COSO

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management

ENABLING ORGANIZATIONAL AGILITY IN AN AGE OF SPEED AND DISRUPTION

By

Dr. Paul L. Walker
James J. Schiro / Zurich Chair in Enterprise Risk Management
Exec. Director, Center for Excellence in Enterprise Risk Management
St. John's University

February 2022

Author

Dr. Paul L. Walker
James J. Schiro / Zurich Chair in Enterprise Risk Management
Exec. Director, Center for Excellence in Enterprise Risk Management
St. John's University

Acknowledgements

This paper benefited from many anonymous interviews.
Those risk leaders were invaluable and graciously shared their insights and wisdom.
I'd also like to acknowledge the help of the COSO Board.

COSO Board Members

Preface

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence.
COSO is a private-sector initiative jointly sponsored and funded by the following organizations:

American Accounting Association (AAA)

American Institute of CPAs (AICPA)

Financial Executives International (FEI)

The Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

COSO
Committee of Sponsoring Organizations of the Treadway Commission

coso.org

Enterprise Risk Management

ENABLING ORGANIZATIONAL AGILITY IN AN AGE OF SPEED AND DISRUPTION

Research Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

February 2022

1234567890 PIP 198765432

Design and layout: SergioAnalco.com.

Contents

INTRODUCTION

The speed of change, disruption, and risk in the environment is changing business and operating models on a scale not seen before. Many organizations have adopted approaches based on agile methodology to help get ahead of the change and disruption. Agile started out as an IT approach with a focus on customer value, but it has gone beyond that and altered entire organizations. All five of the largest publicly valued companies today are considered "agile," in addition to being called tech companies. A broader business view of agility suggests that in a world of volatility, disruption, uncertainty, and complexity, companies respond by using processes, people, and technology to anticipate, see, understand, and respond to a dynamic fast-changing world. This paper focuses on this broader view of agility.

Because agile practices are being used to manage risk in processes and to manage risk at the organizational and strategic level, it is imperative that enterprise risk management (ERM) practices be considered to help organizations meet their objectives and achieve enhanced value as they pursue their mission and strategies in a world that is rapidly changing. The Committee of the Sponsoring Organizations of the Treadway Commission (COSO) 2017 framework, *Enterprise Risk Management – Integrating with Strategy and Performance* (COSO ERM or the Framework), addresses some of these agile areas directly. For example, the Framework addresses the importance of linking risk and strategy and also addresses aligning both strategy and performance across all areas of the business. The Framework is aligned around principles and components (see Figure 1). This document highlights many of the COSO ERM risk principles (Principles) and how they relate to agile. Appendix A provides an overview of the components, principles, and agile implications for each principle.

Figure 1. **COSO *Enterprise Risk Management – Integrating with Strategy and Performance Framework***

2017 COSO Enterprise Risk Management – Integrating with Strategy and Performance

Proper risk management can help make agile practices more successful. When companies are adopting agile practices, they are sometimes changing the culture and sometimes analyzing the new strategic context and trying to pivot to a changing context. Companies practicing agile methods may be reassessing the strategy set because their environment and context is changing so rapidly. At other times, they are moving faster and need to manage the risk but also view the objective and risk in a portfolio. They are, in some cases, taking and creating new risks, which need to be identified, assessed, prioritized, and managed. Many agile companies also feel a need to stay in constant contact with a substantially changing environment, and they need to build processes to assess those changes and the potential new or altered risks. At all times, they are trying to enhance performance and meet or set new objectives. Thus, COSO ERM is valuable because it provides a complete picture of the components, principles, and approaches to apply to risks when agile practices are adopted.

PART I. SPEED, DISRUPTION, AND RISK ARE CAUSING CHANGE

Things have changed — one risk after another keeps smashing the shores of normality. Astute leaders get this and know that long-term strategic plans and assumptions are not the best approach in times like this. Examples of this are everywhere. A recently appointed CEO at a Fortune 100 company changed the company's motto to "Faster, stronger, and better." A chief strategy officer of one of the world's largest energy companies declared, "We've given up trying to predict the future. We just want to be agile." A new CEO of a not-for-profit adopted a strategic vision focused on speed, adaptability, and taking risk. Other headlines in the news have CEOs telling employees to make mistakes and Wall Street analysts warning companies, "Disrupt yourselves, or else!" Further, this occurred before the pandemic, social unrest, political climate, continued calls for climate change, or ESG (environmental, social and governance) action — plus a host of other globally challenging uncertainties. It is not surprising that companies are looking for ways to improve, adapt, and become more agile as they also search for the new normal.

The new normal likely includes new anticipatory risk skills and new agile and adaptability skills. For those responsible for understanding and managing risks — including business owners, enterprise risk management, internal audit, senior leadership, and boards — the new normal includes a rethinking of when, how, and where to apply strategic risk thinking and ERM.

Example 1

A major health and wellness company rolled out a new strategy and vision along with a focus on new markets, scale, and speed. The company sensed that uncertainty was accelerating from linear to exponential and that they needed to respond. The company wanted to change how they worked, including adding such things as robotics. As part of this approach, the company set up an Agile Center of Excellence. The company began to switch from a "plan and act" to an "act and learn" approach, having recognized the difficulty in relying on long-term strategies and emphasizing the importance of agility and learning on a rapid basis. The company wanted to apply agile methods to how they work for both strategic and operating projects to avoid major risks such as getting to the end of a long-term project and finding out the project was no longer relevant or wanted by the customer.

Agile Needs and Practices Influence Strategy and Strategic Thinking

Agile methods can be a way to get things done faster and better and can also be a strategic response to prodigious strategic risk and uncertainty. There are a variety of approaches to the speed of change and uncertainty, including moving faster, working differently, and becoming more agile in many areas. To make changes, companies can leverage COSO ERM's Governance & Culture component and principles relating to rethinking how they approach strategy and oversight (Principle 1), traditional organizational structures (Principle 2), traditional mindset and culture (Principle 3), and how they operate while aligning with their core values.

Agile started out as an IT movement, and later moved into operations, business units, strategy and onto the radar screen of the C-suite and board. Original agile practices included sprints, scrums, and focused, cross-sectional empowered teams moving quickly to solve customer-centric problems.

Adopting agile practices allows teams to work much faster, eliminating low value work, and solving problems better than with a traditional hierarchical approach where decision-making has a longer process. This concept of being agile changed how management operates, too. Who doesn't want to solve the right problem faster and better? More than just management adopting some of these IT ideas, real agile gains come with adopting an agile mindset and changing the culture. Real agile gains also come with applying agile methods, when needed, on bigger organizational and strategic risks and not just on project risks. Importantly, adopting agile practices can also lead to the need to fully embrace risk and to recalibrate how ERM is practiced.

Example 2

A large nonprofit adopted a new mission to solve problems for their clients. The mission includes a new culture emphasis on speed and risk-taking. Speed, or moving quickly, enables the organization not only to identify solutions faster but also to see other opportunities in the market. The mission means having agile processes. Taking risks means the organization openly accepts the large risk that comes with change and wants to take them.

Organizational and Strategic Adoption of Agile

Adopting agile practices at the organizational and strategic level encompasses a few key concepts. The obvious first concept is *speed*. Companies believe that their world is changing, and they must adapt more quickly. A second and related key concept is *direction*. The combination of speed and direction is known as *velocity*. In guiding an organization, leaders cannot just move fast; they must also have a sense of direction. Note that this direction can be a broad window. There can be a sense that the future is fairly clear and the organization just needs to compete in that future. It can also mean that the direction is completely unclear. In this case, direction and steering the organization, even moving fast, must account for a wide variety of options and business models that could play out. This leads to other key concepts, including the ability to *pivot,* the ability to *adapt,* and the ability to *accelerate* (when needed). Pivoting, adapting, and accelerating all are about managing strategic and business risk but they also can create risk. Objectives are more likely to be achieved when the context is understood (consistent with Principle 6) and the potential new risks are identified (refer to Principle 10).

There are a variety of things to consider when the organization adopts an agile approach at the strategic level. One obvious strategic risk is the speed of the company versus the speed of competitors and the environment. Companies moving at the speed of an e-bike cannot compete with companies driving Ferraris. At the same time, those driving Ferraris have to understand the future change and disruption coming from electric vehicles or autonomous driving or the growing and dramatic change that could come from remote working after the pandemic.

ERM Function Implications — Start the Dialogue

Board members are critical in helping organizations see and understand the necessity and importance of new strategic and organizational approaches and the related risk. It is also important that the business leaders, those who provide products and services, be involved and aligned with the change and agile efforts. This could require broad acceptance and a culture change and might even mandate that the business units adopt agile practices. When external parties, senior leaders, and others are pushing agile methods, the ERM function can feel completely out of sync with the business and will need to rethink its approaches and methods. ERM leaders will be more likely to stay in sync with the business when they regularly rethink and improve their ERM approach, as outlined in Principle 17.

The first step for the ERM function is to encourage a dialogue around the questions/lessons/practices raised previously. The success of this dialogue is likely to depend on the relationship established between the business owners and executives.

Question the Strategic Alignment and Fit

The dialogue should be guided to address the fit between the business and operating environment and the current strategy. This could include an assessment of the type of environment in which the organization is operating. Understanding the changing strategic context (Principle 6) is critical. The traditional strategic approach of "plan and execute" might not work well in an environment full of disruption, change, risk, and overall speed of these factors. One approach to assessing the environment involves determining the level of uncertainty around the current business model on a scale from "easily determined" to "completely indeterminable." Plan-and-execute strategic approaches are much less likely to succeed when the future is unclear, or the approach is not able to be influenced or has a high rate of change and risk. The results of the assessment of the environment can lead to the determination to change strategy and become more agile. Seeing this too late can be devastating.

The Status Quo and Agility

The dialogue can be extended to include a discussion around the risk of not changing. It might be necessary to accept that the status quo can be a risk. If the environment and competition are changing rapidly, leaders must pay attention and react. In addition, the dialogue should cover whether the organization is agile enough given its conditions. This could include assessing the company's agile maturity. Highly predictable and changing environments require more agile and adaptable approaches as well as continual adjustments. Organizations should compare their environment and competitive needs to their own ability to be agile. The result of this assessment could lead to changes in strategy, vision, and organizational structure. Boards and leaders need to recognize that in these more uncertain environments beating the competition (which traditional strategy emphasized) and creating advantages may be only temporary fixes and difficult to maintain.

New Board Approaches and Skill Set

Board risk oversight (Principle 1) must also change must also be considered the organization is adopting agile approaches. The board can make a large difference by igniting the right conversations. Boards are under pressure nowadays to reconsider the very purpose of organizations. They are also being advised to compare strategic risks to external risks to assess strategic exposure. Others are suggesting that boards should challenge legacy business models and that not challenging these legacy models is a red flag. The legacy business model itself could be identified as an enterprise risk and must be assessed. In some countries, boards are being legally mandated to assess emerging and principal risks, with principal risks being defined as risks that threaten the business model (note, this is strongly related to and supports Principle 15). An additional change for boards is a push to adopt some form of adaptive governance that establishes a board culture of constructive challenge and open dialogue. Finally, boards are being told to upskill themselves to learn to adapt and oversee a more disruptive world.

The CEO of one large nonprofit recently stated that its largest risk was, in fact, a lack of management and board skill and talent for addressing a certain disruptive, fast-moving risk. In a world that demands more agility, boards might want to compare the needs of the company's strategy to their own skill sets to ensure they are up to date and meet the company's strategic needs. This could suggest that more board turnover is necessary than in the past or that requirements for recruiting new board members are updated to reflect the concerns. Some major companies are already starting to identify stronger ERM skills as a sought-after skill for new board members. From an internal perspective, it certainly suggests a strong review of the company's current talent level to ensure capable individuals are in key positions (Principle 5). Strong board risk oversight is essential.

Factoring in External Data and Conducting a Strategic Risk Analysis

When the board is reviewing ERM reports or when management risk committees are discussing risks, there should be a consideration of whether the current strategic approach is consistent with the environment, including the speed of that environment, in which the organization currently competes and wants to compete. Such consideration should include how the company knows its strategic risks beyond an annual survey or workshop and what external data, analysis, etc. has been conducted. Organizations could also consider a separate strategic risk analysis that pulls apart the business model and value proposition and challenges the major assumptions in the current approach. Analyzing the changing business context on a timely basis can provide valuable information for a strategically agile organization. Organizations need to understand that categorizing the current set of risks (identified via internal surveys or interviews) into strategic, operating, financial, etc. is not the same as seriously considering and conducting a strategic risk analysis.

Rethink Strategic Objectives as the Baseline

When speed and agility are at higher levels, the ERM function needs to help leaders rethink strategic risks and objectives (Principles 8 and 9). If companies are moving faster and being more adaptive, having strategic plans written down and clear objectives identified are less likely to be documented. Those charged with identifying risks need to get more creative. One major technology company that has been labeled "agile" has an ERM team that does not wait for strategy and vision to be in writing. Instead, the ERM team listens to all speeches and interviews given by the CEO to ensure the team is in sync with the strategies discussed in such speeches. In an age of speed and agility, strategic plans on paper could be either not used or less relevant.

In a fast-paced uncertain environment, those responsible for risk oversight and risk management might need to accept that strategy is never really set due to ongoing experimentation instead of planning. Therefore, identifying risks to strategic objectives is less relevant and more difficult. Strategy could become evolutionary and dynamic to keep up with the changing environment. Some CEOs will never define the strategy but instead will define direction, focus, speed, agility, and options. Although COSO ERM notes the distinction between risks around the strategy chosen and risks to strategy, this might not be true for companies working in a dynamic environment because there will not be a clear line between setting and executing strategy.

These changes can be seen in the Strategy in Context (see Figure 2). COSO ERM identified how strategy and objectives can be linked to the mission, vision, and core values. Furthermore, the Framework identified how there can be 1) risks to strategy and performance, 2) the possibility of strategy not aligning, and 3) implications from the strategy chosen. In a fast-paced uncertain environment with agile strategic approaches, the three lines become blurred and the imaginary circle capturing these three dimensions is spinning faster and is changing direction. The circle may actually be one continually developing circle with no clear distinctions except perhaps that alignment (both internal and external) is emphasized and more important. In other words, an agile and risk mindset is a necessary condition to achieving alignment in these environments.

Build and Apply New Strategic Risk Tools

Moving beyond just strategic objectives and categorizing risks requires ERM leaders to build their tool kit. They might also want to improve their own skill sets in the areas of analyzing context and evaluating alternative strategies (Principles 6 and 8). The tools needed for working through these questions can include workshops on black swan events, strategic disruption, scenario analysis, futurists, business model generators and analysis, value propositions, assumptions risk analysis, or trend analysis. Reviewing trends by monitoring disruption patterns or technology and patent patterns can provide valuable insights regarding potential future trends. The lesson is that just identifying risk to objectives is only a partial view of the strategic risks. Executives, board members, and risk leaders must step up their ability to see and interpret strategic risks that challenge whether the company has the right strategy, especially in a world that is moving at an accelerated pace.

Figure 2. **COSO *Enterprise Risk Management* – in the Context of Mission, Vision, and Core Values**

2017 *COSO Enterprise Risk Management*

PART II.
BUSINESS UNIT AND TEAM ADOPTION OF AGILE ERM IMPLICATIONS

During the height of the pandemic, financial executives at a finance conference were asked to rank the most important risks they faced. The pandemic was not ranked first — it was considered the third most important risk. The second most important risk was the potential recession. The most important risk was the change in the business model. All risks come back to asking about strategy, business model, value proposition, customer dimensions, etc. In a highly disruptive and fast-changing world, companies must be agile and able to pivot. The pandemic necessitated many business models to change overnight. It exposed organizations with weak business models; companies that were not resilient; and business models that had all their risks in one company, product, market, supply chain, customer channel, etc. Other executives have echoed that the key to getting through and managing disruptive risks is to understand the business model impact. You cannot just see the risks; you have to be able to interpret when, how, and whether to change your current business model. For many of those changes to occur, the business units must be aligned with the strategic and agile approach.

It is a Normal Organization

One way to think about ERM when a business unit or area has implemented agile approaches is to think of it as an organization that could apply and adopt ERM framework components and principles. This area or unit could have objectives, products, risk appetite, risk mitigation, strategy, etc. It could also have many types of risk such as business continuity, technology, and products. What is different is that the group adopting agile practices may be focused on just a few major risks around customer, value, or speed to market. In some cases, they are focusing on one existential risk. The ERM function has to balance (a) not slowing down (for all of the reasons agile was implemented) and (b) helping them to see and manage the risk portfolio (refer to Principle 14).

Example 3

One company chose to adopt an agile mindset and emphasized moving more quickly, being more relevant to customers/guests, and being more focused on technology and data. Part of that change emanated from a new CEO and a new CIO. As IT adopted agile methodologies and mindset and began to move faster, it influenced the other parts of the company, and soon several business units were adopting an agile approach. Not long afterward, many of the remaining units in the company began to feel out of step and misaligned.

Applying Tools to the Existential Risk

Many tools could be applied to an existential risk. The first tool would be identifying and mapping top risks to an agile team's mission, for instance, launching a product. This helps the agile team think through such risks, prioritize them, and potentially manage or mitigate them to increase the chances of meeting its objectives. ERM leaders can use the opportunity to help the agile teams see risk dimensions beyond mission failure, including risks of safety, reputation, regulatory requirements, among others. They can use the opportunity to link the identified risks to the larger portfolio of risks and map these risks to strategy.

Another tool that could be applied is a premortem analysis. The agile team could allocate time to think through why a product or an idea might only last a short period of time. It could address what changes in the market, environment, or customer needs might lead to the demise. This exercise helps the team identify major risks and increase the chances of success. One additional tool that could be applied is assumption risk analysis. Agile teams could be asked to identify the key assumptions in the product or idea, then explore how to de-risk each assumption via testing or other approaches. As each assumption is tested and refined, the overall risk of the project decreases and its chance of success increases.

The ERM function can provide normal ERM tools to enable teams to properly understand, identify, and manage all related risks as expanded on in the performance component in COSO ERM. Such tools may need to be customized and other tools may become necessary, but the basic ERM tools, technology, framework, risk cadence and reporting, risk identification templates, and action plans are still valuable and should be made available. The tools can help provide consistency. At some point, it is important that the ERM function provide the context and help others connect the risks to other risks and to the broader spectrum of risks and emerging risks facing the organization. Knowing and linking the velocity of emerging risks and other organizational risks that impact the agile teams can increase the teams' chances of meeting objectives.

Incorporating Risk Thinking into the Agile Pod

One key issue is whether an ERM function member should be part of the agile pod or team. As noted in example 4, the ERM function can be viewed as another stakeholder and naturally be included in the pod. In an agile pod working on credit card development, the stakeholders might include marketing, digital channels, financial analyst, and a risk person. The key is to determine which risk person. In example 4, they pick the most relevant risk and choose a risk person with expertise in that risk. It could be reputation risk, operational risk, cybersecurity risk, or any other relevant risk. Again, an ERM representative is considered as much a stakeholder in this project as is marketing.

The decision about including ERM on the agile team or pod depends on the risk DNA of the organization. Consider that if ERM thinking is already fully integrated into the DNA of the organization, then assigning an ERM person to the team is less necessary. In other words, if the agile team understands the dimensions and complexity of risk and uncertainty, then it is more likely to naturally consider risks and any impact on the company. Clear lines of communication to those with ERM responsibilities are still necessary.

If a member of the ERM function is not assigned to a pod, it is possible to have a one-to-many relationship where ERM is not part of the team but is available to the team. In this scenario, the ERM person could stay in touch, provide support, feedback, highlight other related enterprise risks, and share risks overcome by other pods. If an ERM person is not assigned to the pod and risk acumen is not in the DNA of the company, then the ERM team may need to train the agile teams (or at least the leaders of the teams) so that the teams have the necessary risk perspective and the right risk mindset. That combined mindset can be used to understand and identify risks and opportunities as the agile teams focus on solving customer problems. More advanced risk-agile teams could build in risk appetite, risk tolerance, and required risk rollups.

Example 4

A global financial institution uses agile practices when solving problems. This institution views agile and ERM as perfectly compatible. Its view is that pods (or nimble teams) with the right people and the right tools make decisions faster. Having the right people depends on the stakeholders' needs and that sometimes includes a risk stakeholder.

Collaboration

Another approach to ensure that risk thinking does not get dropped involves cross-team collaboration. In this approach, the ERM function creates cross-team collaboration that leads to opportunities for teams to discuss risks of other agile teams. One approach involves having pods present to other pods the value proposition of the idea and the associated key risks. One broader goal of collaboration is to help the pods understand how risks are traded off against other risks. The portfolio of risks should be clear and understood. For example, a move into one new product, area, or innovation could be strategically great but create risk outside the bounds of risk appetite of the organization (refer to Principle 7). An example would be an agile team focused on solving technical partnerships that learns to consider the data privacy or environmental risks that are created by its new solutions.

Embedding ERM

As noted previously, a variety of approaches can be used to ensure that business units and agile teams consider risks. Important first steps include offering ERM training, being part of the team, providing cross collaboration, and providing ERM tools. Most important is ensuring risk acumen embedded in the organizational DNA in the first place. Agile companies should have ERM embedded throughout the organization's culture (Principle 3). When one of the approaches is not followed, the likely result is that risks will be identified only after the fact. It is okay and normal to have risks; it is not okay to either not know them or not manage them.

Agile units should be reminded that they still own the risk. The business unit leadership is responsible for the agile teams' identification and response to significant risks. The key for ERM leadership is to find the best combination of approaches to raise the risk conversation and help respond to those risks. The ERM function can bring transparency and urgency, and help agile teams connect the risks. It is valuable to have ERM members involved up front as much as possible. No matter which approach is used, when agile practices are adopted, ERM will need to make changes to keep up. The key is to find the correct balance that lets agile teams focus and go faster while still managing the risk along the way — without creating other risks that outweigh the risk they are trying to manage.

Example 5

A major insurance company believed it had made all the improvements in its business that traditional business improvement approaches could make. Its next step was to adopt an agile approach the CEO called "self-disruption" over complacency. Its goals were better service, delivery, collaboration, and innovation. Its approach included two-week sprints, empowered cross-functional teams, scrums, speed and moving forward, customer feedback connected to iterative development, and failing fast. The process was a cultural change for the company and it took about two years to get everyone on the same page.

Months after many agile teams were launched, the CRO, who monitored the company's risk dashboard, noticed risk indicators rising, but because she was not involved with the agile team, she was not able to recognize that a new agile solution had created this increase. Thus, from the CRO's perspective, risk was not always fully considered by some agile teams. The risk was eventually discovered when an external consultant conducted a review and found that the risk had left the company vulnerable for six months.

PART III.
AGILE CHANGES THE ERM APPROACH

The previous sections highlighted ways the ERM function might get involved at the organizational or business level. This section highlights changes the ERM function should consider applying to itself. One starting point is to make sure the ERM team understands agile ideas, the agile manifesto, and phrases such as epics, scrums, sprints, etc. From there, a fresh look at the ERM approach may be fruitful.

Assess and Rethink ERM and the Core Competencies

In example 6, the company's ERM directors have many approaches to stay in step with the corporate changes. They have a well-developed ERM cadence, common tools, regular reporting, executive risk teams, and board reporting. As a key element, they also regularly reassess the ERM mission. When organizations are becoming more agile, it makes sense for ERM teams to rethink their approach to ensure they support the strategy, culture, and organizational changes that occur when agile practices are adopted. Other ERM teams have done similar updates to their ERM programs. For example, while self-assessing their approaches, one ERM team identified adaptability and change as ERM core competencies for success.

Example 6

One organization made strategy and management adjustments as a result of social and consumer changes impacting the demand for their products and services. The company's new CEO launched a strategy focused on faster speed to market, improved insight-led strategies, and greater performance and growth. The company strives, among other things, to see change faster, to change the culture, to take advantage of consumer trends, to increase agility, and to decrease bureaucracy.

The New Mindset and the Desired Culture

As seen in example 7, agile approaches can be a response to strategic risk and can also be a technique for managing a large internal culture risk. To this organization, adopting an agile mindset and practices meant revisiting the risk map and rethinking which risks were really the highest priority. Human resources and culture were top risks and, by implementing these agile changes, it hoped to mitigate the risks while also improving overall organizational performance. It also had a top strategic risk related to being out of step with the market. Again, this new approach was expected to help mitigate this risk and also enable it to move faster and react better to external market and environmental changes. In its view, an agile approach forces it to think forward rather than backward.

From a risk perspective, this mindset can turn into one that encourages taking risk and seeking opportunity. Companies that take an agile approach of speed and empowerment in innovations can improve risk-taking and ideation by encouraging this risk and opportunity mindset. When companies define the desired culture (Principle 3) as one that accepts and allows for failure, they are building a culture that encourages new ideas and encourages risk-taking. Companies that do not accept failure or limit creativity create a culture that is risk-averse. If the strategic environment necessitates risk-taking, speed, and new ideas, then this risk-averse culture is the wrong fit to compete in that environment.

Example 7

One NGO's mission is to produce evidence-based policy guidance, expertise, and advanced research. After getting a new leader, it also launched a new vision and agile approach throughout the organization for many reasons. First, the new vision was considered a necessary urgent change because of the need to be more effective in a highly risky, volatile, and uncertain environment. The NGO wanted to have an operating model that was a "more modern, agile and results driven approach." Second, the NGO believed it was out of sync when it came to organization reforms as compared to external priorities of its region (market). Third, the NGO had an internal culture risk it wanted to manage. It believed it had become too bureaucratic and centralized and that this was holding it back. Its new approach would help it transition to an "agile, decentralized, results-oriented way of working" that would empower the staff. Part of the past bureaucratic problem was too much of a silo approach within the organization that limited collaboration and slowed down decision-making.

Assessing Risk Culture

Because agile practices change culture, ERM teams that are assessing culture or risk culture will need to factor in the impact of agile on that assessment. The organizations in several of these cases all wanted to change the culture. Other agile-adopting companies have specifically told employees to increase risk-taking, to innovate more, and to accept failure. The organization in example 7 specifically wanted teams to be able to get comfortable with failure and that was a concept not accepted in the pre-agile era. As ERM teams continue assessing culture and risk culture, they will need to factor in the importance of both learning to fail and embracing risk in their approaches.

New Skills and Behaviors — An Agile Talent Approach

Agile practices will also have an impact on talent — both current and new talent. Organizations wanting to develop talent and involve them in agile practices will need to train them in agile behaviors and skills (consistent with Principle 5). For the ERM function, this is also an opportunity to insert ERM training and a risk mindset into the overall training. It is also a time for ERM leadership to rethink the skill set it needs.

Companies seeking to retrain their current employees will need to emphasize the sought-after agile behaviors. HR and talent are already a top risk for some companies, but when speed and agility are in play, talent is constantly changing and how risk is viewed and understood may need to change. One major technology company adapts to this by incorporating the ability to learn new concepts and techniques. In other words, they expect employees to have not just certain skill sets but also the ability to obtain new skill sets. Its CEO has publicly talked about how the environment dictates an agile talent approach, emphasizing the importance of the link between a highly complex environment and highly valued skills. These changes highlight the importance of thinking about risks and ERM practices across the principles and their connections. In this particular case, there is a clear connection between pursuing the desired strategic context and the desired culture and talent.

When hiring new people who will be involved in more agile type practices, the hiring should reflect the desired agile behaviors. Some of the agile skills and behaviors could include hiring employees who are comfortable with ambiguity, change, and flexibility (versus sticking with a plan). Strategic alignment risk would potentially exist for companies that are pursuing agile but who are not changing the desired behaviors and skill sets.

It is worth noting that one additional reason the risks can change and must be timely managed is that agile approaches can change the incentive systems of employees and executives (examples include creating incentives and rewards for teams instead of individuals and making appraisals occur more immediately instead of annually). Business leaders will need to consider how the change in incentives impact potential risks and risk-taking.

Benefits to ERM

A new appreciation and understanding of risk and a perspective that sometimes includes more diverse teams can increase risk awareness and improve ERM practices. Agile practices will benefit and complement the ERM function and efforts in other ways, too. One way the ERM function benefits is that agile practices may break down existing silos because it uses cross-sectional nonhierarchical teams. Another way agile practices impact ERM practices is that the agile teams could have already identified the objective and assumptions and, potentially, the risks. Those stated objectives can be used for initial risk identification.

In example 7, the agile approach includes processes that focus on meeting outcomes and then working backward to pull out the logic, steps, and key assumptions that it will take to get to that objective. Key theories and assumptions about the project are challenged on a regular basis (about every three months) in addition to every new project being mandated to identify these assumptions (potential risks) up front. In other words, strategic risks to objectives are potentially identified at the beginning of projects, with no need to wait for the ERM team to mandate a risk assessment. The ERM team can use these processes as starting points for identifying risks related to agile projects and for rolling up these risks into the broader risk portfolio and reporting.

Engaging at the Right Time & Elevating

Agile practices might also require further changes in ERM practices. For example, one thing that might need to change is when the ERM team engages with the business leaders. When agile teams are moving fast and are nontraditional and nonhierarchical, ERM teams may need to ensure they have access to and communication with those teams. Furthermore, for the business units to be successful, they need to know how far they can go and how much risk exists. For the future, this could mean the ERM function adapting the yearly risk assessments, but, for now, it means reserving the right to approach executive-level risk committees at any time throughout the year about any change in existing risks or new risks that come up. It also means having the ability to elevate a risk at any point in time. The ERM function cannot remain rigid in its approaches in this environment. The ERM function might need to revisit policies and approaches for escalation and reporting (refer to Principle 19).

Determining Agile Team Contacts

In addition to changes in elevating risks and engaging the business, some ERM teams have changed their primary contact with whom they have conversations. If, for example, the ERM process leans toward a top-down, enterprise-level risk approach, then the ERM team might spend more time talking to higher-level management and executives. If, however, agile practices are being adopted, the ERM team might want to consider talking to agile teams because some of the agile teams will see certain types of risks sooner and, if not tied into the hierarchy, the agile teams' risk information might not flow up to the higher-level management with whom ERM normally engages. In one organization, instead of talking to 20 executives, the ERM leader will talk to the networked teams for potential changes in enterprise-level risks or to uncover new risks and risk connections.

Reading the Signals — Review and Revision in an Agile World

Assessing substantial change is a concept and principle (Principle 15 in COSO ERM) that appears especially important when agile approaches are adopted and implemented. The principle emphasizes the importance of organizations assessing substantial change that impacts the objectives. Companies that are moving fast, or are in an environment that is moving fast, have a greater need for building a sophisticated process to identify the change. The change can be from internal or external change, but either way, companies are best served if they know what these changes are on a timely basis. This suggests they build a more formal emerging or horizon risk process that feeds into ERM and strategy — in essence, building their risk-sensing capabilities. Some companies today have boards requesting that an external view be added to the ERM process. The key problem is that if companies did only an internal risk survey or workshop, then these external views and emerging type risks would be more likely to remain unknown or at least misunderstood. When these risks are moving fast and necessitate a more agile approach or change by the company, missing these risks can lead to considerable losses in value and competitive position. One key method for managing this risk is to have an emerging risk process that is updated regularly and timely.

Filtering the Noise into Emerging Risks

There are a variety of approaches for companies to improve in this area. Some companies use AI and machine learning to see patterns in unstructured data, news, social media, etc. to help them see the potential risks. In essence, they filter the noise into emerging risks. Others build internal processes that rely on internal workshops and surveys to identify the noise and potential risks. Some use black swan or strategic disruption workshops to try to imagine the unimaginable. A simple baseline approach is to be ever aware of risks listed by thought leaders in risk management and to compare risks to competitors' published sets of risks (when possible). No matter which approach is used, companies must decide what to do with the identified risks. Options vary but can include putting the identified risks on the enterprise risk list, monitoring them, or ignoring the risk (at the time). Of course, the importance of linking these risks to the business model cannot be underestimated.

Example 8

To increase the agility of the ERM and audit group, one risk executive changed the approach with the business unit. The old interactions with the business units consisted of an annual risk assessment that took two months to complete but then was not touched again for ten months. The old approach also was not proactive. The leader of risk and audit changed the approach to be more proactive and increased the amount of interaction and communication with the business units. This newer and more frequent communication included asking more questions about strategic objectives and the related efforts that could use some attention from ERM or audit. The company now uses ERM as the lens for the conversation by focusing on strategy, objectives, and related risks. This company still does traditional auditing and ERM and even has a twelve-month plan. Now, the plan is locked for only two quarters at a time, enabling risk and audit to increase their agility.

Another risk executive adopted an agile mindset and took an empowerment view of things. This executive's view included a "pick up the next thing" approach instead of long-term planning. They wanted to build and show the business they had the ability to change in a moment's notice, as risk changes. They also began to ask of old practices, "Should we still do this?"

Example 9

One internal audit team chose to meet with the business more frequently to focus on meeting the business needs. By focusing on problems the business was trying to solve — rather than following a traditional approach — the team helped the business more and gained its respect. These sprint-style meetings usually started at a higher level and left open the option of just walking away after gaining that view. The team adopted a "choose" approach rather than a "must do" approach. In some cases, the team did short sprints to get to the root causes more quickly. In other cases, it did a sprint alongside the business unit's sprint.

Sprinting with the Business

When organizations are changing their organizational and business approaches while trying to be more agile, it can lead to many reactions in risk management. As examples 8 and 9 show, those reactions can lead to being more proactive, focusing more on business needs, and sprinting with the business. Sprinting with the business can lead to more real-time risk identification and assessments.

Assessing the Right Risk and Assessing Dynamically

Some ERM leaders see the need to rethink risk assessments when the organization has adopted an agile approach. Some organizations will change strategy and, at other times, these organizations will emphasize risk-taking and speed and agility. To the extent that the risk to the strategy can be identified, then assessing the risk is possible. This may, however, require rethinking what strategy is — whether it is something written down or just a direction given by the CEO.

Stress-testing the business model can help management think through disruptions in a cascading manner so as to determine the impacts across the organization. Studying the connectedness of risks, applying scenario analysis, or using risk implication wheels and mind maps can be especially insightful in uncovering where, when, and how risks will play out. Stress-testing could include going beyond business continuity and moving toward assessing the robustness and resilience of normal business risks to the business and operating model. During the pandemic, too many organizations were caught not fully understanding business resilience. The ability to move fast can matter during a crisis, such as a pandemic; the inability can be a source of strategic risk. Board members, executives, and ERM leaders have to identify and manage these larger risks that don't specifically emanate from strategic objectives.

Traditional approaches to assessing risk on a quarterly and yearly basis are still critical and do help manage risk and increase the likelihood of meeting objectives. As one ERM leader pointed out, however, these traditional approaches have one flaw: they lean more toward risk awareness and monitoring by many companies. To manage the risk better, it is important to get closer to the decision that creates the risk. Hence, the involvement of the ERM team in agile practices is not only a good idea but especially helpful in improving the management of risk. A few ERM leaders have been pushing the identification of risk into decision-making and an agile organization seems to be a good place to continue doing that.

Original agile practices emphasized the pace, continuous attention, and — at regular intervals — reflection, retuning, and adjusting. The ERM function may need to replicate this approach when companies are trying to become agile — moving fast and responding to rapidly changing environments. At one end of the spectrum is the yearly risk assessments, which are still valuable and should not be abandoned. The cadence of how ERM is applied, the tools, reporting, etc. are also still critical. But what speed and the need for agility suggest is that sometimes risks need to be assessed more dynamically, perhaps in real time. Executives used to having more dynamic assessments of risk, even in real time, during the pandemic, may want that same type of assessment going forward. ERM teams should be agile and be ready to deliver.

PART IV. SUMMARY

Change and disruption are happening at a rapid pace and creating havoc for companies as they try to meet their objectives and manage their risks. Many companies are turning to new approaches to help them succeed and that includes agile practices. Some companies are adopting agile practices at the organization and strategic levels, while others are adopting and implementing more agile-oriented practices at the business-unit level. Either way, risks must be identified, assessed, and managed. An ERM framework and the ERM team can play a crucial role in helping organizations manage the risk. Furthermore, the ERM function itself needs to be updated to keep up with these changes in the organization and business units or the ERM function will quickly be out of step with the rest of the organization. Numerous ways are identified that show how the COSO ERM principles link to agile approaches. A broad overview and summary of some of these connections is discussed in Appendix A. The COSO ERM framework provides a great method for thinking about how and where risk should be considered as companies become more agile.

The following summarizes concepts that ERM leaders can use to succeed in an agile environment.

1. The speed of change, risks, and disruption is driving organizations to rethink their vision and strategy.
2. Being agile is an extension of strategy and could also be the best strategic choice in certain environments; not being agile could be a strategic mistake.
3. Organizational leaders should regularly assess the environment in which they operate and the ability of the strategic approach to succeed in that environment.
4. Greatness includes taking risks but never blindly.
5. New normals and new business models must factor in the speed of change, risks, and disruption.
6. Agile helps manage some risks but can also lead to other risks.
7. New tools and methods are available for assessing noise, the environment, the strategy, and the business model, and linking noise to the business model.
8. Superior ERM approaches can be a huge factor in helping the organization be more successful by focusing on the right strategies and risks.
9. Gathering and understanding the noise in the market and how it impacts the business and operating model, as well as building an early warning system, is becoming critical.
10. Organizations should regularly assess ERM and revisit the purpose, mission, and alignment of ERM with the current environment, strategic approach, and business units.

Appendix A. **Consideration of COSO ERM Principles In a Fast, Agile World**

2017 *COSO Enterprise Risk Management*

Governance & Culture

P1 – Governance might be enhanced by having boards upskill and reconsider approaches to strategic agile connections, questioning legacy business models, reviewing principal risk assessments, requiring external data, implementing adaptive governance, and assessing when the strategy and business model is at risk.

P2 – Operating structures could be redone to reconsider traditional hierarchical approaches and traditional decision-making processes and replace with agile practices.

P3 – The desired culture can be updated to include an agile and a risk mindset.

P4 – New core values could include taking risk and embracing uncertainty.

P5 – Agile talent and skill sets might be sought and rewarded, including the ability to be agile.

Strategy & Objective Setting

P6 – The business context and subsequent business model could be changing more frequently and need to be analyzed on a timely basis. This principle is especially important when agile practices are needed.

P7 – Risk appetite should be clearly communicated to agile teams, perhaps even adjusted to accept more risk.

P8 – The one-strategy approach is less likely to be successful. Multiple strategic choices may need to be implemented at the same time. The ability to exit one strategy and pivot may be critical.

P9 – Objectives are still critical but less likely to be written down or remain static.

Performance

P10 – Risk may need to be identified at the agile team level and assessed relative to the current strategy versus the environment and external changes.

P11 – Risks may need to be assessed dynamically. De-risking new ideas could also be valuable.

P12 – Risk prioritization should factor in all risks in agile projects and consider the speed of change and how it is changing the risks.

P13 – Risk response could include adopting agile at the strategic and business level.

P14 – A portfolio view is still a challenge when agile pods and the external environment is changing rapidly. Training agile teams on ERM may be fruitful, as well as reinforcing overall risk culture and embedding ERM into the organization.

Review & Revision

P15 – Building an emerging risk process and linking to the business model becomes a necessity. An early warning system should also be considered.

P16 – Performance could include metrics on meeting strategic and visionary positions and not just financial performance.

P17 – Improving ERM should include rethinking the purpose of ERM and if ERM is in sync with the speed of change facing the organization.

Information, Communication, & Reporting

P18 – Data should be analyzed for insights on how strategy and the environment is changing.

P19 – Communicating risk changes could include frequency of touch points and risk escalation approaches with the business and board committees.

P20 – Risk culture reports should cover agile team's progress on adopting a risk mindset.

ABOUT THE AUTHOR

Dr. Paul L. Walker,
James J. Schiro / Zurich Chair in Enterprise Risk Management
Exec. Director, Center for Excellence in Enterprise Risk Management
St. John's University

Dr. Walker co-developed one of the first courses on Enterprise Risk Management (ERM) and has done ERM training and advising for executives and boards around the world. This includes helping boards develop risk oversight practices, benchmarking ERM practices, working with organizations to develop the risk and strategy connection, helping organizations link risk to innovation, building a strategic risk identification profile, conducting black swan and strategic disruption workshops, and advising organizations on ERM process development.

In addition to helping organizations he has presented ERM to audiences more than 100 times around the world and published more than 50 books and articles on ERM, Dr. Walker has researched ERM at the headquarters of companies such as Wal-Mart, Microsoft, DuPont, Intuit, Harley-Davidson Inc., Raytheon, and more than 75 other major organizations. Some of his scholarship includes *Improving Board Risk Oversight through Best Practices, Making Enterprise Risk Management Pay Off, Enterprise Risk Management: Pulling it All Together, Is your Board Ready for ERM?, The Strategic Advantage of ERM, Managing Risk: An Enterprise-Wide Approach, A Road Map to ERM, ERM and the Strategy-Risk Focused Organization, The CFO as Chief Risk Manager, Noise to Signals to Business Models*, and *The Clunky Dance between Strategy and Risk*.

Dr. Walker currently leads the graduate degree programs in ERM and runs the Center for Excellence in ERM at St. John's University. The Center develops cutting-edge intellectual capital on ERM and brings together executives, leaders, and students to have the right conversation about risk.

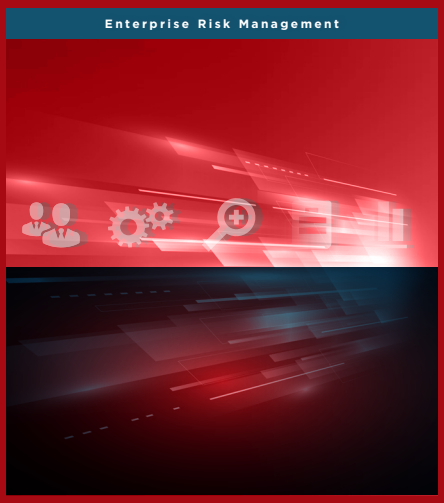
ABOUT COSO

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence. COSO's supporting organizations are the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Management Accountants (IMA), and The Institute of Internal Auditors (IIA).

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

coso.org



ENABLING ORGANIZATIONAL AGILITY IN AN AGE OF SPEED AND DISRUPTION

COSO

Committee of Sponsoring Organizations of the Treadway Commission

coso.org