National Audit Office

GOOD PRACTICE

Managing risks in government

Financial Management and Reporting

Our vision is to help the nation spend wisely.

We apply the unique perspective of public audit to help Parliament and government drive lasting improvement in public services.

The National Audit Office scrutinises public spending on behalf of Parliament. The Comptroller and Auditor General, Amyas Morse, is an Officer of the House of Commons. He is the head of the NAO, which employs some 880 staff. He and the NAO are totally independent of government. He certifies the accounts of all government departments and a wide range of other public sector bodies; and he has statutory authority to report to Parliament on the economy, efficiency and effectiveness with which departments and other bodies have used their resources. Our work led to savings and other efficiency gains worth more than £1 billion in 2010-11.

Contents

Summary

1 We have reported regularly through our Value for Money audit programme that more effective risk management would enable departments to be better informed in their decisions, have a greater likelihood of meeting their aims and objectives, and help them to avoid costly mistakes. A common observation arising from our work is that departments are often overly optimistic in their assessment of the risk to projects and programmes, and the effectiveness of the mitigating actions they take to address risk. Management also tends to consider project risk in isolation, without considering how risks in one project can affect other business priorities.

2 With the requirement for departments to achieve challenging targets for structured cost reduction whilst maintaining high quality services, the need for effective risk management should not be underestimated. Changes to organisational structures and increased delivery at arm's-length from government adds to the complexity in identifying and managing risks.

3 Our 2004 report *Managing Risks to Improve Public Services* identified five areas which departments needed to address to take risk management forward. We highlighted requirements for sufficient time, resources and top level commitment; clarity over responsibility and accountability backed by scrutiny and robust challenge; reliable, timely and up to date information; the application of risk management throughout departments' delivery networks; and the need for departments to continue to develop their understanding of the common risks they share and to work together to manage them.

4 We have revisited approaches to risk management in departments and some arm's-length bodies in order to understand the challenges that they face in making the most effective use of their risk management. Our work focused on:

- **the culture around risk management:** who sets the appetite for risk; who drives, encourages, and promotes its use; and what barriers might be in place to effective risk management;
- **value for money in risk management:** where risk management is not just a process but adds value to the business and provides management with assurance that risks are being managed effectively; and
- **the benefits of better risk management:** where risk management is not an end in itself but contributes to performance improvements in the delivery of the organisation's objectives.

5 Within the main body of this report, we have included summaries of the results for departments as a whole against each of the questions asked by our audit teams. Our findings indicate that there have been improvements in the processes which underpin risk management. We have found that a large number of departments and other public sector bodies now have a well developed risk management process, and boards and non-executives are focusing increasingly on risk management information as a tool with which to challenge management.

6 The results are, however, less consistent when considering the extent to which risk management is a key driver in decision-making, and the costing and evaluative aspects of risk management are under developed. In particular, the information which management receives to support its risk management processes is not integrated with performance and financial information. Whilst the risk management process is well developed in the majority of departments, it is therefore difficult for management to make the connection between risk management and its impact on the efficient and effective delivery of services.

7 We have used our findings and the examples of good practice in risk management we have identified, in both government departments and the private sector, to develop six key principles which underpin and support the use of risk management to improve decision-making (**Figure 1**).

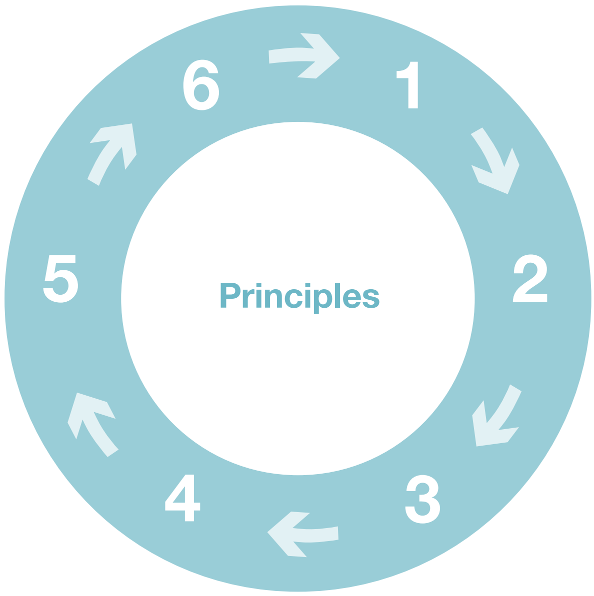
8 Departments face challenges in developing an integrated and consistent approach to managing risks in a dynamic environment and, as such, approaches which are tailored to their own circumstances are likely to be the most effective. Reorganisations to Departmental Boards provide a fresh opportunity for Board members to reflect on the adequacy of arrangements in place in their departments, and those bodies through which services are delivered. We encourage Boards, and where appropriate their sub-committees, to use this report to challenge whether risk management arrangements are being used effectively to improve service delivery outcomes. We have included a series of questions at **Figure 2** to prompt and encourage such reflection and challenge.

Figure 1
The principles of risk management and how they interact

6 Future outcomes are improved by implementing lessons learnt

5 Decision-making is informed by a considered and rigorous evaluation and costing of risk

4 Effective decision-making is underpinned by good quality information



1 An engaged Board focuses the business on managing the things that matter

2 The response to risk is most proportionate when the tolerance of risk is clearly defined and articulated

3 Risk management is most effective when ownership of and accountability for risks is clear

Source: National Audit Office

Figure 2
Challenge questions for the Board

1 How do we ensure that our focus is on managing the things that matter? Are we content that management's assessment of risk is not overly optimistic?

2 Are we clear about where we are prepared to tolerate differing levels of risk and, in turn, how this influences and drives the actions of management?

3 How are we confident that risks are being managed appropriately and that we will be informed of the most significant risks to our business?

4 What information do we need both to take decisions and to challenge the rigour with which risk is managed throughout the organisation?

5 How do we ensure that our decisions are based on a clear and balanced evaluation of the costs and impacts associated with risks and mitigations?

6 How do we learn from successes and failures both within our own and other organisations?

Source: National Audit Office

Principle One

An engaged Board focuses the business on managing the things that matter

1.1 The tone at the top of the organisation has an impact on the priority that management and staff give to risk management. The behaviour and actions of the Board and the senior management team, particularly how they communicate with and challenge the business, reinforces the importance of risk management, and drives and encourages a consistent approach to safeguarding the business.

Why is an engaged Board so important?

- The Board sets the agenda and priorities for the organisation. If management and staff believe that the Board views risk management as a key part of successful management they are more likely to buy into and understand its importance to the organisation. The Board is able to challenge management, to ensure that their views are not overly optimistic in both the assessment of risk and the effectiveness of mitigating actions.
- Transparent communication by the Board of the key threats to the organisation's ability to deliver successful outcomes helps staff to understand and engage with managing these risks.
- The Board sets the tone and can foster a climate of trust, developing a culture where staff feel comfortable in openly highlighting risks, which can then be managed, without fear of blame.

Our findings

1.2 Leadership and ownership of risk management in government departments is inconsistent. Some departments have risk management champions at Board-level whilst others rely on specialist risk managers to build momentum and develop understanding. One recent internal audit report observed that "risk management activities are currently undertaken for compliance purposes only". An emphasis on compliance is acceptable if it encourages the right kind of behaviour but compliance alone may be detrimental to the way that risk management is perceived within the business, as opposed to a culture of pro-active risk management.

1.3 Whilst we found that consideration and discussion of risk is a standard agenda item at Board and sub-committee meetings in most departments, discussions do not always focus on those significant issues which could pose the biggest risk to the department. Departments have improved risk management and most acknowledge that they have some way to go to embed risk management internally and through their delivery bodies but have plans in place to improve.

1.4 The *Summary of Results* at **Figure 3** shows that there is more for Boards to do to visibly communicate their commitment to and understanding of risk management, build a climate of trust and embed risk management in their organisations.

Figure 3
Summary of results

NOTE

1 We have assigned, from left to right, green, amber and red ratings on the basis of evidence collected in response to detailed questions put to departments. In our view, **Green** indicates that there is evidence of good practice in departments; **Amber** indicates that there is evidence that departments are making efforts to improve in this area; **Red** indicates that there is little evidence of any good practice or efforts to improve in this area.

Source: National Audit Office

Good practice examples: why this principle will help

An **NHS Trust** implemented a number of changes to the way risks are managed. There is now a focus on top down and forward looking identification of risk that would prevent the organisation from achieving its strategy. The quality of the contribution from the top of the organisation has improved – it now concentrates on those areas that will make the greatest difference to the Trust's risk exposure. There is substantially more scrutiny from the top of the organisation of the status of key risks and the progress being made to deliver agreed mitigating actions.

A change in legislation introduced director's liability into health and safety legislation. In this context, the Board of a **global mining group** refocused the Group's approach to health and safety risk management. This change in focus at the top resulted in significant improvements in risk management for health and safety as well as for major projects, and has resulted in a dramatic decrease in the number of 'near misses' reported since that time. The Group has also seen a 45 per cent reduction in its total injury frequency rate (a standard measure of injury rates) between 2005 and 2009.

Principle Two

The response to risk is most proportionate when the tolerance of risk is clearly defined and articulated

2.1 An overarching risk appetite for an organisation in isolation is unlikely to be helpful in informing decision-making. By considering its appetite for risk in different areas of the business, such as its activities, functions and delivery bodies, and being clear about where it is prepared to tolerate more or less risk, those at the top can drive the right sort of behaviour. Operational and investment decisions are more likely to be based on a clearer understanding of the organisation's priorities. It can also highlight those areas of the business where controls are excessive and where there is potential for greater risk to be taken without significant impact on service delivery outcomes.

2.2 The Board should consider how risk appetite set for individual projects reflects the overall priorities of the organisation, and consider how a risk which crystallises affects the business as a whole. For example, if a project overruns on cost or time, this may have a disproportionate affect on areas of discretionary spend in the organisation and may impact adversely on other projects. The Board should consider the extent to which the organisation can absorb variances between planned and actual expenditure without such adverse impacts, set tolerances accordingly, and flex these over time and as variances occur.

2.3 The Board should also specifically consider the organisation's risk appetite in relation to the very high impact, very low probability risks that could affect the organisation and direct how these business critical risks are to be mitigated.

Why is a common understanding of risk tolerances so important?

- Clarity about risk tolerances can support decision-makers to take more risk when this is advantageous. Highlighting those areas of the business where excessive controls are in place which can be removed or reduced, can help free up additional resources which can be used elsewhere. Thus, a planned reduction in controls can provide more opportunities to innovate and improve public services.
- When risk tolerances are clearly defined at an organisational and project level, understanding and awareness of the organisation's priorities should improve. Key decisions should become more consistent across the whole organisation, leading to a reduction in decisions which are contrary to the Board's intentions.
- By defining and communicating its tolerance of risk, the Board can empower staff to make decisions, identify priority areas for investment and be clear about when issues need to be escalated for their attention.

Our findings

2.4 Our work identified that some departments do not recognise the importance or benefits of setting risk tolerances, and this is reflected in the *Summary of Results* at **Figure 4**. Many believe that, given the size of the organisation and the diversity of its operations, tolerance to risk is too difficult to define. A few departments and agencies have set risk tolerances for different areas of their business and are using these to manage their business. However, this approach is not common across government and we did not find many good practice examples where clarity about risk tolerances has been used effectively to improve outcomes.

2.5 Whilst most departments might not have formally defined risk tolerances for different areas of the business they are all using them to set thresholds for delegated financial authorities. In delegating responsibility, departments acknowledge that there is risk attached to allowing individuals to incur expenditure. The level of delegation, to an individual with appropriate skills and competence, means that the risk is acceptable compared to the savings associated with having fewer checks and balances in place.

Figure 4
Summary of results

Source: National Audit Office

Good practice examples: why this principle will help

The Audit and Risk Committee and the Board of a **retail company** approved ten ‘operating risk statements’ that collectively set out the company’s current risk appetite. These statements essentially drill down into the previous overarching definition of the company’s risk appetite and stratify risk appetite for the key strategic areas. The statements draw out those areas where the company is either more risk averse or more risk aggressive. As they have been widely communicated across the company, the statements provide an opportunity for greater flexibility at department level when making business decisions.

One aim of risk management in the insurance sector is to enable staff to maximise earnings relative to acceptable overall risk. An **insurance group** models the impact of risk on the assumptions underpinning its model for each group business and for the group as a whole. The model runs both a ‘1 in 200’ scenario (a ‘worst case’ scenario based on assumptions that the Group will have its worst year in 200 years), and a ‘1 in 10’ scenario (based on assumptions that the Group will have its worst year in 10 years). These models are used to set the capital requirement for the Group and individual group businesses, based on the ‘1 in 200’ scenario with a ‘1 in 10’ scenario ‘buffer’, and are a way of focusing attention on the major risks for the Group. By modeling the capital requirement each group business and the Group as a whole needs to hold, and therefore the level of risk which the Group can afford to take, it can identify those businesses which are capable of generating more profit by taking on more risk.

Principle Three

Risk management is most effective when ownership of and accountability for risks is clear

3.1 Responsibilities for identifying, communicating and addressing risk must be clearly defined and communicated so that each individual knows whether they can address the risk themselves (or make decisions on addressing the risk), or whether they need to escalate the risk to another individual (and, if so, to whom).[1]

Why is a clear framework for accountability so important?

- A clear framework for accountability will provide the Board with assurance that management is on top of things and that important risks are being managed effectively and, where necessary, escalated. Such a framework strengthens ownership for delivery but will only be effective if responsibilities have been clearly defined so that it is possible to challenge and hold individuals to account.
- Similarly, a clear framework for accountability will provide the leadership with assurance that the performance of delivery bodies is in accordance with expectations and that risks are being managed effectively and will be escalated to the department where necessary. There should be clear boundaries of authority and action, with arm's-length bodies clearly understanding what issues to escalate and how to do this.
- The consequences of a high impact event cannot be avoided by outsourcing. A framework for accountability, reflected in contractual terms and conditions and supplier management arrangements, will enable the contracting organisation to retain visibility and the ability to intervene on any risks being managed on their behalf by the third party.

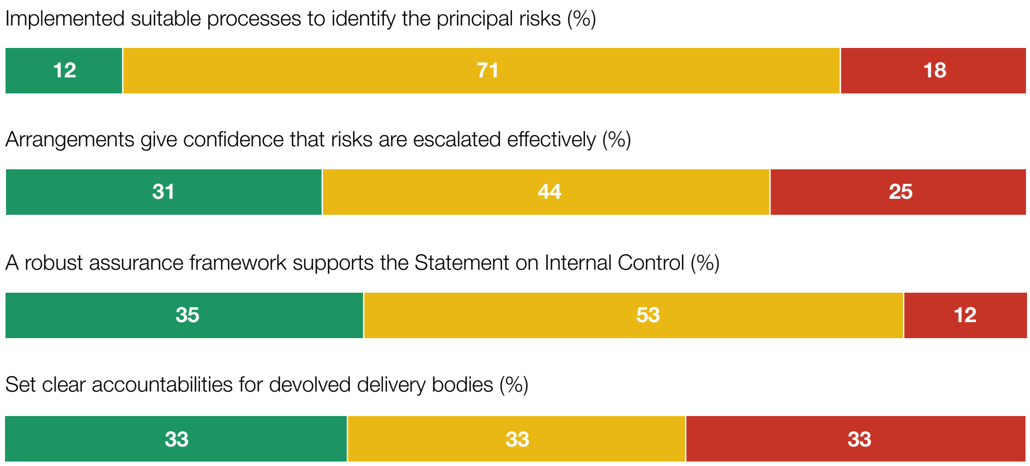
Our findings

3.2 Our work identified that there is often a lack of clarity over the ownership of, and accountability for risks, particularly with respect to devolved delivery bodies. In all types of arrangements, there is a need to improve and clarify risk escalation processes by clearly communicating to staff when risks should be escalated. These findings are reflected in the *Summary of Results* at **Figure 5**.

3.3 There should be a clear understanding that outsourcing operational activities does not mean that accountability can be outsourced. Whilst department officials hold regular discussions with delivery partners, there is a lack of clear guidance in some departments on when risks should be escalated.

1 *Management of Risk: Guidance for Practitioners,* Office of Government Commerce.

Figure 5
Summary of results



NOTE
1 Figures may not add up to 100 per cent due to rounding.

Source: National Audit Office

Good practice examples: why this principle will help

The **Home Office** has a representative from each of its business areas at its Risk Committee. This ensures that those responsible are clear about the ownership of both each risk and the agreed mitigating actions.

A **large energy company** operating within a highly regulated industry has implemented a risk management approach across the company to address safety, environmental and legal considerations. The company has developed a clear hierarchy of risk management accountability, with the respective responsibilities of each layer clearly defined and monitored. There are internal forums and reporting structures that enable each location to manage the risks present in its various projects. At company level, the focus is placed on risk management activities across all locations, as well as those risks that span the company. This, in turn, is reported to the parent body which considers risk across all of the companies within the Group.

Principle Four

Effective decision-making is underpinned by good quality information

4.1 Risk management can only be as effective as the quality of the information used. Board members require clearly presented information which provides insight and explanation to inform discussions and support the decisions made. The Board should demand integrated risk, performance and financial information, linked clearly to the organisation's objectives. Good quality information requires effective systems to be in place to capture data and the Board should challenge actively both the information and assumptions which support its decisions. The Board should also seek an appropriate level of assurance that risks are being properly considered and evaluated throughout the organisation.

Why is good quality information so important?

- Integrated financial, performance and risk information, linked clearly to the delivery of the organisation's objectives, allows the Board both to challenge the quality of the information provided and judge value for money in its decision-making. This requires management to acquire a more sophisticated understanding of performance and will drive improved optimisation of the allocation of resources through the organisation.

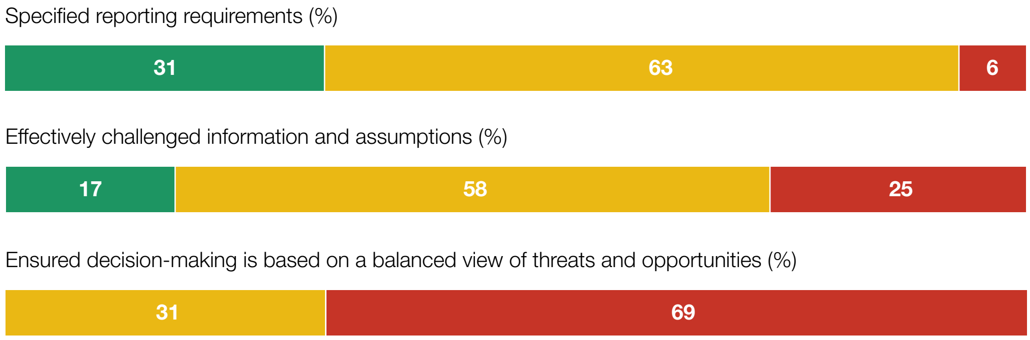
- Concise and focused reports based on good quality information, which are well-written and summarised appropriately, but which can be backed up by more detail as required, enable the Board to focus on the issues which require their particular attention. For example, a report which provides a summary of issues and focuses the discussion on the low probability and high impact risks which could take the organisation by surprise. Comprehensive reports on all strategic and operational risks and reports based on poor quality information are unlikely to make the best use of the Board's time and may result in sub-optimal decisions.

- Good quality information which focuses on and prompts consideration of both current and future risks to the organisation and the delivery of its objectives forms an integral part of decision-making. In setting the strategy and objectives for the organisation, the Board needs to look not only at what has happened but what could threaten the organisation in future.

Our findings

4.2 In many cases, the risk information reported to the Board is not fully integrated with performance and financial information. Many discussions around risk are focused on the content of the risk register and the 'RAG' (red, amber, green) assessment rather than a focused discussion on the actions required to mitigate the key risks. While risk registers are an effective way of capturing risks and mitigations, they may not drive the right type or level of discussion which allows either management to make informed decisions, or the Board to challenge and scrutinise, based on a proper assessment and evaluation of the key risks. This is reflected in the *Summary of Results* at **Figure 6**.

Figure 6
Summary of results



Source: National Audit Office

Good practice examples: why this principle will help

The Department for Business, Innovation and Skills' Management Board and Audit and Risk Committee have requested changes to the format and timing of reported information so that it is easier to understand and facilitates a full discussion of priority risks at meetings. Members had previously commented that the RAG risk reporting system was confusing as traffic lights mean one thing when it comes to monitoring performance against targets but another when it comes to management of risks. The Department's internal audit has since commented favourably "They are talking more about risks and their implications independently from the process behind it as part of their routine operations and relationship with stakeholders".

At **HM Revenue and Customs** the monthly Performance Report is used to measure progress against objectives and to identify areas of performance requiring further action. The Performance Committee and the Performance Hubs in the Lines of Business discuss this data and consider key risks to success. The Performance Committee are concerned with risks and issues that affect the Department's performance now or in the near future. They review the individual risks captured on the department's risk register as part of their discussions, integrating their view of risk into performance.

Principle Five

Decision-making is informed by a considered and rigorous evaluation and costing of risk

5.1 The management of risk is part of the discipline of ensuring the achievement of the organisation's objectives within its available resources. Decisions on how to manage risk should be taken on the same basis as any other investment decision. This should include an evaluation both of the contribution to the achievement of strategic objectives and the cost of alternative options. The organisation should start by quantifying the likelihood and potential impact arising from specific risks to achieving their objectives. This estimate can then be compared with the costs associated with options for mitigating action and the extent to which the risk, and the potential financial impact, is reduced.

5.2 We acknowledge that costing risks is challenging for government departments, particularly where risks are significant to society as a whole, apply across government and have other reputational or non-financial implications. However, evaluating the costs of mitigating actions, for example, to safeguard reputation, is likely to be more achievable. An approximate quantification is better than making no attempt to cost the risk associated with alternative decisions.

Why is evaluating and costing risk so important?

- Evaluating and costing risk and mitigating actions ensures that decisions to implement controls are proportionate to organisational objectives and priorities.

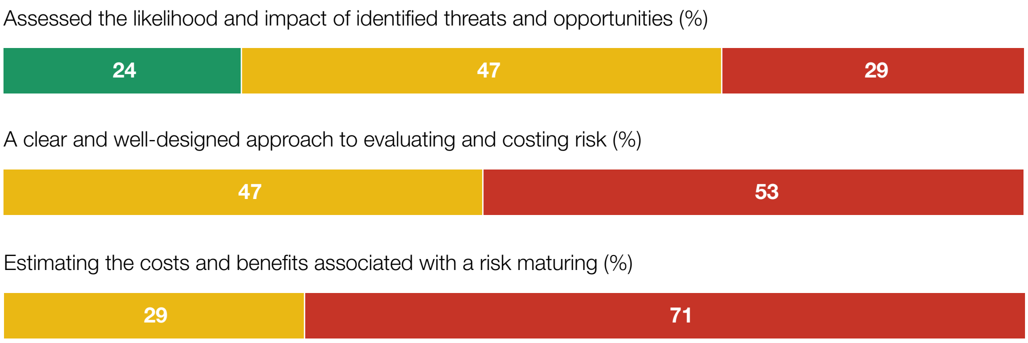
- Organisations need to be able to justify and defend their decisions. Analysis of the options and associated costs and potential impacts should support the choices they make. Such analysis should include a range of scenarios and assessment of the sensitivity of the assumptions made and the potential volatility of the environment.

- Boards will be looking increasingly to cut those processes and parts of the organisation that add least value. Added value can be accomplished in a number of ways but through more effective management of risks, it is likely that there will be improvements to resilience in dealing with unexpected events, reducing volatility of results, and increasing efficiency and effectiveness.

Our findings

5.3 Whilst many government departments have developed and follow their own guidance on how to assess and evaluate risks in terms of their likelihood and impact, our work has identified little evidence of the costing of risk and mitigations to evaluate and inform decision-making as part of normal business. This is reflected in the *Summary of Results* at **Figure 7**. There is some evidence, in the discipline of the management of major projects, of costing both of risks and mitigating actions to support decision-making. A few departments are currently exploring the extent to which they can cost risks through the use of pilot testing in certain areas of their business. However, most departments express the view that the costing of risk is either not practical or is too difficult given the nature of their business operations.

Figure 7
Summary of results



Source: National Audit Office

Good practice examples: why this principle will help

HM Revenue and Customs identified the key risks to its strategic objectives as part of its preparations for the Spending Review. The Department examined the actions that would mitigate these risks and calculated the profile of costs of the mitigating actions over time. The costs of the mitigating actions formed part of the Department's submission to HM Treasury, and the Department believes that this information and supporting analysis helped it to secure the funding required to manage some of its key risks.

One product contributes significantly to the profitability of a **consumer goods company**, and large quantities of the product are held in stock for a significant period of time before it is sold. Management identified a catastrophic incident at the storage location as a risk that could result in a large fluctuation in outturn against future target profits for a number of years. A simple financial model was used to forecast the effect on the company's future outturn should, for example, a fire in the warehouse lead to loss of the stock. The cost of various scenarios which would mitigate the risk was subsequently forecast. The result provided compelling evidence in support of a business case to invest in the use of other storage facilities to reduce the risk to the loss of stock. This process has provided the Board with significant confidence that they have appropriate procedures in place to mitigate this significant risk for the company.

Principle Six

Future outcomes are improved by implementing lessons learnt

6.1 Organisations should invest time in reflecting and learning lessons from their own and others' experience about how risks have been managed. The Board has a role to play in encouraging consideration of what has gone before and driving improvements in behaviour in the future, including through challenging management to demonstrate how learning is driving improvements in the business.

Why is learning from experience so important?

- Identifying and taking action to implement lessons from both good practice (including risk management techniques that have been demonstrated to work) and failures can enable organisations to apply a more consistent, efficient and effective approach to risk management.

- If one organisation encounters a new risk and devises an effective control to deal with it, communicating that lesson to parts of its organisation or to other organisations that may encounter the same risk will provide them with the opportunity to consider potential mitigating actions.

Our findings

6.2 Whilst we found that most departments are very good at capturing and sharing lessons by way of newsletters or staff bulletins there is little evidence that these lessons are learnt and used actively as part of a drive towards continuous improvement. This is reflected in the *Summary of Results* at **Figure 8** which suggests that there is still more work to be done to ensure that reflection on past performance results in performance improvement.

6.3 Internal audit functions within departments often repeat findings within their audit reports that they have highlighted previously. Our own value for money reports often comment on the same systemic issues within government departments, such as failures to conduct full assessments and evaluations of the risks associated with specific projects.

6.4 Most departments have a representative on the Risk Improvement Group, a cross-government group coordinated by HM Treasury, which is a useful forum for risk and assurance specialists to meet and discuss risk management practices, and provides the opportunity to learn from others and share good practice.

Figure 8
Summary of results

Source: National Audit Office

Good practice examples: why this principle will help

HM Revenue and Customs' Performance Committee produces a note after each of its meetings, summarising the key actions, including risks, concerns and celebrations. This note is sent to all Director Generals for dissemination further down the organisation. Feedback is often communicated in meetings with staff so that the most relevant points can be emphasised. The concerns list what the concern is, what caused it and what is being done about it. The celebrations include a statement of what went well, and the lessons learnt or impact. The reporting of internal frauds is a good example of how lessons are acted on. Specific organisational learning events are held to share lessons from cases of proven internal fraud.

The Ministry of Justice uses the network of its risk group to identify how risks are managed within other organisations to see if anything could work well for the Ministry. For example, the Corporate Risk Team looked at the risk management capability review process within both the Department for Work and Pensions and the Home Office, and incorporated some elements of these capability models whilst tailoring them to specifically suit the Ministry of Justice.

Methodology

The main elements of our fieldwork took place between September 2010 and January 2011.

Method	Purpose
Interviews with departmental staff. We spoke to staff in most of the departments we reviewed.[2]	To understand the current status of the organisation's approach to managing risks.
Document reviews. We reviewed departmental internal documents including minutes of Board and Audit Committee meetings, and associated agenda papers which included reported risk information.	To understand the nature of the discussions that take place and the types of information which are reported.
Report reviews. We reviewed all NAO reports issued in the past 12 months, and revisited our previous report on risk management in government.	To review the nature of previous comments and recommendations made in response to the management of risks.
Engagement of consultants. We commissioned PwC to provide case study examples across the public and private sector of where organisations use risk management to deliver business results.	To influence departments to embed good practice approaches to risk management in pursuit of better decision-making.

Departments included in the review

HM Revenue and Customs

Department for Transport

Department for Environment, Food and Rural Affairs

The Home Office

Department of Energy and Climate Change

Ministry of Defence

Foreign and Commonwealth Office

Department for International Development

Department for Work and Pensions

Department for Communities and Local Government

Ministry of Justice

Department for Business, Innovation and Skills

Department for Culture, Media and Sport

Department for Education

Department of Health

Other organisations included in the review

Serious Fraud Office

The National Archives

Crown Prosecution Service

2 For the Department for Work and Pensions our findings were restricted to document reviews.

Where to find out more

The National Audit Office website is
www.nao.org.uk

If you would like to know more about the NAO's work in this area please email Z5-FMGP@nao.gsi.gov.uk

www.nao.org.uk/financial-management

Twitter: @NAOorguk

This report has been printed on Consort 155 and contains material sourced from responsibly managed and sustainable forests certified in accordance with FSC (Forest Stewardship Council).

The wood pulp is totally recyclable and acid-free. Our printers also have full ISO 14001 environmental accreditation. This ensures that they have effective procedures in place to manage waste and practices that may affect the environment.

Design & Production by
NAO Communications
DP Ref: 009592-001

Printed by Precision Printing

National Audit Office

www.nao.org.uk