Internal control over financial

ICFR and PCAOB updates: What leaders need to be aware of

With changes in internal control over financial reporting (ICFR), insurance organizations must stay current with emerging and developing issues that may impact their control environment and program. The approach regarding some emerging issues — noncompliance with laws and regulations (NOCLAR); completeness and accuracy of data; automation; and environmental, social, and governance (ESG) and cybersecurity reporting — remains critical.

NOCLAR proposal expands auditor requirements

The Public Company Accounting Oversight Board's (PCAOB) NOCLAR proposal aims to expand auditor requirements for public companies to evaluate potential noncompliance with laws and regulations. The amendments, proposed in early 2023, were open for a two-month comment period that closed in early August.

The proposal essentially expands the requirement of auditors for public companies to identify any noncompliance with laws and regulations with likely material impact on the financial statements. This will involve a judgment call by the auditors as to what is in fact material to the financial statements.

The proposed NOCLAR amendments received substantial feedback and spurred conversations on long-term impact on organizations and internal control processes. There is also the question of conflicts between the proposal and existing rules and regulations by the Securities and Exchange Commission (SEC). If the proposal is issued as a final standard by the PCAOB, then the SEC will also review the broadened scope for auditors and will need to approve the standard before it is effective.

If the proposal is finalized, then one significant effect will likely be additional time and effort on the part of auditors to examine material impacts and potential noncompliance with laws and regulations.

Additionally, it is presumed that management will need to provide information that could encompass documentation of processes, documentation, flowcharts, risk identification, and control/monitoring evidence, which will be subject to audit. This will ultimately increase both auditing fees and internal control and compliance efforts for companies.

Currently, the PCAOB is reviewing feedback received during the comment period, and the timeline and subsequent steps for implementing NOCLAR are unclear. However, likely impact, developments, and conversations need to be on the radar.

> Meeting the NOCLAR requirement is assumed to be a pretty significant effort, including by management. As auditors, it is presumed we will need additional subject matter professional involvement to comply.
>
> — **Scott Stein,** Partner, Audit, KPMG LLP

How leaders can respond: Enable greater collaboration between functions

Due to the differences in laws and regulations across jurisdictions where business is conducted, NOCLAR may make it necessary for lawyers to assist auditors and companies in effectively evaluating compliance. This will involve close interplay between the chief financial officer, chief compliance officer, finance controllership, compliance, and the legal function. Leaders will have a critical role in setting the tone and facilitating the process.

This is also expected to add complexity to the audit process. The substantial increase in auditing and internal control efforts could also raise questions regarding the cost-benefit balance of the proposal.

Continued challenges with completeness and accuracy of data

Observations from ICOFR testing programs and monitoring of comments from external auditors highlight that completeness and accuracy of data used in internal controls continue to be a challenge. In fact, the PCAOB in its annual inspection reports has indicated that the deficiency rate in terms of completeness and accuracy of data is increasing up to an average of 40 percent over the last few years.

This topic takes on even more importance as insurance companies continue to update and transform their legacy processes and systems. So, companies must consider data governance with a focus on the downstream impact, including data feeds, data warehouses/repositories, queries, scripts, and report writers, among other potential impacts.

> An organization should enhance its efforts in validating completeness and accuracy of data used in financial reporting and internal controls. I would challenge that a similar effort should be focused in areas outside of financial reporting, including planning, capital management, and other decision-influencing areas. Automation can help enable effectiveness in this area.
>
> — **Jason Freund,** Partner, Internal Audit & Enterprise Risk, KPMG LLP

How leaders can respond: Understand the opportunity from transformation

System transformations are creating opportunities for management to harness data and review or assess information in different ways. Leveraging the enhanced data governance required by these initiatives, control owners, ICFR programs, and auditors makes it possible to demonstrate completeness and accuracy and enable more continuous monitoring or testing activities, resulting in more timely and enhanced assurance versus a traditional sample-based approach.

Further, the creation of dashboards and reports to identify outliers or exceptions as indicators of the condition of the control environment is emerging.

> Providing observations at points in the project lifecycle and giving various stakeholders an opportunity to address risks and consider the redesign of controls prior to implementation, enables effectiveness and efficiency.
>
> — **Shivakumar Rajam,** Managing Director, Tech Assurance Audit, KPMG LLP

ESG and cybersecurity reporting

ESG reporting requirements continue to evolve and leading organizations are focused on documenting their processes and enhancing their internal controls, including evidence operation effectiveness at an appropriate level of precision.

New rules are also putting the spotlight on cybersecurity and required disclosures. The rules can be classified into three broad categories—cyber incident and reporting, cyber risk management, and cybersecurity, governance, and oversight. With several organizational functions linked to cybersecurity, the onus does not lie on IT alone. Strong emphasis should be placed on both quantitative and qualitative analyses in determining the materiality of cybersecurity breaches or events in an organization's public filings. All internal stakeholders need to be made a part of the transformation journey, so that risks and controls can be better addressed.

How leaders can respond: Integrate key risk-related processes

Leaders must take a proactive stance in integrating these requirements into their financial reporting and risk management processes. This will involve facilitating a collaborative approach between finance, internal audit, IT professionals, and other governance areas (e.g., Disclosure Committee) to assess and address potential ESG and cybersecurity risks.

Navigating the way forward

With the scale of change and compliance, open, transparent communication between external auditors, management, legal experts, and regulators will remain crucial. Assessing likely impacts, breaking functioning siloes, implementing leading practices, and implementing technologies with robust controls can help ensure effective internal controls and financial reporting compliance.

Contact

Jason Freund
Partner,
Internal Audit and Enterprise Risk
jfreund@kpmg.com
KPMG LLP

Scott Stein
Partner,
Audit
scottstein@kpmg.com
KPMG LLP

Shivakumar Rajam
Managing Director,
Tech Assurance Audit
srajam@kpmg.com
KPMG LLP

This information was originally presented at the KPMG 35th Annual Insurance Industry Conference.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**