This thought leadership paper will provide insights and practical approaches to enhance strategic planning by anchoring enterprise risk management (ERM) into existing strategic planning processes and enabling actionable risk-informed decision-making.

**Risk-Informed Strategy is a board priority**

This year, the EY Center for Board Matters published Top priorities for boards in 2019, which highlighted the importance of organizations’ aligning risk management with strategy and operating performance as a key board priority.

Furthermore, it emphasized the need for organizations to fully embrace the duality of strategy. This includes considering the facets of short-term goals against long-term considerations and continuing to build their knowledge bank around fully understanding the intricacies of risk vs. opportunity. The bottom line is, organizations must construct a more resilient strategy focused on delivering performance results and enabling long-term viability while leveraging risk insights gained through enterprise risk management.

The need for organizations to link risk and strategy was further underscored in two recent ERM framework updates:

- The 2018 ISO 31000 ERM framework update emphasizes the need for organizations to further integrate risk and strategy.
- The September 2017 release of the COSO publication Enterprise Risk Management – Integrating with Strategy and Performance, an update to its 2004 publication, similarly highlights the importance of considering risk in both the strategy-setting process and in driving performance.

**The importance of risk-taking**

This emphasis on the role of risk makes sense: risk-taking is fundamental to economic reward. The challenge (opportunity) for organizations is to recognize which risks offer the greatest potential to impact business outcomes and to clearly understand how to manage those specific risks to enhance performance, drive value creation and enable long-term viability.

In practice, effective risk-informed strategy decision-making must answer the following fundamental questions:

- Are we taking the right risks – risks that create value?
- Which strategic risks should we accept and which should we avoid?
- Are we allocating capital on a risk-adjusted basis to optimize our finite resources?
- Are we taking the right amount of risk, and more importantly, are we getting the appropriate return for the risk we have taken on?

**The c-suite expects ERM to play an increasing role in strategy**

Many organizations are now realizing that their strategic planning efforts lack a risk vs. opportunity discipline and an integrated performance management focus. Furthermore, many conventional ERM programs remain largely disjointed from strategic planning – the modus operandi of most businesses. Unfortunately, this disconnect means that ERM is not well positioned to add organizational value by informing business decision-making and ensuring that limited resources are allocated to the most significant
risks. The reality is that most ERM programs have not evolved to enable critical risk-informed investment decisions that align with the organization’s strategic goals and objectives.

EY’s global governance, risk and compliance survey 2015 highlighted that senior leadership still maintains conventional ERM and heat maps which summarize risks simply as red, yellow or green – which offers extremely limited and little value today. In simple terms, ERM is not helping leaders make risk-informed business decisions.

Ernst & Young LLP surveyed over 1,200 business executives across multiple industries, and the results highlighted three specific strategic planning and risk management gaps that must be addressed. These opportunities include:

- More explicit integration in business decision-making
- A heightened focus on strategic and external risks
- An enhanced ability to leverage risk information to adjust business strategy

The underlying issue, according to the survey, is that chief strategy officers, chief financial officers and other executive leaders do not believe ERM is positioned and leveraged to help the business “run the business.” Instead, ERM generally focuses on operational (downside) risks and protecting the enterprise.

Organizations must make a transformative shift from a singular focus on protection to a strategic grow-and-protect business mindset. This shift will enable business leaders to focus on seizing the upside risks that can be realized through risk-informed strategic business decisions – from mergers and acquisitions, to launching new products and services, to expanding into new geographies.

Trust by design: looking at risk identification in the Transformative Age

Efforts to identify and evaluate risks tied to strategic goals and objectives must consider:

- Risks that organizations know well and are capable to prevent or effectively mitigate
- Risks that are recognized as inherent to strategy and demand more focus
- Risks that are not fully recognized and may not be capable to prevent

To enable a strategic risk management framework, organizations must understand the types of risks they will face. There are three key categories of risks: upside, outside and downside. Each of these categories requires a different management approach that will benefit organizations.
Know the three categories of risk

<table>
<thead>
<tr>
<th>Upside risks</th>
<th>Outside risks</th>
<th>Downside risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶ Risks that offer benefits</td>
<td>▶ Risks that offer negative or positive benefits beyond the company’s control</td>
<td>▶ Risks that offer negative impacts</td>
</tr>
<tr>
<td>▶ Risks significant to the company’s ability to execute its strategy and achieve its objectives</td>
<td></td>
<td>▶ Risks a company is focused on eliminating, avoiding, mitigating or transferring in a cost-effective manner</td>
</tr>
</tbody>
</table>

1. **Upside risks** – offer **benefits and present opportunities** to enable business strategy and achieve performance management objectives.
   - They focus on the risk opportunity, “there is no return without risk”.
   - Examples of upside risks that could impact an organization include innovation, technology as an accelerator, and/or expansion into new markets.
   - Upside risks differ from downside risks because they are not inherently undesirable.
   - A strategy with high expected returns generally requires an organization to take on upside (strategic) risks, and effective management of those risks is critical to capture the potential gains.
   - Upside risks cannot be managed through a rules-based control framework. The approach to managing those risks requires the selection of risk-strategic risks to take, such as:
     ▶ Improving an organization’s ability to manage risk events if they occur
     ▶ Establishing risk tolerances
     ▶ Predicting the impact of possible risk events
     ▶ Monitoring of key risk indicators (KRIs)

2. **Outside risks** – risks that arise from events outside of the organization’s control. These risks can **offer negative and/or positive benefits**. Organizations cannot influence the likelihood of these events, but they can be prepared and reduce the cost of an impact. Examples include:
   - Competition
   - Legislation
   - Natural Disasters

   Addressing these risks requires a different approach, one that includes identification and mitigation of their impact through scenario analysis and stress testing to determine whether the organization has the minimum resources to weather the full impact of external events.

3. **Downside risks** – internal risks that arise within the organization that are controllable and should be eliminated or avoided. These risks **present only negative impacts**. Examples include:
   - Cybersecurity
   - Fraud
   - Regulatory noncompliance

   The approach to managing these risks comes through active prevention and designing the controls to mitigate these risks. Much of the investment in the controls framework will be driven by preventable risks. It also provides structured monitoring of the threat level of the identified preventable risk.
Gaining competitive advantage – upside and outside risks

Leading organizations recognize the shortfalls in their risk identification processes – and are consequently educating themselves on the implications of upside and outside risks, particularly as it pertains to strategic planning and performance management.

When it comes to upside risk, they are implementing steps to identify, monitor and proactively manage these risks and seeking out opportunities to leverage the upside potential of these risks. In taking this approach, leading businesses are seizing a competitive advantage by engaging with the various unknown opportunities they will encounter. They’ll then prepare to proactively convert these unknowns into strategic opportunities.

In addition, companies realize that outside risks can threaten the very existence of any organization and can have a significant impact on an organization’s strategy. All companies are exposed to these risks originating from outside their direct sphere of influence. However, companies often struggle to identify them, assess them, and quantify them.

Only a few manage outside threats with the level of rigor that corresponds with the level of potential impact of these risks. Furthermore, many organizations only focus on outside risks that seem obvious – but they fail to recognize the full universe of forces that can affect their business. And importantly, management of outside risks is often disjointed from strategic planning which results in a missed opportunity for more insightful risk-informed resource allocations and capital investments.

Considering these limitations, organizations should shift their mindset to identify the opportunities and challenges presented by upside and outside risks whilst simultaneously embracing risk measurement.

Strategic decision-making and enhanced risk-measurement

The EY approach to ERM is evolutionary, going far beyond strictly value protection and compliance to focus directly on value creation through the integration with business performance objectives and metrics. Having ERM anchored in strategy will not just encompass avoiding or managing threats, but it will also maximize value to enhance business performance and resource allocation for the opportunities that lie ahead.

This approach enables organizations to understand the relationship between performance drivers and the associated range of scenarios influenced by risk drivers. It is achieved through the development of a “Performance Framework” that aligns risks and opportunities with an organization’s strategic imperatives.

To implement this method, it is important to understand:

- What constitutes success as defined by the “Performance Drivers/dimensions”
- How that success is measured via “Performance measures/KPIs”
- The application of performance measures to strategic drivers

This method is an essential toolkit for avoiding scenarios that might result in detrimental impacts to an organization that would be outside the performance appetite, shifting the focus from “cost vs. benefit” to “risk vs. reward.” Overall, management teams will see a benefit by applying this approach to how they make their decisions and the impact of those decisions through a performance lens.

Leveraging risk measurement for risk-informed decision-making

Our vast experience across industries reveals that the relationship and dependencies between strategic goals, underlying value drivers, and related risk factors are not clearly understood. Thus, the selected risk response strategies typically ignore the...
organization’s risk appetite and tolerances. This misalignment means that the risks that have the greatest potential impact to strategic initiatives and/or the competitive viability of the business model could result in a potential loss of competitive advantage.

The reality is that organizations want — and frankly need — ERM to inform business decision-making using data and metrics. This need shift requires organizations to evolve from qualitative to quantitative ERM. To add “measurable” organizational value, ERM must be able to help the organization understand and analyze its risk drivers in relation to strategic objectives. In addition, ERM must help organizations identify the key financial metrics and focus targeted mitigation strategies that will reduce the volatility related to business outcomes and financial performance.

Starting with strategic business objectives, organizations can build a performance driver tree focused on each strategic objective that measurement though outcome measures, Key Performance Indicators (KPI’s), and Key Risk Indicators (KRI’s). This structured approach leverages metrics and risk quantification and allows organizations to identify the critical sources of volatility that can adversely impact its strategic objectives and performance outcomes.

### Performance Driver Tree and Strategic Objectives

<table>
<thead>
<tr>
<th>Strategic Business Objective</th>
<th>Outcome measure</th>
<th>Key Performance Indicator (KPI)</th>
<th>Key Risk Indicator (KRI)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Outcome measures provide an evaluation of overall business performance aligned to the defined strategic objectives</td>
<td>KPIs serve as outcome measures of business operations that align to the outcome measures.</td>
<td>KRI’s provide predictive insight to the level of volatility and resultant uncertainly in the achievement of business objectives.</td>
</tr>
<tr>
<td>Measured by</td>
<td>Goal</td>
<td>Threshold</td>
<td>Lower limit</td>
</tr>
<tr>
<td></td>
<td>Trend</td>
<td>Target</td>
<td>Target</td>
</tr>
<tr>
<td></td>
<td>Variance</td>
<td>Range</td>
<td>Upper limit</td>
</tr>
</tbody>
</table>

### Better risk integration for better benefits

For organizations to fully leverage the benefits of risk measurement, it is essential that they define how this quantitative information is integrated into strategic planning, and more broadly, how the organization makes decisions. Business planning routines such as strategic and annual planning serve as the natural vehicles for organizations to make capital and resource allocation decisions. Keeping this in mind, rather than creating a separate routine, ERM must be seamlessly integrated as an input and output these existing business planning routines, often referred to as the “rhythm of the business.” This practical approach will:

- Enhance the accuracy of risk management analysis to setting strategic objectives
- Strengthen its overall oversight to the risks across the organization
- Align risk with performance management goals by balancing risk vs. reward
- Drive consistency in data gathering, analysis and reporting to the board and executive management
Illustration: Enabling the “rhythm of the business” for informed decisions

<table>
<thead>
<tr>
<th>Strategic plan and financial target development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy and value drivers</td>
</tr>
<tr>
<td>Long-range strategic plan</td>
</tr>
<tr>
<td>Strategic risk assessment</td>
</tr>
<tr>
<td>Strategic initiatives and financial targets</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business planning, budget and forecast process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business-level objectives</td>
</tr>
<tr>
<td>Detailed planning analysis for business plan</td>
</tr>
<tr>
<td>Business-level risk assessment</td>
</tr>
<tr>
<td>Business-level budget, forecast and operating plan</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quarterly business performance review process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarterly revenue and earnings</td>
</tr>
<tr>
<td>Quarterly review against business plan</td>
</tr>
<tr>
<td>Quarterly risk profile review</td>
</tr>
<tr>
<td>Business-level performance measurement</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ongoing performance monitoring and reporting process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined risk response plan for key risks</td>
</tr>
<tr>
<td>Monitoring of progress against plan</td>
</tr>
<tr>
<td>Enhanced risk-based performance metrics</td>
</tr>
<tr>
<td>Ongoing management reporting and business insights</td>
</tr>
</tbody>
</table>

Upside and outside risks won’t wait for you

The business environment is dramatically evolving and will continue to do so at an ever-increasing rate. Organizations must develop more resilient risk-informed strategies focused on delivering performance results and enabling long-term viability. To meet this challenge, they must understand how upside and outside risks could impact their strategic goals and objectives, and leverage risk measurement to make more risk-informed business decisions, including resource allocation decisions.

Biggest risk – ignoring risk

Through explicit integration into existing business planning and management routines, organizations will have a natural vehicle to engage the cross-functional leadership team and establish more risk-informed business decision-making. By not developing and implementing such a risk-informed strategy, leaders are putting the organization in a precarious position. Because of the ecosystem they have created, they can’t see dangerous outside risks before they hit. Simultaneously, they’re missing out on exceptional opportunities within upside risks – ones that could bring game-changing transformation and increasing their competitive advantage. Risks, viewed more holistically, can become rewards. Learn more about how EY is driving strategy for risk management that covers all the bases at https://www.ey.com/en_gl/advisory/risk-transformation.
Questions for strategy leaders and CFOs to consider:

- Are we taking the right risks, and do those risks create value?
- Which strategic risks should we accept and which should we avoid?
- Are we allocating capital on a risk-adjusted basis to optimize our finite resources?
- Are we taking the right amount of risk, and equally important, are we getting the appropriate return?

John Rogula  
john.rogula@ey.com

John Rogula is an Executive Director in the Advisory Risk Transformation Services Practice of Ernst & Young (EY) LLP. He has over 28 years of experience in management consulting and 17 years of ERM experience advising a multitude of healthcare providers, healthcare payers, and life sciences companies.

Phil Maxwell, MBA, RIMS-CRMP  
phil.maxwell@ey.com

Phil is a senior manager in the Advisory Risk Transformation Services Practice of Ernst & Young (EY) LLP. He has over 24 years of broad industry experience in risk management, strategic planning, operations, and finance including an extensive background in enterprise risk management (14+ years) where he built two ERM programs from the ground-up.