Illustration by Sylvia Neuner

Embracing complexity with value-based risk management

Reaching strategic goals in times of uncertainty

Kurt Baes, John Barker, David Boulton, Rick Eagar, Willem Romanus, François-Joseph Van Audenhove

The principles of risk management are well-established across large businesses, which clearly recognize that they need to manage uncertainty in order to meet their strategic objectives. This has never been more so than at present. Increasing industry convergence, accelerating technological disruption, and ever-higher ethical and social standards add further degrees of complexity to the mix.

Enterprise risk management (ERM) is a widely-adopted framework used to manage the full range of corporate risks. In a recent survey focusing on the energy and resources industry[1], 82% of respondents indicated that they had some form of ERM system in place. However, despite the prevalence and maturity of ERM systems, companies are still regularly caught out by significant unwanted events, sometimes catastrophic in nature, leading to loss of life or destruction of the business. Indeed, so-called "black-swan" events are less rare than is sometimes perceived, as we showed in a previous Prism article that predated the Deepwater Horizon drilling rig explosion[2]. More recent examples include the highly publicized use of engine management software by Volkswagen to pass emissions tests. Strategies that expose an organization to risk in order to achieve an objective are common – but in this case it appears that the significance and/or likelihood of the unwanted event were underestimated.

In the current environment uncertainties seem to be everywhere, making strategic planning more difficult than ever. Many companies use enterprise risk management (ERM) as a proven framework for managing risk. However, businesses are now looking to improve their track records when it comes to understanding and overcoming unwanted events. In this article the authors explore issues related to risk management and how the 6C framework can help.

[1] Risk Intelligence in the Energy and Resources Industry. Deloitte Touche Tohmatsu Limited, 2014

[2] Black Swan Events – Should you be concerned? Arthur D. Little PRISM, 2008.

As companies face a future of increasing uncertainty, disruption and complexity, it is therefore reasonable to ask whether current approaches such as conventional ERM are really still up to the job. Based on recent work in risk management with a range of global companies, we believe there are some practical ways to significantly improve the effectiveness of corporate risk management approaches: collectively, we call this value-based risk management (VBRM). In this article we explore issues related to such risk management and how VBRM approaches can help.

Conventional approaches to risk management

If we exclude the specific domain of financial risk management, conventional risk management approaches can be conveniently classified in two categories: Type A: which we could call the "accountant" approach, and Type B, the "assurance" approach. (See Table 1.)

	Type A: The "Accountant" approach	Type B: The "Assurance" approach
Focus	■ Detailed ERM system based on exhaustive listing and documentation of **all risks** in the organization ■ Heavy effort invested into risk evaluation (impact, probability) and risk ranking ■ Detailed upward cascade-based reporting of top risks to management	■ Focus on justifying risk ”assurance“ and their consequences ■ Upward reporting focused on taking comprehensive action for known hazards in order to mitigate risk ■ Comprehensive mitigation plans exist for those known areas in focus
Drawbacks	■ High management effort ■ Counterproductive in risk-averse company cultures (hides bad news) ■ Insufficient "practical tool" functionality for top management	■ Little effort is typically made to identify new risks (such as due to a change in the business environment) ■ Sometimes viewed too much as "complaint management" (not root-cause focused)

Table 1 **Conventional enterprise risk management approaches**

Source: Arthur D. Little

The "Accountant" approach tends to focus on comprehensive and exhaustive risk documentation and reporting, with heavy effort on screening, ranking and evaluation. It has the advantage that it is usually comprehensive, but may be less effective at deciding practical actions. This approach, is often used by service organizations. The "Assurance" approach, on the other hand, focuses more on known major risks and how these can be mitigated. Consequently, it is often less effective at identifying new cross-business risks as circumstances change. This approach is often used by the high-hazard industries, such as oil, gas and chemicals.

The prevalence of these two approaches is associated with a number of common risk management challenges, for example:

- **Poor response to complex systems:** In our article Becoming the Next Practice Business[3], we explored the different characteristics of complex and complicated systems. In a complicated system the relationship between cause and effect is knowable, but requires application of expert knowledge. In a complex system with multiple interactions, specific outcomes cannot be predicted irrespective of available expert knowledge. Safety risk management, which follows the "Assurance" philosophy, tends to assume that systems are complicated rather than complex, and there is little appetite for accepting uncertainty (for example, stakeholders, especially the regulator, do not accept that an employee might be injured or killed unless that probability has been quantified within specific limits). In the case of non-technical risks, such as reputation, the relevant multi-stakeholder systems are certainly complex rather than complicated – companies often fail because they try to over-simplify and model cause-and-effect, rather than applying strategies that accommodate the complexity.

[3] Bate (2015) Becoming the Next Practice Business: How to apply the strategy and management practices of creative disruptors to transform established business. Prism, Issue 1, 2015. Arthur D. Little.

- **Confusing documentation with management:** The "Accountant" philosophy can produce false confidence that risk management is effective. Formal safety risk management produces "safety cases", a structured, evidence-based argument that demonstrates a system is acceptably safe. These and similar outputs rely on a paper trail of documented risk management activities, but documentation does not necessarily give an indication of the quality of risk management activity. For example, in a recent review of a utilities operator a function-by-function ERM risk register was presented as evidence of good risk identification, assessment and mitigation across the business. However, cross-checking across the functions showed a severe cross-business risk relating to a lack of available, competent staff which had not been picked up by the system because of the focus on documentation rather than critical review.

- **Overemphasis on control of unwanted outcomes:** In both conventional approaches there is a tendency to overemphasize the "check" part of the "Plan-Do-Check-Act" cycle. Many ERM systems mandate specific control responses when certain risk thresholds have been reached. Such risk controls can work well for complicated systems where cause and effect is predictable (see earlier discussion), but for complex systems a cause may have unpredictable effects. Controls are often outcome-focused (i.e. managing the "effect") for reasons of simplicity – for example, controls acting on the level of reported risk or the time taken to implement a risk mitigation. In safety and technical domains, some progress has been achieved in managing so-called precursors (preceding indicators of potential future events), but this remains a difficult area. Overemphasis on outcome-based risk controls also diminishes active risk management and ownership by line managers. For example, we recently worked with a manufacturing company that had introduced a risk control at stage gates that mandated no risks above a certain level. Product managers had a tendency to "duck" the control by temporarily downgrading certain risks, which then re-emerged once the stage gate had passed.

What is value-based risk management and how can it help?

VBRM is a balanced approach to risk management that is more effective in managing these challenges than either the "Accountant" or "Assurance" approaches. VBRM is all about responding to change and dynamically focusing risk management efforts where they deliver the most value to the business. There are four main pillars to the approach (see Table 2) which are discussed in detail in the sections that follow.

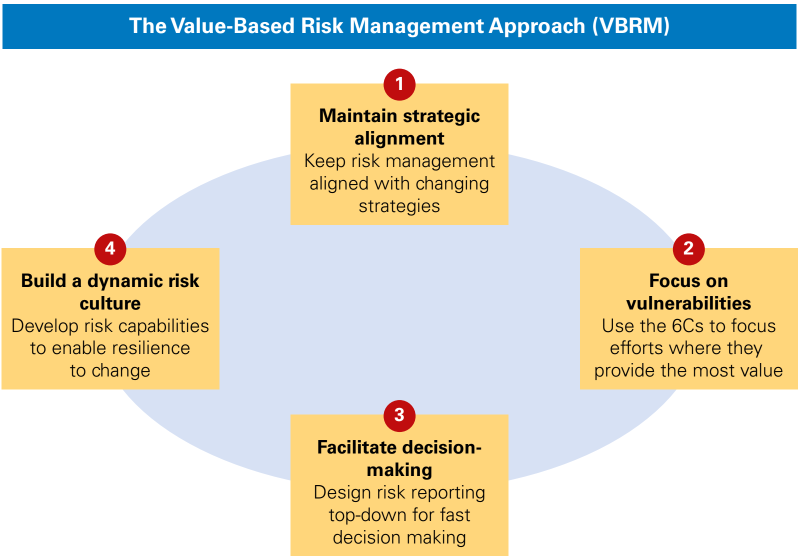

The Value-Based Risk Management Approach (VBRM)
1
Maintain strategic alignment
Keep risk management aligned with changing strategies
2
Focus on vulnerabilities
Use the 6Cs to focus efforts where they provide the most value
3
Facilitate decision-making
Design risk reporting top-down for fast decision making
4
Build a dynamic risk culture
Develop risk capabilities to enable resilience to change

Table 2 **Value-based risk management**

Source: Arthur D. Little

The VBRM approach has been applied effectively in large organizations with existing ERM systems in situations in which unwanted events persisted in occurring, or in which companies felt that they were not getting the return they were expecting from their ERM investments.

1. Maintain strategic alignment: Keep risk management aligned with changing business strategies

At its simplest, strategy is a high-level plan to achieve one or more goals under conditions of uncertainty. Strategies can be developed and changed rapidly – but the supporting management systems and processes that implement the strategy have much greater inertia. The root causes of poor risk management are often found in this disconnect between the strategy and the management systems and processes that implement it, when the former has changed but the latter has not kept pace. This is increasingly important in today's uncertain business environment, in which agility and the ability to flex strategies rapidly is a key success factor in staying ahead.

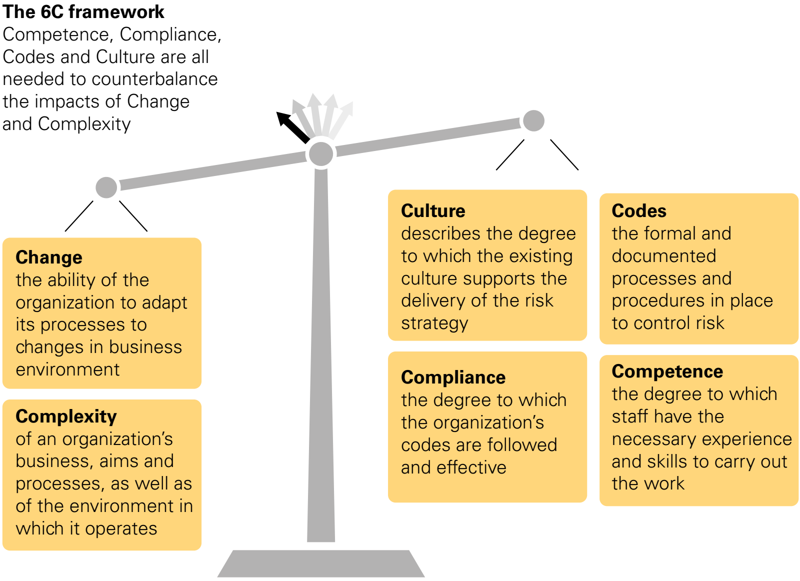
So what needs to be done in practice to keep risk management aligned with changing strategies? First of all, maintaining alignment means making choices between risk areas so as to avoid making decisions that do not support strategy, and communicating those priorities clearly to business units. For example, a European utility conglomerate developed a list of its top strategic risks from knowledge of recent adverse industry events – such as significant reputational damage reported in national media. This outcome-based assessment of priorities was completed to confirm alignment of all risk management activities throughout the organization. Only those activities that aligned with the top strategic risks and key investment projects were continued. Strategic reporting of all other risk management activities was reduced.

Second, maintaining alignment means allocating clear risk ownership, and ensuring that responsibilities and suitable empowerment for adapting systems and processes to respond to changing risk profiles are clearly defined. Some major risk areas will naturally align with business and functional units and ownership will be clear. However, many risks are transversal, and in such cases risk ownership will need to be specifically agreed.

2. Focus on vulnerabilities: Use the 6Cs to assess where to focus efforts

As we have seen, one of the drawbacks of conventional ERM systems is that they tend to be poor at indicating where best to focus efforts, i.e. they do not always identify clearly the areas of vulnerability, by which we mean areas where risk controls are potentially the weakest. This could be, for example, the absence of properly documented risk management processes across different business units. There are few pragmatic diagnostic models available to the risk manager for assessing vulnerabilities across all risk dimensions. An approach that has been developed by Arthur D Little to help in this process is the so-called 6C models. (See Table 3 below.)

Recommended approach: The 6C Framework



The 6C framework
Competence, Compliance, Codes and Culture are all needed to counterbalance the impacts of Change and Complexity

Change
the ability of the organization to adapt its processes to changes in business environment

Complexity
of an organization's business, aims and processes, as well as of the environment in which it operates

Culture
describes the degree to which the existing culture supports the delivery of the risk strategy

Codes
the formal and documented processes and procedures in place to control risk

Compliance
the degree to which the organization's codes are followed and effective

Competence
the degree to which staff have the necessary experience and skills to carry out the work

Table 3 **The 6C Framework**
Source: Arthur D. Little

The 6Cs are Codes, Compliance, Competency, Complexity, Change, Culture. Experience has shown that these six categories can support reasonable understanding of vulnerabilities without detailed quantification being necessary.

To apply the 6C, an assessment is made using each of the categories in turn. The assessment often begins with an evaluation of the suitability and completeness of rules, standards or practices (Codes), followed by the degree of Compliance with them. This already gives an outcome in terms of vulnerabilities – in many other existing approaches this is as far as the assessment goes. However, the 6C approach goes on to consider two other important factors which can greatly escalate risk: Competence (the degree to which staff have the necessary skills and experience) and Culture, which refers to how supportive and mature the culture is for to the delivery of the risk strategy. This can often provide evidence of new vulnerabilities which were not apparent based only on the more static "snapshot" picture provided by only looking at Codes and Compliance. For example, cultural reticence to acknowledge and report emerging risks (observed through the behaviors of senior management when risks are reported to them) can prevent an organization from being risk aware. Organizations with such cultural weaknesses may still have strong codes and good compliance with those codes – but risk management activities will most likely be ineffective.

Finally, the 6C approach goes on to consider two situational factors which can also significantly affect risk ranking: Change, the ability of the organization to adapt rapidly to changes in the business environment; and Complexity, the inherent complexity of the business and its environment. As we have indicated earlier, these are two factors that are increasingly important in today's uncertain business environment.

In practice a 6C assessment can be conducted fairly rapidly with the help of word-models to define levels of performance, as shown in

	Basic Performance	Common Practice	Best-in-class
Culture	Culture focuses on technical and procedural solutions; risk management is not seen as important to the business	There is organizational awareness of the need for risk management and employee involvement in risk control	All within the organization strive to deliver innovative risk control relevant to their job functions. No evidence of complacency
Codes	Codes are incomplete, with identified gaps or inconsistencies between documents	Codes demonstrate systematic management of all risk dimensions and are substantially complete	Codes demonstrate how the organization achieves continuous improvement against current best-practice
Compliance Lever	Some employees are aware of the need of risk management, but their work is largely seen as not relevant by others	Risk management is seen as integral to business processes, but still largely the work of specialist risk advisors	Responsibility for risk management is accepted by all as integral to job responsibilities and accountabilities
Competences	There is no single clear approach to the management of risk-related competencies	Training in risk competencies is provided in business units on an ad-hoc basis	An organization-wide competence management system provides all employees with required risk competencies

Table 4 **How 6C can help organizations to become best-in-class**

Source: Arthur D. Little

Table 4 below for Culture, Codes, Compliance and Competence. With the help of these word models, organizations can see not only where their real vulnerabilities are, but also what levers for improvement and evolution are the most appropriate (with that lever being compliance in the table above). The 6C approach has particular advantages in that it helps to cover cross-business vulnerabilities which may not be apparent from a conventional business-by-business review, and it focuses on situational and circumstantial issues such as Change and Complexity, which are often neglected in conventional approaches.

3. Facilitate decision-making: Design risk reporting top-down for fast decision-making

One of the most common problems in ERM systems is that the mode of reporting to top management does not lend itself well to making decisions. The most common high-level overview is a semi-quantified (i.e. with high-to-low ranges) matrix of likelihood vs severity showing the top 10-20 corporate risks. These often acquire a state of semi-permanence and end up as "wallpaper" behind more pressing top-management reporting information. This is a particular problem when situations are changing rapidly, as is often the case today. It is essential therefore that reporting systems are designed to provide better pointers to rapid top-management decision-making and action. In general, actions could be around obtaining better information to understand a risk better, taking the right sort of direct risk mitigation measures, pursuing a back-up option, or increasing levels of monitoring.

One of the key features of the VBRM approach is therefore to ensure that top management has the right risk management reporting systems to enable rapid response and decision-making, triggering actions that effectively reduce risks before they materialize. This way, the links between strategy execution and risk management controls remain close and surprises are kept to a minimum. In practice this means designing reporting tools that:

- Provide specific risk data (such as for key projects, businesses, ventures, etc.) as well as for the corporation as a whole

- Are concise in how they summarize and aggregate data

- Include a ranking of urgency for action

The case study on the opposite page illustrates an example of such a system for an automotive company.

4. Build a dynamic risk culture: Develop risk capabilities to enable resilience to change

One of the most effective levers to ensure that a company's risk management approach is able to cope well with change and complexity is to focus on strengthening capabilities, culture and awareness. This provides the means to proactively identify new and emerging risks, and to take the right actions to adapt management systems and processes rapidly in response. (See also point 1 above.) This culture and capability aspect is often neglected in conventional ERM approaches.

Of course, culture change within any organization is difficult and risk management culture change is no exception. However, the VBRM approach includes a number of measures which can be effective, including:

- Providing a clear path of evolution towards risk management excellence: as mentioned in point 2, the 6C approach, with its supporting tools and templates, can provide a clear focus for what needs to be done to progress. Ultimately, this clarity of direction will lead to culture change.

- Engaging employees in pilot projects: As mentioned in the Case Study, the use of specific projects and initiatives to run pilot projects is an excellent way both to demonstrate impacts and effectiveness, and to engage employees in practical work. In our experience intense focus on a few areas (for example, a small number of pilots of new risk management approaches) is the best means of effecting change. Involving staff from a range of different functions to work in the pilot teams is also important.

Case study: Deploying a management action-oriented risk management approach for a large automotive OEM

Company D is an automotive OEM, managing multiple brands across a global production and distribution network. Problems in the performance of critical development projects, as well as increasing complexity and rapid change in the global mobility and regulatory landscape, prompted Company D to re-appraise its risk management approach as part of broader strategic changes.

Previously, risk management had been a corporate activity that did not make deep-dives into focused projects, but kept an overall company-wide view, relying on operational entities managing the risks at their level. Regular reporting to the Board of risk management activities gave a false sense of security. Despite all anecdotal evidence suggesting increased levels of risk, the top risks reported to the Board remained the same. These misgivings were proved to be correct when it was identified that the OEM had insufficient R&D capability to meet deadlines within two critical development projects due for completion within the same quarter. This risk had not been identified.

Given the criticality of a number of other complex, large-scale, highly connected and interdependent projects for the future success for the firm, it was decided that a new risk management approach was needed, which would be piloted on two such projects in different locations.

The new approach required the OEM to "define and implement actions to achieve project success". The focus was therefore, by and large, action oriented. Although classical risk management frameworks were used for identification and assessment, the main top-management tool was the "action matrix for risk management", which set out clearly the time-limits and urgency of management action for particular risks.

Risk level			
High	**ACT NOW**	**Urgent**	**Plan**
Medium/High **Medium**	**Urgent**	**Monitor**	**Monitor**
Low	**Monitor**	**Monitor**	**Monitor**
Time limit for action	**Short** Before the next gate	**Middle** Up to two gates away or a continous risk	**Long** More than two gates away

This approach, adopted alongside a range of other tools and approaches to ensure a dynamic and responsive risk management approach, proved to be highly effective in ensuring that rapid action was taken in response to changing situations. The OEM found its top risks changed significantly with application of the new approach, leading to further refinement of overall strategy and better understanding of the level of risk that the Board was willing to accept.

- Identify your burning platform: Numerous companies that have implemented risk management fail to keep momentum. A commonly-understood “burning platform” is a key way to promote risk awareness and the importance of pragmatism and action-orientation. Burning platforms can result from an unwanted event or near-miss within the company, a major loss suffered by a competitor, or a significant change or disruption in the business environment. Sometimes senior management can even “engineer” a burning platform, for example by highlighting particular risk areas to which the company is exposed.

Insight for the Executive

In today’s business environment of increased uncertainty, complexity and continuous change, conventional risk management approaches can be ineffective: they are often poor at dealing with complexity, too bureaucratic and slow to adapt to changing circumstances, and overemphasize rigid controls on outcomes rather than causal factors.

In our work with companies, we have seen how these problems can be overcome with a more dynamic and focused approach to risk management. VBRM is such an approach, and can be readily applied by companies irrespective of the ERM systems they already have. The essential elements of VBRM are:

- Maintaining alignment of risk management systems and processes with changes in strategy, through establishing risk-based priorities in strategy implementation, and allocating clear responsibilities and empowering risk owners to adapt management systems and processes as required.

- Focusing risk management efforts on areas of vulnerability, ensuring that not only Compliance but also factors such as Competence, Culture, Complexity and Change are taken into account in risk ranking. The 6C approach, for example, provides a practical way to accomplish this.

- Designing risk management reporting systems to facilitate and enable rapid top-management decision-making, meaning that they should include specific risk data for key projects, provide concise summaries and include a ranking of urgency for action.

- Building a dynamic risk culture through active involvement in pilot projects, engaging the organization in progressive evolution towards excellence, and identifying a genuine burning platform that people understand and believe in.

The business world is not the same as it was when many of today's ERM approaches were put in place – we think it's time for a change.

Kurt Baes
is a Partner in the Brussels office of Arthur D. Little, and member of the Strategy & Organization and Operations Management practices. He heads the Energy & Utilities and Manufacturing practices in the Benelux.

Dr John Barker
is a Principal in the Cambridge office of Arthur D. Little and member of the Risk Practice.

Dr David Boulton
is a Principal in Arthur D. Little's Risk Practice, specializing in safety-critical systems and risk management.

Rick Eagar
is a Partner in the London office of Arthur D. Little and global head of the Technology & Innovation Management Practice.

Willem Romanus
is a Principal in the Brussels office of Arthur D. Little. He is member of the Strategy & Organization and Operations Management practices.

François-Joseph Van Audenhove
is a Partner in the Brussels office of Arthur D. Little. He is a member of the Strategy & Organization and Risk practices and heads Arthur D. Little's Global Competence Center in Rail and Urban Mobility.