The shortfalls of ERM

Why organizations struggle to see the value in enterprise risk management (ERM) and how to transform ERM into value-added decision-making capability: NextGen ERM
Recent crises like COVID-19 have made it evident that the way ERM is organized today is not nearly as effective as it needs to be.

Back in 2008, the value of enterprise risk management was being questioned after the financial crisis which, at the time, was the most significant financial event that wreaked havoc across the globe, negatively impacting organizations of all sizes, across all industries and geographies. Shortly after the 2008 crisis, organizations asked themselves what went wrong and how they could be better prepared for the next crisis. Criticism was that ERM should have better prepared organizations for such an event, but instead it was flat-footed, reactive and focused only on highly likely risks. Because of this, ERM was not effective in signaling or preparing for the 2008 crisis. The question was posed then and could be posed again now with respect to COVID-19: where’s the value in ERM if it didn’t see a major crisis coming?

In the years between these two major crises, many organizations evolved their ERM program to try to address these questions and align with the refreshed COSO ERM Framework in 2017. Some organizations had grand intentions to take ERM to a value-added capability, but only made incremental progress due to competing priorities or not allocating the appropriate resources to make it happen. Other organizations relied on a check-the-box annual risk
Where's the value in ERM?

Some organizations piggybacked on their Internal Audit (IA) risk assessment process, naming the process ERM, but not moving beyond the risk assessment phase. Only a small set of organizations were truly able to make ERM more forward-looking and improve their risk responses and planning. However, since most organizations were not in this small set, and even with enhancements to their ERM programs, like the financial crisis over a decade ago, many organizations were caught by surprise by the effects of COVID-19 on their business.

Multiple crises have made it quite evident that the way ERM is organized today is not nearly as effective as it needs to be. This paper explores the key ERM shortfalls and what organizations need to do to fundamentally transform their respective ERM programs to be forward-looking and focused on delivering the organization’s strategic goals and performance objectives: what we call NextGen ERM.
What’s wrong with ERM?

While ERM affords notable benefits such as providing C-suite risk visibility and supporting board risk reporting, there are three main shortfalls which preclude ERM from providing the value that leadership and boards desire in today’s dynamic business environment.

1. Over-reliance on qualitative assessments

Board of Directors, C-suites, and key stakeholders find themselves asking why pandemic risk was not identified as a top risk prior to COVID-19. At first glance, it seems that ERM completely missed identifying this as a possible risk, but a closer look reveals a more telling story. The reality is that many organizations identified pandemic as a potential risk, but only a few had prioritized it as a top risk (or what is referred to as a Tier 1 risk). The EY AI-enabled research revealed that approximately 20% of S&P 500 organizations included pandemic risk or pandemic-related risk exposures in their SEC Form 10-K Risk Factors Disclosures. Furthermore, during a recent EY Centers for Board Matters webcast, over 1,100 board members were asked the following polling question “Pre-COVID-19, did your board consider a pandemic or potential health crisis as part of its scenario planning?”. Unexpectedly, close to 40% responded yes. Both of these data points beg the question, "why then was COVID-19 considered such a surprise event?" 

The first reason is that enterprise risk assessments, a key component of the ERM process, are qualitative in nature. While ERAs apply structure and use standard rating scales to assess potential risks to an organization, they are still subjective in nature. In best cases, C-suites discuss ERAs in a group forum but are not equipped with objective data to ground their assessments. Consequently, they lean on their institutional knowledge and experiences to ballpark potential impacts to prioritize top risk. The level of assessment rigor is just not enough in today’s dynamic business environment.

While qualitative assessments can be directionally helpful, inherent bias is also a shortfall. A recent study conducted by Duke University polled between 2,000-3,000 CFOs each year over a 6-year period for their predictions of their company’s future S&P 500 returns with an 80% confidence interval, and the actual returns matched the CFOs’ predictions only 38% of the time¹, with the other 62% falling either higher or lower than actual returns. This study concluded that bias of estimation error or overconfidence can lead to improper managerial decisions, such as overallocation of resources and investments.

Leaders who participate in qualitative ERAs are faced with similar biases when estimating the relative impact or likelihood of select risks. Some organizations have augmented their qualitative ERAs to help minimize this bias using data which is encouraging. For example, a fortune 100 food and beverage company leveraged internal data to inform its ERA. The leadership team qualitatively assessed “quality risk” as a risk, but did not include it as a top risk due to the perception that the company had made recent sizable risk mitigation investments. However, when the leaders were presented with internal quantitative data that showed an increase in quality-related complaints in spite of these investments, they quickly did an about face and added quality risk as a Tier 1 risk.

Secondly, qualitative ERAs tend to discount low likelihood risk events without fully appreciating the potential impact of the risk. For example, a 100-year flood can be easily dismissed because it seems so unlikely, but the reality is the magnitude of this low likelihood risk event can be devastating. Compounding this issue, qualitative impact assessments often put too much weight on recent similar risk events. This may explain why pandemic risk was assessed with a potential low impact: the impact rating was erroneously based on SARS or the avian flu, which were recent epidemics, but did not have nearly the same level of widespread disruption as COVID-19, a global pandemic.

Lastly, even if a pandemic was shortlisted as a Tier 1 risk, qualitative assessments are not able to equip leaders with the necessary insights to make risk-informed resource allocation decisions. This shortfall occurs because risk management activities often wane after the annual ERA. If leaders had taken the time to go beyond the ERA and perform scenario analysis around a pandemic risk, the outcome may have been different. Through more detailed analysis in the later stages of ERM and utilizing more quantitative data, leaders may have become more aware of potential ways that a pandemic could influence other risks – such as supply chain, operational integrity, employee retention, debt and liquidity – and therefore they could have been better prepared for the domino effect that one risk may have on other risks. The true value in ERM occurs well beyond the qualitative ERA and requires robust risk response planning and on-going risk monitoring using data and metrics.

² https://corpgov.law.harvard.edu/2018/02/12/ceo-tenure-rates/
Annual assessments do not align with the pace of business today and agile methodologies

The pace of organizational change continues to accelerate. As such, more organizations are employing agile methodologies to act more nimbly and adapt to the environment. Yet many ERM frameworks adhere to static activities that are not positioned to operate in today’s agile-fueled world. The scenarios around which risk happens are changing so fast that the traditional annual ERA becomes outdated very quickly and does not enable organizations to nimbly respond - or be proactive - to changes in their risk profiles.

While most ERAs are conducted annually and, in some cases, align with more frequent Internal Audit’s risk assessments, they are usually not aligned with the pace of change driven by external risk events. Markets, economies, political regimes, regulations and other external factors change throughout the year and many of these dynamics can significantly impact an organization's risk profile. This means that risk mitigation plans that are based on an understanding of a risk exposure from 6-12 months ago can become stale quickly. Without updated analysis of external events, organizations may be severely misunderstanding the appropriateness of their mitigations and even more importantly, may be missing opportunities to capture the risk upside.

In the case of COVID-19, some organizations were able to monitor external factors, anticipate potential impacts to their business, and put in proactive risk mitigation plans to minimize the impact to their operations.

CEO tenure does not align with organization's long-term sustainability

According to Dan Marcec’s research at Equilar, Inc., noted by the Harvard Law School Forum on Corporate Governance, CEO transitions have become more common in the five years preceding 2018. This means that the turnover rate of CEOs has been increasing, while CEO tenure durations have been falling. Average CEO tenure, which is weighted by long-standing CEOs with several decades of service, also dropped in that timeframe, decreasing from 7.5 in 2013 to 7.2 in 2017. With new C-suite leaders coming and going more quickly, the pressure is high to make a mark on the business, drive the strategy and increase profitability - all within a relatively short timeframe. Considering these circumstances, it can be difficult for heads of the business to spend their limited resources to mitigate a future risk, especially for a low likelihood risk or “black swan”, which may occur at a later point in time and may even not occur during his or her tenure.

This CEO tenure phenomena could be mitigated if ERM were integrated into strategic planning activities and C-suite discussions, but that’s generally not the case. Many organizations still are not explicitly aligning risk management with their strategic planning and performance management goals. Instead ERM is often a strategic planning bolt-on and is relegated as a nice-to-have and not a capability that enables strategy and the achievement of performance management goals. Without seeing ERM as a critical capability to understand risk exposure and provide the insights to make risk-informed decisions, C-suites will likely continue to invest their limited bandwidth sponsoring other priorities, leaving a significant gap in ERM sponsorship and capabilities. This miss is a lost opportunity for organizations.

For example, as early as 4Q 2019, a global automotive manufacturer saw potential supply chain disruptions in China that would manifest in early February. This insight resulted in the company expanding production as long as possible during 4Q. To further reduce their supply chain risk exposure, they also flew in auto parts to their factories in Europe in order to continue production, rather than waiting six weeks for a cargo ship to deliver necessary parts. However, many organizations did not have this foresight and were forced to halt operations completely during the COVID-19 lockdowns due to supply chain disruption.
How can organizations turn these ERM wrongs into rights?

While the three points outlined above highlight how ERM may not be providing the value it is capable of, many organizations can change this path going forward with the following transformations:

1. **Build upon qualitative risk assessments to quantitative risk insights**

ERM cannot stop at the ERA anymore - period! Organizations need to embrace an end-to-end risk management focus and employ more rigorous risk response planning and analysis. To put this perspective into guidelines, ERAs consisting of risk identification and assessment activities should not take more than ~10% (less than 1 month of effort) of annual risk management efforts. That means approximately 80% of ERM efforts should be focused on managing the risk through rigorous risk response planning and ongoing risk monitoring using data and metrics. The remaining ~10% is reserved for risk reporting which rounds out an end-to-end risk management program.

Effective risk response planning requires quantitative risk insights achieved through data and metrics - including quantifying risk exposures and/or leveraging forward-looking key risk indicators (KRIs). This is where NextGen ERM comes into play. NextGen ERM quantifies risk exposures using scenario planning and stress testing to equip leadership with the data points needed to understand a range of potential outcomes (e.g., best case, expected case, worst case). NextGen ERM then leverages cost-versus-benefit analysis to understand where to most effectively make risk mitigation investments and how much to invest. Instead of telling leadership a risk (e.g., pandemic or cybersecurity) is a top risk, NextGen ERM transforms ERM discussions by using data to support risk-informed decision-making on how much and where to employ resources to manage risk exposures.

ERM also requires forward-looking risk insights to track mitigation plan effectiveness and support risk escalation routines. That is where quantitative key risk indicators (KRIs) come into play. For each top risk, quantitative KRIs must be defined to help anticipate when a risk might occur. The goal is to put in metrics to help see a risk coming before the risk occurs so that ERM is more forward-looking and less flat-footed. Once established, KRIs then must have clearly defined acceptable thresholds (upper and lower limits) to support risk escalation and risk monitoring routines. In practice, risk owners need to know when and how to escalate risks for leadership discussions and action. KRIs serve as the triggers to support actionable risk monitoring. NextGen ERM has a bias for action, not simply reporting.

Organizational leaders do not want ERM to communicate the obvious - that pandemic or cybersecurity is a top risk. Rather, leadership wants and needs ERM to (1) provide quantitative insights using risk modeling and scenario planning to communicate that a 100-year flood or a pandemic would impact Operating Income 35%-40% and then (2) provide the risk insights, level of risk tolerance and cost-versus-benefit analysis to prioritize risk mitigation investments. Now that’s helpful information for leadership to make risk-informed resource allocation decisions and is an ERM game changer.

2. **Embrace rapid risk assessments to align with the pace of today’s world**

Risk respects no boundaries. ERM must be better positioned to nimbly assess risks in today’s agile-minded and rapidly changing business environment. ERM requires reassessing risks more frequently, more than once per year, to keep a forward-looking posture to identify new and/or emerging risks. Notably, ERAs cannot be done in a vacuum and must incorporate ever-changing internal and external environmental factors as well as consider other organizational risk assessments. For example, many functions such as IA, Compliance, IT and SOX also conduct risk assessments within an organization - and in some cases more frequently than ERM. Recognizing that the stakeholders of risk information are usually the same across the organization will help to drive the function to align their processes and data. Amplifying risk capabilities by using technology and aligning towards a common risk taxonomy, risk tolerances and appetites and driving efficiencies in reporting across all lines of risk can make the risk function more agile overall.

To further enhance rapid risk assessments, leading organizations are leveraging digital collaboration platforms to perform these quick risk assessments to deliver a refreshed risk profile in as short as a week or two. As highlighted above, the real ERM value is in risk response planning and on-going risk monitoring, not an exhaustive ERA, so do it quickly and act upon it.
For example, a leading power and utilities organization undertook a rapid risk assessment immediately after COVID-19 to understand changes to its risk profile. Leveraging this updated risk information, the assigned risk owners were able to adjust their risk mitigation investments and activities to align with the emerging risks. In another example, a global media and entertainment organization used artificial intelligence (AI) to scan the internet and leverage authoritative data sources to assess the external environment. Their objective was to use ‘out of the box’ thinking to identify new potential risks that would impact its industry, market, and geographies and ultimately impact their organization’s risk profile. Essentially, they addressed the question, “Did we miss any potential risks?”.

Notably, in both of these examples, leadership was keenly focused on how new and/or emerging risks would impact their organization’s strategy and performance management objectives and then could quickly use the data to make decisions and inform needed changes to the strategy.

The rapid risk assessments serve another purpose which is to quickly identify potential and/or emerging areas of opportunity. Organizations need to consider how their business can adapt their operations or services to align with changing market needs. For example, a well-known clothing company was able to reconfigure their manufacturing facilities to provide health care workers with needed gowns and supplies during the COVID-19 pandemic. In the recent EY Center for Board Matters webcast event, overall 1,000 participants were asked to vote on how their board could be more effective in the COVID-19 environment. Of the applicable respondents, 33% of them voted that “more agenda time for emerging risks and trends” would make their board more effective, with 23% voting for “more frequent updates to scenario models and forecasts.” Being agile is important to capture new opportunities and in most cases, new opportunities present themselves in a non-annual timeframe. If organizations assess risk only annually, these opportunities may be missed.

In addition, boards and C-suites want and need more from risk reporting. In the same EY Center for Board Matters webcast noted above, 37% participants said that board reporting would be improved by including insights into the “impact of evolving risks on organizational performance” and another 18% indicated that “advancement of predictive and prescriptive risk insights” would be beneficial. A distinct CRO position would help the organization “focus” on top risks and opportunities and “ensure” these risks and opportunities are aligned with the defined, acceptable risk tolerance levels. While other functions may have risk-related responsibilities, there is a heightened focus on risk which a dedicated position would bring. The IA function and many times the chief audit executive (CAE) oversee, or even lead the ERM function. In order to remain independent and provide assurance on the ERM function, it is important to separate the activities and name a CRO separate from the CAE.

In conclusion, it is past the time for organizations to transform their ERM frameworks to be more forward-looking, risk insight driven and quantitative. It’s time to quash the question “where’s the value in ERM” by turning ERM naysayers into ERM advocates by helping the organization see risks coming and enabling the organization to proactively manage the risks and seize upside opportunities. It is time to coordinate risk management activities, including working together with IA and other risk functions to increase the overall value to the organization. It is now time to show that ERM adds real value by enabling strategy and the achievement of performance management goals.

3 Raise ERM’s profile to be a strategy enabler

One major governance enhancement can play a critical role in transforming ERM’s value to organizations. It’s time for CROs to take their seat as a member of the C-suite, broadly across organizations of all sizes and in all industries. While some organizations have appointed a CRO, most do not have this position nor have they added the “R” moniker to a C-suite member’s accountabilities. Carving out this risk-focused executive role is especially important, considering that boards and audit committees have ever-increasing expectations for managing risk which is difficult to incorporate into other C-level roles without overwhelming individuals. In the same example as above, a COO or similar type position may be best positioned to determine if the clothing manufacturing facilities are able to be repurposed, it is the role of the CRO to aid leadership in decision making by informing them of the underlying risks associated with shifting production to the new product. By employing a C-suite role focused solely on risk and a lens on performance and strategy, organizations can create a strong tone from the top about risk and better ensure that the executive team continues to look through a risk-focused lens to enable the achievement of strategic goals and performance management objectives.
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2020 Ernst & Young LLP.
All Rights Reserved.

US SCORE no. 09796-201US
2006-3517771
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com