

A man with a beard and mustache, wearing a blue suit jacket over a light blue shirt, is shown in profile from the chest up. He is looking down at an ATM screen and has his hand on the keypad. The ATM is red and has a perforated metal screen. The background is a blurred outdoor setting. A large, dark, semi-transparent diagonal shape covers the left side of the image, serving as a background for the text.

INSIGHTS FROM THE BDO FINANCIAL INSTITUTIONS & SPECIALTY FINANCE PRACTICE

**EVOLVING COMPLIANCE
REPORTING
WHAT FINANCIAL
INSTITUTIONS
NEED TO KNOW**

BDO[®]

The regulatory landscape for financial institutions and financial services companies is ever evolving. Consumer behavior and expectations are primary catalysts for new or amended regulation. Consumers expect their data to be secure; they also expect their banks and financial partners to hold corporate values that reflect their own.

Reporting requirements are shifting to reflect this landscape. Banks and other financial institutions should pay close attention to changing reporting requirements related to data privacy and ESG: two key areas where the industry will see clear calls for action in the months and years ahead. Those financial services companies that devote resources to implementing best practices and robust compliance programs will position themselves for continued growth and customer loyalty.



Areas of focus for the coming year

DATA PRIVACY PROTECTION

New reporting requirements follow mounting pressure from customers and shareholders, as well as increased scrutiny from regulators such as the Security and Exchange Commission.

Data privacy protection: Banks have long been popular targets for cyberattacks and breaches. The frequency with which these incidents occur is increasing; in 2022, the cost of cyberattacks [reached \\$18.3 million annually](#) per organization.

Digital banking: The growing use of technology-enabled processes exposes banks to new data privacy risks and responsibilities. BDO's 2021 Financial Services Digital Transformation Survey found that [84% of banks](#) currently offer a mobile banking option. As most consumers, especially younger customers, opt for online banking, financial institutions must protect their clients' personally identifiable information. This will require iterating on current processes and programs—as hackers' tactics evolve, so should a bank's defenses.

At the same time, lawmakers are addressing privacy concerns at the state and federal level. In 2021, The Federal Trade Commission announced updates to the Safeguards Rule, which put enhanced parameters in place for financial institutions' cybersecurity programs. In April 2022, the SEC proposed new disclosure rules that would "reduce the time in which companies must disclose a breach to a mere four days after deeming it material," [according to data security providers like Spirion](#).

Chief information security officers (CISOs) have more recently focused on "corporate data and systems impacts." But under the proposed SEC disclosure rule, CISOs will need to maintain open lines of communication with their boards, disclosing any breach to the board within one to two days of discovery to "determine whether the incident is material." If so, disclosing the breach within that four-day window becomes paramount for compliance.

Additionally, a new rule regarding notification requirements for FDIC-supervised banks and their service providers was issued at the end of 2021 by the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve, and the Office of the Comptroller of the Currency. Under this rule, which went into effect in May of 2022, the FDIC must be notified as soon as possible – no later than 36 hours – if a computer security incident occurs that has been elevated to the status of a notification incident. A notification incident is a computer-security incident that has already or is likely ["to disrupt or degrade" banking services](#).

As regulators increase their focus and propose new rules such as these, banking executives should consider whether their data breach response program is sufficiently robust, accurate and timely.



ESG

A demonstrable commitment to ESG is quickly becoming imperative for banks. Though lawmakers are working on standardized rules and reporting requirements, one unified reporting framework for U.S. banks does not yet exist. Banks must wade through a sea of rules and reporting frameworks, most of which are voluntary in nature.

Many financial institutions opt into ESG reporting because corporate ESG initiatives are closely tied to expectations of key stakeholders, long-term profitability, greater access to capital, improved resilience and risk mitigation. Some banks, such as Bank of America and Citi Bank, have joined together in the [Net-Zero Banking Alliance](#) to demonstrate their commitment to ESG standards and "align their lending and investment portfolios with net-zero emissions by 2050."

Financial institutions expect disparate frameworks will converge overtime, as a result of the efforts of standard setters such as the International Sustainability Standards Board, to offer corporate guidance on ESG reporting, planning and decision-making. Of note, in March 2022, [the SEC proposed a new rule](#) that would establish mandatory climate-related disclosures, with a focus on environmental impact, for public companies to report on their climate-related risks. This would include disclosure of a registrant's greenhouse gas emissions. Further, the SEC is expected to issue a proposed disclosure standard on Human Capital in the ensuing months.

DON'T FORGET ABOUT FASB

Outside of the priority areas of data privacy and ESG, private financial institutions are also expected to maintain a keen focus on rule changes from the Financial Accounting Standards Board (FASB). Private companies should be aware of additional reporting requirements, such as the [ASC 842](#) update on lease accounting that went into effect in early 2022.

In a move away from traditional GAAP reporting, ASC 842 will largely eliminate off-balance sheet reporting. This will likely lead to more liabilities on a company's balance sheet. The goal, according to FASB, is to establish more transparency related to leasing transactions and augment disclosure requirements. Because ASC 842 is still fairly new, impacted institutions should regularly reassess their compliance with the new requirements.

Other compliance reporting mandates to consider throughout 2022 and into 2023 include Know Your Customer and Anti-Money Laundering programs and processes.

MOVING FROM LIBOR TO SOFR

Finally, it is worth noting one other regulatory change banks have been working on for some time: the move from the London Interbank Offered Rate (LIBOR) to the Secured Overnight Financing Rate (SOFR). This rule went into effect and had to be completed by the beginning of 2021. The most notable difference between these two rates is how they are produced. While LIBOR is based on panel bank input, SOFR is a broad measure of the cost of borrowing cash overnight, collateralized by U.S. Treasury securities, in the repurchase agreement market. By the end of the second quarter of 2023, banks will no longer have to submit the information that has traditionally been required to calculate USD LIBOR.



Reporting Best Practices

DATA PRIVACY PROTECTION



Document data breach response programs and reassess them often to ensure programs are robust, as well as up to date with the latest regulatory requirements coming from multiple regulatory bodies.

Develop customer notification programs and processes that adhere to strict reporting compliance guidelines and allow the banking organization to quickly identify those impacted by a breach and then efficiently contact them with pertinent details.

Communicate new and/or shifting regulatory expectations and reporting requirements to all stakeholders, which should and often does include the CFO, CISO, CCO, CLO/General Counsel and/or the board.

ESG



Implement specific ESG policies and related reporting processes

- ▶ These could include climate-risk disclosures, sustainability reports and/or human capital disclosures, pending updated reporting guidelines



Assess internal resources needed to incorporate ESG practices into annual reports and other regulatory disclosures. These steps may include:

- ▶ Developing a cross-departmental process
- ▶ Conducting an ESG risk assessment
- ▶ Amending financial statement and earnings impacts

PREPARING FOR THE REGULATORY ROAD AHEAD

As regulators continue to scrutinize the financial services and banking industry, companies must prioritize data privacy protection and ESG reporting to maintain regulatory compliance. Amid new reporting expectations and complex compliance requirements, financial institutions are rising to the occasion. More and more banks are meeting the moment to capture new market share, meet shifting customer expectations, embrace transparency and increase sustainability.

Consider working with an experienced third-party advisor to help navigate the landscape of financial compliance. BDO's professionals can help your organization implement new technology and security protocols, establish an ESG framework and finetune reporting processes. We'll work with your team to help make your organization a cut above.

People who know
Financial Institutions, know BDO.
www.bdo.com/financial-institutions



ABOUT BDO

At BDO, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the U.S., and in over 160 countries through our global organization, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. www.bdo.com

Material discussed in this publication is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2022 BDO USA, LLP. All rights reserved.