4 Regulatory Areas of Focus for Banks in 2022

By Craig Brown, Kyle Duckers, Tyler Langenkamp, Jeffrey Ulmer, and Mike Willhelm

With the continued pressure and increased adoption of banking regulations and data privacy globally and regionally (e.g., the European Union's Markets in Financial Instruments (MiFID II) directive), the impetus for financial institutions to align their organizations with the regulatory environment has never been stronger. Even in areas where there is heightened awareness and no current legislation in process, the writing is on the wall — in this environment, more regulation is coming.

In the wake of every financial crisis, most recently the global financial crisis of 2007 to 2009, consumer and governmental scrutiny of banking increased dramatically. Today, banks are being held to standards beyond financial stability to meet new requirements for the environments in which they work.

Domestic and international regulatory bodies have put out separate guidance outlining their views on the nature of risk in the industry

Key Actions for Banks

For each of the four areas of focus, there are specific action steps banks should be taking now to position themselves to respond to impending legislation.

- With regard to ESG, banks should begin intentionally researching the kind of data they will need to produce and start setting up the systems and processes required to deliver these reports.
- To get ahead of upcoming cybersecurity legislation, banks should continue to conduct penetration testing on a recurring basis and regularly look at their control environments to ensure they are capturing emerging cyber threats.
- Banks should also review their anti-money laundering programs in light of the FinCEN priorities and start preparing to update their operating models, policies, and procedures to account for new regulations.
- The current operating environment is evolving at a pace faster than any other time in history. So continued evolution of the operational risk framework is necessary to mitigate emerging risks.

as well as potential focus areas for future legislation, including data privacy, cybersecurity, and cryptocurrency or digital assets.

To prepare for potential new regulations or interpretations of existing regulations, banks should focus on these four regulatory areas in 2022.

Environmental, Social, and Governance (ESG) Regulations

From 2019 to 2020, climate risk disclosures generally increased across the board among the S&P Global 1200 and the Russell 3000. As of mid-2021, only 20% of U.S.-based corporations voluntarily reported their carbon footprint.

While ESG guidelines in the U.S. have yet to be formalized, global trends toward increased regulation hint at impending domestic legislation. Legislation combined with public calls for improved corporate responsibility underscores a global shift in reporting. In fact, Reuters reports that sustainable finance bond issuance topped $859 billion in 2021 (a 60% increase over 2020).

As the global economy seeks to address the impacts of climate change, as outlined in a recent report by the United Nation's Intergovernmental Panel on Climate Change (IPCC), the European Union is leading the charge in terms of regulations. The bloc's Sustainable Finance Disclosure Regulation (SFDR) and the Corporate Sustainability Reporting Directive are only two laws passed in recent years aimed at improving transparency on ESG investment and making disclosures compulsory.

The International Sustainability Standards Board (ISSB) is set to release a set of standards for disclosing climate-related and sustainability risks. Banks that want to forgo potential missteps and manage their reputational risks should begin formulating a plan for ESG reporting now.

Both the Federal Reserve and the Department of the Treasury have been tasked by the current administration to review specific aspects of climate risk. They are studying the models currently being deployed in Europe and have provided commentary on potential expectations. The recent edict by President Biden has set very finite timelines to have a more in-depth discussion on climate risk.

On Dec. 16, 2021, the Office of the Comptroller of the Currency (OCC) requested feedback on principles for climate-related financial risk management targeted at institutions with $100 billion of assets. The largest banks have worked together with professional organizations to provide feedback on the principles set forth by the OCC in hopes of shaping regulation in a manner consistent with the risk of the organization and in hopes of leveraging existing regulatory frameworks.

Saying you are compliant is no longer good enough. Companies will have to be able to prove any sustainability claims they make.

Cybersecurity Regulations

Cybersecurity is another major area of focus for financial institutions today. With regular breaches common among even the biggest names, consumers are looking for better and more reliable security for their money and financial information as well as disclosures related to all cyber incursions.

With a rapidly evolving threat landscape, security regulations are regularly added or changed to keep pace. Thus, staying on top of cybersecurity legislation requires constant vigilance for financial institutions. The National Institute of Standards and Technology (United States) and International Organization for Standardization are the primary frameworks used for creating appropriate cybersecurity standards.

The General Data Protection Regulation (GDPR), Sarbanes-Oxley (SOX) Act of 2002, Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, Dodd-Frank Act, and California Consumer Privacy Act (CCPA) are just

five of the more commonly known laws in place today. However, there are several others globally that will impact U.S. banking operations. The U.S. Federal Trade Commission (FTC) has also announced plans to require disclosures of cybersecurity attacks.

The sheer complexity of this regulatory landscape can make enforcement a challenge, but oversight groups are beginning to crack down. Several financial institutions have been in the news in recent years with regard to fines and mediation of their reporting deficiencies, data breaches, and cybercrimes, etc. Additionally, banks face significant reputational risks from cyberattacks and therefore should focus considerable attention on their information security controls and create a culture of transparency related to risks and incidents.

Financial Crimes Regulations

Another area where banks are under the regulatory microscope is financial crime. In mid-2021, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued a list of national priorities for the U.S. aimed at countering these activities:

- Corruption
- Cybercrime
- Terrorist financing
- Fraud
- Transnational criminal organization activity
- Drug trafficking organization activity
- Human trafficking and human smuggling
- Proliferation financing

Federal banking agencies (The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the OCC) have signaled their plans to review and update their individual anti-money laundering (AML) regulations to incorporate these priorities.

While not required to make immediate changes to their programs, banks should begin considering how they incorporate the priorities into their risk-based Bank Secrecy Act (BSA) and AML programs. The guidance offered by FinCEN will be helpful for banks in formulating their responses to the coming updates to domestic financial crime regulation. Doubling down on innovation in areas like transaction monitoring, suspicious activity reporting, and sanctions screening can not only help financial institutions comply with any new legislation but will help support the U.S.' role in the global fight against money laundering and terrorist financing.

Emerging Risk

Banks' active management of risk and return has never been more important or under more scrutiny by regulators. Risks related to creditworthiness, capital adequacy, liquidity, ESG, cybersecurity, financial crime, and rate risk exposure are still top of mind for the entire industry.

Much like the post-2008 era brought on stress testing and other required measures, the COVID-19 pandemic, recent international tensions, and climate change (among other current global influences) will also likely impact the financial and operational health of banks. New and additional data attributes will be required in real time in order to understand the scope and amount of risk in financial systems and allow for timely management of emerging risks while keeping leadership and regulators informed.

Also expect to see more scrutiny of the models used to measure historical data and forecast future performance. Can the models banks use be validated against actual results? How are these models controlled in the organization like any other accounting or reporting system? What was once the domain of open-ended spreadsheets and free-form modeling tools will now need to be used in a much more controlled manner.

The new dynamics brought on by the pandemic, the introduction of digital assets into the financial system, the expansion of artificial intelligence,

and the emerging geopolitical landscape have introduced new and unique operational risks into the financial services system. Given the continued emergence of these activities, the operational risk landscape for financial services will require the continued evolution of mitigants and controls, data and reporting capabilities, and enhancements to existing policy and framework.

huronconsultinggroup.com