Chartered Institute of Management Accountants

Margaret Woods
Aston University, UK

Aston University

airmic

Reporting and managing risk

A look at current practice at Tesco, RBS, local and central government

Research executive summary series

Volume 6 | Issue 8

Key findings:

- Risk management is no longer solely a financial discipline, nor is it simply a concern for the internal control function.
- Where organisations retain a discrete risk management cadre – often specialists at monitoring and evaluating a range of risks – their success is dependent on embedding risk awareness in the wider culture of the enterprise.
- Risk management is most successful when it is explicitly linked to operational performance.
- Clear leadership, specific goals, excellent influencing skills and open-mindedness to potential threats and opportunities are essential for effective risk management.
- Bureaucratic processes and systems can hamper good risk management – either as a result of a 'box-ticking mentality' or because managers and staff believe they do not need to consider risk themselves.

This research was funded by the Chartered Institute of Management Accountants in association with the Association of Insurance and Risk Managers.

Comments from the Association of Insurance and Risk Managers

The Association of Insurance and Risk Managers (AIRMIC) welcomes this report on a topic that has increasing relevance to the success and good governance of all types of organisations. While the case studies are diverse, the common messages are obvious, providing information and guidance for senior management, as well as offering lessons to risk managers who are seeking to make an enhanced contribution to the success of their employer.

The importance of maintaining a risk aware culture is recognised in the new UK Corporate Governance Code and the components of a successful risk aware culture are described in this report. Also, the benefits of a well developed risk reporting structure (risk architecture) are explained, including the need to establish risk escalation procedures. Risk communication within risk architecture enables an organisation to achieve a consistent and appropriate risk response. This approach will enable risk management activities to fully support the achievement of the strategic objectives of the organisation.

Overview of the project

This report summarises case studies on risk management practices at four major organisations: Tesco, Royal Bank of Scotland (RBS), Birmingham City Council and the Department for Culture, Media and Sport (DCMS). The full case studies themselves are available in a book along with supporting material on risk management. A link to the site where the book can be ordered is given at the end of this document.

The authors of each report interviewed key staff to gain a sense of how risk management was working at their organisations, as well as incorporating material from annual reports, other publicly available statements and internal risk management documents. In each case, the authors have also explored any external pressures on risk, particularly from regulators or legislation.

These case studies are a snapshot of risk management at an important time for both the public and private sectors. Tesco has continued to thrive during the recession and remains a robust and efficient group of businesses despite the emergence of potential threats around consumer spending and the supply chain. RBS, by contrast, has suffered catastrophic and very public failures of risk management despite a large in-house function and stiff regulation of risk controls.

Birmingham City Council, like all local authorities, is adapting to more commercial modes of operation and is facing diverse threats and opportunities emerging as a result of social change. And DCMS, like many other public sector organisations, has to handle an incredibly complex network of delivery partners within the context of a relatively recent overhaul of central government risk management processes.

So although these cases provide only a limited insight into risk management across the economy, they nevertheless contain important and timely messages about the effective monitoring, evaluation and control of enterprise risk.

Introduction

CIMA is clear about the importance of 'the process of understanding and managing the risks that the entity is inevitably subject to in attempting to achieve its corporate objectives'. Our definition is carefully worded; risk is not something to be managed away. It is something to be understood and harnessed in pursuit of a clear goal: sustainable performance.

The case studies that form the bulk of this report show that high profile organisations do, indeed, take this to heart. They don't treat risk as a discrete factor to be handled in some dark corner of the enterprise – it's woven into every aspect of management and operations.

That's not to say these organisations don't treat it seriously. Far from it, the use of specific processes to monitor risks – and feedback systems which facilitate appropriate ways of handling them – is a common feature of all these cases. And in each case, some form of internal audit team provides either an oversight function or acts as an expert link in that feedback loop.

These more formal risk monitoring teams and the controls they devise to manage risks are important. But these case studies highlight the need to embed risk management within more easily understood behaviours, consistent with the overall organisational culture. Frontline staff, managers and specialists should be completely aligned on risk, in part just to ensure that there is a consistency of approach. They should understand instinctively that good performance includes good risk management.

Nevertheless, the approaches analysed here are very different. Tesco, with a relatively straight forward business model and easily identifiable risks, aims to keep bureaucracy to a minimum. Royal Bank of Scotland (RBS) faces far more complex risks, is much more heavily regulated – and has a distinct 'risk community' of specialists numbering more than 4,000 strong. Birmingham City Council has incorporated risk management into its core service delivery approach. And the Department for Culture, Media and Sport (DCMS) uses a highly structured risk framework to manage projects that cross divisions and feature a host of third parties.

They offer an insight into the growing profession of risk management – and suggest that while financial expertise (and management accountancy in particular) is still an essential component of a risk strategy, there are a host of complementary skills that go into successful approaches to risk.

Tesco: risk in the round

- Customer loyalty is the group's defining objective.
- An easy to use version of the balanced scorecard helps all staff understand their responsibilities.
- Risk management is embedded in day-to-day operations, but is rarely discussed as such.
- The board sets risk appetite and discrete risks are owned by named managers.
- The personal finance business has required its own set of much more complex risk management approaches.

Tesco is an extremely successful business, thanks in part to a coherent strategy that drives every part of the organisation. Its approach to risk management is closely aligned to the company culture, which in turn is defined by a strong leadership team, clear systems of management and control, a flat structure and simple objectives.

Or, rather, a single objective: customer satisfaction. Tesco's staff, from CEO to shelf-filler, is focused on building customer loyalty. External factors such as competitor activity might affect decision making at the periphery. But the board feels that shareholder value flows from operational efficiencies designed to help its own people exceed customer expectations.

Risk management, as a discrete function at least, is no exception to that rule. That doesn't mean risks aren't analysed or managed. Rather, the culture demands that they are handled as part of the customer service proposition. Risk management is part of a clear and easily articulated objective instead of being a series of systems and controls that might be perceived as counter-cultural, bureaucratic, or worse–box-ticking.

As a simple business – buying and distributing goods, marketing and managing cash – Tesco's principal risks centre on the robustness of its processes. Any failure in the supply chain, for example, damages the business in the eyes of customers. So any risks to its smooth operation must be identified and managed. A relatively flat structure helps. Although it employs almost 470,000 people, Tesco only has five levels of management, so accountability for risks is generally very clear.

Figure 1: The Tesco 'Steering wheel' - its own version of the balanced scorecard.

Financial risks are treated separately by the treasury function. Tesco Personal Finance has risks that have to be managed differently. Many of them were formerly managed by banking partner RBS (see case study two) but with the switch to Tesco Bank and full ownership of that arm of the business, the group is having to develop new skills internally to cope. A key question is whether the group's integrated approach, where risk management is implicit in good performance, can work in this sector.

Tesco has a standard governance hierarchy – a top-level board of directors controlling strategy, supported by more operationally focused subsidiary boards and functional committees. There is no distinction between the UK and overseas businesses, which ensures strong consistency of processes for strategy and risk management.

At the centre of these committees and teams sits the Tesco 'steering wheel' (see figure 1 on page 2) – its own version of the balanced scorecard. This lists the key strategic objectives for five core areas – customers, community, operations, people and finance. The goals are consistent with the group's rolling five-year plan and are further divided into KPIs that connect strategy with day-to-day operations.

This means that the steering wheel works to manage risks from two directions. It ensures staff and management are clear about their objectives – shopworkers can see exactly what's expected of them, for example, in terms of in-store customer experience and understand how risks can devalue their performance. And it helps senior management quickly identify areas where objectives are not being met so they can be addressed.

This ensures that risk management is invisible, but remains fundamental to the business. The board sets a risk appetite, informed in part by line management who identify key risks to the business using a risk and materiality matrix. Risk controls are then built into processes and systems and monitored by both line management and internal audit. Feedback from the process – driven by actual performance – helps the board shape the strategy… and the process repeats.

Internal audit (IA) also facilitates the preparation of risk registers as part of that feedback loop, covering the likelihood and impact level of named risks. These are then assigned to named 'owners' who help to identify controls and processes to manage them. IA ensures those controls are consistent with the board's risk appetite.

So the actual processes behind either exploiting or mitigating risks are quickly devolved to people who are much closer to those risks. There's minimal bureaucracy to risk management, which prevents a drain on resources and minimises distractions for front-line staff. And the group allows a focus on performance to manage risk by default. The simplicity of this risk model reduces the chances of risks falling through any gaps – and ensures there's less to go wrong.

RBS: the value of judgment

- External regulations can encourage 'box-ticking', not proper risk management.
- Internal control bureaucracies can create a false sense of security around risk.
- Organisational culture is crucial to embedding appropriate attitude to risk.
- Financial modelling offers many answers around risk – but human judgment is a key component for managing it.
- In complex groups, the real danger is aggregate, compound risks.
- Effective scrutiny falls down if risk management committees sit beneath the board in the governance hierarchy.

Modern banks pose some of the sternest challenges in risk management. Their core competency is protecting money, but they are evaluated on their ability to profit from taking complex risks. Recent events have thrown these issues into a stark light, particularly for large banks like RBS which engaged in both straightforward banking and in exploiting risk to generate returns across several jurisdictions.

Banks have plenty of external guidance on risk: Sarbanes Oxley, the Combined Code, the Basel II capital adequacy rules or ARROW (the Advanced, Risk-Responsive Operating FrameWork) which is a supervisory tool used by the Financial Services Authority, UK. But the rapid growth of complex and exotic financial instruments complicated things. Banks had to develop new techniques, such as Value at Risk (VaR) to evaluate their levels of risk exposure.

RBS had a well staffed risk management function – which more than doubled in size to 4,250 staff in the two years to 2006, prior to the financial crisis. Group Risk Management (GRM) helped co-ordinate a 'three-line defence'. Managers were the first line, handling risk in day-to-day operations. The second line, GRM itself, was responsible for administering a structured operational risk framework to oversee controls. Finally, internal audit ensured controls were properly applied. The group board spelled out the overall risk appetite for both financial risk and qualitative risks, such as customer satisfaction. High level risks were assigned to a named executive and the audit committee reviewed overall risk management processes.

The chief risk officer in the pre-crisis period was clear that risk management was a multi-faceted role, including enforcement of policies and acting as an ambassador to communicate good practice and a consistent approach across all business divisions. And the risks faced by the organisation were well articulated. Six main categories of risk were clearly defined and evaluated: credit risks (including country and political risks); funding and liquidity; market risk; insurance risk; operational risks (fraud, human error, and external events); regulatory risks; and 'other' (primarily reputation and pension fund risks).

This register was updated constantly. For example, between 2004 and 2006 liquidity risk was separated out and insurance risk was added as a result of its increasing share of the group's income. RBS also used 'horizon scanning' to help it identify and mitigate, for example, forthcoming changes to regulations or economic conditions.

At the divisional level, local CEOs were personally accountable for risk management. Divisional chief risk officers (CROs) also reported to the group CRO (and the divisional risk officers for each category of risk into that category's group head of risk) to ensure a consistency of approach. RBS also claimed its risk philosophy was embedded in day-to-day activities.

So what went wrong with risk at RBS?

There were two changes of chief risk officer after 2007, which clearly complicated matters at a crucial period for the bank. The CEO, whose opinions on risk management may have gone unchallenged, was a dominant figure. With key risk management committees sitting below board level, there were also questions about their level of influence over board decisions.

An aggressive risk culture appears to have permeated down through the organisation. Ron den Braber was working in the bank's London office in 2003 when he became worried that the bank's models were underestimating exposure to credit risk. When his bosses failed to listen to his message, he left the bank.

The compartmentalisation of risk – credit, market and operational risks sat in silos – negated the benefits of a structure designed to cascade risk management down through different divisions. It meant portfolio risks, aggregating across the silos, developed unchecked. Divisional CEOs had return on equity targets that perhaps encouraged them to take risks which were apparently managed within their silo, but not so clearly at group level.

Too much emphasis was placed on the need to quantify risks. Banking products have explicit (if extremely complex) financial values that can be modelled. It's tempting to use even more complex derivatives of those products and yet more sophisticated models to declare the risk on those activities 'fully mitigated' – and to forget about the value of complementary subjective judgments about the business and its overall objectives.

Sir Fred Goodwin's successor as CEO, Stephen Hester, identified this as a critical problem in his evidence to members of the Scottish Parliament investigating the crash. *'What was missed was obvious to all. That's not to say that things hidden in drawers should not be risk-managed, that's an incredibly important part of any bank. [But] It wasn't detailed risks that made RBS weak; it was the big macro imbalances.'*

Local government: risk and accountability

- Birmingham City Council addresses risk at both a group and directorate level, delivering both local accountability and corporate assurances.
- Risk management is considered fundamental to the council's ability to deliver core services.
- A traffic light system allows the council to prioritise risk control efforts.
- Internal audit offers assurance on systems and controls, as well as supporting risk management and mitigation efforts.
- Investment in dedicated risk systems helps keep risk registers current and effective.

Local government in the UK is broken down into county, borough, district and unitary authorities which have responsibility for providing local services such as education and housing. Council policies are set by elected officials, but they are managed and run by full-time staff. Although largely autonomous, councils are subject to oversight by central government agencies – including audits of internal controls. Central government also provides the bulk of their income.

The Chartered Institute of Public Finance and Accountancy's local government risk framework is based on a belief that 'good governance structures enable an authority to pursue its vision effectively as well as underpinning that vision with mechanisms for control and management of risk'. In other words, risk management is implicit in good performance.

Since 1999, the application of best value rules for councils, Comprehensive Performance Assessments (CPAs) and the Comprehensive Area Assessments (CAAs) – mean both senior management and elected members must manage key strategic risks and develop formal risk management systems.

At Birmingham City Council, the largest local authority in England with one million inhabitants, there are a wide range of risks that need to be carefully monitored and managed. Individual directorates – such as 'adults and communities' – each handle a number of services and have their own governance structures. So risk dependencies are extremely clear, providing all parties communicate well and are explicit about the scale, likelihood, consequences and tools for mitigating risks.

At the corporate level, the council has a clearly articulated risk management strategy to ensure it can achieve its objectives – so the link with performance is explicit. It emphasises the integration of risk management into the culture of the council; the need to anticipate risks in several different domains; address the costs of risks; and spread the risk message to external agencies serving council ends.

The corporate director of resources heads up risk management. The directors deliver annual assurance statements which form the basis of the mandated chief executive's review of internal control – considered a more demanding statement than that required of private companies under the Cadbury Code.

Birmingham Audit (BA), the council's internal audit team, handles risk management on a day to day basis. To avoid conflicts of interest, the team is split in two – one side auditing, the other helping design and implement risk management processes. Traditional financial assurance and propriety is now just 16% of their workload. The remainder is risk management, corporate governance and operational support activities, including training staff on risk identification, monitoring and mitigation. BA staff tend to train with the Institute of Internal Audit or Institute of Risk Management rather than seek an accountancy qualification.

The council's risk management methodology has five parts.

Firstly, risk and opportunity identification. Internal audit prompts decision makers to consider a number of different areas in any service area, including environmental, legal, political, financial, social, reputational, managerial, physical and technological risks. The results are codified into a risk register. That need to attach risks to the ability of the council to deliver its services also applies at a corporate level to account for interdependencies and plan for much more general threats and opportunities.

Example: library service

Risks may include:

- Failure to comply with legislation on disability access.
- Theft of books/DVDs/CDs.
- Under performing on level of library usage for the CPA target.
- Poor security of buildings which may increase the risk of burglary.
- Lack of funding to offer internet facilities at neighbourhood libraries, despite a promise to do so in the current 3 year plan.

Secondly, analysis. Risk managers use tailored likelihood/impact matrices to create two-dimensional views of how inherent risks might impact delivery. This enables them to

move to **stage three, a prioritisation matrix.** This drives a traffic light system. High probability, high impact risks (the 'red' ones, coded 'severe') are immediately communicated through the chain of command and addressed to secure service delivery. The council's risk appetite defines which areas of the matrix are coded for amber ('material', requiring close monitoring and cost-effective control improvements) and green ('tolerable', simply requiring review).

If action is called for, it happens in **stage four, management**. The key decision here is whether to accept, control, modify, transfer or eliminate the risk. Once the reasons for the decision have been recorded, an individual is assigned responsibility for implementing it and an action plan agreed. The aim is to shift the risk from 'severe' to 'tolerable' in the prioritisation matrix – at a reasonable cost.

Finally, monitoring. The risk registers and action plans are reviewed continuously and BA keeps a check on the effectiveness of the policies in play. BA also works to maintain a consistency of approach across the council, partly though monitoring, but also via training and clear communication of the aims of internal audit. Staff should see the link between risk and performance.

Birmingham places a lot of emphasis on strong systems. It uses the Magique risk management software that supports training; real time updates to the risk registers; an events log; and scope for communication of risk information across directorates. It drives the collation and analysis of information relevant to risk at every level in the council. Council databases are shared to ensure, for example, benefit fraud is automatically spotted, freeing up fraud control staff for more complex risk management functions.

Central government: structures for risk

- Risk management disciplines have become much more structured in recent years.
- Strong government-wide approaches to risk are complemented by clear risk management policies at the Department for Culture Media and Sport.
- Managing risk across numerous partner organisations and departments for each programme or project remains a challenge.
- Risk expertise is brought in from a sister department to make up for limited in-house resources.
- Communication and accountability are the key aspects of department risk culture.

A structured approach to central government risk management has become the norm in recent years thanks to so-called new public management. In 2004, a risk improvement programme was rolled out in government, which incorporated best practice from the private sector and benchmarks from a variety of public sector and commercial organisations around the world. It also laid out a formal risk assessment framework – a standardised tool to help departments judge their risk management capabilities in areas such as leadership, strategy, people, partnerships and processes.

Today, the Treasury's risk support team co-ordinates risk management at strategic, programme and operational levels. A framework sitting above 'policy domains' ensures projects that cross departmental boundaries or that incorporate third parties are properly controlled. It also helps avoid systemic or aggregate risks building up. Each department also applies its own context-specific processes and systems. Local approaches allow for risks to be handled appropriately – for example, the Ministry of Defence has a different view on IT security to the libraries service.

The Department for Culture Media and Sport (DCMS) has a broad spread of activities – including lead policy responsibility for 54 public sector bodies that fall outside its departmental accounting boundary. So its risk challenges are complex, yet typical of a central government department. Its 2009 Risk Management Guide sets out a feedback loop to ensure risks are handled properly. It starts with clear objectives for the department. Then a strategic risk register is mapped onto the major objectives described in the corporate plan. Programme level and project/operational risk registers help ensure that strategic objectives are properly cascaded through the organisation.

The first step in the DCMS Risk Management Framework is to identify risks to those objectives, then assess them. A response appropriate to the risk is formulated – which is then reviewed, helping to further clarify objectives and strengthen each of the other steps. The guide also includes a list of broad risk areas to help staff stay open-minded and about the full range of risk management requirements (see table on page 7). Some key areas of risks (see table on page 7) – relationships, operations and governance – are also shared with delivery partners such as the non-departmental government bodies.

Table: Common Types of Risk Facing DCMS

RISK CATEGORY	EXAMPLE
1. EXTERNAL: not wholly within the department's control	
1.1 Political	Change of government or cross cutting policy decisions
1.2 Economic	Global economic conditions
1.3 Socio-cultural	Demographic change
1.4 Technological	Systems obsolescence; procurement costs
1.5 Legal	EU legislation/directives
1.6 Environmental	Changes in attitudes to the environment from government, media and consumers
2. OPERATIONAL: related to current operations – delivery, capacity and capability	
2.1 Delivery	
2.1.1 Service/product failure	Failure to deliver within agreed terms
2.1.2 Project delivery	Failure to deliver on time/budget
2.1.3 Capability and capacity	
2.1.4 Resources	Poor budget management; insufficient HR capacity/skills; loss of assets e.g. via fraud or theft
2.1.5 Relationships	Lack of clarification of partner roles; poor customer satisfaction levels
2.1.6 Operations	Overall capacity to deliver
2.1.7 Reputation	Lack of confidence or trust
2.2. Risk management performance and capability	
2.2.1 Governance	Compliance with requirements
2.2.2 Scanning	Failure to identify threats/opportunities
2.2.3 Resilience	IT system capacity to withstand attack
2.2.4 Security	Of physical assets
3. CHANGE: created by decisions to pursue objectives beyond current capability	
3.1 PSA targets	New and challenging targets
3.2 Change programmes	Programmes that threaten capacity to deliver
3.3 New projects	Investment decisions; project prioritisation
3.4 New policies	Expectations create uncertainty about delivery

Once identified, the risks are assessed – at a departmental level, to ensure they are not compartmentalised in individual projects or divisions – using a matrix. This plots impact against likelihood on a three-by-three axis of low, medium and high. Each category is defined – for example, 'high' impact is cost over £1m, impaired ability to meet objectives, extended recovery time and/or serious impact on reputation.

Depending on where the risk falls on this matrix, it's coded from one to nine – with one being the highest 'red' risks that are automatically escalated up the hierarchy. All risks rated one to four require contingency plans. Items are evaluated against the departmental risk appetite, set by the heads of division and project directors. Those rated higher than the 'tolerable' level of risk trigger the introduction of controls.

The residual risk – that which remains after controls are in place – is then compared to the risk appetite to test the efficacy of the controls. A traffic light system is used to highlight those where the controls will not reduce the risk to an acceptable level. This is entered into the risk registers to highlight problem areas.

There are four elements in the risk monitoring process at DCMS: individual ownership; maintenance and updating of risk registers; internal audit/risk reviews; and the end of year risk self assessment. Risk should reside with those most able to act on it, and all staff are encouraged to embed risk reviews into their personal feedback processes to avoid the need for of a bureaucratic layer of risk professionals.

Most risks end up on project or sector risk registers – close to the related operational responsibility – although partnering arrangements can complicate things. For example the strategic objective of encouraging enjoyment of sport includes a number of partners, such as local authorities. So each partner group has a DCMS lead whose responsibilities include risk management. Joint risk registers are also used to clarify ownership of particular risks. Central government has been providing additional guidance for these situations – for example, the OGC's 2005 publication *Managing risk with delivery partners*. The concept boils down to careful scoping, articulation and assignment of risks during the formulation of partnership agreements.

Conclusions

Awareness of risk management as a discipline is obviously at an all time high. Quite apart from the emergence of dedicated risk management teams and new regulations on internal control that place a huge emphasis on risk, there is a growing body of risk professionals with their own sets of qualifications and intellectual frameworks. That much is evident from the number of risk committees and policies, as discrete from the traditional control structures and audit functions.

Both private and public sector organisations have to meet the needs of an increasingly diverse range of stakeholders. That means risk is no longer treated solely as a financial calculation. Indeed, while the finance function and its related departments – particularly internal audit and treasury – clearly maintain a huge role in risk management, it is increasingly the norm for organisations to look more broadly at non-financial factors and embed them at an operational level.

Implicit risk management

This is most obvious at Tesco and DCMS (although also true in the other case studies). Tesco specifically avoids discussing 'risk management' and instead has designed a way of linking corporate strategy with day-to-day activities that includes risk monitoring and management. At DCMS, a relatively small department, every effort has been made to prevent the emergence of a bureaucratic risk management function.

There is a remarkable consistency of approach between the case studies. In each organisation, the stated strategy includes an intention to bed risk management into the culture of the organisation; compliance with a broadly shared notion of best practice and/or regulations; some kind of forward planning; and the clear communication of risk responsibilities. In each case, risk management is designed to protect and enhance the delivery of corporate objectives.

Interestingly, three of those four key functions are not merely mechanical responses to risk, they require both subjective judgments and the kind of softer skills that have become much more important for management accountants generally over the past 20 or 30 years.

While the finance function and any discrete risk management team still need to apply some of their traditional skills – such as calculating value at risk (VaR), analysing the risk-adjusted rates of return that projects require, assessing balance sheet robustness in different risk scenarios and so on – these softer roles are now incredibly important.

Culture and leadership

The Tesco case study shows these skills working in practice – largely thanks to a straightforward strategy (customer satisfaction) that is communicated from the very top of the organisation. Although Tesco's business model is extremely simple by comparison, it's still a stark contrast to RBS – where a box-ticking mentality and lack of human judgment fatally impaired the execution of group-wide risk policies.

A massive and discrete risk management bureaucracy failed to identify, communicate and/or mitigate the effect of both localised and aggregate risks. The result was a catastrophic financial performance at the bank. Faced with an ever greater tension between the need to drive up returns and manage risk conservatively, the organisation erred on the side of the former in part by relying on a highly mechanical analysis of risk exposure. That process ticked all the compliance boxes, but was rarely reviewed in terms of judgements, rather than just mathematical models.

Professional risk managers appear not to have had either the authority or the influencing skills to change the approach to risk. And because operational managers were remunerated on financial performance – seemingly without sufficient reference to long-term risk factors – there was limited incentive to look more deeply at either localised risks, or the build up of cross-departmental risk dependencies.

The public/private split

As the case studies show, the public sector has already learned a lot about risk management from the commercial world. Apart from the usual nods to corporate governance codes, it's worth noting that risk and service delivery are considered as one in both local and central government. And there are clear financial risk/reward calculations at work in both Birmingham City Council and the DCMS.

High profile risk management failures – such as the loss of personal data by government departments – have also resulted in a broader range of risks being considered by the public sector. Again, this maps well onto the kind of brand risk management implicit in the Tesco case study.

Can the process work the other way? It's difficult to draw too many conclusions from this small set of case studies. But both Birmingham City Council and the DCMS demonstrate a much more advanced approach to managing complex and interdependent risks than did RBS (although that may be an extreme example). In the public sector, clear guidance stresses the need to factor in macro risks; the need for transparency between divisions and up through the hierarchy; and provide procedures for the appropriate allocation of risks among partner organisations.

Back to finance?

It will be obvious to any reader with an accounting background that these case studies are light on analysis of financial risk management. For example, there is little reference to project risk evaluation or the use of risk-adjusted returns for budgeting and capital allocation.

Of course, that's not to say these organisations don't engage in this kind of activity, far from it. However, in focusing on the processes, systems and controls around risk management, the case study interviewees have highlighted one important factor: risk has broken out of the finance function.

For management accountants with the training to handle risk in a formal way, this creates an opportunity. By applying their core disciplines – alongside softer influencing skills – to these broader risks and opportunities attached to individual projects, they can deliver the kind of rigour that's essential to organisational success in a more unpredictable and faster moving world.

Further reading

The full report can be purchased at **http://www.routledge.com/books/details/9780415591737**
Individual full case studies can also be purchased through this link.

The author is interested to hear from practictioners who would like to discuss any of the issues raised in this report and perhaps also share their experiences of risk management practice. To contact the author, please email m.woods@aston.ac.uk

About AIRMIC

AIRMIC has a membership of about 950 people and represents the risk managers of about 75% of the FTSE 100, as well as very substantial representation in the FTSE mid 250 and other smaller companies. AIRMIC members facilitate risk management activities within their employer organisations and many AIRMIC members are also responsible for the purchase of insurance.

AIRMIC is actively involved in undertaking research into the design and implementation of successful enterprise risk management (ERM) frameworks. Recent AIRMIC reports have addressed such topics as the benefits of ERM; the definition and application of risk appetite; and the design of an effective risk architecture. These reports are available free of charge from the AIRMIC website **www.airmic.com**

In co-operation with ALARM, (the Public Risk Management Association) and the Insitute of Risk Management, AIRMIC has recently published a guide entitled *A structured approach to enterprise risk management and the requirements of ISO 31000*. The guide sets out an approach to ERM that is compatible with the requirements of the UK Corporate Governance Code. Appendix A of the guide provides a checklist of the actions required to embed a comprehensive enterprise risk management culture within an organisation. A copy of the guide is also available free of charge at **www.airmic.com**

ISSN 1744-7038 (online)

Chartered Institute of Management Accountants
26 Chapter Street
London SW1P 4NP
United Kingdom
T. +44 (0)20 8849 2285
E. research@cimaglobal.com
www.cimaglobal.com