and financial inclusion	
Expanding the scope of financial risk management	18
Capital	
Liquidity	
Climate-related financial risk	
Looking forward to an active 2023	22
Endnotes	23
Contacts	26



# 'Still work to do' to meet core and emerging supervisory expectations

The banking system was subjected to significant forces in 2022, including inflation, rising interest rates, equity and bond market declines, plunging cryptocurrency prices, consequences (political, trade, economic) of the Russia-Ukraine conflict, lingering effects of the COVID pandemic, and—to at least some extent—the reemergence of consumers from pandemic isolation.

Despite these challenges, banks overall have maintained adequate capital and liquidity levels signifying their underlying strength to withstand stress and suggesting that there is no bank crisis at present or on the near horizon.<sup>1</sup> As was true in 2021, no Federal Deposit Insurance Corporation (FDIC) insured depository institution failed in 2022. However, concerns about systemic risk and resolvability in the banking sector persist. In 2022, regulators resurrected the too-big-to-fail moniker with a renewed focus on applying certain resolution requirements to those large banks that are not considered Global Systemically Important Banks (G-SIBs). Providing regulatory decision-makers with “more options” in the event of large bank failure was the catalyst behind the potential pushdown of G-SIB requirements including single point of entry, total loss absorbing capital, and separability to the largest of non-G-SIBs.<sup>2</sup> The systemic risk and resolvability of non-G-SIBs are two topics that may also flow through to ongoing revisions of the Bank Merger Act.<sup>3</sup>

The stark contrast between the runs, liquidity issues, and other troubles evident in the cryptocurrency sector, and the comparative stability of banks and their affiliated enterprises within US bank holding companies (BHC), raises important public policy questions.

For example, some would argue that the differing results between the banks and nonbank/crypto markets demonstrate the effectiveness of the stringent regulation and supervision within the bank regulatory perimeter and a need to pull additional activities within that perimeter or otherwise subject them to bank-like regulation.<sup>4</sup> Others would credit the actions (or perhaps inaction) of the banking regulators in keeping cryptocurrencies and related activity largely outside of that perimeter and would argue for further scrutiny of bank and nonbank interactions. Still others would cite luck, noting the still relatively small size and nascent

status of the crypto-asset market.<sup>5</sup> Whatever your view may be, it is not a leap to believe that the events of 2022 will lead to additional regulation and supervision, including further pressures at the perimeter separating banks and nonbanks.<sup>6</sup>

With fintech companies and nonbanks looking to offer a range of payment and financial services products enabled by technological developments, we are seeing races across the industry to get access to the regulatory “assets” (e.g., access to the payments system and access to FDIC-insured deposits) that can drive sustained returns. The federal banking regulators continue to carefully guard the keys, all while subject to the scrutiny of their congressional leaders.

In the meantime, to the extent that bank regulatory policies (e.g., regulations, supervisory guidance) have been slowed by a transition in administrations and pandemic considerations, those headwinds are abating. Onsite examinations are returning to full swing, following whatever respite might have occurred during the height of the pandemic (when supervision focused on offsite monitoring). In stating its supervisory priorities for 2023, the Federal Reserve Board of Governors (FRB) stated that banks still have “work to do” to meet supervisory expectations, especially for governance and controls.<sup>7</sup> Elements of governance and controls are also emphasized by the Office of the Comptroller of the Currency (OCC) and deemed priority objectives for 2023.<sup>8</sup> The OCC classifies operational risk as “elevated,” and “risk-focused” supervisory plans for individual institutions will likely be developed using these objectives as a basis.<sup>9</sup> Outside of stated priorities and expressed expectations, the FRB, OCC, FDIC, and Consumer Financial Protection Bureau (CFPB) will likely assess compliance and risk management frameworks during the normal course of supervision.

The Biden administration now has key policymakers in place, including new Vice Chair for Supervision at the FRB Michael S. Barr; recently confirmed FDIC Chairman Martin Gruenberg and a full slate of FDIC directors; CFPB Director Rohit Chopra; and active Acting Comptroller of the Currency Michael Hsu, who appears to be fully aligned with the administration's priorities. As detailed in this outlook, important regulatory proposals have been made, and more actions are anticipated in 2023.

Banking regulators have exhibited increased supervisory collaboration and are effectively connecting themes between supervisory events to draw conclusions and identify emerging risks throughout the banking sector. This collaboration is driving ever-increasing regulatory expectations and a “race to the top.”

Against this backdrop, our *2023 banking regulatory outlook* will take a deeper look at 2022 developments and possible 2023 regulatory actions from core safety and soundness to fortifying governance and controls across the following key areas:

- Responding to forces of innovation
  - Digital assets: Permissibility versus advisability
- Fortifying governance and controls as part of core safety and soundness
  - Data governance and reporting
  - Cyber and information technology (IT) risk
  - Bank Secrecy Act (BSA)/anti-money laundering (AML) and sanctions
  - Consumer protection and financial inclusion
- Expanding the scope of financial risk management
  - Capital
  - Liquidity
  - Climate-related financial risk



With fintech companies and nonbanks looking to offer a range of payment and financial services products enabled by technological developments, we are seeing races across the industry to get access to the regulatory “assets” (e.g., access to the payments system and access to FDIC-insured deposits) that can drive sustained returns.







# Responding to forces of innovation

Federal banking regulators are watching the transformation of banking by innovative means and using their existing supervisory capacity to maintain the safe and sound operation of banks. A recent “Joint Statement on Crypto-Asset Risks to Banking Organizations” (joint statement) captures the hardline view of the FRB, OCC, and FDIC on supervised banks and their engagement with crypto-related banking activities.<sup>10</sup> A broad definition of crypto-assets, list of key risks, and cautionary statements about certain activities that may be permissible, but not advisable, are the primary components of the joint statement.<sup>11</sup> Regulators will likely refer back to the joint statement to amplify existing concerns in advance of more prescriptive regulation.

As the regulatory perimeter evolves in response to a shifting competitive landscape, disruptive forces are reshaping banking business models, products, and services. Indeed, there are several industry trends transforming the banking value chain, including fast-growing digital banking offerings; an increasing interest in digital assets, particularly cryptocurrency-related activity; banking as a service (BaaS); and AI-enabled tools deployed in front- and back-office operations and integrated into core banking products and services.

For example, artificial intelligence (AI) can help organizations improve efficiency, lower costs, enable growth, boost differentiation, manage risk, comply with regulations, and upgrade the customer experience. ChatGPT, released in November 2022, experienced significant adoption at the onset with one million users signing up in five days.<sup>12</sup> Utilization of this AI-driven tool in the banking sector is expected to support legal analysis, investment research, bank financial condition summations, faster generation of written documents, and other activities. As banks look to reduce funding costs given inflation and macroeconomic impacts, we expect optimization efforts to be front and center. While many organizations were already investing in AI enablement, the pandemic also heightened customer expectations around digital banking.<sup>13</sup> This prompted many banks, especially those with substantial brick-

and-mortar presence, to examine how they deliver services to their customers, many of whom now demand compelling, intuitive digital experiences on both mobile and online platforms, similar to what they receive from leading e-commerce companies.

As banks change the way they deliver services to address changing customer expectations, bank-fintech partnerships are growing in number and sophistication. Banks are plugging fintechs into their core platforms to obtain leading capabilities such as intuitive user interfaces or onboarding experiences. On the flipside, banks are also serving as the back end to fintechs, often providing customer access to FDIC-insured deposit accounts and payments systems, as well as loan funding and other capabilities.

## Digital assets: Permissibility versus advisability

The FRB, OCC, and FDIC’s January 3, 2023, joint statement reinforces previous regulatory views and draws a clear line in the sand on regulatory sentiment about the permissibility versus advisability of crypto activities.<sup>14</sup> The definition of crypto-assets set forth in the joint statement is very broad, including stablecoins and other tokenized assets, and along with the connotation of the advisability language, the messaging in the statement represents a proverbial brick wall to at-will bank engagement. The OCC was the first mover among federal bank regulators, establishing a process for national banks to obtain the OCC’s non-objection before engaging in new crypto-related activities in 2021.<sup>15</sup> In 2022, the FDIC (for state nonmember banks) issued guidance, and the FRB (for state member banks) has followed suit.<sup>16</sup> While these notification processes have not stopped bank crypto-related activities dead in their tracks, they have introduced meaningful speed bumps, and now must be built into the planning processes for banks seeking to engage in these activities.

The relationship between innovation and risk became apparent as “crypto winter” (an elongated time frame during which crypto prices decline and remain low) reduced valuations and resulted in bankruptcies of significant players.<sup>17</sup> Regulators have largely stalled bank activity in the crypto sector, insulating some banks from significant losses, and preventing further spread throughout the financial system and real economy. This distinguished the “crypto winter” events from past significant market disruptions that resulted in government interventions. This result was not preordained. Several factors limited the spread of turmoil in the crypto market. These factors include the still relatively small size of the crypto-asset ecosystem, the reticence among regulators to allow banks to fully engage with the asset class, and the absence of crypto-assets on bank balance sheets.

As we look to 2023, significant questions remain about how the regulatory perimeter should expand to address known risks that investors and consumers are facing, including clarity on how banks should engage with distributed ledger technologies and digital assets more broadly. The industry continues to focus on the long game with the belief that distributed ledger technology and the tokenization of assets will be a transformative shift for markets. We expect regulators to be forced to deal with policy and supervisory questions of what is acceptable and how it should be governed. We also expect that enforcement and other supervisory actions may have unintended consequences. As one recent example, a possible unintended consequence of the Security and Exchange Commission’s (SEC) 2022 Staff Accounting Bulletin No. 121 (SAB 121) may have been to push core digital-asset custody activities to less regulated market participants.<sup>18</sup>

With the industry hoping for clarity across a wide range of regulatory questions, the level of complexity of the US regulatory system continues to pose a unique challenge relative to other jurisdictions in addressing core, open questions. Nevertheless, firms continue to explore use cases for distributed ledger technology (DLT) and tokenization.

For market participants, we expect actions from regulators to increase as they use existing supervisory tools to enforce and protect the US banking system.

We explore the following pathways for significant action on digital assets by lawmakers and regulators:

- Banking agency enforcement and interpretive activity
- Congressional efforts to legislate

### Banking agency enforcement and interpretive activity

Regulatory activity in 2022 (guidelines, rule proposals and finalizations, and public consultations) at the state, federal, and international levels created strong disincentives for banks to engage with crypto-assets.

It remains to be seen whether regulators’ industry engagement will enable them to process requests more efficiently in 2023. Also unknown is the extent to which regulators’ learnings will inform and lead to their issuance of broader-based regulations and other guidance. Given the market events of 2022, and subject to the potential enactment of federal legislation, we expect the regulators to continue to move cautiously regarding crypto-asset activities in 2023. With that said, we expect a more coordinated approach from the federal regulators in 2023 and increasing heightened supervisory actions.

### Congressional efforts to legislate

2022 saw vigorous development and introduction of bills to clarify the regulatory treatment of crypto-assets. Despite the perceived enthusiasm and calls for legislation by the Treasury and Financial Stability Oversight Council (FSOC) via the Executive Order (EO) reports in late 2022, no federal legislation was enacted last year. Several bills proposed in 2022, albeit prior to a significant crypto-exchange bankruptcy and related events in late 2022, outline possible approaches should legislation happen.

When and what sort of legislation eventually might pass remains the subject of intense speculation, but stablecoin legislation may be a place where consensus is possible.<sup>19</sup> From a global perspective, the United States is falling behind in its development of a policy framework, with the European Union agreeing to text for its Markets in Crypto-assets regulation and the United Kingdom making an earnest attempt at legislation as well.<sup>20</sup> Given recent market events, we expect the legislative and regulatory rulemaking process to make headway in 2023.

### Looking ahead

While progress on the policy front has been slower than many market participants would like to see, 2022 offered glimpses of the potential future state. In 2023, all eyes will be on a new Congress for potential federal legislation to address stablecoins, other crypto-assets, and potentially a US Central Bank Digital Currency (CBDC).

Banks can play a key role in the institutionalization of the asset class as the US regulatory framework develops. From a policy perspective, the cautious stance of regulators has pushed many activities to entities outside of the bank regulatory perimeter. Banks, as highly regulated entities, can serve as reliable custodians and issuers if certain regulatory hurdles are cleared.

It is critical, in the absence of legislative clarity, for banks and nonbanks to keep close tabs on regulatory developments and to be mindful of banking regulators' risk management and general safety and soundness expectations. We expect banking regulators to continue to heavily scrutinize new digital-asset product launches, including continuing to place a heavy emphasis on third-party risk management.

When focusing on **digital assets**, banks should consider several actions:

- **Engage in early and frequent regulatory dialogue and satisfaction** of any applicable regulatory application or non-objection processes.
- **Demonstrate use of existing control frameworks** (e.g., new product approval) that are tailored to the risks presented by the proposed product, service, and third-party relationships.
- **Ensure alignment of digital-assets strategy** with the organization's overall strategy and risk appetite.
- **Demonstrate the actual product has a real market and consumer utility** and that the benefits are substantive.
- **Equip the board and senior management with resources and staff** to undertake these initiatives.





# Fortifying governance and controls as part of core safety and soundness

The federal banking regulators have signaled that their entrance into the upcoming supervisory cycle will be characterized by an intense focus on post-pandemic financial risk. The increase in large bank supervisory findings over the first half of 2022 was met with the OCC and FRB's commitment to assess remediation of outstanding supervisory findings, with particular emphasis on Matters Requiring Attention (MRAs) in 2023.<sup>21</sup>

Following up on remediation efforts has shifted from a routine touchpoint—usually, a given within the normal course of supervision—to a known supervisory priority for the federal banking regulators. This is a clear indication that banks will need to be intentional about addressing identified weaknesses in a comprehensive way to prevent the escalation of open MRAs to Matters Requiring Immediate Action (MRIAs), or even more severe enforcement actions. Regulators have reiterated this point with recent emphasis on the delineation of roles and responsibilities across the three lines, including enterprise governance and oversight, before confirming successful and sustainable remediation.

Under the FRB's large financial institution (LFI) ratings system—currently applicable to 37 holding companies with banking subsidiaries supervised across the FRB, OCC, and FDIC—"governance and controls" is the catch-all ratings component where the broadest range of topical areas are covered and similarly where supervisory issues are the most heavily concentrated for large banks.<sup>22</sup> Elements of governance and controls are also engrained in the supervisory framework for subsidiary banks and are an equally important supervisory focal point at both the bank and holding company levels. We see the following topics as fundamental to improving key functions and capabilities contributing to a bank's governance and controls as well as its safe and sound operation.

## Data governance and reporting

Effective management, including crisis management, depends on reliable and timely information in a rapidly evolving environment. Regulators need data to assess economic developments and analyze interconnectedness within the financial system. For regulators to properly monitor risks and the effects of policy, banks need to provide real-time data, which will be collected more frequently. In times of stress, regulators may need to collect data not captured by current reports or that is currently captured only at infrequent intervals to monitor the effectiveness of policy measures.

Increasing data availability and improving data quality represent two critical priorities for banks. As bank regulators become more data dependent, they are driving the already high prioritization of strategic data programs at the banks that they supervise. The demand for better data is resulting in banking regulators placing sustained pressure and emphasis on banks to improve their data quality for risk, management, and regulatory data purposes. These expectations are underscored by recent enforcement actions and supervisory findings citing banks' lack of internal controls, ineffective governance, weaknesses in data infrastructure, and fragmented technology environment. Regulators are aware that the remediation of weaknesses associated with data generally requires more time as compared to other risk management weaknesses; however, the supervisory focus is placed on the presence of appropriate controls to promote data availability and quality during the remediation process.<sup>23</sup>



## Data governance weaknesses continue to concern regulators

The need to provide granular levels of information, with increasing frequency, presents operational challenges and significant reputational risk for many banks. Regulators' data concerns are based on banks' historic lack of:

- Governance structure that enforces accountability, measures data quality, and allocates resources to address data and financial reporting challenges.
- Firmwide data integrity and quality assurance programs that cover management information systems (MIS), financial reporting, and regulatory requirements.
- An 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 with emphasis on a streamlined technology infrastructure.

The lack of sufficient data governance leads to inefficient data quality, negatively affecting data used for managing risk and compliance with regulatory rules and standards. This has the potential to lead to supervisory concerns across firms' legal entities, prompting data-related examination activities that include the assessment of:

- Effectiveness of remediation plans and the execution of timely and complete deliverables as outlined in these plans.
- Effectiveness of data offices in improving data quality.
- Data lineage that ensures data is traced to the source (end-to-end lineage), including documentation for Authorized Data Sources (ADS), which tracks controls for data quality at the data source and subsequent transformations.

Firms still struggle with siloed data storage and significant manual intervention. To meet these regulatory demands, firms will need to create a dynamic data environment where the processes and

infrastructure can quickly adapt to changing needs for financial, nonfinancial, and risk data, especially in times of stress.

In executing the road map to deliver a sustainable data environment that can meet regulatory requirements and expectations, there are several considerations and challenges to overcome. To start, the firm should commit to strengthening overall governance over the end-to-end data life cycle. Since data ownership is commonly segregated from the data aggregation function, a lack of consistency in the process and controls mindset, if not under a common framework, leads to data quality issues. Standardizing the processes and controls across the firm is imperative.

Underlying the efforts to create a flexible data model is the need for investments in foundational data elements across the firm that can solve multiple reporting needs with single, rather than repeated, remediation. Understanding where data issues reside and how they impact reporting is critical when setting out the road map. Efforts to evaluate outstanding supervisory findings should provide organizations with the ability to clean up outstanding thematic items and build strategic solutions. Just as important as the strategic solution is maintaining controls and level of quality on existing data while the controls and infrastructure continue to undergo enhancements.

To enforce high data quality across the firm, accountability models need better enforcement and linkage to data governance management programs. This includes developing actionable measures and metrics. To ensure high data quality standards are met, a greater focus on conformance testing and controls around data transformations is needed.

Meeting the data expectations of regulators continues to challenge banks. Transforming legacy technology solutions into a strategic data environment is a foundational investment firms should make, not only to meet current expectations but be agile enough to meet future requirements and regulations. Data supervisory findings have linked the impact of IT architecture and its complexity. Solutions should be an enterprisewide activity needing senior management and board support that can be sustained over time.





To meet regulatory expectations for data and reporting sustainably, firms need to develop a firmwide data culture that values data processes and data quality. Achieving a true firmwide data culture can be elusive. A thoughtful road map needs to be developed that includes achievable milestones and deliverables.

When focusing on **data governance and reporting**, banks should consider several actions:

- **Migrate to a product-level view** away from a specific report view and establishing traceable ADS.
- **Strengthen overall governance** over the end-to-end data processes.
- **Integrate the firm's data management programs with the regulatory data environment.**
- **Emphasize accountability of key stakeholders** (including the first line), improve coordination between impacted areas, and create actionable metrics.
- **Invest in finance, risk, and data architecture and information technology (IT) infrastructure** to increase the data capabilities needed to achieve these actions.
- **Enhance internal controls around the report preparation life cycle** (all lines) and establish independent quality assurance (QA) functions and broader data-quality programs.
- **Strengthen the competencies and training of the data resources** at the corporate and business levels.
- **Emphasize the 'attestation' approach across reports**—all reports should maintain core foundation requirements for attestation and awareness of data being reported.

## Cyber and information technology (IT) risk

Sweeping changes in technology have led to accelerated technology adoption and innovation, businesses becoming more interconnected, and customers being empowered with “digital first” experiences. These advancements, however, also present cyber risks. Like business leaders, policymakers are also taking notice and updating laws, regulations, and practices to work with critical infrastructure industries for an organized approach to cyberthreats. A watershed change in the policy approach can be traced to the Biden administration’s 2021 EO.<sup>24</sup>

Most noticeably, the EO called for a standard set of operating procedures and definitions among federal agencies. Regulators have used the transitional time since the announcement of the EO to update their guidance on cybersecurity, encouraging engagement from the top, advising multilayered control environments, standardizing incident response, and governing third-party relationships.

### Regulators are continuing to raise the bar

Over the past several years, regulators have increasingly raised expectations by demanding greater organizational responsibility for managing cybersecurity risk. While they historically have provided flexibility for adoption based on the size, nature, and complexity of the organization, the regulations have become more prescriptive and are mandating that **all organizations** adopt minimum “cyber hygiene measures” that demonstrate that the requirements have been implemented.

The shift to remote work has also increased the need for stronger cyber defenses. For example, multifactor authentication, previously seen as an advanced capability, is now becoming a requirement, as seen by the New York State Department of Financial Services (NYDFS) mandate on heightened authentication requirements for access to nonpublic information as well as to other sensitive data, systems, and interfaces.<sup>25</sup>

With increased digitization levels, where data is stored and how it is further used creates opportunities and

risks. Regulators are trying to keep up and are focusing guidance on risk management principles for the cloud, AI, and machine learning (ML). This presents an opportunity for organizations to shape and influence the emerging regulations.

### Engagement and governance from the top

Deficiency in effective cybersecurity policies and procedures to secure organization assets and data is an increasing concern of regulators. They continue to emphasize increased involvement and accountability of the board and senior leadership in setting the strategy and overseeing the organization’s cybersecurity program. A mature cyber strategy aligns with business strategy and enables an organization to meet its business objectives. Setting the tone from the top requires organizations to streamline their governance, reporting, and communication structure, where cybersecurity is treated as a core business function and capability. Proposed supervisory guidance includes new considerations making it clear that board responsibilities (e.g., approval of significant contracts or plans, oversight of the third-party risk management program) can only be delegated to a “designated board committee” (or potentially existing committee with specific mandate) that reports to the board.<sup>26</sup>

### Transparency and standardization in incident response

Regulators’ disclosure requirements continue to become more rigorous to reflect changing risks and investor needs. With the heightened frequency and severity of incidents in the financial industry, regulators are increasingly focused on transparency and standardization in incident notification and management. In March 2022, Congress passed a landmark bill, “Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),” which requires owners and operators of critical infrastructure in 16 sectors to report an incident that they reasonably believe has occurred to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours.<sup>27</sup> In addition, the CISA must be notified of any ransomware payments within 24 hours. Although not in effect yet, this “game-changing” regulation strives to close visibility gaps that impede incident response for government agencies.

Similarly, prudential banking regulators have also moved away from “as soon as possible” reporting requirements to more stringent reporting requirements such as a “36-hour window” for banks and bank service providers for incidents that they believe in good faith could cause material disruption.<sup>28</sup> While the requirements vary, almost all regulators are requiring early notifications and disclosures of incidents that cause significant business disruptions with issuance of follow-up reports as the investigation evolves. Banking regulators are extending their reach beyond the banking organizations to service providers as well, requiring vendors to notify affected bank customers immediately after the vendor experiences a cybersecurity incident.

Accountability for cybersecurity incident response and notification is shifting from information technology leaders to the board and business leaders. Regulators are urging organizations to have greater involvement of senior leadership and board members both during and after an incident has occurred. The Financial Stability Board’s (FSB) October 2022 consultative document takes a comprehensive approach for encouraging standardization, including common terminologies and a standardized format for reporting.<sup>29</sup>

### Governance of third-party risk management (TPRM)

Banks are outsourcing their business and risk management activities to harness the wide array of innovative products, services, and capabilities offered by third parties. The outsourcing of activities has, in many cases, led to bank and nonbank relationships that rely on new technology (e.g., from fintech firms) and present new risks to banks. These relationships have grown rapidly over the past few years and tend to cause regulatory concerns where nonbank activities are generally not subject to the same level of oversight as banks. The prevalence of bank and nonbank relationships adds another layer of complexity where increasing ransomware attacks have recently plagued service providers and other third parties placing even more emphasis on TPRM.<sup>30</sup> The OCC has emphasized that organizations must manage risks that third parties may pose and continue to make TPRM a key element of focus in their examinations.<sup>31</sup>

With increasingly sophisticated attack methods, it is expected that organizations undertake a wider security lens to manage third-party relationships. TPRM policies and procedures should outline the organization’s strategy and identify the inherent risks related to the engagement with the third party, including details on the due diligence and governance around vendor selection. Banking organizations should perform ongoing monitoring commensurate with the risk level and complexity of the relationship and periodically reassess existing relationships to determine whether the nature of an activity by a third party becomes critical.

When focusing on **cyber and information technology (IT) risk**, banks should consider several actions:

- **Delegate cybersecurity board responsibilities** as needed to a board committee with a clear mandate and directors with IT-related skills, as needed.
- **Establish a robust policy management program** that can account for more prescriptive changes to laws, regulations, practices, and supervisory expectations; test for efficiency regularly; and update when needed to ensure effective linkage to IT architecture, IT risk assessments, and broader views of financial crime.
- **Involve board and senior leadership during and after a cybersecurity incident** and ensure that the necessary processes and controls are in place to assess the severity of the incident in the context of the Computer Security Incident Notification Rule.
- **Reassess existing critical third-party relationships** to ensure that the appropriate amount of ongoing monitoring is in place.



## Bank Secrecy Act (BSA)/ anti-money laundering (AML) and sanctions

Going into 2023, we see three primary areas at the forefront of regulators' agendas: (1) meeting their obligations under the AML Act of 2020 (AMLA);<sup>32</sup> (2) sanctions; and (3) the increased prevalence of digital assets throughout the banking ecosystem.

### Regulators to meet obligations under AMLA

Since the passage of the AMLA, the Financial Crimes Enforcement Network's (FinCEN) accomplishments have included its publication of National Priorities, the first of three final rules on Beneficial Ownership, and the Notice on Trade in Antiquities and Art.<sup>33</sup> However, the agency continues its efforts to meet AMLA commitment deadlines, including proposed updates to BSA reporting thresholds and a study on effective information for law enforcement.<sup>34</sup>

Most notably, FinCEN has delayed issuing guidance on effective AML programs and the use of emerging and innovative technologies to assist in BSA compliance. Interim leadership at FinCEN has indicated that the advance notice of proposed rulemaking (ANPR) related to these areas is in the works.<sup>35</sup> The AML Program effectiveness proposed regulation amendment was initially published in September 2020 and given that it is now more than two years after the close of the comment period, we expect to see progress in 2023.<sup>36</sup>

On September 29, 2022, FinCEN issued a Final Rule implementing the Beneficial Ownership Information (BOI) requirements of 2020's Corporate Transparency Act (CTA) legislation.<sup>37</sup> The BOI reporting requirements go into effect on January 1, 2024, and are considered some of the most comprehensive changes to the anti-money laundering and countering the financing of terrorism (AML/CFT) compliance framework since the USA PATRIOT Act of 2001.

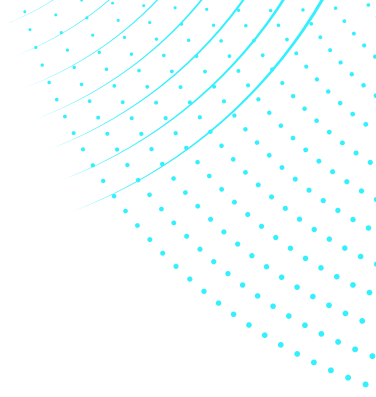
FinCEN is expected to establish protocols for access to and disclosure of beneficial ownership information and revise FinCEN's May 2018 Customer Due Diligence Rule (CDD Rule) through additional rulemakings.<sup>38</sup> The CTA does not mandate a deadline for the issuance or protocols for accessing and disclosing information, but FinCEN is required to amend the CDD Rule no later than one year after the effective date of the final version of the Proposed Rule to conform to the CTA's implementing regulations.<sup>39</sup> This leaves a potential gap of one year where banks could request beneficial ownership information from their customers who would be exempt from reporting this information under the new rule.

### Sanctions evasion requires enhanced diligence

The implementation of financial sanctions has changed drastically with the start of the Russian invasion of Ukraine. Since the inception of the war in February 2022, regulatory bodies from the United States and European Union (EU) have imposed multiple sanctions and export controls on Russia and their allies supporting this invasion attempting to influence a change in policy, impose a significant cost, and weaken Russia's military capability and its ability to continue with this war.

We do not believe that the pace of new sanctions will be slow moving. As each round of sanctions is imposed, Russia continues to identify methods to circumvent them, resulting in a tug-of-war between Russia and the jurisdictions imposing sanctions. Most recently, the US Department of the Treasury has identified Russian entities attempting to dodge sanctions using cryptocurrency.<sup>40</sup> Additionally, Russia may leverage front companies formed outside of Russia and utilize fraudulent end-user licenses to import sanctioned goods.<sup>41</sup> Institutions must ensure their capabilities to update sanctions screening filters and know-your-customer (KYC) information are designed to keep pace with the frequency of new sanctions issuances.

Banks and nonbanks should remain diligent and proactive in identifying direct or indirect techniques related to sanctions evasion. Institutions should also continue to train their compliance staff in identifying and escalating potential circumvention, monitor for new sanctions, and be rigorous in updating their procedures and processes and closing any potential program gaps.



## Digital assets remain an enforcement focus

As digital assets continue their push toward the mainstream, we are seeing increased enforcement actions in that area, and we expect to continue to see this trend throughout 2023. Regulators are looking for prudent risk management of digital assets and their AML risks, particularly the scaling of resources, technology, governance, sanctions screening process, related transaction monitoring identification, investigation, and reporting.

Institutions are methodically assessing opportunities, including custody and payments products and services, banking digital-asset exchanges, and supporting commercial clients as well as other crypto-related areas. Banks are currently walking a fine line between meeting their compliance obligations under AML/CFT requirements and respecting the wishes of consumers who are attracted to digital assets for their privacy and simplicity features. As much as institutions may want to prioritize the customer experience, it's critical to remember that while there is a need for clarity of AML expectations for digital-assets firms and specific rules may not be in place, current AML/CFT requirements still extend to digital-assets products and services.

When focusing on **BSA/AML and sanctions**, banks should consider several actions:

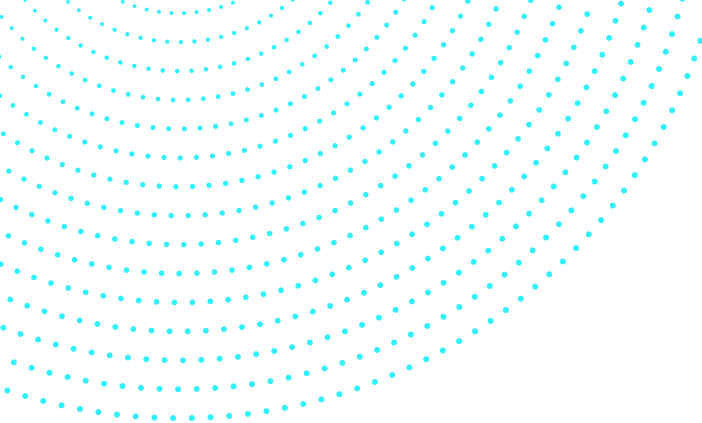
- **Don't wait for FinCEN** to consider what "effectiveness" in AML/CFT compliance means for your institution; develop metrics accordingly.
- **Consider the staffing and procedural implications of a final rule requiring BOI** for legal entities.
- **Update sanctions screening filters and KYC information** in place to keep up with the pace of new sanctions.
- **Continually assess third-party risk** and put appropriate safeguards in place.
- **Develop a strategy** to meet compliance obligations for new digital products.

## Consumer protection and financial inclusion

We expect regulators' continued enforcement momentum in protecting against consumer harm under current agency leadership in 2023, especially at the margins of the "regulatory perimeter." This continuing pressure means that the legal arrangements and cultural differences and potential governance gaps between banks and nonbanks need to be clearly understood and addressed by all stakeholders to ensure effective compliance.

The tone at the top of all the federal banking agencies increasingly suggests an enhanced focus on consumer harm, and heightened levels of scrutiny are evident. The CFPB is expected to maintain its proactive stance on a range of consumer protection issues, as prudential banking regulators work in tandem to address the root cause of core risk management breakdowns that may lead to consumer protection shortfalls. Several of the CFPB's actions have drawn strong negative reactions from the financial services industry for the interpretations and the processes followed by the agency in adopting the rule or guidance in question. The reactions have included litigation brought by a broad range of industry trade groups seeking to invalidate at least one significant CFPB action.<sup>42</sup>

In addition, a 2022 Federal Fifth Circuit Court of Appeals decision, finding the CFPB's funding mechanism to be unconstitutional, introduces a wild card with potentially far-reaching implications.<sup>43</sup> That decision could have a material impact on the agency's ability to take enforcement actions going forward. It appears that the final resolution of this question will await an ultimate appeal to the Supreme Court and its decision (which, unlike the Fifth Circuit decision, would be national in its impact). The divided results from the midterm elections, together with divided views in Congress regarding the CFPB and its mission, means that any congressional action to address this issue will remain challenging.



We anticipate movement on the following regulatory initiatives during 2023:

### **Expanded unfairness definition strengthens principle of fair banking**

The application of unfair, deceptive, or abusive acts and practices (UDAAP) for discrimination, purportedly beyond what is covered by the Equal Credit Opportunity Act (ECOA), is currently being contested in litigation.<sup>44</sup> While the outcome of that action could limit the citation of an unfairness violation, vigilance to ensure fair treatment of customers remains a core tenet of banking services.

### **Open banking around the corner**

The Advanced Notice of Proposed Rulemaking to implement requirements of Section 1033 of the Dodd-Frank Act (DFA) is a key initiative for achieving increased competition and consumer choice throughout the banking industry.<sup>45</sup> The final rule promoting data access standards will be released for comment, with final issuance targeted for 2023. Adoption of this rule will likely have a material impact on the business models of all banking service providers with downstream implications in areas such as security, privacy, and innovation.

### **Fraud in peer-to-peer (P2P) payments**

The CFPB has communicated concerns about fraud in using P2P payments. The agency is particularly focused on whether entities are following through with protections provided by existing regulations, and whether current practices are meeting the spirit of these rules. Additional guidance is expected to be issued on this topic.<sup>46</sup>

### **Buy now, pay later (BNPL) UDAAP exposure**

The BNPL industry has been closely evaluated by CFPB with findings from the agency's 2021 information request published in a recent report.<sup>47</sup> The report highlights concerns that protections afforded under [Regulation Z](#) (Truth in Lending) and [Regulation E](#) (Electric

Fund Transfers) are not afforded to consumers due to the structure of BNPL transactions. The CFPB is expected to issue an interpretation that addresses the potential gaps in protection. In addition, examinations and investigations will likely apply UDAAP with the requirement in Regulations Z and E serving as the basis for meeting the UDAAP elements.<sup>48</sup>

### **Cryptocurrency and the impact on consumers**

Growing consumer engagement with cryptocurrency companies and investment in crypto-assets have prompted similar increases in related consumer complaints collected by the CFPB, most of which were received within the past two years.<sup>49</sup> The CFPB's analysis of crypto-related consumer complaints covered a range of issues and shortfalls that present measurable challenges in and detract from the reputation of the crypto-asset markets. The federal banking regulatory agencies recognized the potential adverse impacts that crypto-related activities may have on consumers in a 2021 joint statement regarding a crypto-asset policy sprint initiative and, at that time, committed to providing "coordinated and timely clarity" around these matters.<sup>50</sup> The FDIC's issuance of resources reiterating deposit insurance applicability and coverages and providing guidance on compliance with the Federal Deposit Insurance Act is one example of a regulatory action taken to provide the necessary clarity.<sup>51</sup>

We expect to see more consumer-focused rules and guidance as Congress and the federal banking regulators address the need for an overall supervisory and regulatory cryptocurrency framework. In the interim, the federal banking regulators have used their enforcement authority to seek corrective action, where needed. For example, the FDIC issued several informal enforcement letters against cryptocurrency companies, and the CFPB issued a Civil Investigative Demand involving a cryptocurrency company.<sup>52</sup> These actions signify the agencies' readiness to use their existing toolkits when addressing crypto-related consumer matters in the coming year.



## Section 1071 to change small business lending compliance

The small business loan data collection rule is expected to be released early in 2023.<sup>53</sup> The proposed rule includes adding a new subpart (subpart B) to the CFPB's Regulation B to implement Section 1071's requirements. The proposed rule requires "covered financial institutions" that engage in small business lending to collect and report data on loan applications, creating a comprehensive database of small business credit applications and allowing regulators to identify and address fair lending concerns related to small businesses.<sup>54</sup>

If the requirements in the proposed rule remain, as we expect they will, there will be organizational changes required across people, processes, and technology. This proposed rule introduces a substantial shift in how both banks and nonbanking institutions, including fintech companies, manage small business lending across the entire life cycle. In advance of the rule change, banks should establish the proper data capabilities and technology, integrate within fair and responsible bank management programs, and coordinate oversight across the three lines.

## Interagency Community Reinvestment Act (CRA) rule to reflect banking advances

This rule is expected to be finalized on an interagency basis in early 2023 and will result in material changes to the information considered in the evaluation based on an entity's size and how that information is assessed.<sup>55</sup> The proposed change in the CRA regulation recognizes the reduction of geographic banking boundaries and accelerates the use of digital banking with mobile applications.<sup>56</sup> These developments will likely yield more appropriate CRA assessments for financial institutions and better evaluation outcomes as the activities align with the true service area. One other particularly notable change is the addition of a "Retail Services and Products Test" category, which will require data-gathering capabilities that may not currently exist within an institution.

When focusing on **consumer protection and financial inclusion**, banks should consider several actions:

- **Assess data collection, aggregation, reporting, and analytics capabilities** to meet new CRA, 1071, and 1033 requirements and increasing expectations in other areas.
- **Review the TPRM oversight program** and ensure there is awareness of the consumer compliance risks and requirements. Evaluate legal agreements and risk oversight with respect to nonbanks, and document the impacts these arrangements have on the bank's risks, controls, and other processes.
- **Ensure change management programs are functioning effectively** and reach beyond new product offerings to include material operational changes regardless of the cause.
- **Perform fair lending assessments for potential discrimination** beyond lending activities under the tenets of unfairness.
- **Assess model algorithms for underwriting and appraisals** for unintended discriminatory outcomes.
- **Evaluate consumer complaint analytics capabilities** to ensure adequate identification of emerging issues.
- **Determine the pervasiveness of adverse consumer impacts** when compliance concerns are detected, and fully remediate the harm.







# Expanding the scope of financial risk management

The banking system closed out 2022 in overall sound condition, with sufficient capital and liquidity levels generally noted across individual banks and BHCs. The ability of existing risk management processes to capture risks resulting from external factors will be a focal point for regulators in 2023. Specifically, the potential impact of changing fiscal and economic conditions on banks' capital and liquidity positions will need additional consideration in stress testing and other risk management measures. To the extent that geopolitical events may have an adverse impact (direct or indirect) on bank financial results, those risks will also need to be accounted for. Risk management practices related to climate-related financial risk should be materializing in anticipation of banking regulators' finalized guidance, adding yet another layer to financial risk management for banks.

## Capital

Capital planning uncertainty will continue in 2023 as new risks emerge, including the impacts of inflation and rising interest rates, that have not been experienced since the early 1980s. New capital requirements are anticipated, in conjunction with the US finalization and implementation of the Basel III international regulatory standards, as well as the potential pushdown of large bank total loss absorbing capital (TLAC) requirements on the largest regional banks, that may further constrain the size and types of assets held by banks.

Capital planning models and underlying assumptions should be nimble to predict financial performance, growth, and level of capital distributions. With increasing variability of outcomes, even the most mature capital planning models and processes will be challenged to maintain accurate forecasts. Banking agencies will endeavor, through policy, oversight, and stress testing, to ensure the levels of capital in the banking system are sufficient to absorb losses. Stress testing will continue to evolve to use more dynamic scenarios as new risks emerge.

The coming year will likely bring more direction to the agencies' capital-related priorities. Supervisory priorities for 2023 include financial stability, managing interest rate risk, and strategic and operational planning.

## Basel III endgame impact

The Basel Committee on Banking Supervision (BCBS) recommended Enhanced Basel III rules (popularly referred to as "Basel III endgame") to be effective starting in January 2023. US regulators have indicated the effective date for implementing these capital rules will be extended to January 2025 for US banks, consistent with the timing for banks in the European Union.<sup>57</sup> The US regulators' proposed rule is expected to be published in early 2023.<sup>58</sup>

Updates to the new framework include adjusting the supplementary leverage ratio, countercyclical capital buffer, and stress testing and are expected to strengthen financial stability and resilience.<sup>59</sup> The proposed revisions are also expected to align with prior Basel III implementation decisions in the United States (e.g., no reliance on external ratings for risk weights) and are meant to increase simplicity, risk sensitivity, and comparability of regulatory capital across banks.

The complexity of revisions to the market risk regulatory framework, including the Fundamental Review of the Trading Book (FRTB) rule, will require substantial efforts to comply with the new requirements. This includes significant modeling efforts, the need for sourcing additional data attributes from internal and external sources, and implementing operational processes to support the new data requirements.

Regulatory capital requirements, either existing or new, require that banking organizations maintain rigor around governance and controls over new operational processes, regulatory capital interpretations, data quality, and testing.



## Asset growth and regulatory implications for regional banks

Regulatory oversight of large banks remains a priority as they continue to increase in size and complexity, through both recent organic growth and merger activity. As banks (often “regional”) cross the regulatory thresholds of \$50 billion and \$100 billion, regulatory requirements increase. These banking organizations will experience the supervisory effect across capital planning, liquidity risk management, stress testing, regulatory reporting, enterprisewide risk management, and enhanced governance. In response banking organizations increasing in size and complexity need to ensure that the required capabilities, processes, and technology infrastructure are appropriately supported across all products and legal entities.

Regulators are also focused on containing the systemic effect should a large bank that is not designated as a G-SIB with a high level of deposits fail. This has led regulators to issue an ANPR, imposing TLAC for large banks that are not already G-SIBs. The ANPR would require these banks to hold minimum levels of eligible long-term debt at the holding company level, similar to existing requirements for larger and more complex G-SIBs.<sup>60</sup> If adopted, there is the possibility that conditions—addressing resolvability and similar matters, including TLAC—will be added to large bank merger approvals, especially with the Bank Merger Act subject to revision.<sup>61</sup>

When focusing on **capital**, banks should consider several actions:

- **Develop detailed plans** to understand the impact of capital changes on levels and how it is measured (or revisit existing plans where necessary).
- **Confirm resources and skill sets** in capital processes, and assess that modeling resources allow for stress testing and loss forecasting in rapidly changing economic scenarios.
- **Maintain and enhance rigor** around governance and risk management, regulatory capital interpretations, and data quality over capital and forecasting processes.
- **Enhance risk processes** as growth occurs, especially when crossing thresholds, to demonstrate control over risk management as size and complexity increase.

## Liquidity

Consumers and businesses parked cash in depository institutions throughout the pandemic at unprecedented levels. From the end of 2019 to the beginning of 2022, deposits at domestic commercial banks rose by more than 35%.<sup>62</sup> This trend, along with the stimulative effects of FRB asset purchases and other programs, led to a substantial increase in banks’ total assets and liabilities.

The increase in deposit funding and the reduction of the FRB’s balance sheet are key factors for regulators reviewing Internal Liquidity Stress Tests (ILST) in 2023. ILST requirements are intended to help firms determine adequate levels of liquidity to maintain in the event of idiosyncratic and/or market-wide stress. Scenarios and assumptions, unique to each institution, are based on several factors and incorporated to provide a more realistic view of how the institution expects its operations to function in times of stress.

As regulators evaluate the effects of the pandemic and the rising interest rate environment, they are examining the components of ILST and the scenarios and assumptions used by institutions in their ILST models. Regulators are looking for institutions to provide more robust scenarios that include historical events and produce a forward-looking assessment of the institution's risks. With most liquidity processes designed to handle more predictable economic cycles, regulators may require more dynamic scenarios to cover emerging risks. Additionally, there is more scrutiny being placed on assumptions to ensure they are based on sound data and tailored more to the institution's liquidity risk profile.

In 2022, the FRB expanded liquidity reporting on the *Complex institution liquidity monitoring* report (FR 2052a/6G) to incorporate data needed to calculate the Net Stable Funding Ratio and present a balance sheet view of this data. The 6G is a complex set of data requirements that requires firms to do a good deal of interpretative analysis to meet the requirements. In 2023, we believe the FRB will likely provide firms clarity on reporting issues and feedback on the new data requirements.

When focusing on **liquidity**, banks should consider several actions:

- **Refresh ILST scenarios and assumptions** given significant changes in the macroeconomic and interest rate environment.
- **Examine deposit management practices** to ensure proper oversight of risk, that there are adequate analytics to segment client concentrations and documentation to describe capabilities to support potential inquiry from regulators.
- **Test the resiliency of the recent 6G 2052a implementation** ahead of horizontal reviews to ensure the sustainability of updates and the accuracy of data.

## Climate-related financial risk

Domestic and international supervisors have reached a consensus around the need to manage climate-related financial risk given the potential for unmanaged risk to have an adverse and possibly disparate impact on the local and global financial systems. Related proposed guidance and recommendations are outstanding at the OCC, FDIC, and more recently the FRB. The US federal banking regulators have solidified their perspectives on the importance of climate-related financial risk management in the banking sector and intend to issue interagency principles for large banks in 2023.

Banks will also need to align risk management programs and practices with expectations set forth by the BCBS,<sup>63</sup> FSB,<sup>64</sup> Task Force on Climate-related Financial Disclosures (TCFD),<sup>65</sup> Network for Greening the Financial System (NGFS),<sup>66</sup> the proposed and eventual final federal bank regulatory guidance, and state banking departments, as applicable. Cross-jurisdictional coordination is likely already underway for banks with international operations, as international regulators are generally further ahead with the finalization of guidance and expectations. Whether domestically or internationally, banks will need to be aware of all applicable requirements and understand the extent to which inconsistencies in regulatory requirements and expectations may create operational, reporting, or other challenges.

### Scenario analysis

The distinct difference between climate-related scenario analysis and stress testing continues to be a focal point for the FRB. The FRB took a significant step last year with its commitment to leading a piloted climate-related scenario analysis in 2023. The FRB's pilot will involve a subset of systemically important banks.<sup>67</sup> No firm-specific information will be published, and the pilot will have no capital or supervisory implications.<sup>68</sup> The pilot may inform future interagency guidance or be considered a steppingstone toward the development of a climate-related financial risk scenario analysis framework.

The publication of the scenarios used in the analysis and key insights of the analysis should help inform a broader portion of the banking population, possibly assisting with their preparedness for like analysis in the future. This will be important given that large banks more broadly will need to incorporate internal scenario analysis into their risk management frameworks as outlined in applicable draft guidance.

The FSB and NGFS have preliminarily assessed global macroprudential and microprudential scenario analysis exercises at varying stages of completion in 36 countries, including the United States.<sup>69</sup> The joint FSB and NGFS report reflects differences in approaches, modeling, and scenario development having a limiting effect on comparability between analyses. While the FSB and NGFS have gained insight into the nature of existing vulnerabilities, the report communicates a common view that “exposures and vulnerabilities” may be underestimated.<sup>70</sup> Data scenario analyses will likely require time for maturation prior to reliance on results for policy development purposes.

### Being data-driven

In conjunction with the application of disclosure requirements and key metrics associated with climate-related financial risk, banks are tasked with the collection and maintenance of new or enhanced data. Challenges with climate-related data include determining appropriate data sources that are well defined. Once the sourcing is determined, banks will need to establish that the processes, governance, and controls are in place to onboard the necessary data and ensure the quality of data can be achieved through end-to-end processes.

When focusing on **climate-related financial risk**, banks should consider several actions:

- **Assess the requirements outlined in all applicable guidance** (final and proposed) to understand where the requirements exceed those of existing risk management practices or require new policies, procedures, and limits.
- **Understand any inconsistencies between requirements** across regulators with supervisory oversight responsibilities and account for the totality of expectations in operations.
- **Review existing scenario analysis frameworks** for consistency with proposed principles, and refer to international lessons learned for opportunities to improve current approaches.
- **Develop an approach to data acquisition, maintenance, and reporting** for use in scenario analysis and other data-driven risk management activities.





# Looking forward to an active 2023

In 2023, marketplace developments will continue to pressure Congress and regulators to better define who is within the federal bank regulatory perimeter and the supervisory regimes these insiders (banks and nonbanks) will face. To the extent that there are newly included business types within the regulatory perimeter, either Congress or regulators will need to assign supervisory authority and delineate oversight requirements. There are still unknowns in terms of frameworks and authorities that the regulators will need to address for banks to engage in an expanded range of activities. It is unclear if the pace of policy decisions in this area will catch up to the speed of innovation.

Banking regulators are positioned at the forefront of the ongoing transformation in the banking sector and, in many cases, have vocalized their priorities and concerns. With capital at the top of the interagency policy agenda and the FRB's large bank framework—including elements of the supervisory stress testing regime—the agency is leaning toward periodic review of capital policy and the development of flexible policies that are adjusted to satisfy the changing needs of the banking sector. The OCC and FDIC are similarly focused on capital from an examination standpoint and as a policy initiative tied to the finalization and implementation of the Basel III capital accord in the United States.

Measuring and accounting for systemic risk and matters of resolvability in non-G-SIBs are items that the regulators will likely tackle in the year ahead. We could see additional capital considerations and requirements become applicable to the largest of the non-G-SIBs this year, and these requirements may have an impact on how these firms are treated from a merger and acquisition perspective. The realization that the presence of significant systemic risk has trickled down into large banks is a regulatory turning point, and banks will need to watch for regulatory movement in this area.

The swift pace of change in the current banking environment has introduced new consumer protection concerns and reiterated the importance of existing ones in the eyes of federal banking regulators. The CFPB has made considerable headway with both bank and nonbank supervisory activities, consistent with CFPB Director Chopra's aggressive approach to consumer protection regulation. The application of a dormant supervisory authority to examine nonbanks beyond those identified by statute or regulation was a strategic move that confirmed the continuation of regulatory intensity going forward. The CFPB has been known for using its supervisory and enforcement resources to probe industries and activities that may pose consumer harm and to hold them accountable, when warranted. It is expected that the agency will continue to proactively pursue policy as well as supervisory initiatives in light of innovation concerning consumer-facing financial products and services.

Regulators are planning to take a more aggressive approach to risk management supervision with a sharp focus on outstanding supervisory issues. The need for banks to work toward remediation of supervisory findings and sustainability of remediation efforts will be paramount to avoid escalation of supervisory matters. The process of cleaning up the basics will help banks to get ahead and stay off the path of adverse supervisory actions. Banks will need to tune in to what regulatory leadership is saying and how that translates into what examiners on the ground are doing.

Forthcoming regulation will need to reflect a fresh take on banking, one which accounts for changes in bank size and activity over time and recognizes risks associated with aspects of climate-related financial risk, technology, bank-nonbank partnerships, and even the entrance into new business lines, such as digital assets.

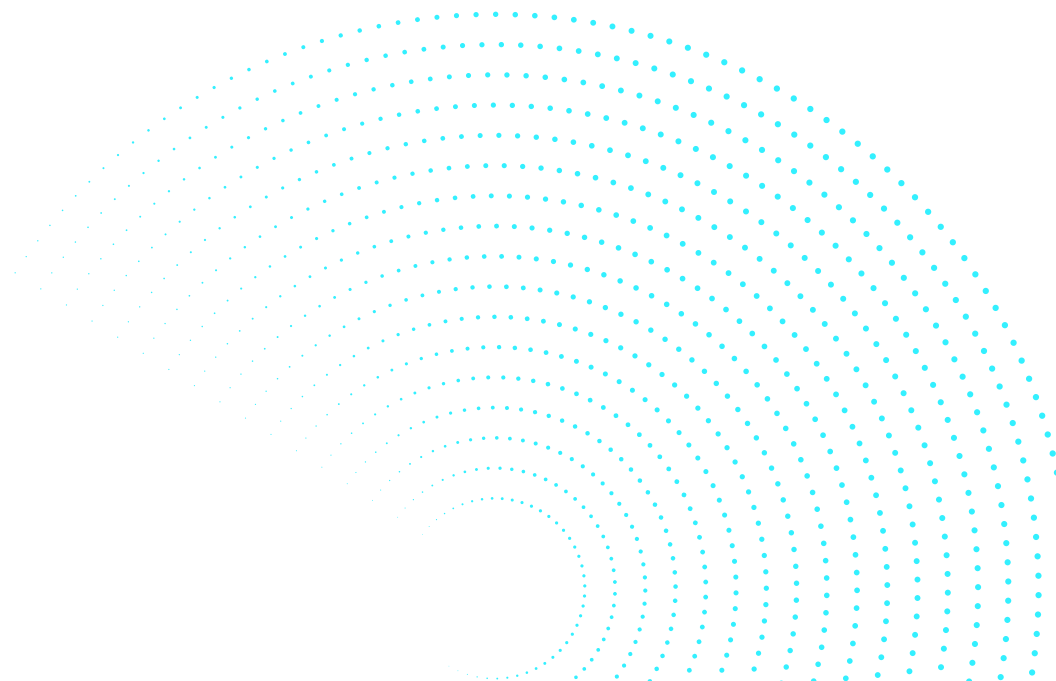
# Endnotes

1. Board of Governors of the Federal Reserve System (FRB), "[Supervision and regulation report](#)," November 10, 2022; Office of the Comptroller of the Currency (OCC), "[OCC reports on key risks facing federal banking system](#)," news release, December 8, 2022.
2. OCC, "[Acting Comptroller of the Currency Michael J. Hsu Remarks before the Wharton Financial Regulation Conference 2022 on Financial Stability and Large Bank Resolvability](#)," April 1, 2022.
3. Deloitte, "[Playing catch-up: The FDIC takes first steps to modernize the Bank Merger Act](#)," accessed January 9, 2022.
4. Financial Stability Oversight Council (FSOC), "[Financial Stability Oversight Council annual report 2022](#)," December 16, 2022.
5. Financial Stability Board (FSB), "[Assessment of risks to financial stability from crypto-assets](#)," February 16, 2022.
6. FSOC, "[Financial Stability Oversight Council releases report on digital asset financial stability risks and regulation](#)," press release, October 3, 2022.
7. FRB, "[Supervision and regulation report](#)."
8. OCC, "[OCC releases bank supervision operating plan for fiscal year 2023](#)," news release, October 6, 2022."
9. OCC, "[OCC reports on key risks facing federal banking system](#)," news release, December 8, 2022."
10. FRB, "[Agencies issue joint statement on crypto-asset risks to banking organizations](#)," joint press release, January 3, 2022.
11. Deloitte, "[Banking regulators reinforce wall for bank involvement in crypto-assets](#)," 2022.
12. David G.W. Birch, "[ChatGPT is a window into the real future of financial services](#)," Forbes, December 8, 2022.
13. Monica O'Reilly et al., "[2023 banking and capital markets industry outlook](#)," 2022.
14. FRB, "[Agencies issue joint statement on crypto-asset risks to banking organizations](#)."
15. Deloitte, "[Cryptocurrency notification protocols and readiness](#)," April 11, 2022.
16. Federal Deposit Insurance Corporation (FDIC), "[FIL-16-2022: Notification of engaging in crypto-related activities](#)," press release, April 7, 2022; FRB, "[SR 22-6 / CA 22-6: Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organizations](#)," August 16, 2022.
17. FSOC, "[Financial Stability Oversight Council releases report on digital asset financial stability risks and regulation](#)."
18. Securities and Exchange Commission (SEC), "[Staff Accounting Bulletin No. 121](#)," April 11, 2022.
19. Deloitte, "[Navigating the crypto regulatory landscape](#)," accessed January 5, 2023.
20. European Parliament, "[Markets in crypto-assets \(MiCA\)](#)," November 29, 2022.
21. FRB, "[Supervision and regulation report](#)."
22. FRB, "[SR 19-3 / CA 19-2: Large Financial Institution \(LFI\) Rating System](#)," February 26, 2019; FRB, "[Supervision and regulation report](#)."
23. FRB, "[SR 19-3 / CA 19-2: Large Financial Institution \(LFI\) Rating System](#)."
24. The White House, "[Executive Order on Improving the Nation's Cybersecurity](#)," May 12, 2021.
25. New York State Department of Financial Services (NYDFS), "[Guidance on multi-factor authentication](#)," December 7, 2021.
26. FRB, "[Agencies request comment on proposed risk management guidance for third-party relationships](#)," joint press release, July 13, 2021.
27. Cybersecurity and Infrastructure Security Agency (CISA), "[Cyber Incident Reporting for Critical Infrastructure Act of 2022 \(CIRCA\)](#)," accessed July 28, 2022.
28. FRB "[SR 22-4 / CA 22-3: Contact Information in Relation to Computer-Security Incident Notification Requirements](#)," March 29, 2022.
29. FSB, "[FSB makes proposals to achieve greater convergence in cyber incident reporting](#)," press release, October 17, 2022.

30. OCC, "[OCC reports on key risks facing federal banking system.](#)"
31. OCC, "[Agencies request comment on proposed risk management guidance for third-party relationships.](#)" news release, July 13, 2021.
32. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, [H.R. 6395](#), 116th Cong. (2019–2020).
33. Financial Crimes Enforcement Network (FinCEN), "[FinCEN Notice on Antiquities and Art \(FIN-2021-NTC2\)](#)," March 9, 2021.
34. FinCEN, "[Prepared Remarks of FinCEN Acting Director Himamauli Das during the ABA/ABA Financial Crimes Enforcement Conference](#)," December 6, 2022.
35. FinCEN, "[Prepared Remarks of FinCEN Acting Director Himamauli Das during the ACAMS AML Conference](#)," October 12, 2022.
36. FinCEN, "[Anti-Money Laundering Program Effectiveness](#)," September 17, 2020.
37. FinCEN, "[FinCEN issues final rule for beneficial ownership reporting to support law enforcement efforts, counter illicit finance, and increase transparency.](#)" press release, September 29, 2022.
38. FinCEN, "[Beneficial ownership information reporting rule fact sheet](#)," September 29, 2022.
39. Ibid.
40. FinCEN, "[FinCEN and BIS issue joint alert on potential Russian and Belarusian export control evasion attempts](#)," June 28, 2022.
41. US Department of the Treasury, "[Treasury-Commerce-State Alert: Impact of Sanctions and Export Controls on Russia's Military-Industrial Complex](#)," October 14, 2022.
42. Bloomberg Law, "[Chamber of Commerce of the United States of America et al. v. Consumer Financial Protection Bureau](#)," filed September 28, 2022.
43. Jody Godoy, "[Consumer agency asks U.S. Supreme Court to review case that invalidated its funding](#)," Reuters, November 15, 2022.
44. US Chamber of Commerce, "[U.S. Chamber files coalition lawsuit challenging the Consumer Financial Protection Bureau's recent update to the Unfair, Deceptive, or Abusive Acts or Practices section of its examination manual as unlawful](#)," November 29, 2022.
45. Consumer Financial Protection Bureau (CFPB), "[Consumer Access to Financial Records](#)," October 22, 2020; CFPB, "[Director Chopra's Prepared Remarks at Money 20/20](#)," October 25, 2022.
46. CFPB, "[Electronic Fund Transfers FAQs](#)," December 12, 2021.
47. CFPB, "[CFPB study details the rapid growth of 'buy now, pay later' lending](#)," press release, September 15, 2022.
48. CFPB, "[Unfair, Deceptive, or Abusive Acts or Practices \(UDAAPs\) examination procedures](#)," March 16, 2022.
49. CFPB, "[CFPB publishes new bulletin analyzing rise in crypto-asset complaints](#)," press release, November 10, 2022.
50. OCC, "[Joint statement on crypto-asset policy sprint initiative and next steps](#)," news release, November 23, 2021.
51. Deloitte, "[The Federal Deposit Insurance Corporation \(FDIC\) heightens its enforcement of the Federal Deposit Insurance \(FDI\) Act](#)," 2022; FDIC, "[FDIC Law, Regulations, Related Acts - Federal Deposit Insurance Act](#)," last updated August 31, 2021.
52. FDIC, "[FDIC issues cease and desist letters to five companies for making crypto-related false or misleading representations about deposit insurance](#)," press release, August 19, 2022; CFPB, "[Decision and Order on Petition by Nexo Financial LLC to Modify Civil Investigative Demand](#)," November 22, 2022.
53. Deloitte, "[Impact of updates to Section 1071 on small business lending](#)," accessed December 7, 2022.
54. CFPB, "[Summary of proposed rulemaking: September 2021 proposal regarding small business lending data collection](#)," September 1, 2021.
55. OCC, "[CRA NPR infographic](#)," accessed December 7, 2022.



56. Deloitte, "[Community Reinvestment Act and Digital Banking Activities](#)," accessed December 7, 2022.
57. Deloitte, "[Implementing Basel 3.1 in the EU: Delay, defer, diverge - and more...](#)," October 28, 2021.
58. FRB, "[Agencies reaffirm commitment to Basel III standards](#)," press release, September 9, 2022.
59. FRB, "[Speech by Vice Chair for Supervision Barr on making the financial system safer and fairer](#)," September 7, 2022.
60. FRB, "[Federal Reserve Board invites public comment on an advance notice of proposed rulemaking to enhance regulators' ability to resolve large banks in an orderly way should they fail](#)," press release, October 14, 2022.
61. Deloitte, "[Playing catch-up: The FDIC takes first steps to modernize the Bank Merger Act](#)," accessed December 13, 2022.
62. Andrew Castro, Michele Cavallo, and Rebecca Zarutskie, "[Understanding bank deposit growth during the COVID-19 pandemic](#)," FRB, June 3, 2022.
63. Basel Committee on Banking Supervision (BCBS), "[Principles for the effective management and supervision of climate-related financial risks](#)," June 15, 2022.
64. FSB, "[Supervisory and regulatory approaches to climate-related risks](#)," press release, October 13, 2022.
65. Task Force on Climate-related Financial Disclosures (TCFD), "[Recommendations of the Task Force on Climate-related Financial Disclosures](#)," June 29, 2017.
66. Network for Greening the Financial System (NGFS), "[Guide for supervisors: Integrating climate-related and environmental risks into prudential supervision](#)," May 2020.
67. FRB, "[Federal Reserve Board announces that six of the nation's largest banks will participate in a pilot climate scenario analysis exercise designed to enhance the ability of supervisors and firms to measure and manage climate-related financial risks](#)," press release, September 29, 2022.
68. FRB, "[Speech by Vice Chair for Supervision Barr on making the financial system safer and fairer](#)."
69. FSB, "[Current climate scenario analysis exercises may understate climate exposures and vulnerabilities, warn FSB and NGFS](#)," press release, November 15, 2022.
70. Ibid.



# Contacts

## Richard Rosenthal

Principal | Deloitte & Touche LLP  
[rirosenthal@deloitte.com](mailto:rirosenthal@deloitte.com)

## Contributors

### Digital assets

#### Roy Ben Hur

Managing Director | Deloitte & Touche LLP  
[rbenhur@deloitte.com](mailto:rbenhur@deloitte.com)

#### Richard Mumford

Independent Senior Advisor to Deloitte & Touche LLP  
[rmumford@deloitte.com](mailto:rmumford@deloitte.com)

#### Naresh Nagia

Independent Senior Advisor to Deloitte & Touche LLP  
[nnagia@deloitte.com](mailto:nnagia@deloitte.com)

### Data governance and reporting

#### Ken Lamar

Independent Senior Advisor to Deloitte & Touche LLP  
[kelamar@deloitte.com](mailto:kelamar@deloitte.com)

### Cyber and information technology

#### Julie Bernard

Principal | Deloitte & Touche LLP  
[juliebernard@deloitte.com](mailto:juliebernard@deloitte.com)

#### Sunil Kapur

Managing Director | Deloitte & Touche LLP  
[sunilkapur@deloitte.com](mailto:sunilkapur@deloitte.com)

#### Sean Hodgkinson

Senior Manager | Deloitte & Touche LLP  
[seahodgkinson@deloitte.com](mailto:seahodgkinson@deloitte.com)

### Bank Secrecy Act, anti-money laundering, and sanctions

#### John Wagner

Managing Director | Deloitte Transactions and Business Analytics LLP  
[johnwagner@deloitte.com](mailto:johnwagner@deloitte.com)

## Scott Zucker

Senior Manager | Deloitte Transactions and Business Analytics LLP  
[szucker@deloitte.com](mailto:szucker@deloitte.com)

## Zachary Oliver

Manager | Deloitte Transactions and Business Analytics LLP  
[zoliver@deloitte.com](mailto:zoliver@deloitte.com)

## Johnny Li

Manager | Deloitte Transactions and Business Analytics LLP  
[johnnli@deloitte.com](mailto:johnnli@deloitte.com)

### Consumer protection and financial inclusion

#### John Graetz

Principal | Deloitte & Touche LLP  
[jgraetz@deloitte.com](mailto:jgraetz@deloitte.com)

#### Paul Sanford

Independent Senior Advisor to Deloitte & Touche LLP  
[pasanford@deloitte.com](mailto:pasanford@deloitte.com)

#### Chris Tucker

Senior Manager | Deloitte & Touche LLP  
[chtucker@deloitte.com](mailto:chtucker@deloitte.com)

#### Jessica Golden

Manager | Deloitte & Touche LLP  
[jegolden@deloitte.com](mailto:jegolden@deloitte.com)

### Capital

#### Courtney Davis

Principal | Deloitte & Touche LLP  
[coudavis@deloitte.com](mailto:coudavis@deloitte.com)

#### John Corston

Independent Senior Advisor to Deloitte & Touche LLP  
[jcorston@deloitte.com](mailto:jcorston@deloitte.com)

#### Krishna Blanchard

Senior Manager | Deloitte & Touche LLP  
[kblanchard@deloitte.com](mailto:kblanchard@deloitte.com)

#### Sudarshna Kalyanaraman

Manager | Deloitte & Touche LLP  
[sukalyanaraman@deloitte.com](mailto:sukalyanaraman@deloitte.com)

### Liquidity

#### Carrie Cheadle

Principal | Deloitte & Touche LLP  
[ccheadle@DELOITTE.com](mailto:ccheadle@DELOITTE.com)

#### Courtney Davis

Principal | Deloitte & Touche LLP  
[coudavis@deloitte.com](mailto:coudavis@deloitte.com)

#### Ryan McDevitt

Senior Manager | Deloitte & Touche LLP  
[rmcdevitt@deloitte.com](mailto:rmcdevitt@deloitte.com)

### Climate-related financial risk

#### Ricardo Martinez

Principal | Deloitte & Touche LLP  
[rimartinez@deloitte.com](mailto:rimartinez@deloitte.com)

#### Ken Lamar

Independent Senior Advisor to Deloitte & Touche LLP  
[kelamar@deloitte.com](mailto:kelamar@deloitte.com)

### Deloitte Center for Regulatory Strategy

#### Irena Gecas-McCarthy

Principal | Deloitte & Touche LLP  
[igecasmccarthy@deloitte.com](mailto:igecasmccarthy@deloitte.com)

#### Jim Eckenrode

Managing Director | Deloitte Services LP  
[jeckenrode@deloitte.com](mailto:jeckenrode@deloitte.com)

#### Michele Jones

Research Leader | Deloitte Services LP  
[michelejones@deloitte.com](mailto:michelejones@deloitte.com)

#### Meghan Burns

Research Manager | Deloitte Services LP  
[megburns@deloitte.com](mailto:megburns@deloitte.com)

#### Kyle Cooke

Sr. Strategy & Operations Specialist | Deloitte Services LP  
[kycooke@deloitte.com](mailto:kycooke@deloitte.com)

## CENTER *for* REGULATORY STRATEGY AMERICAS

### **About the Center**

The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services industry 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.

# Deloitte.

### **About Deloitte**

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication 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 advisor.

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

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2023 Deloitte Development LLC. All rights reserved.