KPMG

Voice of the CFO

A recurring conversation with CFOs on finance-related issues

June 2024

CFOs tackle enterprise risk management

In our conversations with chief financial officers (CFOs), we're struck by the multiplicity of job duties held by the CFO. While their comfort level may be with profit and loss and the balance sheet, their organizations feel differently. CFOs are also called upon to manage risk with decision-maker responsibilities. Why so? There is a disconnect in managing enterprise risk between functional risk owners and the board and executive team. Boards and leaders lack oversight. CFOs bridge the gap, so risks are prioritized, capital is allocated, and informed decisions by leadership are made. Given the risks that companies face today from economic and geopolitical to cyber and third party, all demand enterprise risk management (ERM). For CFOs, ERM is a hot topic with many different connections and players, as well as consequences for inaction. Along with ERM, CFOs are also dialed in on the latest in climate reporting obligations required by the Securities and Exchange Commission (SEC), as well as other sustainability standards in the US and worldwide.

On the CFO agenda

Identifying and prioritizing risk

A never-ending critical process

Managing enterprise risk

CFO as ERM risk leader

Climate reporting

Striking the right balance

Identifying and prioritizing risk

A never-ending critical process

KPMG LLP (KPMG) sponsored a chief risk officer (CRO) survey with findings on 400 risk areas, including the top risks that cause the most pressure and garner the most funding.

Pressure and funding are of high interest to CFOs. Most identify the most relevant risks to their organizations, prioritizing to a top 10 risks or classifying a handful of risks as top tier that require ongoing risk owners and escalation paths.

Joey Gyengo, who leads enterprise risk management services for KPMG in the US, knows the importance of risk prioritization. "Risks are multifaceted. When you have a third party or cyber incident, for example, you receive 10 different reports on what happened and what went wrong."

That's the value of ERM. It's a more holistic approach to managing risk that accounts for the multifaceted aspect of risk and specifies more structured processes for mitigation. For CFOs, the top risks vary based on the industry their business operates in. For a company with a strong emphasis on employees, talent is a top risk. For another organization, the CFO sees reputational risk entering their top 10 and wonders if the fact that news spreads so much faster today has anything to do with that. For other firms, cyber risk is always on the agenda at the quarterly meeting.

There is consensus among CFOs on a couple of points. One, don't overwhelm the board with too many risks. A better number is three to five. Two, all top risks need risk owners or committees with mitigation plans regularly reviewed and updated.

CFOs with highly regulated businesses have double duty: compliance and risk management. Compliance designed to address a known risk can help lessen risk, but residual risk remains. A CFO for an insurance company devised a way to bridge the gap while accomplishing value creation.

"We have a dual model—check-the-box for regulators, and then we have our ERM program that drives value for the company."

Risk identification and prioritization is a never-ending critical process. Many CFOs perform an annual risk assessment that is reviewed with audit and risk committees. This leads to identifying new risks, new metrics to add, and risks to drop from the list.

Managing enterprise risks

CFO as ERM risk leader

The standard risk management tools include metrics, heat maps, bowtie analysis, tabletop exercises, and scenario planning, as well as various governance, risk management, and compliance platforms. CFOs fund the use of many of these tools, but they differ on whether they employ a CRO.

Joey Gyengo knows the reason for the demarcation. “The more regulated businesses tend to have CROs.” Gyengo believes roles and responsibilities have changed with ERM, like compliance officers picking up risk with their unique perspective and audit leaders sharing their expertise to risk professionals enabling business leaders to be successful.

CFOs armed with risk personnel, risk committees, and risk tools are well equipped to communicate with the board and senior leadership about the status of the ERM program. However, challenges exist. For many, it’s a third party that leads to a cybersecurity incident.

The CFO for a global financial services company shared the fallout from a third-party incident. After disaster recovery and termination of the vendor relationship, it was time for business resumption. In going through that process, the company determined that resuming operations was a key step of managing third-party risk. As an extension of the company, the outgoing vendor was critical to operations and must be replaced.

Another CFO changed their vendor management program. Instead of staffing a large team to manage vendors, they put the onus on vendors to meet the company’s standard for doing business. Other companies may want to follow that logic when onboarding new vendors.

The CFO for a major transportation and logistics company follows a three-step process for managing ERM risks. It’s straightforward:

Step 1: Review last year’s ERM key risks with leaders and cover what’s changed and what’s new.

Step 2: Take outcome from meeting to risk owners and ask, “Do we need to mitigate this? If yes, what’s the plan? If no, do we accept the risk at some level? Mitigation plans are then developed.

Step 3: Check in on mitigation efforts. Have risk owners report to the board.

That three-step process ensures the right risks are addressed, and the board is in the loop.

Climate reporting

Striking the right balance

The current topic of conversation in compliance circles is the SEC Climate Rule currently paused. Does it make sense to conduct some initial prep work or just put it off until the rule moves forward?

Maura Hodge, KPMG sustainability reporting leader, knows the critical dates that CFOs should be aware of.

"The rule is stayed, but the SEC has said they will reconsider the effective date of January 2025 once the stay is lifted. We are watching closely if that means the effective date will be pushed to January 2026 with first reporting coming in early 2027."

Hodge continues: "There are various timing phase-ins on disclosures. Additionally, greenhouse gas emissions disclosures can be filed in the Q2 10Q and just be incorporated by reference in the 10K, giving relief on having to calculate your greenhouse gas inventory faster than you have historically."

For CFOs with global operations, climate reporting isn't coming in the future; it's here. For those doing business in the European Union, compliance with the Corporate Sustainability Reporting Directive (CSRD) may begin January 1, 2025. Closer to home is California's rules on emissions disclosures, which are also effective January 1, 2025.

Angst for CFOs correlates with what is in scope at their companies. International reporting requirements may necessitate hiring an ESG controller.

A CFO reflected on his view of climate reporting. "We're just trying to create a process, make it as simple as possible, and try not to get sucked into details because we're not sure we'll ever be able to deliver high quality doing it this way."

"It takes an extraordinary amount of time and capital to comply with climate rules that add very little value to our shareholders," said a CFO for a global energy service company.

Hodge assures the CFO's approach to compliance with climate rules should be practical. "With CSRD, you can report that you have not set policies, actions, or targets around this, and we don't plan on doing it or plan to accomplish in the next three to five years. Of course, taking this stance brings with it reputational risk, but it allows for a more thoughtful response and timeline."

"Making explicit statements about how the board and management identify, monitor, and mitigate climate risk is the only SEC disclosure that will be required in every case."

Maura Hodge, KPMG Sustainability Reporting Leader

Key considerations

- Review and adjust top risks quarterly or annually based on your company needs.
- Give extra attention to cyber and third-party risks due to higher incident rates.
- Recall that statements on climate disclosures turn into disclosure risks.

Additional resources

2023 Chief Risk Officer Survey
SEC Climate Rule Live Event Series
Podcast: ESG reporting update

Sanjay Sehgal
Principal, Advisory Head of Markets
KPMG LLP
T: 330-283-6187
E: sanjaysehgal@kpmg.com

Joey Gyengo
Principal, Advisory, and US Enterprise Risk Management Solution Leader
KPMG LLP
T: 404-520-5327
E: jgyengo@kpmg.com

Maura Hodge
Partner, Sustainability Reporting Leader
KPMG LLP
T: 617-988-5959
E: mhodge@kpmg.com

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**