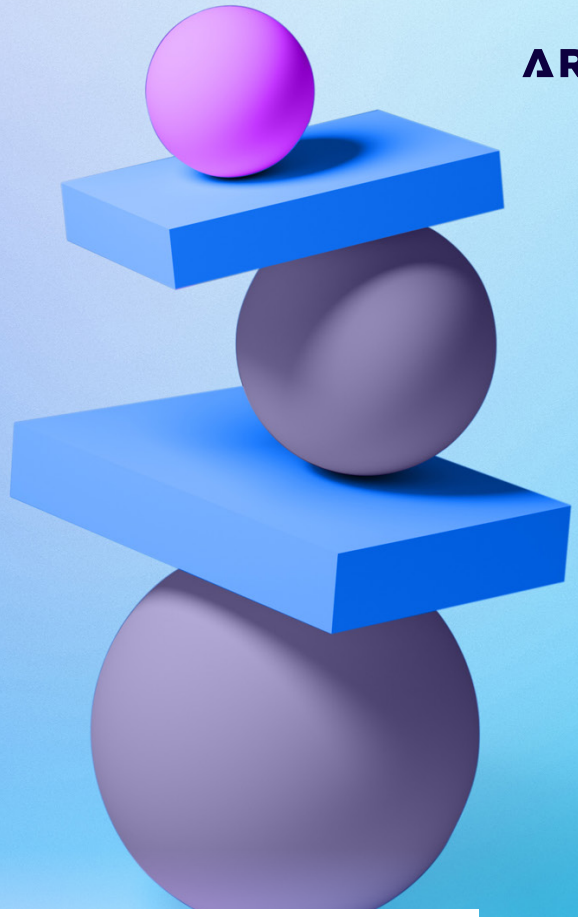
VIEWPOINT

ARTHUR D LITTLE
2023



REINVIGORATING ENTERPRISE RISK MANAGEMENT

How to strengthen organizational resilience & avoid pitfalls

AUTHORS

Marcus Beard

Tom Teixeira

Ben Hansen

Kerri McGowan

Enterprise risk management (ERM) has been regarded for three decades as a vital practice for navigating the broad spectrum of risk faced by an organization and ensuring the right balance is achieved between risk mitigation, transfer, and retention. Most transport and mobility companies have captured a register of enterprise risks, but few successfully embed and integrate ERM into their ways of working in a way that delivers real and sustained value. In this Viewpoint, we explore whether traditional approaches to ERM are still sufficient to support effective strategic decision-making and share a more risk-intelligent, forward-looking, and maturity-driven approach that can add value.

ERM AS WE KNOW IT

Enterprise risk management is a strategic business discipline. It addresses an organization's full spectrum of risks and manages their combined impact via an enterprise-level risk profile, which supports the organization as it works to achieve its objectives. The term "enterprise-level" typically refers to the corporate tier, where risks are managed and expressed through the lens of a corporate risk appetite; these risks are neither compartmentalized nor tackled in isolation on a project or discipline level. Thus, establishing an interrelated enterprise-level risk profile is essential to understand the potential risks of failing to meet strategic objectives, and to gain a competitive advantage in a rapidly changing business environment.

ERM has existed as both a concept and discipline since the early 1990s; consequently, many organizations have a reasonably mature ERM system in place, which usually consists of:

- An overall risk management policy
- An overall framework to support top-down/bottom-up risk management processes
- A central enterprise risk register and designated risk representatives
- Managers responsible for reporting on risk and updating risk registers

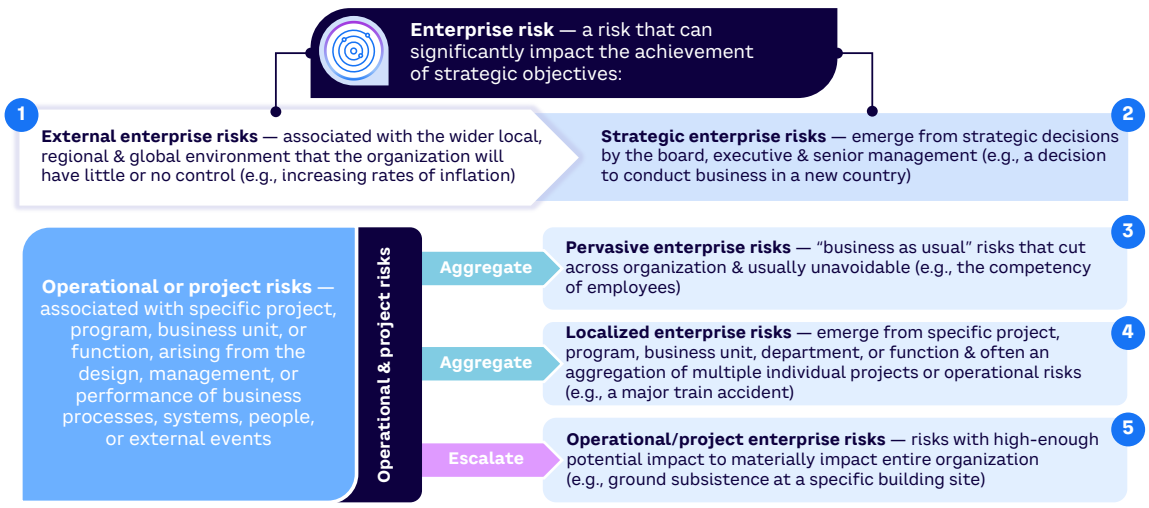
MANY ORGANIZATIONS HAVE A REASONABLY MATURE ERM SYSTEM IN PLACE

The inherent challenge

A mature ERM system needs to accommodate the different types of risks typically faced by large, diverse, and complex organizations. In our experience, a typical enterprise risk profile consists of risks across five broad categories (see Figure 1).

In practice, the different types of risks shown in Figure 1 are managed and controlled very differently. In several cases, there are external risks that cannot be controlled at all, and many are interrelated and correlated at different levels and in distinct ways. For example, it is inherently challenging to design an ERM system that caters for both broad strategic risks, such as beginning operations in a new geography, and isolated operational risks, such as technical asset degradation. The characteristics of these risks and their controls are completely different and yet both are of interest at the enterprise level as they can have a material impact on the corporation.

Figure 1. Five categories of enterprise risk



Source: Arthur D. Little

Therefore, designing and implementing an effective ERM approach poses fundamental challenges, including:

- Accounting for complexity and diversity
- Driving useful management engagement and action
- Keeping pace with changes
- Providing confidence in building an overall strategy

SO WHERE ARE WE TODAY?

Our experience with transport and mobility companies shows that executives generally appreciate and understand the basics of ERM and the value it can add. Yet, it is commonly the case that the corporate view of risk, usually held in an enterprise risk register, neither aligns well with actual risks nor does it keep up with the pace at which these risks change. Indeed, the enterprise view of risk often lags reality, reducing the value of the entire system over time to a repository of static and backward-looking information about well-known risks. Such an outdated resource cannot drive management action. In the early days of ERM, building a register was essential and considered an added value as it provided a snapshot view of risk that was previously unavailable. But, over time, incremental updates to such registers are of decreasing value and it is common for things to stagnate.

Many organizations, despite having well-established ERM systems, find they can be caught unprepared by unexpected loss events.

The system simply is unable to keep pace with sudden emergences of risk that appear at high velocity or from less predictable causes. Indeed, we often observe executive-level clients discussing issues of concern that may not be captured properly or at all in the ERM system, despite expending extensive effort and resources to manage that system. It is easier for them to discuss lists of concerning "issues," rather than administer the addition of these into what has become an increasingly complex and stagnant register.

An analysis of the root cause of recent major rail accidents highlights this problem effectively. The most common reasons for rail accidents in the last 10 years relate to human error and mechanical failure. Most transport organizations recognize safety-critical asset management and the competency of safety-critical employees as key enterprise risks, but simply recording these risks in an ERM system does little to alert senior management to a potential issue that could lead to a major accident.

In summary, current approaches typically fall short in three key ways:

1. **Large organizations' view of risk is often outdated:**
   - *Outdated and static registers.* Enterprise risk registers often stagnate, since risks that are material to the organization do not change significantly and rapidly. As such, the register is only reviewed periodically (sometimes annually) with a light touch. While aspects of certain business-as-usual (BAU) risks may be relatively static, the causes of risk events and the effectiveness of critical controls can change rapidly in response to changes in context.
   - *Poor engagement.* ERM is often perceived as a separate activity for the risk champion or risk manager tasked to report risks at the executive or board level, rather than the day-to-day actions of individuals. Indeed, some organizations no longer use the term "enterprise risk management," preferring to focus instead merely on "risk management," which better encompasses the need to manage risk from the operating level all the way to the boardroom. In this construct, "enterprise risks" are simply those risks with potential to cause business-wide damage.

2. **Large organizations' view of risk is often disconnected from the business and the way it operates:**
   - *The wrong risks.* Top risks are often allocated based on judgment, or what has occurred historically, either in the organization or elsewhere. This may not reflect the latest operating internal or external environment.
   - *Poor integration and alignment.* Organizations can struggle to align their ERM approach with more "working level" bottom-up risk management; these can become disconnected with poor escalation of risk upward.
   - *Failure to connect to emerging risks.* Organizations find it difficult to identify emerging risks and, even more so, how to practically connect these to the ERM framework to drive useful insights and management response. This means risks that may be on the distant horizon often materialize before they are properly captured with risk-mitigation strategies in place.
   - *Poor aggregation of total risk exposure.* It is often unclear how the complex web of underlying operational and project risks faced by a large organization interacts. In many cases, their aggregate impact on the whole enterprise cannot be determined.
3. **Risk management efforts do not focus on the effectiveness of critical controls:**
   - *Critical controls.* It is rarely clear which of the many controls for the top risks are actually critical (i.e., those whose failure would likely result in significant corporate damage). It is therefore impossible to assure well-controlled risk.
   - *Misaligned assurance and risk.* Risk-based assurance involves focusing assurance activity on the highest inherent risks an organization faces, so critical controls can be corrected or improved according to what risks are the most urgent and have the highest potential for loss. Often, organizations do not have a risk-based approach to assurance, meaning large amounts of effort and resources are spent on assurance activities that deliver relatively little value.
   - *Lack of appropriate data or metrics.* Organizations can struggle to build an evidence-based approach that provides the right mix of lagging and leading indicators for risk and just as importantly — a measure of the effectiveness of controls for those risks.

CHALLENGING THE CURRENT APPROACHES

We suggest executives ask themselves the following questions to help them start getting ERM back on track:

1. Are we confident our critical controls are actually effective?
2. Are we confident we have visibility at all levels of the organization?
3. Does our organizational culture and capability ensure problems/potential issues are reported before it is too late, and are we always honest about our risks?
4. Do we understand how changes in context affect our risk exposure?

Are we confident our critical controls are actually effective?

Determining the effectiveness of a control can be difficult and requires careful judgment of the balance between risk and benefit (see Figure 2). The overall effectiveness of the control is a combination of aspects of its design and its implementation, which in practice are difficult to measure and quantify. A view of control effectiveness can be formed from various methods of assurance (e.g., audits, monitoring, reviews, and deep dives across the **three lines of defense** [see sidebar on next page]).

Three lines of defense

The three lines of defense is a risk management framework commonly used by organizations to identify, assess, and manage risk:

1. **First line of defense** — the day-to-day management of risks by individuals directly responsible for the activities, processes, and controls within the organization.
2. **Second line of defense** — includes the oversight functions that ensure policies, procedures, and controls are in place and effective at managing risk. The second line also monitors the first line and provides guidance.
3. **Third line of defense** — an independent function that provides assurance to the board by evaluating the effectiveness of the first two lines and making recommendations as required.

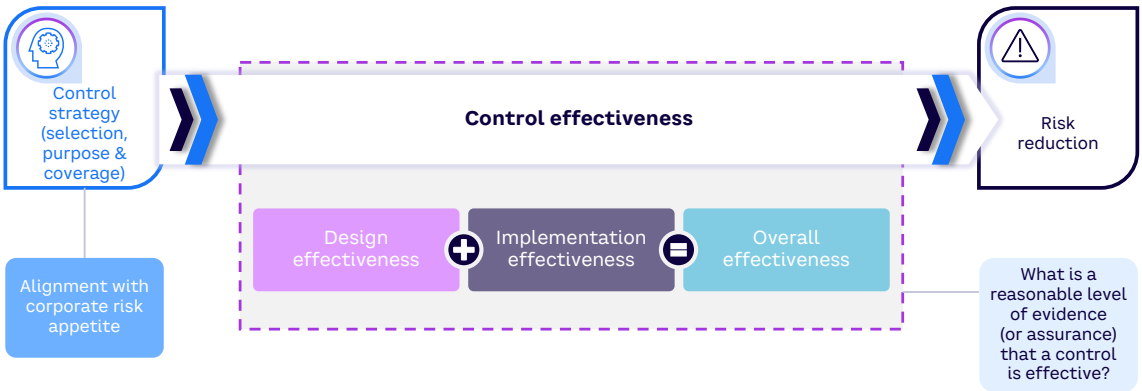
However, it is difficult to determine whether the right controls have been selected in the first place, as such decisions were often taken in the past and are rarely revisited. Effectiveness covering control selection and strategy leads to multiple existential questions around risk acceptance principles, organizational risk appetite, required levels of safety integrity, and the purpose of risk management.

Our recent work in the rail industry has shown that it is common to make assumptions about the effectiveness of risk controls, particularly those that have been in place for some time, with the focus of risk management being on recording and reporting events. This is perhaps inevitable, as judging the effectiveness of a risk control can be time-consuming, subjective, and difficult. However, having confidence in the effectiveness of critical risk controls is critical to prevent loss, ensure compliance, secure stakeholder trust, protect reputation, preserve business continuity, and make decisions that are right for the business. A focus on control effectiveness provides assurance that your organization is actually controlling risk within appetite.

Shifting the focus from "risk level" to "control effectiveness" is highly beneficial. This means seeking confidence that critical controls are adequate, in place, and working. This is not a one-off task; critical controls are effective when the organization takes the following actions:

1. Ensures all lines are risk-based and working well, and critical controls are known
2. Defines what it means for a control to be effective with defined performance criteria
3. Establishes a comprehensive set of indicators that reveal control deficiencies
4. Achieves high levels of competence in all aspects of risk management
5. Confirms that escalation processes are working well

Figure 2. The control-effectiveness equation



Source: Arthur D. Little

6. Takes actions to respond to weaknesses is working well
7. Understands risk appetite and judging control effectiveness

Are we confident we have visibility at all levels?

Executives of large companies face a delicate balancing act. On one hand, they require a simplified, consolidated view of risk that encompasses the entire organization. This high-level perspective is crucial for making strategic decisions and maintaining a clear understanding of overall exposure. On the other hand, executives need enough granular detail to instill confidence that risks are being managed properly at the operational level. Striking this balance is not easy but ensures executives can steer the organization effectively without being overwhelmed by minutiae. This requires integrating a top-down ERM approach and a traditional bottom-up project or operational approach, which is challenging for large diverse organizations. Large organizations often have multiple business units, departments, and projects that operate independently, often with their own risk management processes, systems, and stakeholders. An integrated approach is particularly challenging as it requires high levels of coordination and collaboration. In addition, enterprise-level risks often involve broader strategic considerations, while operational or project risks are more specific to individual projects or divisions. Integrating the two requires translating project and operational risks into the language and context of enterprise risks.

Improving alignment and increasing top-down visibility is a process of continuous improvement with relatively few quick wins. Steps organizations can take include:

1. **Monitoring risk drivers** through leading key risk indicators (KRIs) and lagging key performance indicators (KPIs) that can be tracked across operations and projects. This allows organizations to proactively identify trends and patterns that may signal emerging threats.
2. **Developing a comprehensive risk taxonomy supported by escalation and aggregation principles** to systematically identify all risks facing an organization and support escalation and aggregation of common risks to the enterprise level for an improved top-down view.
3. **Developing consistent risk assessment methodologies, criteria, metrics, and reporting mechanisms.** Standardization across an organization promotes consistency and comparability when evaluating risks.
4. **Driving awareness of enterprise issues across the organization** to ensure project and operational teams consider the impact of their specific risks on the enterprise as a whole, not just their area of responsibility. This can be achieved by facilitating coordination between the ERM teams and operational/project teams (e.g., attendees from both functions in a risk assessment workshop) and fostering improved risk communication across the organization to enhance overall risk awareness.

Does our organizational culture & capability ensure issues are reported?

An ERM system, framework, and tools is all well and good, but their effectiveness depends on the leadership, competency, commitment, and engagement of the organization's employees with respect to risk. Many organizations have developed apparently sophisticated risk management processes, but they fail in implementation because employees lack competency with regards to identifying, articulating, and managing risks and often consider risk to not be part of their day job. This is clearly a dangerous assumption, as risk controls have to be implemented at the sharper end of a business. Another problem is that risk is seen as a side activity to other line management duties, which is fundamentally flawed.

Like any aspect of business, strengthening the risk culture and competency within an organization requires a concerted effort and commitment from all levels of the organization (including the very top). The steps organizations can take include:

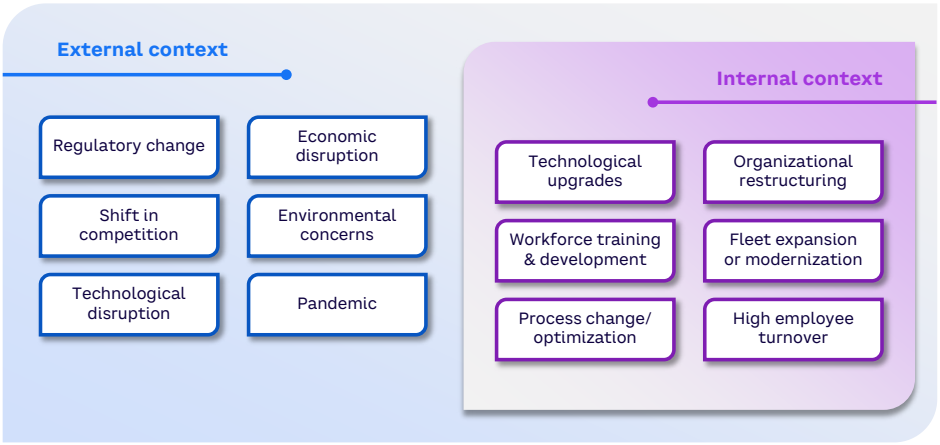
1. **Make everyone a risk manager.** The importance of risk management needs to be integrated into day-to-day decision-making. Strong leadership commitment is crucial for shaping and promoting a positive risk culture.
2. **Provide comprehensive training programs.** This enhances risk awareness and knowledge among employees; incorporate individual scorecards and renumeration models to track progress and incentivize improvement.
3. **Establish clear lines of responsibility and accountability.** Define roles and responsibilities for key stakeholders when it comes to risk management.
4. **Embed risk considerations into project planning, performance evaluations, and all decision-making processes.** Risk management should be an integral part of the organization's systems and procedures.
5. **Promote collaboration and cross-functional engagement in risk management.** Encourage teams from different departments to work together to assess risks, share best practices, and develop controls.

Organizations must realize that managing risk is not a separate siloed activity. It is embedded in every decision that is made by anyone, anywhere in the business. Risk "experts" (as members of the risk team) are there to support and advise, but they do not manage the risk.

Do we understand how changes in context affect our risk exposure?

In risk management, a change in context is any change to the circumstances that comprise and surround the organization. Changes in context can be either internally driven, such as a significant internal transformation, or externally driven, such as a change in local regulations. Figure 3 shows some typical external and internal context changes that could affect a large transport organization (typically identified through a horizon-scanning process). Changes in context add significant complexity to ERM because registers must be manually updated after an upcoming change has become apparent or occurred. For the large and complex risk registers typically seen in organizations with mature risk management systems, it is often not clear how to do this efficiently, as multiple correlated risks are affected. This seriously devalues the entire process of risk management, as it is not evident how risk exposure is affected by the change, and it becomes an administrative exercise rather than one that serves the needs of the business.

Figure 3. Internal vs. external context for a large transport organization



Source: Arthur D. Little

THE ERM SYSTEM OF THE FUTURE WILL NEED TO UTILIZE EMERGING TECHNOLOGIES LIKE AI AND NLP

As discussed throughout this Viewpoint, enterprise risk is complex, interconnected, and increasingly difficult to manage in a way that balances value and effort. Standard tables and lists fail to accommodate the challenges of managing risk effectively. The ERM system of the future will therefore need to utilize emerging technologies like artificial intelligence (AI) and natural language processing (NLP), which can much more readily work with poorly structured data at much higher speed and with lower effort. An ERM approach enhanced by AI and associated technologies goes beyond standard technology solutions (usually a governance, risk, and compliance system) seen in most organizations, moving businesses away from a static view of risks to a "push of the button," up-to-date view of risks — allowing relevant risks to be instantly updated, reports to be complied as required, and risks to be targeted, as necessary. AI and NLP approaches are highly synergistic with horizon scanning and can enhance various parts of the process with automated data collection and processing, automated identification and (real-time) updates of relevant risks, topic and trend detection, predictive insights, and real-time monitoring/alerts.

For example, NLP algorithms enable AI systems to understand and extract relevant information from unstructured data sources, such as reports, documents, and textual data. This capability can be particularly valuable for updating and maintaining risk registers in response to changes in context by identifying new risks, updating existing risk profiles, and populating risk registers with accurate and timely information. This can save considerable time and effort in data entry, ensuring the risk registers remain up to date and reflective of the current risk landscape. Furthermore, AI can identify patterns and uncover hidden insights from an organization's risk information and automate the generation of risk reports to present this information. This saves time and effort in compiling risk reports, and by presenting information in a visually appealing and easily understandable manner in almost real time as internal and external context changes, AI-powered reporting and risk visualization enable more informed decision-making, based on the latest information.

While using technology like AI and NLP to improve enterprise risk management can offer numerous benefits, an organization looking to implement a solution of this nature should be mindful of potential challenges:

- **Data quality and accuracy.** AI and NLP models rely heavily on high-quality and accurate data for machine learning. If data used to train these models is incomplete, outdated, or biased, it can lead to incorrect insights and therefore poor decisions. AI algorithms can also inherit bias present in the data they are trained on, which could unfairly impact or prioritize certain types of risks. Developing an accurate and robust initial data set for training should be the first step for any organization looking to implement an AI solution for risk management; however, this can be a time-consuming and costly process. Utilizing unsupervised AI can still add value quickly, but organizations should be mindful of potential problems with this method.
- **Overreliance on technology.** Relying solely on AI and NLP systems for risk management can lead to a disconnect between human judgment and automated insights. Human expertise is still crucial in understanding the context and nuances that may not be accurately captured by algorithms.

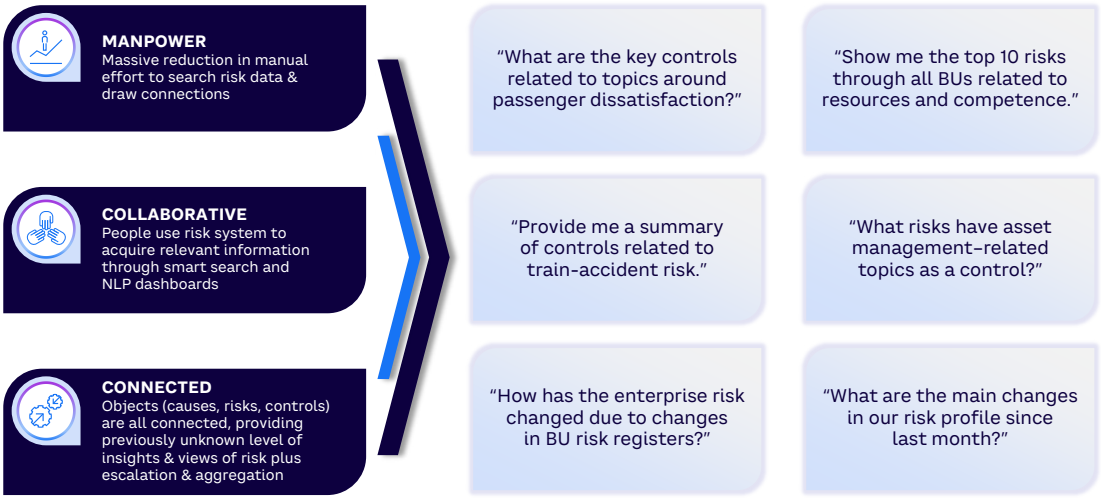
- **New risk.** Introducing AI and NLP solutions introduces new risks that may not be immediately apparent. These could include technical glitches, model vulnerabilities to adversarial attacks, issues with data privacy and security, and unintended outputs due to complex interactions within the system.

Figure 4 shows illustrative examples of how a technology-driven ERM approach could transform how an organization manages risk.

Enhancing ERM for a major rail operator

A leading transport operator in Asia worked with ADL to develop an enhanced ERM framework to improve the quality of risk information visible to executives and ensure t hey are not "caught out" by an event. A smaller set of principal risks were developed to provide a top-down view of the risk profile, and bespoke comprehensive control-effectiveness criteria were created to shift the focus of risk management from reporting to control effectiveness for each principal risk. This information was summarized in a series of executive dashboards. For the executive dashboards to work effectively, it was essential that the bottom-up risk management processes that fed key risk information upward were also updated to drive closer alignment between ERM and operational/project risk management and ensure high-quality and robust risk information was incorporated into the top-down view. We achieved this by standardizing risk definitions, processes, and assessment criteria across the organization; developing a centralized risk taxonomy; supporting escalation and aggregation principles; and building a competency framework with accompanying training/awareness modules to improve the risk culture across the organization.

Figure 4. AI could transform relationship with risk



Source: Arthur D. Little

CONCLUSION

AN HONEST APPROACH TO RISK MANAGEMENT

ERM IS BECOMING AN EXTREMELY HIGH-EFFORT AND RESOURCE-INTENSIVE ACTIVITY THAT ADDS DIMINISHING VALUE

Managing enterprise risk effectively requires strong leadership commitment and alignment, along with an honest approach that allows challenging the status quo. Risk expertise is not centered on a few individuals but rather is dispersed through people at all levels, in all departments, and in the information scattered in documents and databases throughout the organization. Traditional ERM approaches centered around registers and slow processes of escalation and reporting simply are unable to cope with the real complexity of risk. Organizations become complacent, and as the ERM system becomes complex over time, it can be difficult to challenge what already exists, or require so much effort to overhaul that it becomes a barrier to improvement. The world doesn't stop, and both internal and external sources of threat evolve and are less predictable than ever.

Our experience shows ERM is becoming for many organizations an extremely high-effort and resource-intensive activity that adds diminishing value. Managing enterprise risk is the same thing as managing the business — the two cannot be separated. To improve the overall state of ERM effectiveness, senior leadership should consider the following:

1. **Shift the focus of the risk management effort** away from lists and tables to challenging the effectiveness of existing key controls.
2. **Carry out assurance on the most important controls** to test whether they are really working as expected, or whether other forms of control have even been considered.
3. **Develop an improved set of risk indicators** fed by real, live data, balancing leading and lagging indicators.
4. **Challenge yourself and each other to better understand the culture** across the breadth and depth of your organization and ensure the right level of competencies is in place; upskill and change roles where required.
5. **Constantly question whether risks are under control** as part of day-to-day conversations.
6. **Align top-down ERM processes with bottom-up project/ operational** risk management processes.
7. **Develop a simple horizon-scanning process** to identify changes in context that could affect the organization's risk exposure — involve a wider group as required and make it interesting and engaging.
8. **Fund proof-of-concept experiments** using AI/NLP to see what you can learn about risk, beyond what's provided by your current systems, leveraging larger sources of disparate data.

Arthur D. Little has been at the forefront of innovation since 1886. We are an acknowledged thought leader in linking strategy, innovation and transformation in technology-intensive and converging industries. We navigate our clients through changing business ecosystems to uncover new growth opportunities. We enable our clients to build innovation capabilities and transform their organizations.

Our consultants have strong practical industry experience combined with excellent knowledge of key trends and dynamics. ADL is present in the most important business centers around the world. We are proud to serve most of the Fortune 1000 companies, in addition to other leading firms and public sector organizations.

For further information, please visit www.adlittle.com.