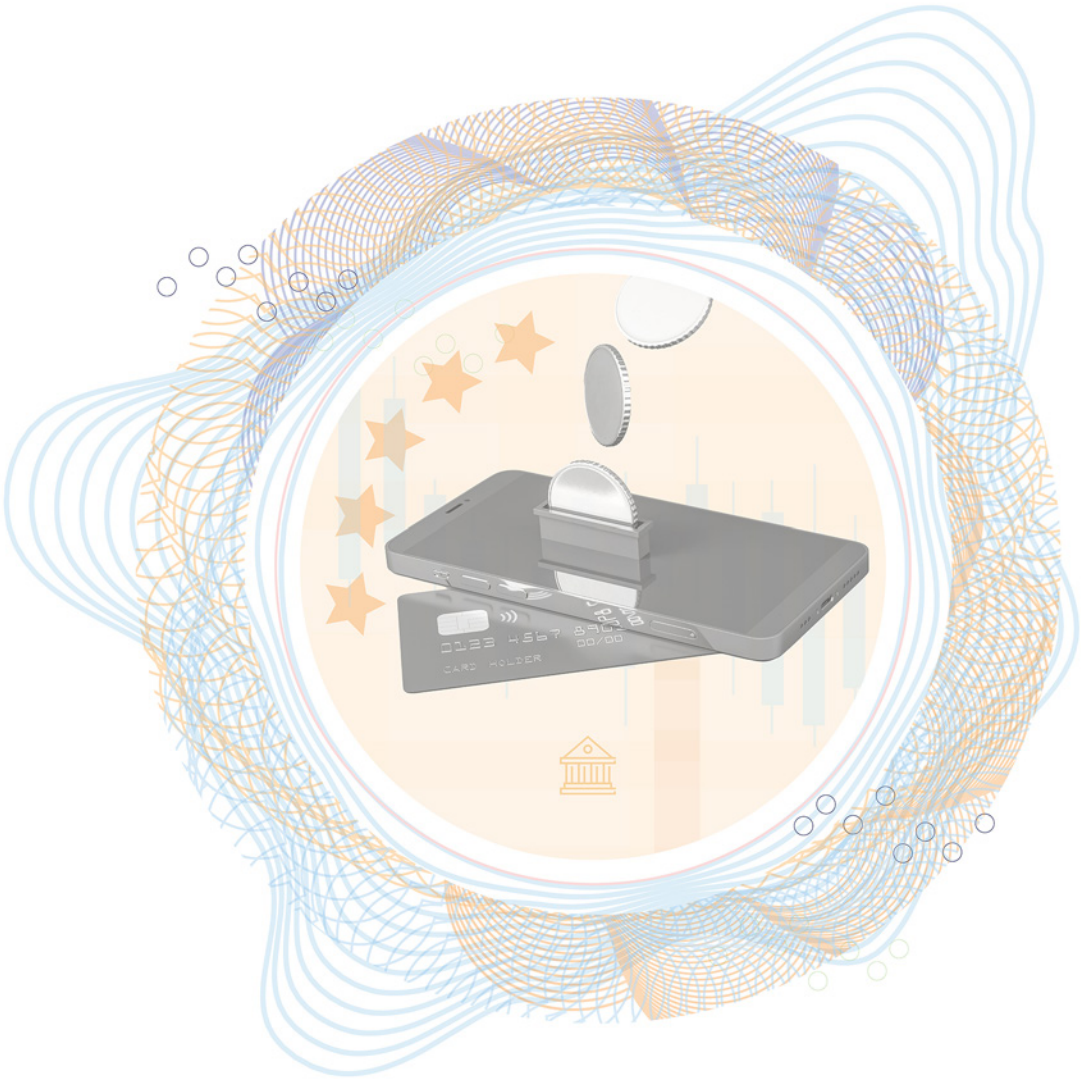
Deloitte.



2022 banking regulatory outlook

Evolution or revolution of banking: How will US regulators respond?

CENTER *for*
REGULATORY
STRATEGY
AMERICAS

Contents

Introduction

After a tumultuous 2020, the next "normal" emerged in 2021 for the economy and the banking business. In the United States, much of the non-client-facing workforce continued to work virtually or through a hybrid model; consumers and businesses alike further embraced virtual online relationships for banking and facilitating financial transactions with a variety of institutions (including banks, securities firms, and non-bank financial services providers); and crypto assets gained broader acceptance and grew at a rapid pace.[1]

The nature of the banking business—and people's understanding of what banking is—continued to evolve in ways that challenge both established industry players (e.g., traditional banks) and new competitors (e.g., fintech companies, crypto-asset companies, and non-banks), as well as US and global regulators' reactions to these trends and their ability to advance their supervisory and regulatory approaches.

The current state of leadership flux at most US federal banking agencies—including the presence of an Acting Comptroller of the Currency; the resignation of two Federal Reserve Governors (Vice Chair for Supervision and Vice Chair) along with the nomination of three others; and the resignation of the Federal Deposit Insurance Corporation (FDIC) Chair following an unprecedented and public FDIC Board struggle—has the potential to make 2022 a particularly challenging year.[2] With many important policy and supervisory matters on the regulatory agenda, key positions at the Federal Reserve Board of Governors (FRB), Office of the Comptroller of the Currency (OCC), and FDIC remain open, making consistent perspectives across agencies less likely and potentially impeding momentum on regulation, supervisory guidance, and approaches for several emerging risk issues and engagement in international forums.

Even if lead federal bank regulatory agency positions are filled early in 2022, it will take time for the agencies to solidify their regulatory and supervisory policy agendas, establish their views, initiate coordination with other agencies, and take meaningful action on both an individual and interagency basis. Also, approved permanent appointments, such as the Director of the Consumer Finance Protection Bureau (CFPB), will change the approach of their predecessors—making it increasingly difficult for agency staff and firms alike to plan for the future.[3] Recent and forthcoming regulatory appointees might have the ability to shift regulatory agendas and perspectives or delay regulatory decision-making. In addition, the continuation of the pandemic's impact into 2022 presents an additional layer of unpredictability, creating a distraction that could add to the slowdown of regulatory actions. As such, the forward-looking impressions in this outlook are presented in the context of a regulatory landscape characterized by uncertainty across four major trends that are noted below:

- **Regulatory perimeter**—Evolution or revolution?
- **Foundational areas**—Back to basics and strengthening core capabilities
- **Accelerating demand**—better enabling infrastructure across data, IT, and their resiliency
- **Emerging risks becoming part of the core**—Digital assets, climate

Regulatory perimeter—Evolution or revolution?

The notion of "banking" being a verb, rather than a noun, is not new or revolutionary. Over the past several decades, numerous business models have arisen and have continued to evolve one step at a time.

For example, many US securities firms have been offering cash management accounts since the 1980s, providing their customers with cash sweeps to money market funds or FDIC-insured bank accounts, check and debit card access, Fedwire and Automated Clearing House (ACH) payment capabilities, and various forms of credit (through affiliated banks and non-banks, as well as unaffiliated third parties), all without being classified as banks.

More recently, the continuing emergence of fintech companies, often partnering with banks under "banking-as-a-service" (BaaS) frameworks to offer a variety of banking services, is consistent with this trend and as such is more evolutionary than revolutionary.

Many elements of the crypto ecosystem and decentralized finance (DeFi) are expected to be truly revolutionary, enabling instant payment and settlement activity that challenges traditional intermediaries. The novelty, rapid growth, and adoption of crypto assets are raising questions about the regulatory perimeter (i.e., the set of regulatory requirements with which entities engaged in US banking activities must comply).[4] More broadly, top-of-mind questions for regulators include whether certain crypto asset–related activities should be limited to banks with FDIC insurance or entities that are subject to comprehensive and consolidated federal bank regulatory supervision.[5]

Building a foundation for the future

Whether the changes in banking are evolutionary or revolutionary, traditional banks, fintech companies, non-bank lenders, non-bank payment companies, crypto asset companies, and US federal and state regulators are all looking closely at the opportunities and risks in the current and future marketplace.

We view 2022 as a time for banks (and non-banks with banking activities) to level up and ensure their core and foundational capabilities are strong. These capabilities include governance, risk management practices and controls, capital adequacy and planning, liquidity management, and compliance with laws and regulations—both internally and in their external ecosystem of partners and third-party service providers. We also view 2022 as a time for non-banks to step up to the challenge of establishing more bank-like governance and risk management standards.

Now more than ever, all entities that are inside and near the banking regulatory perimeter will need a strategic view of how the regulatory landscape will develop that is fully integrated with its business strategy, corporate governance, and organizational structure, products and services, and geographies. Such a strategy typically includes the selection of an appropriate legal entity structure, license, and thoughtful approach to what third-party relationships should be in place. All of this is underpinned by governance, risk management, and controls.

Central to this is understanding what you want to be and where you want to play. This will be a central theme as regulators pressure organizations on whether they have the capabilities and strategy to support the products they are engaging with. Whether you are a traditional bank, a non-bank performing banking activities, or a third-party service provider, you should expect attention from banking regulators going forward.

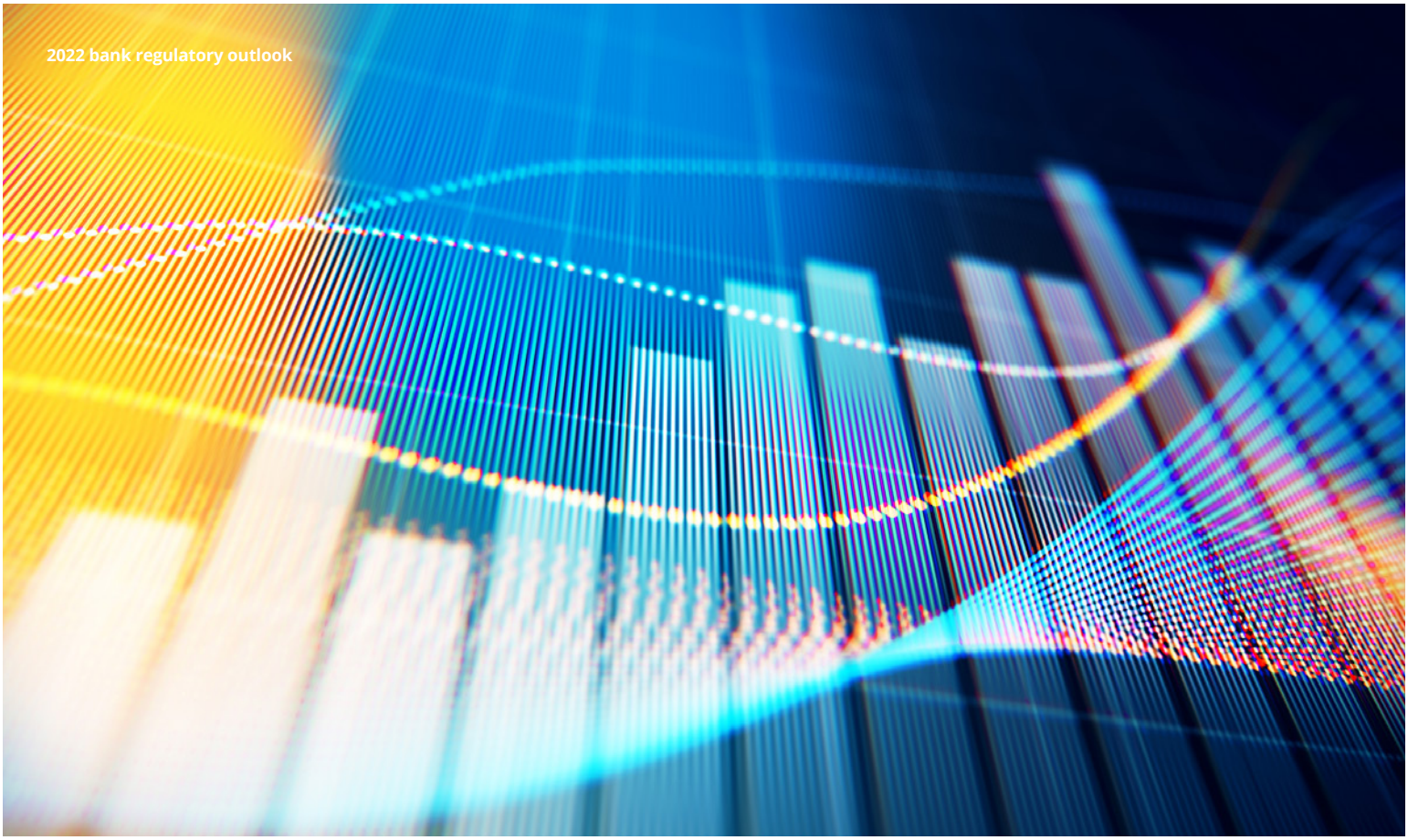
A solid foundation can position an organization for regulatory compliance and potentially deliver competitive advantages, helping to ensure the necessary licenses, people, processes, and capabilities are in place to successfully engage and win in the marketplace (with the appropriate foundation to navigate and adhere to emerging regulatory changes and requirements). Some of the deliberate actions that can be taken include the following:

Form an agile central design group that drives proactive analysis and evaluation of shifting and diverging regulatory impacts on business strategy and profitability, then proposes potential responses, both globally and for key regions.

Double down on global governance, risk management, and controls capabilities that address variations in standards and expectations at the regional, business, and legal entity levels while retaining the ability to measure and aggregate risk and performance at the global level.

Establish advanced analytic capabilities to detect and prevent regulatory noncompliance before significant issues emerge (e.g., understand the impact of technology integration across regulatory requirements and controls between the first and second lines and across functions; enhance capabilities across the regulatory change life cycle in transparent ways that are linked to a holistic, end-to-end compliance framework).

Invest in technology and data to support on-demand reporting and analysis capabilities and a sustainable run-the-bank approach with increased automation and controls and minimal handoffs.



Key regulatory issues and trends

Banks and non-banks alike will need to come to terms with a highertouch regulatory approach. Against this backdrop, we present the 2022 version of our annual report on regulatory trends in the US banking sector.[6] This year's report highlights several regulatory areas that are either foundational, accelerating, or emerging:

Foundational areas

- Pressure on the regulatory perimeter
- Governance and core risk management
- Enterprise compliance and anti-money laundering (AML)
- Consumer protection
- Capital and liquidity
- Data infrastructure and technology resilience

Accelerating areas

- Operational resiliency and mitigating cybersecurity risk
- Third-party risk management (TPRM)

Emerging areas

- Digital assets
- Climate

Foundational areas

The industry, regulators, and academics are looking at how the US regulatory system will need to evolve to handle new activities. We expect fundamental questions (e.g., What activities must be regulated? What is the impact of regulation? Who should the regulator be?) to continue driving discussion and actions in 2022.

The following areas are "foundational" in the sense that regulators—through speeches, guidance, and rulemaking—continue to remind banks and non-banks that the basic principles of risk management must be maintained as banking activities emerge and evolve.

Pressure on the regulatory perimeter

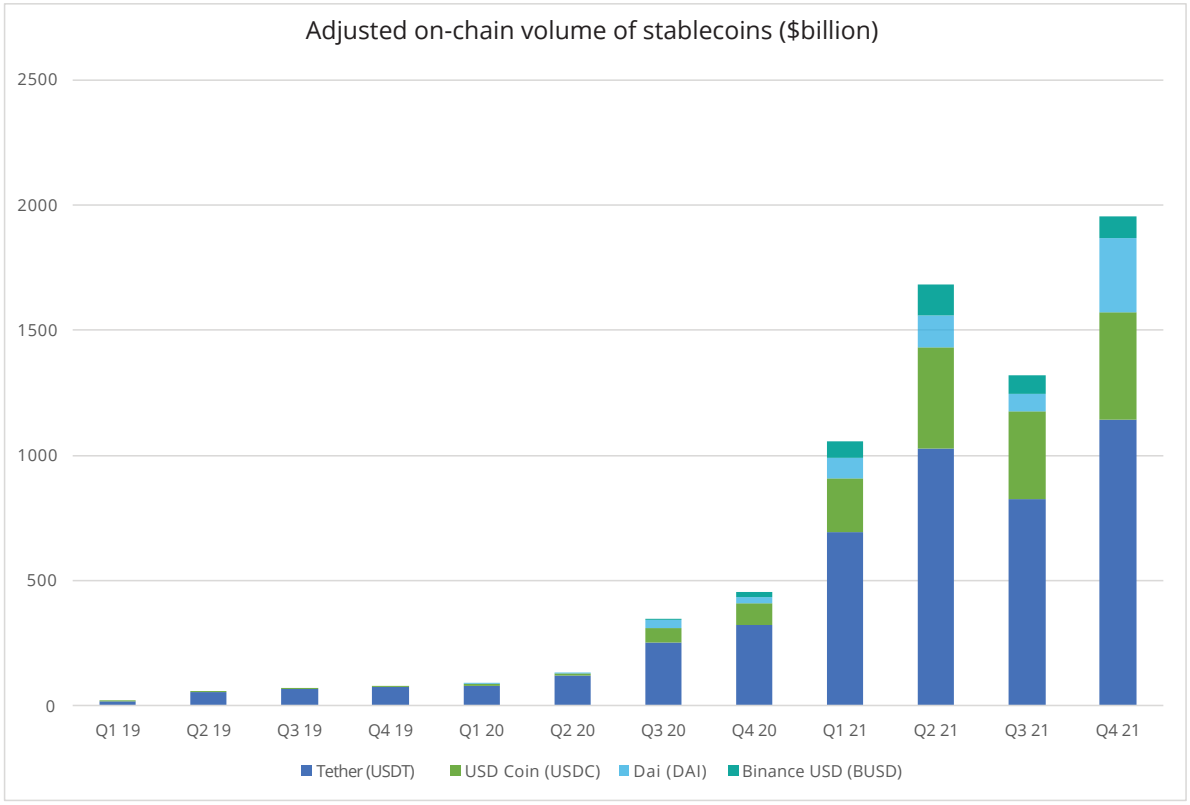
Certain banking activities are always subject to federal oversight and fall within the regulatory perimeter of the FRB, FDIC, OCC, CFPB, and the Financial Crimes Enforcement Network (FinCEN).[7] At the center is the FRB's role in granting access to the US payment system, including Fedwire and reserve accounts.

Several banking activities occur outside of this federal bank regulatory perimeter today. For example, non-deposit-taking trust companies chartered at the state level are supervised by their chartering state regulator. Non-bank consumer lending companies—including non-bank mortgage lenders—are licensed, regulated, and examined at the state level. Money transmitters are licensed, regulated, and examined at the state level, but also have oversight at the federal level by the CFPB and FinCEN.

An example of this is the growing use of stablecoins (current market capitalization of more than $140 billion) and DeFi (more than $150 billion total value locked in smart contracts) becoming systemically important, and all occurring outside the regulatory perimeter (see figure 1).

Disruption and activities outside the bank regulatory perimeter are happening with increasing pace and intensity.[9] Some regulators see non-bank fintech activity as essentially unregulated, with crypto asset activities that occur outside the federal bank regulatory perimeter being viewed as a crisis waiting to happen.[10] However, some state supervisors see things differently and are comfortable relying on prudential and consumer protection requirements under their state money transmission and consumer lending laws. They also point to their supervision of non-depository trust companies and (in some states) their licensing and supervision regimes related to crypto assets.[11] State supervisors argue that they are closer to their local communities, are more accessible than federal regulators, present lower barriers to entry, and can function as sandboxes for the development of new and innovative products—all while protecting their constituents through broad enforcement powers.

Figure 1. Growth of stablecoins and DeFi[8]



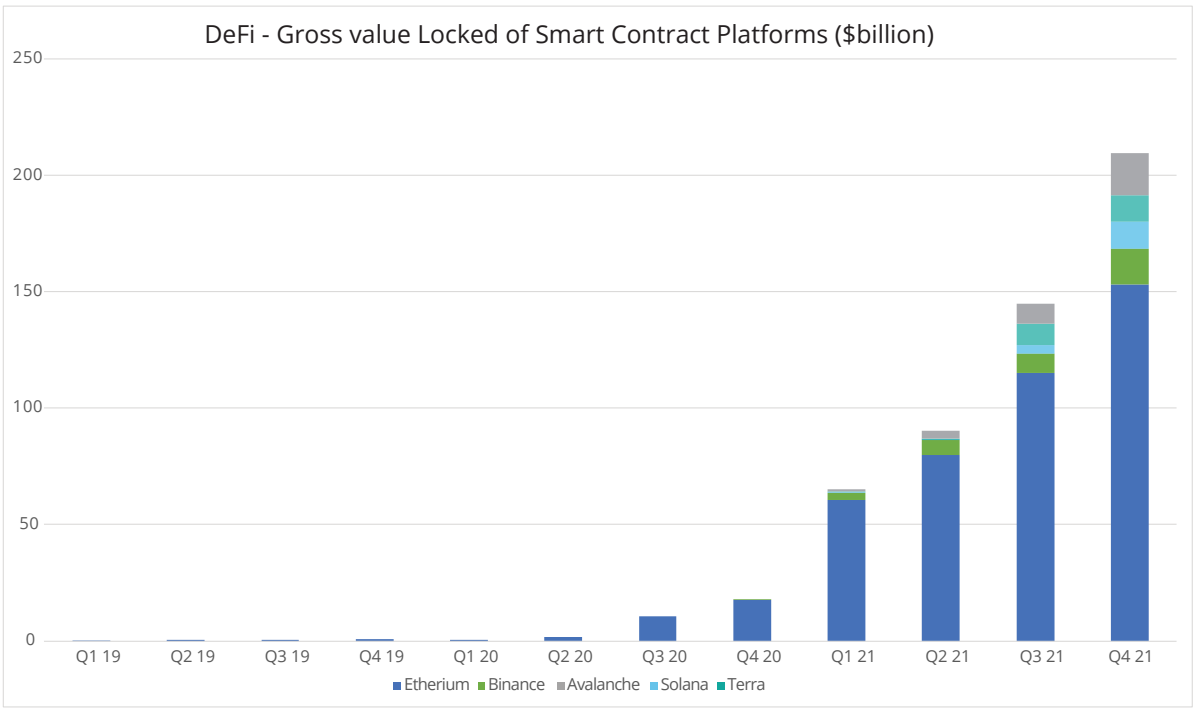
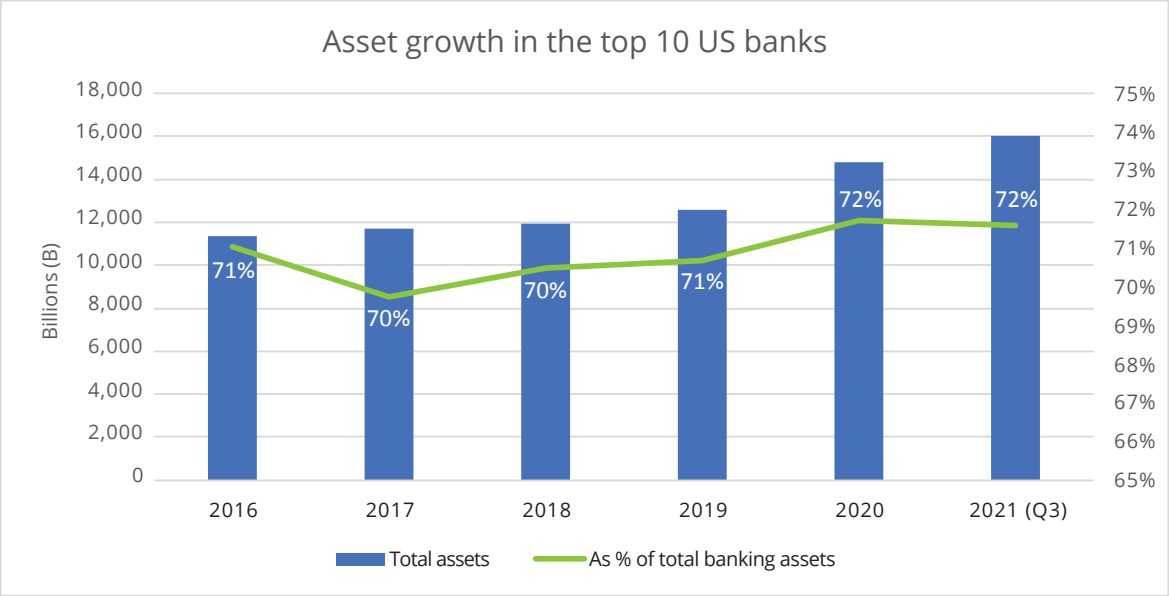
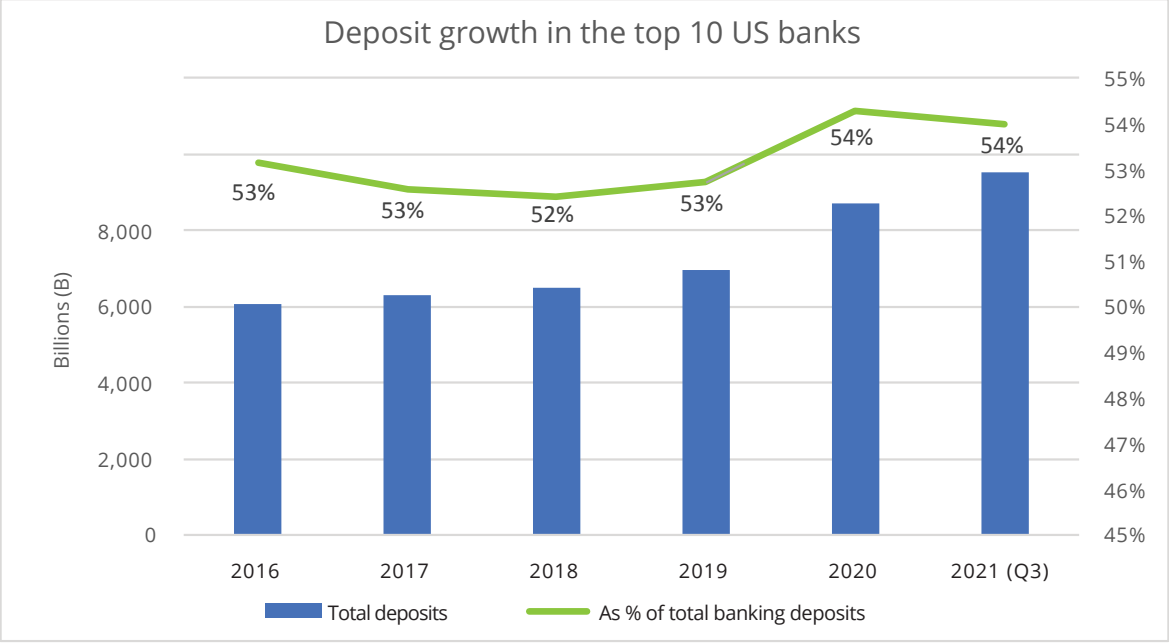


Figure 2. Asset and deposit growth in the top 10 US banks[12]





All of this is adding fuel to the fire for existing legacy banks, which at the same time are trying to scale and adapt to remain relevant given the pace of technological change. Assets and deposits in the top 10 US banks have grown over the past six years at a compound annual growth rate (CAGR) of 7.2% and 9.5% respectively (see figure 2). This included significant mergers and acquisitions (M&A) activity and digital banking transformation. Top banks' rapid growth, coupled with regulatory consent order enforcement events, has raised questions about banks' basic control and risk management structures. It has also led to renewed focus from legislators and regulators on financial stability and systemic risk.

When tackling these issues in the current regulatory and economic environment, Congress will face several competing pressures. On one hand, many legislators may be reluctant to quash their own state prerogatives and risk being seen as potentially stifling innovation—imposing what might be perceived by some as the heavy hand of federal regulation and supervision on emerging business models and technologies that are not currently within the federal perimeter. On the other hand, there are significant risks in doing nothing given crypto asset growth, and federal banking agencies have raised concerns and requested federal legislation.[13]

Additionally, of significant interest is the potential expansion of financial sector participants with access to the US payment system, the presence of alternative asset classes that could become more commonly used as payment for goods and services, and the respective value of that access and usage in the marketplace. Given the closely divided Congress and looming midterm elections, in the absence of a crisis, we believe increased focus by the federal bank regulatory agencies (in the form of guidance, research, and internal working groups that tie back to existing requirements for risk management, oversight, and audit/internal controls) is more likely than federal legislation in 2022. In particular, the following may likely occur:

- **Significant supervisory focus** on new product development, third-party risk management (TPRM), change management, and corporate governance at banks that engage in crypto activities. This will likely result in regulatory findings.
- **A back-to-basics focus on the pillars of risk management** (e.g., escalation, limit setting, risk appetite) and how they will need to evolve given the additional risks that institutions are taking.
- An aggressive effort by the CFPB to **push the boundaries of how consumer protection is embedded** in all aspects of ongoing supervision.
- **No arrival at a "grand compromise"** on how crypto supervision should work across federal and banking regulators.
- Financial Stability Oversight Council (FSOC) taking selected actions to **address the largest risks posed by crypto supervision**.

Given the closely divided Congress and looming midterm elections, in the absence of a crisis, we believe increased focus by the federal bank regulatory agencies is more likely than federal legislation in 2022.

When focusing on the **regulatory perimeter**, banks should consider the following key takeaways:

Be aware of the surroundings.

Even if you were once "outside" the regulatory perimeter, your status may be changing or have changed as regulatory forces continue to shift.

Monitor the regulators.

Changes in regulatory appointees could weigh heavily on regulatory outcomes over the next year. Understanding the players and their views on key topics can help to better anticipate regulatory direction.

Focus on the end goal.

In considering their positioning within the transforming financial system, banks will need to think strategically about the new tools, technology, and businesses that will assist in reaching future goals. The assumption of inherent risk associated with certain fintech advancements and digital assets, for example, will likely impact banks' overall risk appetite, requiring additional attention on prudent risk management.

Repeat the cycle.

Strategies that incorporate the cutting-edge aspects of banking will also need to provide space for the periodic assessment and realignment of risk management practices, as perspectives, best practices, and common themes throughout industry become clearer.

Governance and core risk management

Despite the implementation of new regulations, supervisory guidance, and focused examinations and inspections in the aftermath of the financial crisis, over the past 18 months there have been several headline-grabbing governance, risk management, and control failures in financial services that resulted in nearly $14 billion in financial damage and public enforcement action.[14] These events show that banks have work remaining to protect themselves from risks arising from operating cross-border businesses and legal entities, sustainably operationalize core risk management frameworks, principles, and requirements within the operating model and enable culture of their organizations to outcomes.

For 2022, a few key themes from recent incidents and regulatory actions represent table stakes for the industry: essential capabilities that must be an embedded part of a governance, risk management, and control operating model. A recurring issue from our previous banking regulatory outlooks is banks' need to ensure that foundational risk management and governance expectations are implemented and prove that they are operational. This remains an industry-wide call to action, with urgency calibrated to an organization's size and complexity. In many respects, this is getting back to basics. The need to establish a robust governance model and three lines model remains a constant; however, institutions are also expected to be able to anticipate, prepare for, mitigate, and react to evolving risks in a meaningful way before regulatory identification or intervention occurs.

As banks continue to operate with remote and/or hybrid work models, workforce resilience will continue to be a critical ongoing issue. While banks were able to pivot quickly to alternate working locations in response to the pandemic, over the course of time some employees have evaluated their existing jobs and opted out of their current positions. Together, these influences have put a strain on skillsets, qualifications, and resource availability. To address productivity and control environment issues, many organizations are looking at enhanced communication mechanisms to facilitate teaming, including workflow-based activities that support nonlinear work. Many are also looking at redesigning work through increased use of automation, artificial intelligence (AI), and other technology enablers to improve efficiency and effectiveness, thereby reducing manual, repetitive processes and enabling workers to be redeployed to more valuable activities.

Remote and hybrid work models present significant challenges not only in terms of oversight, accountability, monitoring, and adherence to laws and regulations, but also in terms of serving customers, counterparties, investors, and stakeholders. Banks are expected to continue developing enhanced capabilities that will enable them to effectively monitor their control environments through improved preventative and detective controls. Also, banks are increasing their due diligence and capabilities for spotting bad actors who are trying to take advantage of the remote work model.

Federal and state banking regulators continue to advocate for strong governance and oversight by the board of directors (and for active day-to-day management within three lines of defense model).[15] Governance and controls are sure to remain a hot regulatory topic in 2022, with a few high-profile enforcement actions and fines reminding boards and senior management that continued risk management is essential. Strong governance is required to deliver financial services in a safe and sound manner.[16]

As banks continue to operate with remote and/or hybrid work models, workforce resilience will continue to be a critical ongoing issue.

To that end, regulators continue to focus on governance frameworks during examinations. Regulators have often identified a breakdown in governance and controls as a key root cause when things go wrong. All organizational levels are being scrutinized, from boards and senior management to business lines, independent risk management, and internal audit functions.

Supervisors are increasingly determined to hold senior management accountable for its actions, even in jurisdictions without formal accountability regimes. Regulatory and supervisory focus on individual accountability also continues to grow. Boards and senior management should ensure they are operating within both the spirit and letter of regulations. This includes making sure their decisions achieve demonstrably fair outcomes for their customers, employees, and markets served—and that robust controls are in place to monitor activities and outcomes.

Thematic pain points include:

- **Ownership and accountability of controls are unclear** due to poorly defined roles and responsibilities, resulting in mismanagement of risk
- **Management and staff are underresourced** and face unrealistic "dual-hatting" of responsibilities; three lines operating models are not providing enough resources for the first line to own and manage risk
- **Governance structures and processes are ineffective** and lack end-to-end enterprise connectivity, with insufficient alignment between business strategy, risk, and capital management
- Governance frameworks **do not enable decision-making authority at a regional** level when multiple jurisdictions are in play (e.g., cross-border payments)
- **Risk appetite and risk thresholds** are not credibly managed and governed
- **Risk management structures have not evolved** with the business strategies or risks that are posed
- **Risk exposure is not always evident**, particularly among complex cross-border and intra-business transactions and relationships
- Risk reporting and risk management processes **fail to connect the dots across multiple business relationships** at the enterprise level as well as at the legal entity level
- **Incentives to manage risk** are not credibly embedded in organizations' performance management processes; reporting and escalation challenges limit boards' ability to hold front-office units accountable

To demonstrate effective and sustainable risk management processes, it is essential to understand relevant risks, enhance infrastructure, implement a robust risk framework, and ensure firm culture promotes sound risk practices. When focusing on **governance and core risk management**, banks should consider the following:

Risk assessments representing real consensus. Proactively perform risk assessments against relevant "pain points" to confirm which ones pose the greatest risks, then evaluate controls to determine how to mitigate the risks most effectively. Analyze root causes and lessons learned in earnest, not just as a "check the box" exercise.

Scalable and appropriate risk and control frameworks. Review risk management and control frameworks across businesses, legal entities, and cross-border operations with a clear view of global/enterprise and regional/local tensions. Consider ownership of risk, roles and responsibilities, communication channels, and escalation protocols supported by effective monitoring and reporting processes.

Internal reporting or Management Information Systems (MIS) that is fit for purpose. Identify immediate changes to monitoring and MIS/reporting protocols to ensure all relationships and related risks posed by the customer are captured. Over the longer term, invest as needed in new/improved technology to remove disparate and complex architectures and focus on intercompany/intra-function activities through enhancements to risk architectures, processes, and controls to ensure business risk reporting is prepared, monitored, and used for decision-making and effective challenge.

Escalation linked to issue management. Host challenge workshops that examine the firm's risk appetite and breach protocol, including bright-line boundaries and clearer escalation guidance and protocols that support independent decision-making viewed through business, legal entity, and product lenses.

Resources and skills assessment and refresh. Assess resources sufficiency, skills, and efficiency within strategy, operating model, innovation, and maintenance of core capabilities for alignment to pace of regulatory change and priorities.

Accountability linked to risk-reward. Define incentive structures and staffing levels in a way that ensures roles and responsibilities around risk are adequately performed; "dual-hatting requirements" are adhered to; and employees are encouraged to proactively manage, escalate, and remediate risks.

Business model operating dimensions. Define how governance activities work across legal entities, businesses, and regions.

Credible challenge. Facilitate credible and periodic testing of stress points and conflicts among senior management against realistic "dual-hatting" guidelines.

Resolve conflicts. Incorporate front-office staffing and management composition trends into risk governance reporting and monitoring. Redefine risk appetite and breach governance processes, including bright-line boundaries and decision-making protocols.

Enterprise compliance and anti-money laundering (AML)

Once the sole responsibility of a bank's designated compliance function (with a narrow focus on technical consumer protection regulations), compliance now covers virtually all aspects of a bank's supervised activities and has evolved into a source of risk that the board and all three lines are accountable for managing. This trend of expanding compliance requirements and organizational impacts is expected to continue in 2022 and is especially acute for larger US domestic and foreign banking organizations (FBOs).

As noted throughout this outlook, federal bank regulatory agency rules and requirements are increasingly prescriptive, with clear mandates creeping into areas that were historically within the province of principles-based expectations. The prescriptive compliance perimeter—consisting of a group of compliance requirements for the banking space—now covers new areas such as board governance and TPRM, along with detailed requirements in prudential risk management areas such as capital and liquidity management.

The CFPB is sending clear signals that it intends to exercise its authority for entities currently outside of the federal and state perimeters (such as Big Tech).[17] Meanwhile, state regulators continue to exercise authority over the chartered banks and branches, mortgage and other consumer lending companies, and money services businesses that they oversee. Also, through their attorneys general, many states are enforcing various federal consumer protection rules along with their own state laws governing areas such as fraud and deceptive practices.

When focusing on **enterprise compliance**, banks should consider the following key takeaways:

- **Broadening of the compliance perimeter is ongoing.** Forthcoming developments will continue to have an enterprisewide impact. This will further elevate the importance of monitoring regulatory compliance changes and ensuring that strategic planning is forward-looking, agile, and able to accommodate new regulations without disrupting existing business lines or future revenues.

As noted throughout this outlook, federal bank regulatory agency rules and requirements are increasingly prescriptive, with clear mandates creeping into areas that were historically within the province of principles-based expectations.

An effective compliance management system (CMS) and supporting personnel must effectively cover all these new and nontraditional areas, in addition to the more traditional ground of consumer protection, AML, and the Bank Secrecy Act (BSA). Failure in any of these areas can result in enforcement actions by a bank's primary federal regulator and/or state supervisor (for state-chartered banks or branches). These enforcement actions tend to be long term in nature and have an adverse impact on resources—redirecting them toward remediation and legal expenses—while also negatively affecting business expansion (including acquisitions) and limiting business strategy options.

- **A nimble CMS is essential.** A CMS that can adapt to new regulatory requirements, evolve core testing and monitoring capabilities to be proactive and automated, ensuring clarity across lines of defense, will help avoid compliance inconsistencies and increased regulatory scrutiny.

Implementing a risk-based AML program

AML programs are a prime example of how banks must strike a balance between maintaining compliance and adopting innovative approaches. Public enforcement actions for AML-related deficiencies have declined both in frequency and magnitude over the past several years suggesting that banks are improving in this area.[18] However, President Biden's regulatory appointees are still getting positioned and might be less lenient toward AML-related deficiencies (especially those that fester), given the administration's focus on getting the basics right.

In the US, there is consensus among regulators, legislators, law enforcement agencies, and industry that compliance with AML/Counter Financing of Terrorism (CFT) requirements—including amendments passed after the BSA—has evolved into a layered and inefficient system that does not serve the practical needs of law enforcement.[19] In many instances, this has resulted in regulated financial institutions spending time on activities that do little to mitigate the risks associated with financial crime. On September 16, 2020, FinCEN signaled the start of a multiyear effort to fundamentally reform the AML/CFT regime in the United States through an Advance Notice of Proposed Rulemaking (ANPRM) on AML program effectiveness.[20] The ANPRM introduced a proposed definition of AML program effectiveness, the concept of Strategic AML priorities, and a possible regulatory requirement for risk assessments.

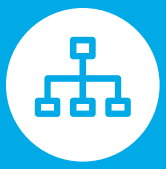
On January 1, 2021, the AML Act of 2020 (US AMLA) became law, reinforcing and codifying a risk-based approach for AML/CFT programs.[21] On June 30, 2021, FinCEN issued the first governmentwide national AML/CFT priorities (the "Priorities"), a significant first step for banks to incorporate the Priorities into their AML/CFT programs, and for regulators and examiners to integrate them into rules, guidance, and examinations.[22] The Priorities, combined with the ANPRM, shift the focus of banks' programs from maintaining technical compliance to a more risk-based, innovative, and outcomes-oriented approach.

Banks and regulators both recognize the need to cement the use of innovative technology (through usage and law) to help achieve a risk-based approach to financial crime. Emerging technologies such as machine learning, AI, analytics tools, and data science can help banks aggregate and analyze significantly more data than in the past. These capabilities will become increasingly important as traditional data (e.g., Know Your Customer information) is supplemented with new data such as that generated by increased use of online banking, all of which can be enriched through aggregation with contextual information from proprietary open-source data providers. The US AMLA, for example, makes innovation and adoption of innovative approaches a regulatory imperative (e.g., required use of "NextGen" models that leverage behavioral analytics and machine learning to improve the effectiveness of financial crime monitoring and investigations). [23]

Beneficial ownership

On December 6, 2021, FinCEN released a Notice of Proposed Rulemaking (NPRM) to implement the beneficial ownership information reporting provisions of the Corporate Transparency Act (CTA).[24] The proposed rule addresses, among other things, who must report beneficial ownership (BO) information, when they must report, and what information they must provide. Two more NPRMs are anticipated around (1) access to the BO registry and (2) harmonizing with the Customer Due Diligence rule.

When focusing on **anti-money laundering/financial crime**, banks should consider the following key takeaways:



Align with the Priorities based on the risk profile of the organization.

Banks need to understand the specific threats related to applicable Priorities and how those threats might intersect with their business activities.

Adjust risk assessment processes.

Banks need to adjust their AML risk assessment processes to focus more closely on applicable Priorities, modifying the risk assessment inputs as needed, including data and expertise.

Align resources with the Priorities.

As banks develop an understanding of their risk profiles vis-à-vis the Priorities, they may need to shift resources from less significant priorities toward higher ones.

Develop metrics that demonstrate effectiveness.

Banks need to develop metrics and examples to demonstrate how their AML programs align to the Priorities (and the associated value of reporting to law enforcement).

Consumer protection

Building on the momentum and renewed focus on consumer protection, we expect banking and financial regulators to accelerate consumer-related supervision and enforcement activities in 2022. This increased scrutiny will be felt not just by banks, but also by entities operating at the edges of the regulatory perimeter such as fintech companies and technology companies (which may be licensed at the state level under lending, money transmitter, or other regulatory regimes). Consistent with the Biden administration's policy around financial inclusion and equitable recovery from the pandemic—and a focus on fair and responsible banking—we anticipate an increased pursuit of predatory, unfair, deceptive, abusive, or other problematic practices, with remediation and restitution to consumers when warranted.

A shifting landscape

While no major changes to banking law or regulations are expected in the near term, changes at the CFPB and OCC have already led to an increased consumer-oriented "tone from the top" and, as a consequence, an enhanced supervisory/enforcement approach. The new tone is leading to new scrutiny at the examination level as the FRB, OCC, and FDIC have a shared framework for assessing the CMS, which is the backbone for ensuring appropriate controls for preventing consumer harm. The novel approach involves, among other things, increased coordination and cooperation among agencies in modernizing the Community Reinvestment Act (CRA), conducting regulatory sprints on digital currency risks, and offering outreach to state financial regulators about shared responsibility on consumer protection matters.

The FRB, OCC, FDIC, and CFPB—driven by consumer complaints and self-identified supervisory oversight gaps—are already starting to fulfill an expectation for protecting consumers beyond the traditional regulatory perimeter.[25] Consumer complaints have spiked over the past year, driven by product innovation in areas such as buy now, pay later (BNPL) financing and digital currencies.[26] These and other innovative financial products are being offered to consumers by non-banking entities, often regulated as money transmitters or non-bank lenders at the state level but in many cases working in partnership with a federally supervised bank. We are expecting (and seeing) multifaceted supervisory scrutiny and targeted rulemaking and guidance from the FRB, OCC, FDIC, CFPB, and states to provide an effective consumer oversight umbrella from a complex web of regulators. For example, the CFPB has initiated an investigation of data privacy and protection practices at certain large technology companies offering payment products.[27]

Potential areas of focus

Looking at specific policy areas, we expect regulators to continue their focus around the concept of fair and responsible banking, which covers a broad array of consumer protection laws and regulations—extending beyond banks to non-bank financial services providers. In addition to fair lending, we expect more frequent citation of UDAP (Unfair or Deceptive Acts or Practices) and UDAAP (the additional "A" stands for "abusive," per the CFPB) when existing regulations do not directly address consumer harm stemming from breakdowns in operational controls. The CFPB has referenced and is addressing "persistent pain points" from the pandemic, with recent public enforcement actions and Supervisory Highlights focusing on adverse consumer impacts (including improper fees charged to borrowers enrolled in CARES Act forbearance) and failure to investigate potential credit reporting or money transmission errors.[28]

Looking at specific policy areas, we expect regulators to continue their focus around the concept of fair and responsible banking, which covers a broad array of consumer protection laws and regulations—extending beyond banks to non-bank financial services providers.

Fair lending. Today's lending environment holds significant reputation risk to institutions. One recent view suggests that there are three primary focus areas for regulators today: fair lending, fair lending, and fair lending.

- **Banks are being investigated and cited for redlining issues**, with recent emphasis on the location of traditional brick-and-mortar branches; the active offering of all lending products across all neighborhoods in a community; inadequate monitoring for fair lending; and, in general, whether banks are meeting their obligations under the CRA.
- **Non-bank lenders are not exempt from redlining,** despite not having a CRA assessment area, and should be cognizant of their office locations and the geographic areas served by their loan originators.
- **Target marketing**, including via social media, raises the potential for Equal Credit Opportunity Act (ECOA) compliance.
- **There will be little slack for entities that do not capture the new HMDA reporting fields** with a high degree of accuracy within regulatory tolerance limits.

Overdrafts. Overdrafts have possible fair lending consequence as well as potential UDAAP implications. Given the correlation between low-income and minority areas, geocoding of consumer overdraft activity might uncover potential disparate impacts even for activities that seem neutral on the surface. This area has been a long-standing concern for regulators (with some having addressed unfair practices or deceptive disclosures as part of the non-public supervisory process). We are seeing accelerating concerns from the OCC and CFPB over the purpose and impact of overdrafts, leading to increased examinations, investigations, and public consent orders.[29] A number of banks have elected to eliminate overdrafts altogether,[30] while others are choosing to meet consumer needs by implementing innovative product changes—for example, allowing people to elect which payments will cause their account to be overdrawn.

Buy now, pay later (BNPL). The expanding use and market growth of BNPL, starting with fintech companies but with increasing participation by banks, has consumer protection implications and should not be viewed as an opportunity for regulatory arbitrage (i.e., taking advantage of a market that is currently less regulated) between banks and non-banks. Banks and non-banks need to clearly understand and delineate their respective roles and responsibilities in product delivery (and how regulations might apply) with an expectation that some of the current ambiguity will be clarified in the short term via future guidance and use of UDAAP.

Consumer harm. The CFPB, FRB, OCC, and FDIC expect institutions to self-identify and initiate corrective action on serious compliance violations, including remediating controls and programmatic weaknesses in the CMS and providing restitution for injured parties. Several recent enforcement actions have cited banks for failing to identify and remediate customer harm.[31] In fact, there is an emerging view from the CFPB that failure to remediate noncompliance constitutes an abusive practice under UDAAP, potentially amplifying the consequences of noncompliance.[32]

When focusing on **consumer protection**, banks should consider the following key takeaways:

Address new product risk.

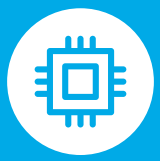
The regulatory expectation that banks should have robust practices for reviewing new products and managing change is long established. When establishing a new product or service, banks and non-banks alike need to identify all applicable federal and state consumer protection laws and regulations and then implement controls to help ensure that all three lines are prepared to carry out their individual responsibilities to prevent, detect, and correct violations.

Reassess CMS adequacy.

Strengthen CMS with an emphasis on risk assessment, TPRM, consumer complaints response and analysis, monitoring and testing, and issue escalation and resolution.

Be selfish.

Get ahead of problems before regulators open an investigation or examination by being "selfish" (self-identify, self-correct, and self-report). Entities that are not proactive in maintaining a robust CMS and addressing consumer harm will not benefit from the CFPB's and other regulators' views on responsible conduct.



Stay current on supervisory guidance.

In this dynamic environment, it is important to stay current on known industry issues (e.g., through the CFPB's Supervisory Highlights and Enforcement Actions), as well as evolving regulatory expectations.

Capital and liquidity

Capital and liquidity planning will likely continue to be unusually complex in 2022. Most capital and liquidity processes are designed to handle economic cycles, which are predictable. However, the current environment is being driven by pandemic-related non-market factors that are much harder to anticipate—particularly government support programs, which are influencing a much broader array of participants than in the past. At the moment, the degree to which these programs will be maintained is uncertain, as is the timing and impact of their potential wind down. This uncertainty has a ripple effect on the key assumptions and inputs that go into banks' business models, stress testing, and internal forecasting. For example, inflation that is higher than recent norms—driven by forces that have not been encountered in the past—could affect both short- and long-term interest rates, resulting in profound impacts on profitability for firms that depend on income from net interest margins.

Since capital planning and liquidity models depend on the predictability of their underlying assumptions, the current market environment is increasing the variability of outcomes and the potential need for higher capital than previously calculated. These areas will likely receive more attention going forward, especially for the largest banks, and the blurring lines between banks and non-banks in activities that have traditionally been highly regulated could make cost structure difference more pronounced. All of this is making it more complicated to quantify capital and liquidity impacts, even for banks with mature processes built around a Federal Reserve and banking agency structure that has become more industry-friendly over the past several years. With anticipated leadership changes we could see more focus on capital and liquidity requirements and impact of those requirements and completion of outstanding policy matters.

For some large banks, the challenge is not just identifying and calibrating external factors, but also understanding their impact on specific business lines. The impact on loans and deposits has become less market-influenced and more sensitive to government stimulus. Deposit inflows at many banks have not only been significant but less predictable and might not be stable over the next year, but also have in many cases outpaced loan demand, prompting challenging decisions about where to invest funds to maintain income objectives.[33]

With anticipated leadership changes we could see more focus on capital and liquidity requirements and impact of those requirements and completion of outstanding policy matters.

For some large banks, supplementary capital requirements are becoming a constraining factor that must be considered when making projections over the next year.[34] And, for large banks that had merger activities as part of their strategic and capital plans, those activities might be delayed due to increased regulatory scrutiny. Also, banks with capital and/or liquidity imbalances that had planned to combine operations might need to adjust their plans.

Non-bank banking

Competition from non-bank organizations getting into bank-like activities will likely increase over the next year. In the past, non-regulated enterprises that offered bank-like services were largely overlooked by regulators. However, as their size and impact grow, they are drawing more regulatory attention and are increasingly being exposed to regulatory forces—making their business projections less predictable. In many cases, these enterprises have little experience operating under stress. As such, market perceptions and concerns about their viability under stress are driving the need for an improved understanding of how to measure the adequacy of their capital and liquidity in a manner similar to their regulated counterparts (but in many cases for higher-growth business models). This issue could make them look for stable strategic partners, such as regulated financial institutions. Similarly, the impact of digital assets on capital and liquidity measurements will not always be clear, nor will the treatment of these activities by regulators, making capital and broader financial planning more difficult.

Uncertain regulatory expectations

Regulatory expectations remain in flux. Internationally, the Basel III requirements have been delayed, and the US rulemaking process will extend into 2022 and likely beyond.[35] With some key lead regulatory agency roles still unfilled, rulemaking on these crucial topics will be stalled. The resulting impact on capital and liquidity requirements is unclear, especially for large banks. However, the overall direction will likely be more conservative than in the recent past. Although most regulated banks have capital planning and liquidity measurement processes in place, the level of onsite scrutiny will likely rise (and minimum levels for the largest banks might increase). As business models expand into areas such as cryptocurrency services that traditionally have not received much attention from regulators, lack of understanding about the associated risks (and/or lack of appreciation for the actions taken to mitigate those risks) could potentially result in higher capital and liquidity constraints.

Rising compliance challenges and costs for regulated banks

Increased costs to respond to regulatory requests will likely be seen in 2022—and more scrutiny of compliance processes. With stress testing struggling to simulate government actions that are hard to predict, capital and liquidity measurement processes and assumptions will likely receive more attention, further increasing compliance costs.

Nimble capital and liquidity processes should be a focus. In addition, proper governance and documentation should be emphasized since the scope of examination work in these areas will likely increase. Model accuracy will likely be more challenging to achieve given that recent performance might not be indicative of future performance, and the skill sets needed to model capital and liquidity are becoming increasingly scarce—making it more costly and difficult to staff up. Maintaining capital and liquidity at levels that regulators are comfortable with will be further complicated by deposit and loan trends, as well as inflation and interest rate trends that will likely be less predictable than in previous years.

When focusing on **capital and liquidity risk**, banks should consider the following key takeaways:

Review and strengthen processes and governance to ensure capital and liquidity modeling remains predictive of future performance, reflecting changes in products, underwriting, and business assumptions that have been made to adjust to recent market conditions and government actions.

Ensure adjustments to modeling assumptions and output are well vetted, challenged by the second line, well documented, and clearly conveyed to all levels of management, including the board of directors.

Assess staffing levels and experience levels that support capital and liquidity modeling to ensure they are adequate and that process controls and schedules can be maintained.

Adjust capital and liquidity planning to reflect the bank's changing business profile, integrating material changes in business activities and models that are nontraditional in nature.

Financial enterprises outside of the current federal regulatory perimeter that are expected to be exposed to increased regulatory capital and liquidity requirements should **assess the extent of the expected exposure** and then **take steps to understand the resource and staffing implications and improve their documentation and governance** of the planning process.

Data infrastructure and technology resilience

Since the financial crisis, the need for granular, near-real-time data has increased. Recently, the pandemic showed how quickly periods of stress can develop, revealing the need for new types of data, often at high frequency. This data is needed for banks to comply with regulatory requirements (e.g., stress testing and standardized reporting) and support risk management. Banks have seen several regulatory reporting changes and additions over the past year, with proposed changes to at least one reporting form currently out for comment, a few where comments are under review, and several others that are finalized and pending implementation in 2022. Regulatory report data is also used for supervisors to make evidence-based policy decisions and has the potential to impact supervisory views and perspectives. Now more than ever, data is a critical asset needed to identify and manage emerging risks and develop risk mitigation responses.

Integrating legacy data and technologies as a first step to an enterprisewide data environment

Large, complex banks continue to use outdated technology that makes it difficult to access data and apply advanced analytics, thereby increasing the need for manual intervention and time-consuming data transformations/aggregations. To address these problems, banks are shifting away from siloed approaches and moving to an enterprise approach for storing data—developing target-state architectures that bring data from approved data sources (ADS). An enterprisewide data environment is a must-have for large banks especially as they address ongoing data needs corresponding to the assignment of tailoring categories (according to size, cross-jurisdictional activity, reliance on short-term wholesale funding, non-bank assets, and off-balance-sheet exposure) and resultant requirements.

Transforming to a data infrastructure with flexible platforms requires firms to overcome challenges in integrating data sources and systems: ingesting data from new sources; enabling data availability; providing data protection and privacy; developing advanced analytical capabilities; and building resiliency.

The FSOC's 2021 Annual Report highlights the presence of data issues related to the scope and usefulness of data that regulators rely on for risk identification purposes. Although firms have improved their data management and governance models, significant effort remains to develop a data infrastructure and environment to support real-time data needs. To meet data demands when unexpected events occur, firms need to shift to a more dynamic approach. Transforming to a data infrastructure with flexible platforms requires firms to overcome challenges in integrating data sources and systems: ingesting data from new sources; enabling data availability; providing data protection and privacy; developing advanced analytical capabilities; and building resiliency. These challenges require looking at technology strategy alongside data strategy.

Involving stakeholders—including the chief financial officer (CFO), chief risk officer (CRO), chief technology officer (CTO), and business-line leaders—in developing solutions is imperative to achieving a well-integrated strategic data infrastructure. Less than a year ago, updates to the Federal Financial Institution Examination Council's (FFIEC) Information Technology Examination Handbook outlined the duties of certain IT-related executive roles (such as the chief data officer, or CDO) and banks continue to move forward with data infrastructure improvements. Transformation of a complex organization is a significant investment with a lengthy development and implementation period. Developing a road map is a key step to understand how to migrate legacy data to an integrated infrastructure. And in order to execute the road map, senior management support and realistic milestones are essential.

Availability of data: Making data an asset across the firm

The tremendous amount of data stored throughout an organization makes it challenging to manage and govern data. Many banks still store data at the business level, making it hard for the rest of the organization to know what exists. This leads to duplicate data that often lacks standard definitions. High-performing banks have activities and programs to manage data at the corporate level, which facilitates the standardization of data definitions, establishment of approved data sources, and development of tools for data users to identify fit-for-purpose data assets across business lines. These activities often occur under the CDO. However, without cooperation across the firm, a true enterprisewide data approach cannot be established. The absence of an enterprisewide data approach for the largest and most complex banks can result in data quality and integrity deficiencies brought forth during routine and specialized examination activities. Consulting the FFIEC handbook for guidance and expectations in these areas should help banks as they manage data across various functions and levels of the organization.

Data privacy and protection: Securing data assets

As data is shared more broadly across a firm, its use should be tempered by the ability to protect the data from cyberattacks, inadvertent loss, and privacy law breaches. This requires protocols and processes to ensure that data losses, including inadvertent disclosure, do not occur. Robust compliance programs and training are imperative, particularly for data privacy, for which local laws and regulations are constantly evolving. The occurrence and implications of cyberattacks and data breaches are discussed in further detail in the Operational resiliency section.

Analytical capabilities: Gaining insight from data

The increasing scale and availability of data increases the need for analytical capabilities to draw meaningful insights from that data. Advanced data analytics such as AI and machine learning are becoming essential capabilities for modeling and correlating data. Advanced data analytics are also becoming increasingly important in creating business rules for data, conducting data profiling, and executing quality assurance processes to ensure fit-for-purpose data is available. A fourth quarter 2021 FSB report reiterates the importance of readily available, relevant, and thorough data coupled with good analytical resources to support analysis and evaluation of pandemic-related financial risk. The report also suggests that the FSB will provide a space for regulators and supervisors to discuss perspectives on data analysis and forthcoming analytical tools. Enhancing data analysis is an area of focus for regulators and supervisors and should similarly be a priority for banks.

Resiliency in data infrastructure: Maintaining data production

With the growing importance of data and its associated operations, a firm's strategic data infrastructure and technology should be designed to ensure resiliency and business continuity—including system availability and data recovery that aligns with core needs. Resiliency becomes even more critical in times of stress when data is needed to manage emerging risks, including operational risk. A key lesson from the pandemic is the need for data platforms to be usable remotely—not only access and execution, but also protection of sensitive data that is accessed off-premises.

When focusing on **data infrastructure**, banks should consider the following key takeaways:

Be informed.

Understand the current data environment and conduct a gap analysis to reach the desired state.

Enlist and empower accountable parties.

Build an accountability structure where stakeholders across the enterprise are assigned responsibility for data.

See deeper into your data.

Invest in analytical capabilities to broaden and deepen your data insights.

Fortify the protection of your assets.

Develop solutions to secure data assets and protect data privacy.

Accelerated areas

Supervisors' approaches to technology, in terms of how they supervise banks and their own internal adoption methods, are accelerating rapidly. In particular, regulators are now playing a role to foster and encourage technology adoption, collaborating with the industry, and changing their supervisory capability to catch up to the industries they supervise. These actions are effectively reinforcing the necessity of banks to have strong core IT infrastructures, governance frameworks, TPRM practices, and robust data infrastructures.

Operational resiliency and mitigating cybersecurity risk

The increased rate of digital transformation that US banks undertook during the pandemic and throughout 2021 presents unique security challenges and risks. According to Federal Reserve Chairman Jerome Powell, cyberattacks are now the foremost risk to the global financial system, even more than the lending and liquidity risks that triggered the financial crisis.[40] A report by the International Criminal Police Organization (INTERPOL) shows an alarming rate of cyberattacks during the pandemic, with a significant shift in targets from individuals and small businesses to major corporations, governments, and critical infrastructure.[41]

Increases in cyberattacks, data breaches, and service outages have steered bank leaders and regulators to focus more attention on managing operational and cyber risks. Regulators spent much of 2021 proposing and finalizing guidance and updating examination handbooks to respond to these threats and risks, and the topic remains a key highlight in both the FRB and OCC's semiannual regulation and supervision reports.[42] Key developments in 2021 included several updates to existing guidance and new regulations that will require further assessment and operationalization in 2022. Supervisory examinations are expected to continue as this remains a top priority.

On June 30, 2021, the FFIEC published an updated **Architecture, Infrastructure, and Operations booklet**, which is part of the FFIEC Information Technology Examination Handbook.[43] To promote safety and soundness, this replacement of the booklet from 2004 emphasizes the interconnectedness between bank assets, processes, and third-party service providers. The new booklet reflects the overall view that banks are responsible for effectively addressing IT risks that affect their business models, and that they need to demonstrate a capability to effectively identify and address IT risks that affect their business models, with an emphasis on governance.

- There is an expectation that banks will define the responsibilities of key IT executive roles.
- Overseeing third-party service providers is newly introduced in this booklet considering many entities are outsourcing AIO activities to one or more third-party service providers (including cloud service providers).
- In order to align with rapidly changing and evolving technologies in the financial market, the booklet also incorporates a new section on "evolving technologies," with general information on emerging technologies like cloud computing, zero trust architecture (ZTA), microservices, and artificial intelligence and machine learning (AI/ML).

On August 11, 2021, the FFIEC issued its "**Authentication and Access to Financial Institution Services and Systems**" guidance, replacing previously issued guidance from 2005 and 2011.[44] The new guidance provides banks with examples of effective authentication and access-risk management principles and practices for customers, employees, and third parties that access digital banking services and information systems. In addition to providing requirements for conducting risk assessments and implementing multifactor authentication (MFA) and layered security, the latest guidance directs banks to:

- Apply the principle of *least privilege* when provisioning access
- Implement monitoring, activity logging, and reporting processes
- Ensure secure credential and application programming interface (API)-based authentication
- Establish controls to secure email systems and internet browsers
- Establish secure processes for customer call center operations, IT help desk operations, and verification of customer and user identities

On November 23, 2021, the FRB, OCC, and FDIC announced the approval of a **final rule to improve reporting of information about cyber incidents that might affect the US banking system**.[45] The final rule requires a bank to notify its primary federal regulator of any significant computer-security incident as soon as possible (and no later than 36 hours) after the organization determines a cyber incident occurred. The rule extends banking regulators' reach beyond the banks they regulate, widening the regulatory perimeter to include the third parties that banks rely on to provide services to customers. A banking service provider is required to notify affected customers immediately after it experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair for four or more hours provision of services that are subject to the Bank Service Company Act (BSCA). No matter where an organization sits within the regulatory perimeter, the broad definition of "security incident" will likely strain its protocols for timely communication. Escalation protocols should address the numerous definitions of incidents that require reporting and notification. They must also align with vendor management and TPRM programs, internal IT infrastructure, and cybersecurity event monitoring. In addition, the protocols will need to define who should be involved in the escalation process (e.g., internal senior management, boards, and regulatory agencies). To achieve and maintain compliance, banks will need to monitor regulatory divergence across agencies and jurisdictions, which could add to the complexity and slow the speed of information flow.

When focusing on **cybersecurity and operational resiliency**, banks should consider several actions including:

Broaden the mindset.

Continue to look enterprisewide at resilience activities and identify interconnections across various domains. Cybersecurity and more broadly operational resilience requires a change in mindset and culture and should consider strategic, reputational, and operational risks, as well as an understanding of human behavior.

Ruthlessly prioritize.

Establish a clear focus on the most critical business services. For the most critical business services, map systems, processes, and third parties that support those services. Direct remediation and recovery priorities accordingly for existing programs and processes related to business continuity management and operations restoration planning.

Create a single view of criticality across the enterprise.

Use an end-to-end view to understand critical business services and then identify the critical path for functions, teams, and systems. Focus on business services that are customer- and outcome-based, risk-aligned, and led or approved by the business. Create accountability for the established priorities.

Prepare for disruption.

Understand and define plausible scenarios for outages and long-term disruptions. Set impact tolerance statements for each critical business service, and act to remain within established thresholds. Establish connection between incident response, recovery, continuity planning, and crisis management capabilities. Pre-define communication protocols. Put contracts in place for important response relationships (e.g., law firms or cyber insurance providers).

Test the plan.

Use war-gaming and table-top exercises as interactive techniques that immerse potential cyber-incident responders in a simulated scenario to help organizations evaluate their incident response preparedness.

Third-party risk management

Continuing expansion of the banking ecosystem and heightened use of outsourcing are increasing and highlighting the importance of a bank's TPRM capabilities. Further, these developments are prompting the revision of supervisory guidance. TPRM is a cornerstone of nonfinancial risk for banks, and banking regulators understand that the banking ecosystem is expanding and integrating with other industries. Outside of the perimeter, there is a high bar that service providers must meet when dealing with entities within the perimeter, as bank TPRM programs require enhanced governance, monitoring, and compliance with applicable laws and regulations (which, in some cases, may be extraterritorial for the service provider).

This expansion is changing the way banks must operate their TPRM programs in three areas: agility and responsiveness, consolidation, and expansion. First, the speed of market change is forcing banks to move from a passive or point-in-time view to more active, continuous monitoring. Second, banks are realizing that third-party risk profile data resides in multiple places, and that consolidation is needed to provide a more holistic view of "true risk." Third, new types of third-party service providers require clearly defined life cycle management, including better definitions around the types of services they provide.

On July 12, 2021, amid a proliferation of changes to the banking ecosystem driven by this increased outsourcing activity, the FRB, OCC, and FDIC proposed an update to their individual guidance on TPRM.[46] In addition, banking regulators are increasingly looking at the role of banks' key service providers as noted in the FFIEC's statement on risk management for cloud computing services and the interagency final regulation for computer incident notification (described earlier).[47]

The agencies' TPRM proposal offers an interagency framework and reemphasizes the investment many banks have made in their TPRM programs. This investment includes skilled resources, effective processes, and enabling technology. While the agencies recognize the advantages that third parties bring, they also emphasize that banks must manage the risks third parties may pose. In addition, the proposal promotes interagency consistency and modernizes current supervisory views.

When focusing on **third-party risk management**, banks should consider the following key takeaways:

Assess current TPRM programs against the proposed interagency guidance, and determine impacts to third-party inventories based on the proposal's new definition of "business arrangement."

Know your ecosystem—both individually with respect to third parties, and together at the operating model level. Build proactive TPRM capabilities, such as monitoring, and integrate insights to better inform understanding of residual risk at the portfolio level.

Prepare for expansion of the regulatory perimeter. Work with ecosystem partners and service providers as regulatory guidance is directed at banks (and on a dual path to the service providers themselves), recognizing that banking regulator reviews under the FFIEC program and BSCA will continue to evolve, expand, and likely extend beyond the traditional borders.

Show that current TPRM programs align with the bank's strategy and risk appetite. TPRM programs do not thrive in isolation; banks must ensure risk tolerance levels are demonstrably linked to enterprise frameworks.

Proactively manage risk. Rapid market change is requiring banks to become more agile and responsive to the risks posed by third parties. To keep pace, banks must move from a passive, point-in-time view of oversight to an active, forward-looking stance.

Emerging areas

Digital assets

Regulators are concerned that digital assets may pose a threat to financial stability as adoption increases, as mentioned earlier.[48] Recognizing the increasing levels of systemic risk and adoption posed by digital assets, policymakers have repeatedly called on Congress to act.[49] In 2022, we expect more regulatory guidance and supervisory action to address the uncertainty and lack of clarity and consensus that currently exists among US regulatory agencies on the future treatment of digital assets. We also expect regulators to use existing supervisory powers where possible. Some key questions that will come into focus in 2022 include:

- Which digital assets are securities?
- Which regulators should supervise what?
- How should stablecoins be regulated?
- How should regulators engage with the DeFi space?
- What is the role of central bank digital currencies (CBDCs)?
- What are permissibility and supervisory expectations across crypto products?

Additionally, the novel and complex nature of digital asset products (e.g., underlying blockchains and use of smart contracts) requires regulators to revisit risk, capital, and compliance frameworks to ensure they evolve with the category's unique risks.

For crypto native companies and fintech companies outside the current federal banking regulatory perimeter, regulators are concerned that the lack of regulatory supervision makes the space highly susceptible to financial crimes and criminal activities, market manipulation, antitrust behavior, and consumer protection issues. The President's Working Group (PWG), in November 2021, released its *Financial markets: Report on stablecoins*, which acknowledged the fundamental gaps in prudential authority over stablecoins used for payment purposes.[50] The report calls on Congress to enact legislation that creates a cohesive federal framework for stablecoin regulation, including imposing bank-like prudential standards on stablecoin issuers and any entities that facilitate the arrangement.

Driven by these concerns, federal banking regulators have issued a forward look at expected areas of regulatory clarification in 2022. The joint statement from the FRB, OCC, and FDIC—as well as an interpretive letter from the OCC—signal to banks operating in the space that they should expect new compliance and regulatory obligations in conjunction with clarification of regulators' expectations.[51] In the case of the OCC, all permitted cryptocurrency, distributed ledger, and stablecoin activities at national banks are expected to require a non-objection prior to launching.[52] Additionally, the Financial Action Task Force (FATF) released its *Updated guidance for a risk-based approach: Virtual assets and virtual asset service providers*, which clarifies the definitions of virtual assets (VAs) and virtual asset service providers (VASPs), and provides guidance on standards, money laundering risks, and registration.[53]

In 2022, we expect more regulatory guidance and supervisory action to address the uncertainty and lack of clarity and consensus that currently exists among US regulatory agencies on the future treatment of digital assets.

State regulators also highlight the strong multi-state coordination role played by the Conference of State Bank Supervisors (CSBS), which includes a national mortgage licensing system now leveraged across multiple state license types, the drafting of model laws, and coordinated multi-state examinations of money transmitters and other licensees.

US federal banking regulators have called for legislation to address stablecoin issuers and other crypto asset participants, and to bring these participants inside the regulatory perimeter.[54] They have further signaled their intent to provide greater clarity throughout 2022 regarding crypto asset activities conducted by banks.[55] Historically, significant US federal banking legislation that introduced new or additional regulation (as opposed to deregulation-focused legislation) has followed some sort of financial crisis.[56] In the absence of such a crisis in the crypto asset markets, it remains to be seen whether significant US crypto asset legislation will emerge in 2022 as a response to concerns expressed by federal banking regulators.

the regulatory perimeter.[57] This is consistent with a general leveling up on governance, risk, and compliance practices across banks and non-banks.

At present, there are two key touchpoints between federal/state governments and digital assets: (1) regulated financial instruments (e.g., deposits, futures, and securities) and (2) regulated entities (e.g., banks, broker-dealers, and money transmission entities). The legal classification of specific digital assets and services will determine the extent of regulatory authority in this area. Firms should be cognizant of the evolving definitions and ensure they are complying with relevant regulations, lest they find themselves targeted with regulatory action in 2022. The PWG stablecoin report should have the entire ecosystem on alert, with firms in the space closely monitoring the situation, planning for intensifying scrutiny, and pro-actively engaging with regulators.

Given the current lack of regulatory clarity on which regulatory requirements and capabilities apply, it is critical for banks and non-banks to comply with the

In 2022, regulators will take a more active role in regulating digital assets, and we expect to see more transparency in supervisory actions and rulemaking. We expect federal and state regulators to use the full extent of their authority to further regulate crypto in the months ahead.

Without legislation, regulatory policy, and supervisory approaches, federal banking regulators will likely establish interim standards. In addition to federal banking regulators, state regulators and securities regulators will also progress in their regulation and supervisory policies. Barring new legislation, standards, and policies on crypto asset matters, the resulting responsibilities of the banking agencies, timelines for development or implementation of rules and frameworks, and the magnitude of potential impacts on the current state of supervision are unknown.

The increased participation of crypto natives and fintech companies operating digital asset products and services outside the federal bank regulatory perimeter has also drawn regulatory attention, raising debates on licensing, supervisory structure, and proper usage of the term "regulated" with regards to digital assets companies' promotional material. Further, with TPRM guidance being finalized, we expect supervisors to increase their scrutiny of banks that provide or receive services to or from firms that are not currently operating within

spirit of existing safety and soundness expectations. We expect banking regulators to heavily scrutinize new digital asset product launches, placing a heavy emphasis on TPRM. Priorities include ensuring early and frequent regulatory engagement; demonstrating use of existing control frameworks (e.g., new product approval); improving alignment with the organization's overall strategy and risk appetite; and ensuring the board and senior management are resourced and equipped to undertake these initiatives. Flexibility will be essential as the rules unfold, and firms will need to respond quickly.

In 2022, regulators will take a more active role in regulating digital assets, and we expect to see more transparency in supervisory actions and rulemaking. We expect federal and state regulators to use the full extent of their authority to further regulate crypto in the months ahead. The frenetic pace at the end of 2021 should only pick up in 2022, with an initial focus on using existing tools that supervisors have the authority to deploy.

When focusing on **digital assets**, banks should consider the following key takeaways:

Remain proactive.

If you are engaging in digital assets products, deploy the full suite of "safety and soundness" controls (e.g., new product approval), and engage regulators early and often to ensure the products are permissible and viable.

Do not ignore.

Crypto and digital asset adoption is widespread. Bank boards and management teams should be engaging with the asset class and understanding how they will respond and engage. The landscape is still in flux regarding the classification of digital assets, their unique risks, the opportunities they present, and other foundational topics. Having a clear sense of where it wants to go will help an organization figure out how to get there despite parameters continually changing.

Be alert.

Stay engaged with new rulemaking, supervisory expectations, and the potential of a CBDC as it may have impacts on how payments are made and managed through the banking system.

Expect Change

Cryptocurrencies and other digital assets are revolutionary game-changers that will force regulators to take a fresh look at how to enforce expectations of safety and soundness in the regulated environment.

Climate

We expect US financial regulators to continue accelerating their climate response in 2022. Executive Order 14030 mandated that the FSOC produce a report on its plans for addressing climate change.[58] FSOC's October 2021 report is a major step forward in that it identifies climate change as "an emerging threat to the financial stability of the United States."[59] It also creates a road map for agency action in 2022. The report notes that many businesses, including large banks, have historically "viewed climate change through a social responsibility lens, instead of a financial risk lens."[60]

However, the shift to the new perspective is now underway with the OCC leading the charge for US regulators. In December 2021, the OCC issued draft principles to guide large banks in the management of exposures to climate-related financial risks, with the expectations that comments on the preliminary framework would be provided by February 2022.[61]

Critically for banks, the report opens the door to future climate stress tests. In 2022, we expect the FRB to issue guidance on what a climate stress test might look like. In September 2021, the Federal Reserve Bank of New York issued a paper on climate stress testing, and the paper's underlying research might inform the development of anticipated guidance from the FRB perspective.[62] Recent testimony by Federal Reserve Chair Jerome Powell suggests that climate stress testing will serve as a key supervisory tool in the future. Since the FSOC report maps climate risks to banks' traditional risks (credit, liquidity, etc.), any proposal for a climate stress test will likely continue to leverage those traditional risk categories.

We expect regulators will seek to improve the quality of data that could inform such tests in 2022. Also, they will likely continue assessing needs and are likely to embark on cross-agency information-sharing arrangements. Banks will be expected to support these efforts to the same extent they do for other types of regulatory data.

When focusing on **climate** as an emerging issue, banks should consider the following key takeaways:

Embrace climate change as a contributing factor to financial risk.

This view is becoming more commonly accepted in the regulatory space, as evidenced by the OCC's ANPRM outlining *Principles on managing climate-related risks*.

Anticipate the impact of climate stress testing.

The addition of climate stress tests, whether supervisory or company run, will have an impact on existing models, systems, processes, and resources. Capacity building in this area will put banks in a proactive position to address any future expectations.

Focus on the data.

Data sourcing, segmentation, and overall quality will be increasingly important in banks' stress testing, forecasting, and strategic planning efforts.

Looking ahead

The year ahead will see continued calls for banking regulators in the United States and globally to determine prudent approaches to key risks facing the banking industry and the expanding regulatory perimeter. However, regulators' expected actions in several key areas remain in the balance, and questions about the pace of interagency work and international coordination are uncertain.

The introduction and use of digital assets, with specific emphasis on innovations tied to cryptocurrencies, is revolutionary and pinpoints an unprecedented time in the history of banking. In response, regulators are in the process of determining the best way to develop frameworks to regulate such assets (and what the frameworks should cover). They are also working to determine their regulatory authority over supervisory activities.

Accordingly, banks and non-banks need to remain vigilant in their efforts to fortify basic risk management practices while also understanding the impact of changes to the banking perimeter and the associated regulatory perimeter. Although the banking perimeter will remain intact, its scope may expand over time to account for developments in the banking sector. Regardless, matters of bank resilience, systemic risk, and financial stability will undoubtedly factor into both regulatory and corporate decision making for the future.

In a shifting landscape where the speed of innovation exceeds that of regulatory execution, 2022 presents an opportunity for banks to reposition themselves in the financial system. Maintaining a focus on the core tenets of effective risk management while also focusing and capitalizing on the evolution of banking will help banks navigate the regulatory environment while positioning themselves for the future.

To plan for the future, banks will need to assess their current capacity, appetite for adaptation, and desired organizational future state. Consideration of short-, medium-, and long-term business strategies (and corresponding risk tolerances) will inevitably have an impact on banks' outlooks and future performance, increasing the value of informed strategic insight and direction. As in the past, strategies will continue to be bound by the regulatory perimeter; however, banks' increased options in the marketplace are expected to give them more freedom to differentiate themselves and achieve their strategic goals.

Banks should adopt a flexible posture assessing and improving the effectiveness of their existing governance, risk, controls, and data processes, while also ensuring the incorporation and implementation of new or revised requirements. Although the details of future legislation, regulation, guidance, and supervisory examination priorities and expectations remain unclear, the increased use of data to better inform the identification, measurement, and monitoring of various risks is inevitable.

Endnotes

1. Alison Auginbaugh and Donna S. Rothstein, "How did employment change during the COVID-19 pandemic? Evidence from a new BLS survey supplement," *Beyond the Numbers: Employment & Unemployment* 11, no. 1 (US Bureau of Labor Statistics (BLS), January 2022).
2. Office of the Comptroller of the Currency (OCC), "Michael J. Hsu to become Acting Comptroller of the Currency May 10, 2021," news release, May 7, 2021; Board of Governors of the Federal Reserve System (FRB), "Randal K. Quarles submits resignation as a member of the Federal Reserve Board, effective at the end of December," press release, November 8, 2021; FRB, "Richard H. Clarida announces his intention to resign from the Board of Governors of the Federal Reserve System on January 14, 2022," press release, January 10, 2022; Federal Deposit Insurance Corporation (FDIC), "FDIC Chairman Jelena McWilliams announces her resignation," press release, December 31, 2021.
3. US Senate, "Roll Call Vote 117th Cong. 1st Session – Rohit Chopra, of the District of Columbia, to be Director, Bureau of Consumer Financial Protection for a term of five years," September 30, 2021.Brian Fung, "Cyberattacks are the number-one threat to the global financial system, Fed chair says," CNN, April 12, 2021.
4. Nicholas K. Tabor, Katherine E. Di Lucido, and Jeffery Y. Zhang, "A brief history of the U.S. regulatory perimeter," Finance and Economics Discussion Series 2021-051 (Washington: Board of Governors of the Federal Reserve System, August 2021).
5. Questions on payment system risk and systemic risk in relation to prospective increases in the use of stablecoins for payment purposes have also raised concerns among regulators. Of note is the absence of stablecoins from existing regulatory and supervisory frameworks and the charge for lawmakers to set forth encompassing legislation. See, for example, President's Working Group on Financial Markets, FDIC, and the Office of the Comptroller of the Currency (OCC), *Report on stablecoins*, November 2021.
6. This outlook is as of the date of publication and is, of course, subject to change based on subsequent regulatory actions, as well as potential changes in regulatory agency leadership.
7. With limited exceptions, companies that control FDIC-insured depository institutions (IDIs) are bank holding companies that, together with their non-bank subsidiaries, are subject to comprehensive consolidated federal supervision by the FRB. IDIs can be chartered at the federal or state level, and together with their operating subsidiaries always have a primary federal banking supervisor (FRB, OCC, or FDIC). Foreign banks operating within the United States may opt for a state or federal license but in all cases are subject to an overlay of FRB regulation, supervision, and examination. Limited purpose federal trust companies are chartered and supervised by the OCC. The CFPB provides oversight for certain consumer compliance laws at IDIs with more than $10 billion in assets. For a more comprehensive outline of banking charters and the corresponding permissibility of activities see our previous publication, "So, you want to be a bank…now what?"
8. CoinMarketCap, "Top stablecoin tokens by market capitalization," accessed January 7, 2022; The Block, "Gross value locked of smart contract platforms," accessed January 7, 2022.
9. Ibid.
10. Michael J. Hsu, "Modernizing the financial regulatory perimeter," Fifth Annual Fintech Conference, Remarks before the Federal Reserve Bank of Philadelphia, November 16, 2021.
11. New York State Department of Financial Services (NYDFS), "Virtual Currency – Information for Applicants," accessed January 7, 2022.
12. Deloitte analysis based on data pulled from S&P Capital IQ.
13. CoinMarketCap, "Top stablecoin tokens by market capitalization"; The Block, "Gross value locked of smart contract platforms"; Financial Stability Oversight Council (FSOC), *2021 annual report*, accessed January 7, 2022.
14. Estimated regulatory settlements and operational losses (including implicit costs such as cost of remediation, business interruption, loss of customer confidence, and others) incurred by G-SIBs and other select risk incidents occurring from January 2020 to August 2021.
15. FRB, "SR 21-3/CA 21-1: Supervisory Guidance on Board of Directors' Effectiveness," February 26, 2021.
16. Ibid.
17. Consumer Financial Protection Bureau (CFPB), "CFPB orders tech giants to turn over information on their payment system plans," press release, October 21, 2021.
18. Financial Crimes Enforcement Network (FinCEN), "Enforcement actions," accessed January 7, 2022.
19. FinCEN, "FinCEN seeks comments on enhancing the effectiveness of anti-money laundering programs," press release, September 16, 2020.
20. Ibid.
21. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong. (2019–2020).
22. FinCEN, "FinCEN Issues First National AML/CFT Priorities and Accompanying Statements," accessed January 7, 2022.
23. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong. (2019–2020).
24. FinCEN, "FinCEN issues proposed rule for beneficial ownership reporting to counter illicit finance and increase transparency," press release, December 7, 2021.

25. FRB, CFPB, FDIC, National Credit Union Administration, OCC, and State Financial Regulators, "Joint Statement on Supervisory and Enforcement Practices Regarding the Mortgage Servicing Rules in Response to the Continuing COVID-19 Pandemic and CARES Act," November 10, 2021; CFPB, "CFPB research shows banks' deep dependence on overdraft fees," press release, December 1, 2021; Erie Meyer, "CFPB calls tech workers to action," CFPB, December 15, 2021.
26. CFPB, "Consumer Complaint Database," accessed January 7, 2022.
27. CFPB, "CFPB orders tech giants to turn over information on their payment system plans."
28. CFPB, "Supervisory Highlights," Issue 25, Fall 2021.
29. OCC, "Acting Comptroller discusses reforming overdraft programs," news release, December 8, 2021; CFPB, "CFPB research shows banks' deep dependence on overdraft fees."
30. OCC, "Acting Comptroller discusses reforming overdraft programs."
31. CFPB, "Enforcement actions," accessed January 7, 2022.
32. Ibid.
33. FRB, "Senior Loan Officer Opinion Survey on Bank Lending Practices," accessed January 7, 2022; FRB, "Federal Reserve Board releases results of annual bank stress tests, which show that large banks continue to have strong capital levels and could continue lending to households and businesses during a severe recession," press release, June 24, 2021.
34. FRB, "Federal Reserve Board releases results of annual bank stress tests, which show that large banks continue to have strong capital levels and could continue lending to households and businesses during a severe recession."
35. Basel Committee on Banking Supervision (BCBS), "Governors and Heads of Supervision announce deferral of Basel III implementation to increase operational capacity of banks and supervisors to respond to Covid-19," press release, March 27, 2020.
36. US Department of the Treasury, "Financial Stability Oversight Council releases 2021 Annual Report," press release, December 17, 2021.
37. FRB, "Federal Reserve Board finalizes rules that tailor its regulations for domestic and foreign banks to more closely match their risk profiles," press release, October 10, 2019.
38. Federal Financial Institutions Examination Council (FFIEC), "Financial regulators update examiner guidance on financial institutions' information technology architecture, infrastructure, and operations," press release, June 30, 2021.
39. FSB, *Lessons learnt from the COVID-19 pandemic from a financial stability perspective*, October 28, 2021
40. Brian Fung, "Cyberattacks are the number-one threat to the global financial system, Fed chair says," CNN, April 12, 2021.
41. International Criminal Police Organization (INTERPOL), "INTERPOL report shows alarming rate of cyberattacks during COVID-19," August 4, 2020.
42. RB, *Supervision and regulation report*, accessed January 7, 2022; *OCC, Semiannual risk perspective from the National Risk Committee*, Fall 2021.Federal Reserve Supervision and Regulation Report.
43. *FFIEC Information Technology Examination Handbook*, "Architecture, infrastructure, and operations," June 2021.
44. FFIEC, "Authentication and access to financial institution services and systems," accessed January 7, 2022.
45. FRB, "Agencies approve final rule requiring computer-security incident notification," joint press release from FRB, FDIC, and OCC, accessed November 18, 2021. Computer-Security Incident Notification Requirements for Banks and Their Bank Service Providers.
46. OCC, "Agencies request comment on proposed risk management guidance for third-party relationships," news release, July 13, 2021.
47. FFIEC, "Joint statement: Security in a cloud computing environment," accessed January 7, 2022.
48. FSOC, *2021 annual report*.
49. US Treasury, "President's Working Group on Financial Markets releases report and recommendations on stablecoins," press release, November 1, 2021.
50. Ibid.
51. OCC, "Crypto-assets: Joint statement on crypto-asset policy sprint initiative and next steps," OCC Bulletin 2021-56, November 23, 2021.
52. OCC, Interpretive Letter #1179, November 2021.
53. Financial Action Task Force (FATF), "Updated guidance for a risk-based approach to virtual assets and virtual asset service providers," press release, October 28, 2021.
54. Ibid.
55. OCC, "Crypto-assets: Joint statement on crypto-asset policy sprint initiative and next steps."
56. Gramm–Leach–Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).
57. OCC, "Agencies request comment on proposed risk management guidance for third-party relationships."
58. The White House, "Executive Order on Climate-Related Financial Risk," May 20, 2021.
59. FSOC, *Report on climate-related financial risk: 2021*, accessed January 7, 2022.
60. OCC, "OCC seeks feedback on principles for climate-related financial risk management for large banks," news release, December 16, 2021.
61. Hyeyoon Jung, Robert Engle, and Richard Berner, Climate stress testing, Federal Reserve Bank of New York Staff Reports, no. 977, September 2021.

Contacts

Vik Bhat
Principal | Deloitte & Touche LLP
vbhat@deloitte.com
+1 973 602 4270

Richard Rosenthal
Principal | Deloitte & Touche LLP
rirosenthal@deloitte.com
+1 212 436 7587

Contributors

Pressure on the regulatory perimeter

Tara Wensel
Senior Manager | Deloitte & Touche LLP
tawensel@deloitte.com
+1 718 508 6795

Governance and core risk management

Irena Gecas-McCarthy
Principal | Deloitte & Touche LLP
igecasmccarthy@deloitte.com
+1 212 436 5316

Enterprise compliance and anti-money laundering (AML)

Richard Mumford
Independent Senior Advisor | Deloitte & Touche LLP
rmumford@deloitte.com

Clint Stinger
Principal | Deloitte Transactions and Business Analytics LLP
cstinger@deloitte.com
+1 212 436 7364

Consumer protection

John Graetz
Principal | Deloitte & Touche LLP
jgraetz@deloitte.com
+1 415 783 4242

Paul Sanford
Independent senior advisor | Deloitte & Touche LLP
pasanford@deloitte.com

Capital & liquidity

Alex Brady
Principal | Deloitte & Touche LLP
alebrady@deloitte.com
+1 415 783 5413

Craig Brown
Managing Director | Deloitte & Touche LLP
cbrown@deloitte.com
+1 212 436 3356

Courtney Davis
Principal | Deloitte & Touche LLP
coudavis@deloitte.com
+1 516 918 7322

Corey Goldblum
Principal | Deloitte Transactions and Business Analytics LLP
cgoldblum@deloitte.com
+1 404 220 1432

Data infrastructure and technology resilience

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

Operational resiliency

Julie Bernard
Principal | Deloitte & Touche LLP
juliebernard@deloitte.com
+1 704 227 7851

Sunil Kapur
Managing Director | Deloitte & Touche LLP
sunilkapur@deloitte.com
+1 609 520 2391

Third-party risk management

Suzanne Denton
Managing Director | Deloitte & Touche LLP
sudenton@deloitte.com
+1 212 436 7601

Brian Adams
Manager | Deloitte & Touche LLP
briadams@deloitte.com
+1 980 701 3287

Digital assets

Richard Rosenthal
Principal | Deloitte & Touche LLP
rirosenthal@deloitte.com
+1 212 436 7587

Roy Ben Hur
Managing Director | Deloitte & Touche LLP
rbenhur@deloitte.com
+1 973 602 4233

Tara Wensel
Senior Manager | Deloitte & Touche LLP
tawensel@deloitte.com
+1 718 508 6795

Florian Studer
Manager | Deloitte & Touche LLP
flstuder@deloitte.com
+1 212 436 7787

Climate

Ricardo Martinez
Principal | Deloitte & Touche LLP
rimartinez@deloitte.com
+1 212 436 2086

Austin Tuell
Manager | Deloitte & Touche LLP
atuell@deloitte.com
+1 212 436 5667

Center for Regulatory Strategy

Irena Gecas-McCarthy
Principal | Deloitte & Touche LLP
igecasmccarthy@deloitte.com
+1 212 436 5316

Jim Eckenrode
Managing Director | Deloitte Services LP
jeckenrode@deloitte.com
+1 617 585 4877

Michele Jones
Senior Manager | Deloitte & Touche LLP
michelejones@deloitte.com
+1 212 492 3882

Meghan Burns
Manager | Deloitte & Touche LLP
megburns@deloitte.com
+1 202 220 2780

Kyle Cooke
Senior Consultant | Deloitte & Touche LLP
kycooke@deloitte.com
+1 202 220 2619

Additional contributors

Prateek Saha
Manager | Deloitte & Touche LLP
prasaha@deloitte.com
+1 470 434 4542

Arpita Mukherjee
Manager | Deloitte & Touche LLP
arpimukherjee@deloitte.com
+1 678 256 9363

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.

Deloitte.

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.