The Top 10 Topics for Audit Committees to Consider in 2022

By: Jon Tomberlin, Lauren Callahan, and Amanda Sterwerf

After an unusual two years of the COVID-19 pandemic, Americans are starting to adjust to the new normal of continued remote and hybrid work environments and moving forward as new and expanding regulatory, financial reporting, and tax changes take effect. To prepare for the year ahead, financial institutions' audit committees should consider the following top 10 topics to discuss with management teams, internal and external auditors, and other advisors. As many of the topics are the result of a fast-paced, changing landscape in a variety of aspects, it may be time to assess the potential need for third-party assistance or personnel enhancements to obtain the requisite skill sets and experience needed to effectively manage and address the challenges and risks of today's financial institutions' management teams and boards.

1. LIBOR Transition

With the formal decommission of the London Interbank Offered Rate (LIBOR) as a rate option, financial services organizations are tasked with identifying and amending the millions of contracts referencing LIBOR-based products. Audit committees should closely monitor their institution's progress as it relates to LIBOR transition. The significant steps in that project would include identifying the population of affected contracts, creating a transition plan for each contract or type of contract, and executing that plan and accounting for it appropriately. Be sure to ask your external auditor how your institution compares to your peers in regard to LIBOR transition.

2. Environmental, Social, & Governance (ESG)

It is no secret that ESG is a current hot topic in the financial services industry. Stakeholders are becoming increasingly interested in metrics surrounding an institution's impact in regard to their environmental and social impact as well as details regarding how the organization governs itself and addresses the impacts on these key areas. Rather than wait until reporting requirements are in place, it is important to get ahead of it now. Audit committees do not want their institutions to be scrambling to respond to mandatory reporting requirements. Doing so can lead to a significant risk of errors and other data quality concerns. Audit committees should gain an understanding of where their institution is in their ESG program. In general, most institutions can take a four-phase approach to build their ESG program as follows:

- Assess – Define what success looks like via dialogue with executive leadership, engage with the investment community to understand how they are integrating ESG into investment decisions, identify ESG risks and opportunities, identify ESG KPIs, and determine which reporting framework(s) to use
- Design – Develop an ESG narrative and messaging plan, identify data sources, develop controls for data reliability, design an ESG report, develop a communication plan for different audiences, provide transparency of reporting processes, and evaluate technology solutions for reporting
- Implement – Draft a report, using a structured, machine-readable format; conduct third-party assurance for confidence in reported information; use financial reporting processes as a model for review and approval; finalize and publish the report; execute a messaging plan; and execute a communication plan
- Monitor – Actively seek key stakeholder feedback; measure and refine reporting and messaging based on stakeholder feedback; and develop systems and processes to capture, prioritize, and assign responsibility to address stakeholder feedback

3. Tax Considerations

Tax reform continues to be an important topic for financial institutions. President Joe Biden's 2023 federal budget proposes an increase to the corporate income tax rate from the current 21% to 28%. While this budget proposal has yet to become law at the date of this publication, many financial institutions are planning and modeling for the potential impact.

ESG reporting is growing due to increased interest from stakeholders to steer decision making. The federal government has established credit programs including investments in the rehabilitation of historic buildings, the generation of renewable energy, and the development of affordable housing. As a result, many financial institutions are considering these programs as they can offer not only federal tax credits, but also can serve to achieve ESG or sustainability initiatives.

For publicly held companies, the American Rescue Plan Act added a new subsection to Section 162(m) of the Internal Revenue Code to expand the application of §162(m) to an additional five most highly compensated individuals effective for tax years beginning after Dec. 31, 2026. Many companies will need to model out the compensation of these five additional individuals to assess the realizability of deferred tax assets related to deferred compensation and stock-based compensation.

As an aftereffect of the COVID-19 pandemic, many financial institutions are seeing an increase in the number of employees working remotely. In addition, some institutions are hiring 100% remote employees outside their legacy footprint. These financial institutions should give careful consideration to potential income and withholding tax filing requirements associated with remote employees.

4. Current Expected Credit Loss (CECL)

Regardless of whether your institution is racing toward a January 1, 2023 adoption date or has been living with its new model for some time now, CECL is a topic almost guaranteed to come up at every audit committee meeting.

If you fall into the first category, ask your external auditor: is your institution ahead of, consistent with, or behind your peers with implementation efforts? Has the committee monitored management's implementation plans, such as understanding which loss methodologies will be utilized, what the costs associated with both implementation and ongoing are projected to be, and whether all of the data needed has been collected? Is management on track with their implementation plan, and have potential barriers to achieving milestones been identified? Where does your external auditor think the institution should be in the process? The implementation of this standard continues to require significant effort on the part of management teams, not only within corporate finance departments, but also in collaboration with information technology, risk management, and other relevant parties. Are any changes needed for processes and controls to address the accuracy of adopting the standards and ongoing accounting post-implementation? As institutions begin to implement a new model to address this standard, it is important to remember model risk management throughout the process. The model should be validated prior to accounting standard adoption, and banks should help ensure there is an appropriate risk governance structure in place to manage through the remainder of the implementation phase.

If your institution has already adopted the standard, the audit committee should be closely monitoring any changes that management has made to the model post-adoption. Do the changes align with the approved allowance for credit loss policy that was established at adoption? Many models will require a recalibration or a refresh of key assumptions used periodically. The audit committee should gain an understanding of this process and monitor it closely. The audit committee should be aware of how often the model will be revalidated and should review the results of the validation as well as management's responses to the results. Finally, remediation efforts for any findings communicated to management and/or the audit committee related to the CECL model's controls from their internal or external auditor should be regularly discussed.

5. Cybersecurity

The cybersecurity threat landscape has dramatically changed over the last several years and so has the approach to dealing with these threats. Financial institutions need to begin their journey from perimeter security design to a well-thought-out "zero-trust" network design architecture. This requires significant network architecture design changes to address the risks of a perimeter security design. This means there should be a hard outer shell, *i.e.*, the firewall, and the internal network behind it is soft, more relaxed, and built for ease of use by end-users and network administrators where internal devices are implicitly trusted as being safe. To better understand this, zero-trust architecture design is the paradigm shift of removing the implicit trust from internal network devices, and everything is as if it is on the internet and no longer behind a trusted perimeter firewall. Under this new paradigm, an eventual breach event is "assumed," and the zero-trust network architecture design shrinks the "blast radius" risk of security incidents/compromised devices down to acceptable levels of risk and limits the number of enterprise endpoints and data that can be affected by security incidents like ransomware. Zero-trust network design restricts adversarial threat actors' ability to compromise large numbers of network devices via lateral movement once inside an organization and helps ensure the continuity of business during a security incident like ransomware. We recommend all financial organizations address their zero-trust journey in their long-term IT strategic plan. Phases that should be addressed in the zero-trust journey via the IT strategic plan should include identity and access, endpoint security, network security, governance based on data classification, policy-based controls for all applications, and protecting hybrid, *i.e.*, on-premises and IT cloud environments, infrastructures.

6. Enterprise Risk Governance

Regulatory expectations around risk management programs continue to increase for community banks, particularly those with greater than $1 billion in assets. Institutions should have internal controls, information systems, and internal audit programs that are commensurate with their size, sophistication, and complexity. Emphasis should be placed on several elements, including the implementation of a board-approved risk appetite statement, identification and assessment of risks on a regular basis, and a risk culture framework supported by training across all levels. It is recommended that an annual meeting is held with the entire board and senior management to discuss the bank's risk management practices.

An effective enterprise risk management (ERM) framework should allow senior management to:

- Assess the interrelationships among various risks across the entity
- Make better-informed cost/benefit decisions about risk mitigation efforts
- Think proactively about future risks

Institutions must demonstrate an ability to effectively identify, measure, and mitigate risks from a governance perspective. When institutions develop their ERM framework, it is recommended that all institutions have a "three lines of defense" model, incorporating best practices from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The front-line business unit of a function owns the risk and the relevant controls. The second line of defense should be independent of the front line and is responsible for the ERM framework. The last line of defense is typically an internal audit or any organizational unit that provides assurance of the soundness and effectiveness of controls. All three elements are necessary to promote risk ownership and a stronger risk management culture, while also reducing inefficiencies, gaps, and overlap that often occur.

7. Culture & Conduct Risk

Conduct risk has received increased regulatory scrutiny over the last few years. Regulators have observed shortcomings in the prevailing culture of financial institutions as the root cause for continued misconduct, and regulators hold board members and senior management directly responsible for establishing and maintaining

their financial institution's culture. Institutions have the challenge of integrating conduct risk into existing risk management frameworks to meet regulatory and supervisory expectations. Identifying and maintaining a strong organizational culture begins at the highest levels of management. In terms of generational changes, baby boomers continue leaving the workforce and are replaced with Generation X, Millennials, and now Generation Z employees. A strong culture is critical among all employees to deliver a consistent brand message that customers can trust, and studies show that organizations that encourage ethical behavior are less likely to face misconduct, including financial reporting fraud. A strong culture should include consistent expectations set by the tone at the top, including accountability, effective challenge, incentives, and integrity. With the shift to more companies adopting a remote or hybrid work structure for employees, maintaining a strong ethical culture where employees feel connected to other team members with a shared purpose is even more important due to the complications of employees working in various locations.

8. Regulatory Compliance – Impact of the Russia-Ukraine War

The U.S. banking system has seen impacts from the Russian invasion of Ukraine in February 2022. Banks should ensure Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance programs are well designed to respond to the additional risks the war has imposed on Russian sanctions to prevent civil monetary penalties for noncompliance. Some things to consider are as follows:

- Management should support an effective BSA/AML compliance program to help ensure adequate resources within an organization to carry out their duties in a timely manner
- Review FinCEN's alert of red flags intended to assist institutions in identifying suspected sanctions evasion activity and stress the importance of BSA/AML reporting obligations
- Enhance Office of Foreign Assets Control (OFAC) monitoring to help prevent potential Russian sanction evasions with sanctions compliance programs that are appropriately tailored to a company's size, products, services, and customers

Annual and ongoing training is an important part of any BSA/AML program to help employees understand their role in preventing regulatory violations

9. Emerging Technologies

Audit committees play a critical role in monitoring impacts on financial reporting as it relates to emerging technologies. As institutions utilize more sophisticated systems and applications to process and move data throughout their organizations, it is important to have tools to evaluate and interpret the information generated. The use of IT tools such as artificial intelligence, robotic process automation, blockchain, and more, whether in corporate finance or internal audit, will allow for efficiencies in accounting and reporting and recognize issues or trends within their data. This may enable management to be more proactive in their operations and help them identify anomalies, detect fraud, and identify and assess risks. However, these new technologies can also pose additional threats to the control environment. The Center for Audit Quality (CAQ)'s Emerging Technologies: An Oversight for Audit Committees publication provides various questions that can be asked by your audit committee—whether the company is just starting down the road of looking at potential technologies to utilize, or if these advancements are already part of the company's financial reporting process.

10. Press the Reset Button

As the demands and new challenges imposed on audit committees have increased significantly over the past decade, it is important to make sure a committee is focused on appropriate topics. What may have been a significant risk or issue for a financial institution five or 10 years ago may not be as much of an issue today, but perhaps the

committee is still discussing and reviewing information in unneeded detail. If not already addressed, take some time to review the committee's focus to determine top priorities. In addition, as financial institutions grow in size but are not required by regulation to have a separate risk committee, many have opted to create a separate risk committee. Given continued emerging risks, including cybersecurity and technology, a separate risk committee can be necessary for the board to maintain sufficient oversight in these areas. Ask some consideration questions as your institution assesses current and future needs. Has there been a recent, rigorous self-assessment of the audit committee, including skill sets or expertise that can help with succession planning for future board members? Are the current members engaged and providing sufficient input to contribute as effective committee members? Press the reset button, study the current state of the committee, and prioritize changes that may be needed to establish your committee as best in class.

If you have any questions or need assistance, reach out to a professional at **FORVIS**.