



**Peyman Mestchian,**  
BEng, MSc,  
MBA, FIRM is  
Head of the  
Risk  
Intelligence  
Practice for  
SAS EMEA. He

has over 15 years experience in risk management, having previously worked as director of the Business Risk Consulting Practice at Ernst & Young, where he led numerous board-level consulting assignments on enterprisewide risk management. He is a Fellow of the Institute of Risk Management and holds an MBA from the London Business School.

## Risk intelligence – from compliance to performance

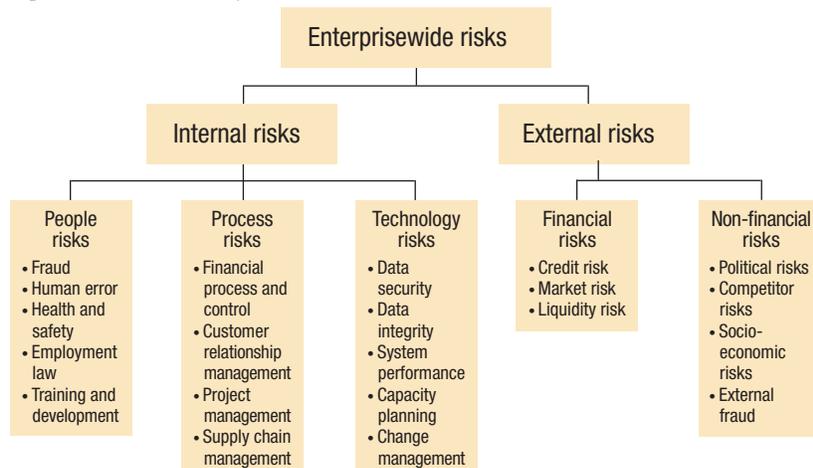
By Peyman Mestchian, SAS EMEA

*“There are risks and costs to a program of action, but they are far less than the long-range risks and costs of comfortable inaction”.*

– John F. Kennedy

Harsh regulatory and economic realities have led many financial institutions to adopt new risk management systems in the hope that those systems will help companies extract greater insights from the data generated by their operational and transactional systems. Basel II, Sarbanes-Oxley and new corporate governance and accounting standards have resulted in organisations embarking on multiple systems implementation and integration projects as part of an enterprisewide compliance programme. Too often the decision making has been “knee-jerk”, piecemeal and tactical. The reality is that most managers are unaware of the fact that risk management systems do not always have a positive impact on the overall risk performance of the firm. This is why, not surprisingly, they are often disappointed about the implementation results of risk management programmes.

Figure 1: A taxonomy of business risks



Unfortunately, research into risk management systems has tended to ignore many of the strategic implementation issues. The purpose of this article is to fill part of this gap.

### What is risk?

Risk is the chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood. Within a business context, risk is the threat that an event or set of circumstances will adversely affect an organisation's ability to achieve its business objectives.

Poor management of risk can have a negative impact on the achievement of business objectives and, ultimately, shareholder value. This can materialise in a number of ways:

1. **Direct loss:** trading loss, assets stolen (by clients, employees or the competition), physical damage, litigation costs, human error resulting in irrecoverable asset or fund transfer, unexpected staff costs, regulatory penalties.
2. **Indirect loss:** brand erosion, loss of market share, key staff leakage, loss of key customers, increased insurance costs.
3. **Opportunity costs:** lack of innovative product development, forgone opportunities to enter new markets, missed opportunities to leverage the latest technologies and gain a competitive edge.

## What is risk management?

Risk management is a subtle and often complex concept. A review of the literature shows that there are a variety of different theoretical and practical approaches to risk measurement and management. Despite the variety of analyses and lack of standards, four key factors are central to most research on risk management. Specifically:

1. Risk management is a process.
2. Risk management belongs to everyone in the firm.
3. Risk management requires qualitative and quantitative data.
4. Risk management needs sponsorship from the top.

At a more detailed level, risk management is about the effective use of resources through improved quantitative analysis, process efficiency, establishment of a sound system of internal controls (including removing redundant and ineffective controls), the sharing of knowledge and good practice, leveraging of technology to collect and analyse internal and external data, and prioritisation of effort. Like any other significant business process, enterprisewide risk management needs to be supervised and reviewed.

Ultimately, risk management is the same as good business management.

## Key challenges

While there is an industrywide consensus that risk should be tackled in this way, organisations are faced

with a multitude of practical challenges on how best to develop effective systems and functions for risk management.

Only a minority of firms are viewing the compliance challenge as a real business opportunity. It is an opportunity to improve systems and operations as well as create real sustainable competitive advantage.

Businesses can gain competitive advantage in many ways – for example, through strategy, systems and people – but these can be short-lived. Strategy can be copied, technology can be reproduced and people can be poached. But a firm’s data is unique and can be the source of competitive differentiation that cannot be copied.

Unfortunately, even after acquiring risk management systems, true competitive differentiation often remains elusive. This is for four main reasons:

- Other firms are probably doing the same thing.
- The power of predictive analytics is not made available to those who need it, when they need it.
- Traditional risk management systems have been deployed tactically in silos that mirror the organisational systems.
- The technology architecture cannot support the risk strategy.

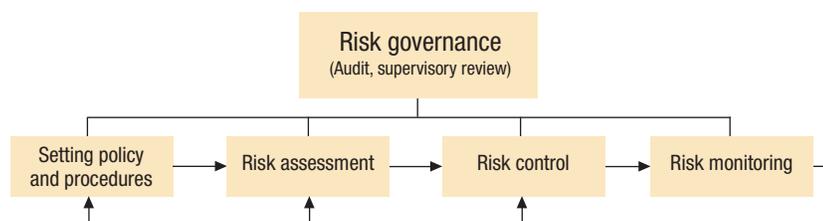
The demand for new tactical systems from the business shows no signs of slowing. The credit risk director

demands best-in-class analytics and modelling functionality. The operational risk director wants a robust enterprisewide system for integrating quantitative and qualitative data. The CIO needs a fully scalable and flexible architecture at minimum cost. The CRO (chief risk officer) wants a consolidated ‘risk dashboard’ to monitor and report on key risk indicators and exposures. The CFO needs a fully auditable and transparent reporting mechanism. The common theme among all of these new solutions is they are not operational, they are informational – not based on information from a single operational system, but from across the enterprise, wherever it may be found.

Company leaders must deliver these tactical systems that meet regulatory pressures, deliver answers quickly and mitigate business risk. And they need to do it all with a reduced budget. Meeting this dual challenge to develop an enterprise view of information while working with a reduced budget means firms need to balance short-term tactical goals against long-term strategic goals that are linked to performance targets.

People and culture issues around risk are significant. By definition, risk is often caused by human-factor failures including human error, fraud and lack of knowledge. Similarly, to truly address risk, risk management needs to be embedded into all business processes and activities. This task requires accountability, responsibility, rewards and empowerment for each individual within the organisation to identify, assess and treat the risks within their sphere of control. Ultimately, the best policies, procedures and systems in the world will not be sufficient unless the people within the organisation understand why these tools are important and are motivated to use them – no one gets credit for fixing a problem that never happened.

Figure 2: A summary of the risk management process.



## Link to performance

While performance (i.e. profits and stock prices) is generally healthy in many segments of the financial services market, delivering results is a lot more risky today than in the past. The key reason is complexity (globalisation, new technology, competition and the current regulatory environment). Shareholder value is created when the reward exceeds the cost of risk: cost of capital is a generalised rate that reflects the riskiness of a given class of investment. If the reward (ROI) is higher than that rate, the investment is worth proportionately more. Risk intelligence is an embedded and systematic approach to managing risk, which means that risk, risk factors, mitigation and capital management programs are considered in relation to business performance, internally and externally. Risk intelligence is about breaking the traditional silos of market, credit and operational risk – shareholders are indifferent to arbitrary compartmentalisation of risk. Risk intelligence is proactive. Risk intelligence is about turning risk data to actionable knowledge.

## Implementation strategies

- Firms should consider how and whether they embed risk management systems in their business processes. It can be argued that risk management can only be successful when systems are strategically embedded. In certain situations firms should adopt a tactical approach – to meet short-term goals. However, all firms should undertake a cost-benefit analysis to ensure that their tactical choices do not result in substantial costs

and rework in the long term. This analysis could also affect the overall credibility of the risk management initiative.

- Firms should move toward a single risk technology platform that builds on existing technology investments to deliver high-quality information to every person who needs it, adding value at every step of the way and providing a single version of the truth. This single platform should provide *breadth* by integrating functions and technologies from across the enterprise; *depth* by reaching all who need risk information, in a way that is relevant to them; *completeness* by providing a comprehensive, end-to-end environment; *advanced analytics* for delivering predictive insight, not just hindsight; *data quality* by giving all applications one validated, verified version of the facts; and *intelligence storage* by meeting the informational needs of risk intelligence applications.
- Top management support is essential for strategic implementation of risk management systems. Such support not only helps to transform the organisation and culture but also ensures the continuation of risk management projects that experience setbacks.
- Finally, firms often consider risk management software the key to success in risk management implementation. Although a substantial part of the risk and governance budget will need to be allocated to software, decision makers should improve the overall risk management process and apply the software to enable and automate that process.

## Conclusion

There is currently a lot of regulatory focus on risk management and corporate governance. This has brought the subject higher up the corporate agenda and has initiated substantial compliance-driven projects across all industries. However, regulatory compliance is not the best reason for enhancing risk management systems and processes. A purely regulatory view will, in general, lead firms to implement the least amount of risk management required for compliance. As a result, these companies are not realising the full business benefits of effective risk management. Thinking beyond compliance and focusing on the significant and unquestionable returns that can be derived from effective risk management will move this discipline into the next phase of development and embed it as part of every company's complete value-chain.