Arthur D Little

Viewpoint

Effective corporate risk governance

Mastering risk governance in an increasingly uncertain and fast-changing world

Failures in risk governance are visible on a daily basis through "breaking news" stories which demonstrate limitations in the effectiveness of typical approaches to risk management. The evolving business environment – breakthrough innovations, new security risks, accelerated diversification of business activities, changing regulatory landscapes, etc. – requires boards to adopt robust but agile approaches to keep threats under control and embrace opportunities. Our experience suggests that a handful of relatively simple key principles and tools can be valuable when designing or reviewing corporate risk governance arrangements, in order to provide agile but robust value-based risk management.

Why generic approaches to corporate risk governance have limited impact

Boards' interest in risk management is evolving under the pressure of both internal and external threats, as well as keenness to exploit opportunities. Companies seeking to go beyond risk management in functional silos draw upon a number of different generic frameworks for enterprise-wide risk management. In our view, efficient risk management should be built around four key principles: maintaining strategic alignment, focusing on vulnerabilities, facilitating decision-making, and building a dynamic risk culture[1]. However, the design and implementation of risk management frameworks usually fail to deliver against these four pillars.

Conventional risk management deals poorly with complexity, is slow to adapt to changing circumstances, and overemphasizes risk reporting. Such approaches provide comprehensive information and reporting of risk data, but little information that truly shapes decision-making. They also frequently assume that business operates in a steady state. Few real companies today operate in such static environments, and changes driven by company strategy or operating conditions greatly influence the risk profiles.

Recent events show that developing an agile, value-focused, risk-based approach is increasingly required to mitigate threats, as well as to make timely decisions to exploit potential opportunities. The media report a constant stream of events, such as cybersecurity (WannaCry, Petya/NotPetya), political and geopolitical tensions (Brexit, the US, North Korea), natural disaster (fires in California, Portugal and Spain, Hurricanes Irma and Harvey), and terrorism. Such risks can have huge impact on businesses, and behind the front page, new business risks are emerging. We briefly review some of the commonly encountered situations and weak signals here.

Growth and expansion

Growth by acquisition is a common strategy for corporations, but presents certain risks. Outside of finance-related risks (such as asset valuation and currency volatility), which are usually carefully assessed and monitored, other strategic risks are often underappreciated – or worse, not visible to boards. For instance, in acquiring the Texas City Refinery as part of its merger with Amoco in 1999, BP failed to address unsafe process systems – issues that had been identified and understood well under the previous ownership. These issues ultimately contributed to an explosion that killed 15 people and injured more than 180 others. BP paid more than US$1.6 billion to compensate victims.

International supply chain

Outsourcing and supply-chain expansion have delivered great benefits in efficiency and agility, but businesses operating across geographical barriers, social disparity, and working cultures are exposed to potential disasters. The Dhaka Fire

1 Arthur D. Little Viewpoint, Why risk management is failing; Embracing complexity and uncertainty with value-based risk management, 2016

(2012, 117 fatalities), the Pakistan Garment Factory Fires (2012, 257 fatalities) and the Dhaka Rana Plaza Collapse (2013, 1,127 fatalities) illustrate how shortfalls in corporate risk management can lead to loss of life, business interruption and reputational damage.

Increasingly complex and extended supply chains also generate significant risk because of difficulties in traceability. These are well known in the food industry, but the problem exists across a wider range of industries. For example, in 2011, an investigation found a huge number of counterfeit parts in the Pentagon's spare-parts stock, which led to a security and safety risk for the US and its armed forces.

Disruptive environment and innovation

Evolving technologies, such as the Internet of Things (IoT), smart buildings, financial technologies, artificial intelligence, and autonomous vehicles, offer fantastic opportunities, but also huge disruption across all sectors. For instance, autonomous driving is extending the boundaries of product liability for manufacturers in the automotive industry, dramatically increasing their share of driving-related risks and their reputational risk. Rapid innovation can be disruptive, affecting complex, interconnected ecosystems, and challenge established industry verticals.

On the other hand, breakthrough innovations are key strategic points for most firms to survive and achieve growth. In some industries, the success rate of R&D projects is very low, sometimes worse than 5 percent. Therefore, the need for efficient project risk management is vital.

Changing regulatory landscape

European Union law now requires the disclosure of non-financial information concerning environmental, social and employee-related policies, outcomes and risks[2] (2014), and as such countries are starting to respond with new laws for example requiring corporate vigilance. The future international standard for occupational health and safety management system (ISO 45001 standard) will also promote strengthening of safety management across the supply chain and impacts on third parties.

Developing a corporate risk governance strategy

In a previous Viewpoint[3], we described various governance styles, along a spectrum of centralization-decentralization. There is no intrinsically wrong or right style – achieving a balance in the level of intervention – the extent to which corporate is involved in actively managing risk, and the devolution of responsibility for risk to business units – is key.

The cursor (***level of intervention***) should be put along the spectrum of centralization (***"heavy handed"***)/decentralization (***"light touch"***). Importantly, to:

A. Align with the **global strategy**; the risk governance should be in line with the global governance of the company.

B. Pinpoint the ***risk governance drivers.***

C. **Tailor the level of intervention** to each type of key risk.

A. Aligning with the global governance strategy

Risk governance arrangements should align with the overall governance structure of the company, including lines of authority, communications, duties, and resource allocations. This allows effectiveness to be optimized by embedding risk-based interventions in the current processes and alignment with organizational culture.

Many larger companies operate on a highly devolved basis, with the business divided into groups along national/regional or functional lines. This means that individual groups often have strong cultural or technical cohesiveness, but operate with different pressures. In these cases, risk governance arrangements should align with the organization of the business – a "one-size-fits-all" strategy will be less effective.

B. Pinpointing risk governance drivers

Two parameters, **risk profile intensity** and **regulatory pressure**, particularly influence risk governance at corporate level. Understanding their respective levels helps with the design of appropriate levels of intervention.

A **risk profile intensity** study should define the nature and level of threats, the likelihood of the effects, the risks spread across the organization, the level of disruption and costs associated with each type of risk, and the effectiveness of control in place to manage the risks. This does not require an in-depth assessment of each type of risk, but more an understanding of the key drivers of the risk profile that can have impact at corporate level.

Regulatory pressure represents the level of expectation imposed on a business to satisfy the prescriptions from a regulatory agency or framework. The regulatory pressure and the level of enforcement can differ from one country to another.

Aviation and nuclear are examples of industries with highly developed safety requirements defined by dedicated regulatory bodies. The regulations are typically accompanied by detailed technical requirements and active enforcement. In this case, the regulatory pressure for safety risk can be considered high.

2 Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups Text with EEA relevance

3 Arthur D. Little Viewpoint, Safety governance: Getting it right; Exercising effective safety governance across large, diverse corporations, 2015

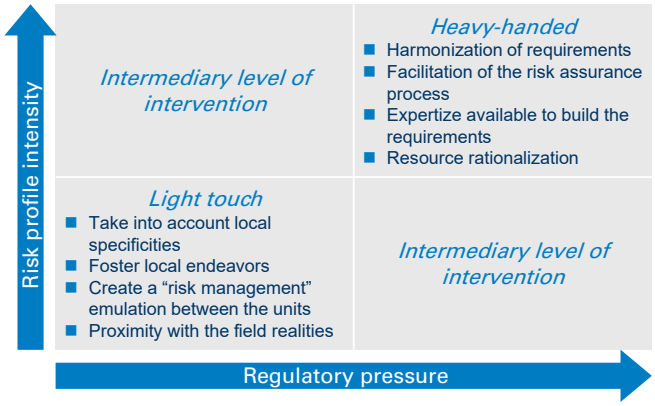
Where regulatory pressure is high, the risk profile presents potential for significant damage, and the risks are similar across the organization, a centralized, more "heavy-handed" corporate risk governance strategy will be most effective. The absence of regulatory pressure or enforcement in certain regions/countries could influence the risk profile negatively. In such cases, a more decentralized, "light-touch" approach, leveraging local expertise and initiatives, may be more appropriate.

C. Tailoring the level of intervention for each risk type

For any business, levels of intervention will vary and should be tailored to different risks. This allows the company to balance some of the traditional benefits of heavy-handed with light-touch risk governance:

- Balance resource optimization and standardization (one standard for all) with promoting decentralization and inclusion of local initiatives.
- Balance centralized expertise with local know-how.

Figure 1: Evolution of the intervention level and corresponding benefits, depending on risk governance drivers



Developing effective risk governance

With an appropriate level of intervention having been determined, the components of risk governance can then be defined. From our experience, risk governance arrangements may be subdivided into: (1) Roles and Responsibilities, (2) Requirements, (3) Communication and (4) Assurance.

Roles & Responsibilities (1) and Requirements (2)

The corporate roles (1) and the associated requirements (2) are usually defined simultaneously and in a coordinated manner ("who does what").

Specific roles should be defined for risk governance, including both executive and non-executive members. Risk leadership from the top of the company is critical for building a culture in which risk is part of what people do (developing risk capabilities to enable resilience to change), and for keeping risk management aligned with strategic priorities. While appointing a chief risk officer at executive level is now a widespread good practice, this role should be focused on guidance and assurance, and not seen as "where risk is managed". At least one risk management objective should be defined and included on the balance scorecard. This objective can then be cascaded and specified depending on the risk portfolio composition at each layer of the organization.

The board must receive advice in line with the company's risk profile. For example, many companies are or will be impacted by the technological disruption, but board members can struggle to understand precisely the potential business impact of technological breakthroughs. Appointing a board member with deep, contemporary understanding of emerging relevant technologies may provide significant value.

Corporate requirements should be limited to the significant risks that can be tackled similarly across the whole organization. High-level arrangements, such as risk identification and assessment, investigations, reporting and risk monitoring, can be substantially defined at corporate-level, even when a "light-touch" approach is adopted. When defining the requirements, we suggest identifying the vulnerabilities that can hinder the implementation of risk controls. A pragmatic approach developed by

Figure 2: Development and components of an effective risk governance

Arthur D. Little to help in this process is the so-called 6C model[4] (for Codes, Compliance, Competency, Complexity, Change and Culture). Our experience shows that it can reveal a good understanding of vulnerabilities without detailed, time-consuming quantification.

Communication (3) and Assurance (4)

The focus for any program-branding and communication campaign should be based on the critical risks detected during the risk-profile assessment. The various communication actions must transmit the commitment of the board for risk management (top-down communication).

Business units should be able to feed back quickly to the corporate level the extent to which corporate arrangements are fulfilling the units' needs, subsequently avoiding loss of adherence in the processes (bottom-up communication). Good practice should be shared between the business units and corporate. This is especially beneficial under a "light-touch" approach, with greater freedom of initiative at the local level, as it allows the corporate level to benefit from experience, and leverage the methods found to be the most effective.

Assurance should check the effective implementation and value provided by risk management arrangements. Assurance arrangements will need to span all organizational levels. There is considerable value in independent review of an organization's risk management capability and performance (up to board level).

A reporting "cascade" should be set up and adapted to the level of oversight, and designed for fast decision-making (key decision-making data).

Conclusion

In a world of increasing uncertainty and disruption, companies are facing severe, complex, unpredictable and fast-changing threats, but also opportunities that can be exploited to gain competitive advantage. Well-publicized significant failures illustrate the imperative for effective risk management that aligns with group strategic priorities, and ensures that the governing levers of controls are appropriately engaged.

Corporate risk arrangements ensue directly from the ***level of intervention*** chosen, and should clearly define four interconnected components:

- Roles and Responsibilities: to define what the specific responsibilities of key staff are, and ensure risk leadership at board level.
- Requirements: to set the objectives together with guidance for implementation.
- Communication: top-down and bottom-up – to transmit the risk message across the whole organization and obtain feedback from the local level.
- Assurance: to monitor that risk performance and "risk duties" are satisfied at every level.

Contacts

Austria
taga.karim@adlittle.com

Belgium
vanaudenhove.f@adlittle.com

China
russell.pell@adlittle.com

Czech Republic
brabec.dean@adlittle.com

France
bamberger.vincent@adlittle.com

Germany
zintel.michael@adlittle.com

India
srinivasan.srini@adlittle.com

Italy
milanese.stefano@adlittle.com

Japan
akamine.yotaro@adlittle.com

Korea
lee.kevin@adlittle.com

Latin America
guzman.rodolfo@adlittle.com

Middle East
kalkman.jaap@adlittle.com

The Netherlands
eikelenboom.martijn@adlittle.com

Norway
mackee.diego@adlittle.com

Singapore
fujita.akitake@adlittle.com

Spain
borras.david@adlittle.com

Sweden
anderlind.klas@adlittle.com

Switzerland
doemer.fabian@adlittle.com

Turkey
baban.coskun@adlittle.com

UK
beard.marcus@adlittle.com

USA
wylie.craig@adlittle.com

Authors

Guillaume Rominger and François Kassel

Arthur D. Little

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. Arthur D. Little 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.adl.com**.

4 Arthur D. Little Viewpoint, Why risk management is failing; Embracing complexity and uncertainty with value-based risk management, 2016