





# Contents

<b>Acknowledgements</b> .....	<b>5</b>
<b>1. Executive Summary</b> .....	<b>6</b>
<b>2. Scope of review undertaken by Airmic</b> .....	<b>8</b>
2.1 Background to the study .....	8
2.2 Rationale for the study .....	8
2.3 Methodology employed .....	9
2.4 Sectors and companies selected (Appendix A) .....	10
2.5 Risk reporting review criteria (Appendix B).....	10
<b>3. Component 1: Risk Agenda</b> .....	<b>12</b>
3.1 Scope of the risk agenda.....	12
3.2 Assurance risk agenda .....	12
3.3 Performance risk agenda.....	13
3.4 Allocation of resources to risk management .....	15
3.5 Commentary on risk agenda disclosures .....	17
<b>4. Component 2: Risk Assessment</b> .....	<b>18</b>
4.1 Scope of risk assessment.....	18
4.2 Procedures for risk assessment .....	18
4.3 Risk impact and consequences .....	19
4.4 Identification of existing controls .....	21
4.5 Commentary on risk assessment disclosures .....	22
<b>5. Component 3: Risk Response</b> .....	<b>25</b>
5.1 Scope of risk response.....	25
5.2 Risk response decisions .....	25
5.3 Evaluation of existing controls .....	26
5.4 Responding to operational disasters.....	27
5.5 Commentary on risk response disclosures .....	29

<b>6. Component 4: Risk Communication</b> .....	<b>30</b>
6.1 Scope of risk communication .....	30
6.2 Risk architecture and protocols .....	30
6.3 Risk documentation and records .....	32
6.4 Arrangements for risk reporting .....	33
6.5 Commentary on risk communication disclosures .....	34
<b>7. Component 5: Risk Governance</b> .....	<b>36</b>
7.1 Scope of risk governance .....	36
7.2 Procedures for risk governance .....	36
7.4 Governance of emerging risks .....	39
7.5 Commentary on risk governance disclosures .....	40
<b>8. Commentary by sector, analysis and conclusions</b> .....	<b>42</b>
8.1 Chemicals / Pharmaceuticals.....	42
8.2 Energy / Mining.....	42
8.3 Engineering / Manufacturing.....	42
8.4 Financial Institutions .....	42
8.5 Food / Drink.....	43
8.6 Media / IT / Telecoms.....	43
8.7 Retail / Leisure.....	43
8.8 Support Services / Transport.....	43
<b>9. Keeping risk management reporting relevant</b> .....	<b>44</b>
<b>Appendix A: List of business sectors and companies selected</b> .....	<b>46</b>
<b>Appendix B: Scope and extent of good risk management disclosure</b> .....	<b>47</b>

# Acknowledgements

**Airmic is grateful for the support and guidance received from the Institute of Chartered Secretaries and Administrators (ICSA) in providing commentary on the structure of this report and the selection of the examples extracted from company annual report and accounts.**

It should be noted that the extracts have been selected as examples of good disclosure practice. The only editing that has been undertaken was to simplify and shorten some extracts, to remove page references and references to specific committees, and/or to make the extract more focused by changing some of the grammar.

The companies that were selected demonstrated better than average reporting practices in the sector they represent. Also, the extracts that have been selected were identified as the best examples of the feature being described. More extracts have been used from some companies compared to others in the same sector. That should not be taken to mean that some companies were considered to be better than other companies in the same sector.

## **About Airmic**

Airmic is a members' association supporting those responsible for risk management and insurance within their own companies. Its membership includes two thirds of the FTSE 100, as well as many smaller companies. Airmic provides training, networking, lobbying and market information for the benefit of members. It regularly commissions research and its annual conference is the leading risk management event in the UK.

## **About ICSA**

The Institute of Chartered Secretaries and Administrators (ICSA) is the qualifying and membership body for company secretaries and other professionals operating in governance, risk and compliance roles. Our members provide a focal point for trusted and independent advice about the conduct of business. Whether working in the corporate, public or not-for-profit sectors, or in public practice, they are key players with the skills, knowledge and experience to contribute to the success of the organisations within which they operate.

With over 100 years' experience, the Institute seeks to promote good governance policy, practice and knowledge through our qualification and training, and our high-quality guidance and support. Our thought leadership in areas such as boardroom behaviour, board effectiveness, narrative reporting and stewardship dialogue is helping to redefine the governance landscape and fuel important debates about how best to achieve enhanced board performance. We work closely with government, regulators and other strategic partners, as well as our members, to develop this agenda.

# 1. Executive Summary

---

Good standards of risk management reporting help to give confidence to shareholders that the company is resilient and is more likely to be successful in the short and long term.

---

**The UK corporate governance code and the Turnbull Report require companies listed on the London Stock Exchange to report their risk management activities. Similar requirements exist for companies listed on stock exchanges around the world. Also, many other types of organisations have to fulfil similar risk disclosure requirements, including charities and government agencies. The publication of information on risk management activities enables shareholders (and other stakeholders) to evaluate the attention that the company pays to the management of the significant risks that it faces. Good standards of risk management reporting help to give confidence to shareholders that the company is resilient and is more likely to be successful in the short and long term.**

Airmic published a report entitled “Roads to Ruin” in 2011, which identified risk management failures that led to a series of corporate failures during the previous decade. This research into corporate risk reporting was undertaken to determine whether these recent catastrophic company failures, together with the global financial crisis that started in 2008, have resulted in enhanced standards of risk and risk management reporting. The presumption being tested was that improved standards of risk management within companies should result in improved standards of risk reporting.

Production of a list of significant risk factors is undertaken by all companies listed on the London Stock Exchange. However, the list can often be very long and sometimes provides little information beyond the generic descriptions of the risks that are faced by all companies in the same sector. For shareholders to be satisfied that the company pays appropriate attention to risk management, information beyond the list of risk factors is required.

Against this background, Airmic undertook a review of selected companies listed on the London Stock Exchange. Eight different sectors were selected, as outlined in Appendix A. Most of the companies were selected from the FTSE100, although a representative from the FTSE250 was selected for each sector. The most recent annual report and accounts for each selected company was reviewed and examples of good risk management reporting were identified.

**The information provided on risk management activities by each of the selected companies was evaluated in five important areas:**

- Risk agenda – the risk agenda for the company sets out the reasons for undertaking risk management activities and the benefits that are anticipated.
- Risk assessment – the extent of the risk assessment exercises in the company facilitate the production of a comprehensive list of the risk factors.
- Risk response – the company should evaluate the existing risk responses and the extent to which the risks facing the company are managed within the risk appetite.
- Risk communication – the information on risks that should be communicated throughout the company to ensure that a risk management glass ceiling does not exist.

- Risk governance – the company should ensure that adequate governance arrangements are in place to provide assurance and confirm that emerging risks are managed.

The findings of the review were that the standards of risk reporting vary considerably between individual companies and, very noticeably, between the different business sectors. Many of the best examples of risk reporting were in the leisure and retail sector, where information was provided on the link between delivery of strategy and the management of risk. Nevertheless, the overall impression is that many companies are undertaking well-structured and comprehensive risk management activities, but are failing to report the full extent of the processes and procedures that they have in place.

This report contains many examples of good risk reporting by a wide range of companies. These risk reports help to give confidence to shareholders that the companies have robust risk management protocols in place. The following extracts from longer examples within this report demonstrate how good risk and risk management reporting can help to give additional confidence to shareholders that the company is well managed.

- Risk agenda – AstraZeneca: “Our approach to risk management is designed to encourage clear decision-making as to which risks we take and how these are managed ...”
- Risk assessment – Serco: “In identifying the potential risks associated with the achievement of our business objectives, we consider both external factors ... and internal risks ...”
- Risk response – Debenhams: “... a framework to build organisational resilience to known threats is in place and that the framework is capable of providing an effective response ...”
- Risk communication – J Sainsbury plc: “The risk register contains the significant risks faced by the business and identifies the potential impact and likelihood ...”
- Risk governance – Johnson Matthey: “The board and audit committee agenda plans are designed to ensure that all significant areas of risk are reported on ...”



## 2. Scope of review undertaken by Airmic

### 2.1 Background to the study

**Since 2007, a company has had a legal obligation to disclose the principal risks and uncertainties that it faces. The significance of this statutory obligation increased in the light of the notable cases of value destruction that occurred in the economic downturn, forcing regulators to revisit existing assumptions concerning governance arrangements inside companies. The subsequent introduction of separate risk committees in financial services companies, and the focus on risk issues in the UK Corporate Governance Code, has increased pressure on companies both to improve their risk management performance and reassure stakeholders that they have done so.**

Company secretaries, in particular, have worked closely with risk colleagues to ensure that their boards receive risk management information that allows them to take well-informed decisions. High-quality risk disclosure in annual reports – providing the required assurance to stakeholders – has resulted from a recognition from those company secretaries and risk officers that disclosure is a communications opportunity rather than a compliance obligation.

In November 2009, Sir David Walker published his final review of the corporate governance of banks and other financial institutions (“BOFIs”). The Walker recommendations require that the boards of a FTSE100 bank or life insurance company should establish a board risk committee separately from the audit committee. The Institute of Chartered Secretaries and Administrators (ICSA) published guidance on the terms of reference for risk committees.

The requirement to have a risk committee is not included in the UK Corporate Governance Code. Therefore, it applies only to BOFI’s and does not apply to other types of listed companies. Nevertheless, the model terms of reference for a risk committee set out in the ICSA guidance have been used as a benchmark when evaluating the risk communications component of risk and risk management disclosures by the selected FTSE350 companies.

### 2.2 Rationale for the study

**Airmic undertook research in 2011 and published a report entitled “Roads to Ruin”. The report considered the consequences of the failure of risk management by undertaking a series of desktop reviews of corporate disasters that had occurred during the previous decade. Conclusions were presented on the risk management failures that have occurred in the case study companies, and in particular, the importance and the contribution of risk management across a wide range of different types of companies were demonstrated by the case studies.**

The “Roads to Ruin” report was published at a time when companies had become increasingly concerned about risk management in the wake of the global financial crisis that started in 2008. Many companies improved their risk management processes and procedures in response to the global financial crisis. The study described in this report aimed to identify whether companies undertaking comprehensive risk management procedures are reporting on their enhanced activities. This reporting should be designed to give shareholders (and other stakeholders) increased confidence in the future success of the company.

Many other types of organisations have to fulfil similar risk disclosure



requirements, including charities and government agencies. The structure used in this report for evaluation of risk and risk management reporting is equally applicable to all types of organisations. The primary purpose of risk disclosure is to help to provide the full range of stakeholders with confidence in the strategy, tactics and operations of the organisation.

The inclusion of detailed lists of risk factors in the annual report and accounts for listed companies has become standard practice. However, this has resulted in many reports becoming standardised and providing generic information that gives little indication of how seriously the company takes the need for a formalised approach to risk management.

Airmic undertook a preliminary review of the annual report and accounts 2012 for a number of companies and compared the risk management section with that of the same company in 2010. This review indicated that there had been a move towards standardised reporting of risk factors with a much reduced level of reporting on risk management processes and activities. Accordingly, Airmic decided that a more extensive and better structured investigation would be beneficial.

## 2.3 Methodology employed

**The approach adopted was to identify the main business sectors where Airmic has a significant membership. From each identified sector, three representative companies were selected, including two FTSE100 companies and one FTSE250 company. The most recent annual report and accounts for each selected company was reviewed and the sections related to risk management were evaluated in relation to the risk reporting criteria set out below and described in more detail in Appendix B.**

The aim of the review was to identify examples of good practice in risk reporting, rather than identify and then criticise companies that did not achieve good standards of risk reporting. The intention of the research was to identify and report on good practice, so that other companies can understand the benefits of good risk management and appreciate the benefits to shareholders associated with reporting the nature and extent of the risk management activities that are embedded within the company.

When undertaking the review of risk disclosure, the methodology employed involved searching several different sections of a typical annual report and accounts. In most cases, risk disclosures were included in a separate part of the report and accounts. In many cases, the information on risk was included, together with information on audit and assurance activities, in the governance section of the annual report and accounts. In some cases, risk was viewed by the company in terms of being both threat and opportunity. In these circumstances, a significant amount of risk information was provided throughout the report and it was often the case that the links between strategy and risk were clearly explained.

## 2.4 Sectors and companies selected (Appendix A)

Airmic has extensive membership within the FTSE100, together with significant representation in the FTSE250. Also, Airmic has extensive membership across most business sectors. In order to identify a reasonable number of companies for further investigation, the review included companies from a wide range of business sectors; a total of eight business sectors were identified with three representative companies from each sector. A review of risk reporting standards within each sector was undertaken and the companies selected in each sector represent better than average risk reporting for the sector.

The business sectors selected, together with the names of the three companies in each sector are set out in Appendix A. Having identified the business sectors and the individual companies that would be investigated, examples of good risk management reporting practice were identified within the annual report and accounts, and brief extracts are included in this report. Each of the extracts has been edited, but only to the extent necessary to make the extract more readable.

## 2.5 Risk reporting review criteria (Appendix B)

**The purpose of the review was to evaluate the risk reporting standards achieved by the selected company, as an indication of the quality of the risk management activities within that company. Accordingly, a comprehensive structure was developed that would enable all relevant aspects of risk management activities to be evaluated. The overall approach was to look for evidence that the company had established why it was undertaking risk management activities, had a structured approach to risk management processes and had achieved identified benefits from risk management activities.**

In developing the overall structure for the evaluation, attention was paid to ISO 31000:2009, Risk management – Principles and guidelines and the risk management process described in that international standard. In order to gain a comprehensive view of risk reporting, the following aspects of risk management were identified, as described in more detail in Appendix B:

- Risk agenda – the risk agenda for the company should set out why risk management activities are undertaken in the company and the benefits that are anticipated in relation to the strategy, tactics and operations of the company
- Risk assessment – the risk assessment activities define the scope of the application of risk management in the company and the output of the risk assessment activities will give rise to the list of risk factors for that company
- Risk response – the only reason for undertaking risk assessments is to determine the adequacy of the existing controls, identify the necessary risk control improvements and ensure that they are designed and implemented

- Risk communication – information about risks and risk management needs to be distributed throughout the company to ensure full awareness of the risk factors and the absence of a risk management glass ceiling
- Risk governance – the governance of risk and risk management processes is essential so that appropriate assurance regarding the management of risks is available to all stakeholders, both internal and external to the company.

More information on each of the five components set out above is provided in the chapters that follow. Many of the companies reviewed provided a full and detailed description of their activities in relation to each of the five components described above. Other companies only supplied information on their activities in relation to some, but not all, of the components.

It is the view of Airmic that attention should be paid to each of the five components in order to achieve successful management of risk and ensure company resilience. If the company is undertaking diligent activities with respect to each of the five components, the information provided in the annual report and accounts should reflect the structured approach taken to the management of risks. This will help to provide shareholders with enhanced confidence in the company.

## 3. Component 1: Risk Agenda

---

The company should provide information on the agenda for risk and risk management, including why it undertakes risk management activities, the resources allocated and the main features of those risk management activities.

---

### 3.1 Scope of the risk agenda

**The risk agenda defines the reasons for undertaking risk management and also describes the resources that will be allocated. There are a number of reasons for undertaking risk management, including reasons related to assurance activities and reasons related to the desire to improve the performance of the company. The scope of the risk agenda is set out in Part 1 of Appendix B and the features of good reporting in relation to the risk agenda are:**

- Clear statement of the drivers for the company when planning and undertaking risk management activities
- Description of the benefits that the company expects to receive from the risk management processes that it has in place
- Information on the resources that are allocated to risk management activities, and whether the wider company believes they are sufficient.

### 3.2 Assurance risk agenda

**Many companies undertake risk management activities for assurance purposes, or simply because it is a mandatory requirement of the UK corporate governance code. Various shareholders in the company may require assurance that risk management activities are being undertaken, including activities by the board and the audit committee. Also, risk management activities may be undertaken so that information is available to facilitate better decision-making.**

The key feature of assurance activities is that the risk management activities are not aimed at improving risk management performance. The assurance risk agenda is focused on monitoring and reviewing or auditing existing risk management performance. This is a legitimate approach to risk management, although it may only be part of the reason why the company undertakes risk management activities. The example of AstraZeneca confirms that the company is undertaking risk management in order to provide the necessary assurance to shareholders and other stakeholders.

#### **AstraZeneca: Managing Risk**

As an innovation-driven, global, prescription-based biopharmaceutical business, we face a diverse range of risks and uncertainties that may adversely affect our business. Our approach to risk management is designed to encourage clear decision-making as to which risks we take and how these are managed, based on an understanding of the potential strategic, commercial, financial, compliance, legal and reputational implications of these risks.

(Edited extract from AstraZeneca Annual Report and Form 20-F 2012)

The example of Barclays shows that the range of motivations for undertaking risk

management can extend from assurance to the achievement of improved control and co-ordination of risk across the business.

#### Barclays: Risk Management Strategy

Barclays has clear risk management objectives and a well-established strategy to deliver them, through core risk management processes.

At a strategic level, our risk management objectives are to:

- Identify the significant risks facing the group;
- Formulate group risk appetite and ensure that business profile and plans are consistent with it;
- Optimise risk / return decisions by taking them as closely as possible to the business, while establishing strong and independent review and challenge structures;
- Ensure that business growth plans are properly supported by effective risk infrastructure;
- Manage risk profile to ensure that specific financial deliverables remain possible under a range of adverse business conditions; and
- Help executives improve the control and co-ordination of risk-taking across the business.

(Edited extract from Barclays PLC Annual Report 2012)

### 3.3 Performance risk agenda

**The development of an assurance risk agenda is the starting point for many companies. Examples were found in the report and accounts of companies that develop the assurance approach to risk management to an approach that was intended to improve business performance and success. A performance risk agenda will seek to improve the efficiency and effectiveness of the design and implementation of strategy, tactics and operations.**

Improvements to risk performance can increase the efficiency of operations within a company and lead to a greater degree of resilience. Paying due attention to risks and risk management will aid the delivery of projects on time, to budget and to quality (or specification). Finally, evaluation of the risks associated with various strategic options will lead to the selection of the most effective strategy and the active management of the risks embedded within the delivery of the strategy. The design and implementation of a performance risk agenda is illustrated by the extract from the Intercontinental Hotel Group (IHG) annual report and financial statements 2012, as set out below.

### **IHG: Proactive risk management culture**

IHG's ambition for risk management is to foster a culture that is well-informed, curious, alert, responsive, consistent and accountable so that risk management becomes instinctive.

We consider risks in a wide number of business activities, these include, but are not limited to:

- key strategic planning and budget allocation processes;
- the processes in the programme office on project planning, management and delivery; and
- design of policies, procedures, internal controls, and our approach to corporate governance.

Our risk management capability is continually developing and growing through ongoing risk assessment, post-project reviews and post-incident and crisis reviews.

(Edited extract from IHG Annual Report and Financial Statements 2012)

Several companies illustrated that they were adopting an approach to risk management designed to improve the management of risk as a means of delivering efficient and effective operations tactics and operations. The description of the ITV risk management process set out below is a good example of the establishment of a performance risk agenda. In the same part of the report, ITV also identifies that the strategic risks are related to the achievement of objectives and this confirms that risk and strategy are fully aligned within the company.

### **ITV: Risk Management Process**

ITV's risk management approach is dynamic and continues to be reviewed and developed.

Our approach covers risks at all levels of the organisation and examines business risks on both a top down and bottom up basis. The approach considers risks in three core groups:

- High Impact, Low Likelihood (HILL) risks – of low inherent likelihood but where there would be major consequences were the risk to materialise;
- Strategic risks – would impact the successful execution of the strategy; and
- Process level risks – embedded into everyday activity within the organisation.

The management board has overall responsibility for the content and operation of the risk management framework and performs regular reviews of both strategic and HILL risks. Each strategic risk has been mapped to one of the four key strategic priorities and, where possible, assigned key risk indicators. Where appropriate, the key risk indicators are aligned to our key performance indicators.

(Edited extract from ITV plc Annual Report and Accounts 2012)

## **3.4 Allocation of resources to risk management**

**When a company establishes the aims and objectives of its risk management initiative, it is valuable for shareholders to understand not only why the company is undertaking risk management, but also how it intends to deliver the anticipated benefits. This will require a description of the resources allocated to risk management in the company.**

Many companies, especially financial institutions, provide a description of the resources that they have allocated to risk management. In particular, details of the people and expertise in the risk management department are explained. Some financial and other institutions describe the position of chief risk officer (CRO), whilst others describe a similar position, without allocating that specific title. The extract below from MAN Group provides an example of the extensive description of the organisational structure for risk management that is being put in place.



### **MAN Group: Organization of the risk management and internal control system**

The structure of the risk management and internal control system is based on the MAN Group management hierarchy. Therefore, roles and responsibilities and committees have been put in place both at group level and in the divisions. In the MAN Group divisions and material companies, there are coordinators for the risk management and internal control system. These ensure that the processes set out in the group policy are implemented. They also play a part in the continuous development and improvement of the risk management system. At both division and group level, cross-functional risk boards have been set up to act as ventral supervisory, management and oversight bodies for the risk management and internal control system.

(Edited extract from the MAN SE Annual Report 2012)

Outside the financial institutions sector, most companies do not specifically identify the resources that have been allocated to risk management, although some non-FI companies confirm that they have appointed a Chief Risk Officer, as described in Chapter 8 of this report. The extract from the Serco Group annual report and accounts set out below illustrates an ambitious approach to risk that implies that appropriate resources will be allocated.

### **Serco: Our approach to risk within Serco Management System**

These controls and processes fall into four main areas: identification, assessment, planning and control and monitoring, so that we:

- Identify business objectives that reflect the interests of all stakeholders and the risks associated with the achievement of these objectives
- Regularly assess our exposure to risk, including through the regular measurement of key risk indicators
- Control and reduce risk as far as reasonably practicable or achievable through cost-effective risk treatment options, and
- Identify new risks as they arise and remove those risks that are no longer relevant.

(Edited extract from Serco Group plc annual Report and Accounts 2012)

### 3.5 Commentary on risk agenda disclosures

**Many companies fail to disclose why they are undertaking risk management activities. This creates the impression that risk management is a compliance burden that does not deliver performance or success benefits to the company. It is beneficial for shareholders to understand why the company is undertaking risk management activities, so that the level of risk maturity of the company can be evaluated.**

Companies that describe the reasons for undertaking risk management activities as being ‘to enhance the performance and success of the company’ help to provide the shareholder with greater confidence that risk management activities are undertaken to enhance the efficiency and effectiveness of strategy, tactics and operations. The company itself will benefit from having established a performance risk agenda that will enhance the resilience of the company whilst ensuring that risk issues are considered as part of the development of the strategy and tactics for the company.

In some of the annual report and accounts, risk was described by the company in terms of being both a threat and an opportunity. In these circumstances, the links between strategy and risk were clearly explained. In several cases, companies explained that they were willing to take risks because of the rewards that would be achieved. These companies made it clear that they have an appetite for taking risk provided that it supports the delivery of strategy, tactics and operations.

Finally, details of the resources being allocated to risk management form part of the risk agenda for the company. In reporting that appropriate resources have been allocated to risk and risk management, the company will help to provide shareholders with additional confidence that the risks to achieving success have been identified and appropriate actions are in place to enhance the risk performance of the company.

#### Checklist for the Risk Agenda

1. The risk agenda should be defined by considering the size, nature and complexity of the company, including consideration of the regulatory framework.
2. The risk strategy should identify whether risk management is being undertaken for assurance or performance reasons and should include details of risk improvement targets.
3. The risks the company is willing to take should be described, together with details of the benchmark tests that are considered significant.
4. The resources to be allocated to risk management need to be identified, including decisions on outsourcing some risk management activities to specialist contractors.
5. The range of risk protocols needs to be identified, such as the standards and procedures that will be introduced for the management of different types of risk.

## 4. Component 2: Risk Assessment

---

The company should provide information on the extent and methodology for undertaking risk assessments, as well as details of the key risk factors with the potential to have a significant impact on the success of the company.

---

### 4.1 Scope of risk assessment

**Risk assessment activities allow the company to identify the significant risk factors and analyse the risks in terms of the magnitude and likelihood of the impact. Another feature of risk assessment and, perhaps, the most important aspect, is to evaluate the likely consequences of the risk in terms of the achievement of strategy, tactics and operations. The factors that are important to risk assessment are set out in Part 2 of Appendix B and the features of good reporting in relation to risk assessment are:**

- Clear description of the risk management procedures that are in place and the information that is utilised
- Explanation of how the level of risk is evaluated in relation to the strategy, tactics and operations of the company
- Description of the use of risk assessment to determine the adequacy of existing controls in relation to established risk appetite.

### 4.2 Procedures for risk assessment

**In order to consider the list of significant risk factors in context, shareholders need to be advised of the procedures that are in place to undertake risk assessments. Details of the procedures will require information on any risk classification system that is used, together with details of who is involved in risk assessment activities, the information that is required and how that information is collected.**

This will include the procedures for undertaking risk assessment. The purpose of reporting on the nature and extent of these risk assessment procedures is to help to give shareholders and other stakeholders confidence that the procedures are comprehensive and are designed to ensure that all significant risks are identified, analysed in terms of the potential impact and evaluated in terms of the anticipated consequences. The extract from the Serco Group annual report and accounts gives an insight into the risk identification procedures.

#### **Serco: Risk identification**

In identifying the potential risks associated with the achievement of our business objectives, we consider both external factors arising from the environment within which we operate, and internal risks arising from the nature of our business, its controls and processes, and our management decisions.

Once identified, we document risks in risk registers which are maintained at a contract, program, business unit, divisional and group level. These Risk Registers change as new risks emerge and existing risks diminish, so that the registers reflect the current threats to the relevant strategic objectives. We review the group and divisional risk registers at least quarterly and more frequently, as required.

(Edited extract from Serco Group plc annual report and accounts 2012)

Another example of the risk identification procedures in place is provided by the

extract from the Rexam annual report and accounts set out below. This example represents a good standard of risk reporting, because information is provided on the extent of the risk identification procedures and the nature of the risk assessment activities.

#### **Rexam: Risk identification**

The drivers and consequences of identified risks are recorded which aids analysis and also the creation of appropriate mitigation plans by considering the factors causing risks to occur. The enterprise risk management function leads and supports the process but is also there to challenge the findings. Executive directors and other senior management are closely involved at critical stages in the process to review, challenge and debate the risks identified from a top down perspective. The resultant output is a list of risks faced by Rexam for each business unit and function – the risk register.

The next stage involves the assessment of each identified risk on the register in terms of its likelihood of occurring and the impact on Rexam, if the risk does occur. Performing an assessment of likelihood and impact at both a gross and net level (before and after the effect of mitigation) enables us to identify the key material risks for each business and function and consider the effect of current mitigations on managing the risk. To aid assessment we use specific tools, such as the heat map matrix and radar, to illustrate the impact and likelihood of different risks and to show their trend over time.

(Edited extract from Rexam Annual Report 2012)

### **4.3 Risk impact and consequences**

**In many companies, it seems that risk management activities take place separately from the formation of strategy, development of projects or tactics and the day-to-day operations of the company. The existence of risk management activities that are separate from the main management of the company will result in the full benefits available from successful management of risk not being delivered.**

In order to align risk management activities with the success of the company, procedures need to be in place that take the output from the risk assessment process and evaluate the consequences for strategy, tactics and operations. The output from the risk assessment process will be confirmation of the level of risk, but this is often presented in a way that lacks relevance. When a company has procedures in place to take the outcome from the risk assessment process, anticipate the consequences for its strategy, tactics and operations, and then make changes to its activities, the full benefits of risk management will be achieved. The extract from the Serco Group annual report and accounts set out below is an example of good risk reporting and demonstrates that this company uses the output from a risk assessment to influence strategy, tactics and operations.

### **Serco: Risk assessment**

We assess the potential effect of each identified risk on the achievement of our business objectives and wider stakeholder interests. To do so, we use a risk scoring system based on our assessment of the probability of a risk materialising and the impact if it does. This is assessed from three perspectives:

- significance of the risk to the achievement of our business objectives
- significance of the risk to society, including its impact on public safety and the environment, and
- our ability to influence, control and mitigate the risk

Analysis of our key risks allows us to assess the impact of disruption to our business objectives, the probability of this occurring.

(Edited extract from Serco Group plc Annual Report and Accounts 2012)

The example below is from the Debenhams annual report and accounts. It shows that the company takes the output from the risk assessment and looks for any accumulations of risks that could seriously undermine the success of the company. This approach demonstrates that the output from the risk assessment procedures is used as a dynamic influence on the management of the company and the achievement of success.

### **Debenhams: Risk evaluation**

In order to understand the impact specific risks would have to the group, each risk is evaluated based on the likelihood of occurrence and its severity. The risk ranking matrix has been developed to ensure that a consistent approach is taken when assessing the overall impact to the group. Likelihood is based on the frequency of occurrence in a rolling 12 month period and severity is determined by the degree of change across key performance indicators.

Management is responsible for ensuring that risks are evaluated correctly, with support from the finance department as required. Individual managers consider the cumulative impact of all risks across their particular area of operation when determining the state of their overall control environment. The purpose of this exercise is to calculate the risk score for each risk identified, which determines the level of treatment expected.

(Edited extract from Debenhams plc Annual Report and Accounts 2012)

## **4.4 Identification of existing controls**

**The main reason for undertaking a risk assessment is to identify the current status of the significant risks facing the company. In order to successfully identify the current status of the significant risks, a consideration of the efficacy of the controls currently in place is necessary. This will ensure that the company is not making incorrect assumptions about the efficacy of the existing controls.**

It is an important feature of the confidence given to shareholders that the company undertakes this appraisal of the existing controls. The reporting on risk management should confirm that the company does not make assumptions about the efficacy of controls but tests the controls in a structured and robust manner. Giving ownership of the specific risks and the associated control to a senior member of management is a useful feature of a successful risk management approach. The extract from Rexam annual report confirms that each risk is specifically honed by a member of the executive leadership team.

#### **Rexam: Summary of key group risks**

The challenge remains the same in terms of identifying the most relevant risks, assessing their impact and importance and developing appropriate methods to eliminate or mitigate them. Brief descriptions of the key types of risk to which the group is exposed are identified and, in each case, their potential impact on the group and the principal processes in place to manage and mitigate the risk. Each risk is specifically owned by a member of the executive leadership team. Not all of the factors listed are within the control of the group and other factors may affect the performance of its businesses. Some risks may be unknown at present and other risks, currently regarded as immaterial, could turn out to be material in the future.

(Edited extract from Rexam Annual Report 2012)

Many companies include consideration of opportunities in their risk management approach. The extract from the Standard Chartered annual report confirms that risk assessments are undertaken on a regular basis, together with a review of existing and new opportunities. This extract illustrates that the output from the risk assessment activities is considered in more detail by the company and the risk assessment exercise is not treated as an end in itself.

### Standard Chartered: Risk Governance

Ultimate responsibility for setting our risk appetite and for the effective management of risk rests with the board. Acting within an authority delegated by the board, the board risk committee, whose membership consists exclusively of non-executive directors of the group, has responsibility for oversight and review of prudential risks including but not limited to credit, market, capital, liquidity, operational and reputational. The committee reviews the overall group risk appetite and makes recommendations to the board. Its responsibilities also include reviewing the appropriateness and effectiveness of the risk management systems and controls, considering the implications of material regulatory change proposals, ensuring effective due diligence on material acquisitions and disposals.

(Edited extract from Standard Chartered Annual Report 2011)

## 4.5 Commentary on risk assessment disclosures

**The output from a suitable and sufficient risk assessment process will be a list of the significant risk factors. However, many companies appear to work on the basis that publishing a list of significant risk factors is sufficient indication that satisfactory risk assessment procedures are in place. In order to achieve good standards of risk reporting, the company needs to describe the risk assessment procedures and protocols that are in existence.**

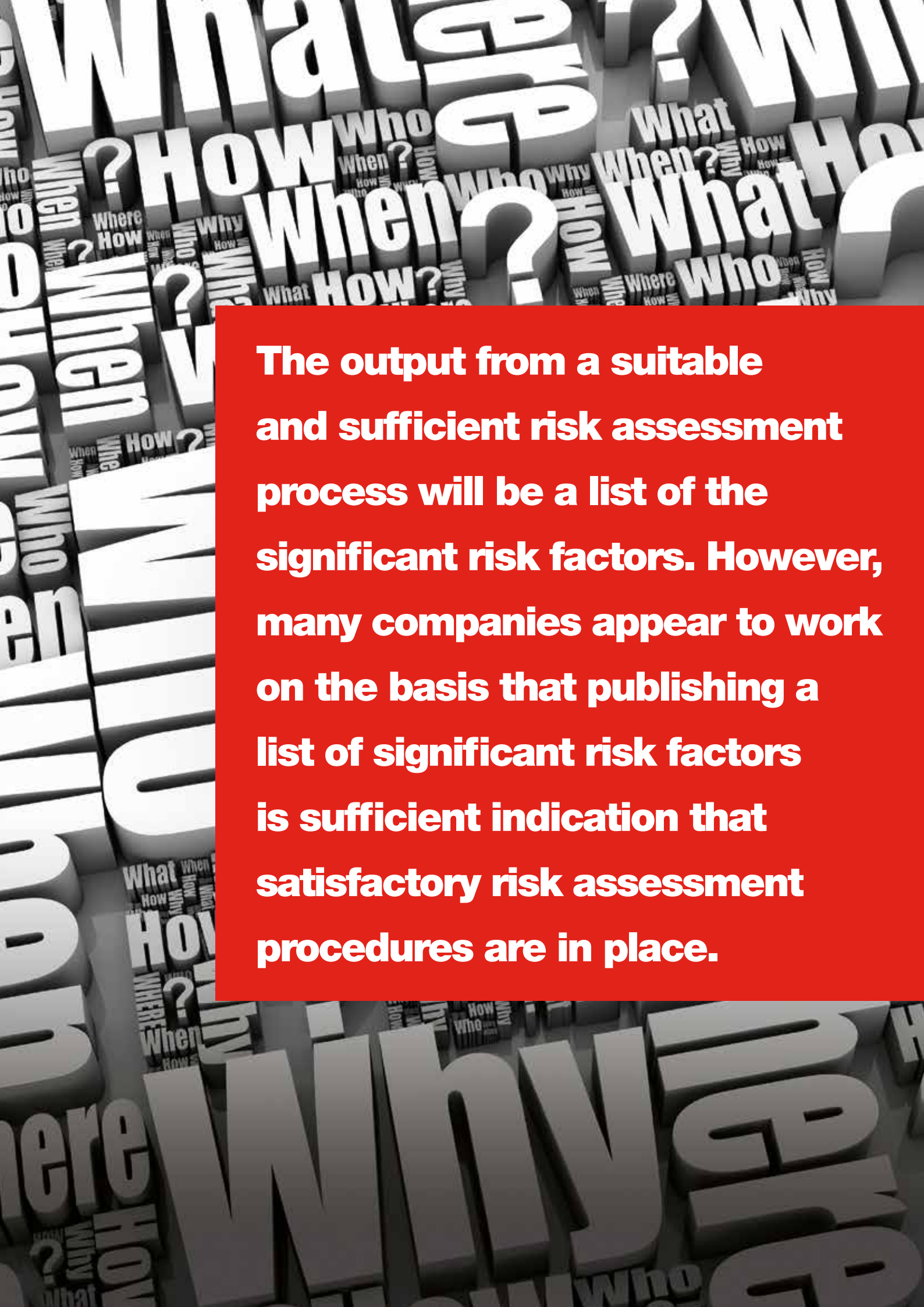
Shareholders will gain confidence in the accuracy of the list of significant risk factors, with a description provided of how these risk factors are identified, the evaluation of controls that is being undertaken and an explanation of how the current level of risk exposure is considered to be within risk appetite. An adequate report of the risk assessment procedures will also help to give the shareholders confidence that the risk assessment outputs are viewed in terms of the anticipated consequences.

This report does not contain information on the lists of risk factors included in all annual reports and accounts, because this type of risk reporting is standard practice. The emphasis of this report is to consider the broader context of risk management and how enhanced risk reporting will help to give shareholders more confidence in the list of significant risk factors that has been produced.



### **Checklist for Risk Assessment**

1. Description of each risk event and how it might be triggered, including information or data on previous experiences with related events should be identified.
2. Analysis of the impact on the finances, infrastructure, reputation and/or marketplace should be completed in terms of likelihood and magnitude of the risk event.
3. Decisions on whether the level of risk identified is tolerable for the company, including the nature of the business imperative associated with the risk need to be established.
4. Evaluation of the anticipated consequences for strategy, tactics and/or operations, including the consequences for the future of the company should be determined.
5. Standard of risk control achieved by the existing controls, compared with the level of risk that is required should be established.



**The output from a suitable and sufficient risk assessment process will be a list of the significant risk factors. However, many companies appear to work on the basis that publishing a list of significant risk factors is sufficient indication that satisfactory risk assessment procedures are in place.**

## 5. Component 3: Risk Response

---

The company should provide information on how it evaluates the efficiency and effectiveness of existing risk controls, decides whether additional controls are required and designs suitable disaster response and business continuity plans.

---

### 5.1 Scope of risk response

**Although all companies produce a list of the significant risk factors in their report and accounts, the way in which they respond to the risk factors is more important. Details of the risk responses and how they are planned and implemented should be provided in the annual report and accounts. The factors that are relevant to risk response are set out in Part 3 of Appendix B and the features of good reporting in relation to risk response are:**

- Description of the procedures in place for the selection of appropriate risk control responses for each risk
- Information on the means for determining the efficiency and effectiveness of existing controls and the need for additional controls
- Description of the means for developing the arrangements for coping with major disruption by way of disaster response and business continuity plans.

### 5.2 Risk response decisions

**These factors include information on the testing of existing controls and whether the current level of risk is within the risk appetite of the company. Also, an important part of describing the risk response component is to help to provide shareholders with confidence that arrangements are in place to cope with major disruption to business operations and that the company has embedded appropriate resilience into its operations.**

Publication of the list of significant risk factors does not provide shareholders with sufficient information. In order to be confident about the level of risk management within the company, information should be reported on the procedures for determining the response to the outputs from the risk assessment exercise. The company will need to decide in relation to each risk whether it is willing to tolerate the risk, wishes to treat the risk further, will seek suitable risk transfer mechanisms or will desire termination of that risk.

The overall intention of risk response decisions is to decide whether the risk is currently within the risk appetite or risk tolerance of the company. Also, if the company has a performance risk agenda, the scope for the introduction of further cost-effective controls should be considered. The extract below from Debenhams annual report and accounts provides information on the overall approach taken by the company to decisions regarding whether further risk responses are appropriate. This reinforces the view that the output from the risk assessment exercise is not an end in itself, but is a means of making further risk management decisions.

### **Debenhams: Risk treatment**

The board is responsible for determining the nature and extent of the risks it is willing to take in achieving its strategic objectives. Risk scores are compared to the risk appetite matrix, which provides guidance on the expected level of treatment, timeframes and authority levels. The four methods used to treat risk are:

- Tolerate (accept risk and take no further action)
- Treat (reduce risk by completing appropriate actions to improve or implement controls)
- Transfer (share risk via insurance policies or asking a third party to take the risk in another way)
- Terminate (avoid risk quickly and decisively by eliminating or re-engineering the activities that lead to the risk occurring)

(Edited extract from Debenhams plc Annual Report and Accounts 2012)

The extract from the Rexam annual report is another example of good risk reporting, because it helps to provide shareholders with confidence that the company has a performance approach to risk management. This includes established procedures for challenging the output from the risk assessment and continuously seeking to improve risk performance.

### **Rexam: Risk mitigation response**

Once risks have been assessed, an appropriate mitigation response is determined for each risk identified. The mitigation response will depend upon the impact and likelihood assessment and, for example, may consist of a control action or insurance. The risk mitigation response reduces either the likelihood of the risk occurring or the impact on Rexam if the risk does occur, or both. Through the course of this year, further work has been done on developing relevant risk mitigation plans.

(Edited extract from Rexam Annual Report 2012)

## **5.3 Evaluation of existing controls**

**Reporting on the fact that the outputs from the risk assessment exercise are constantly challenged is an important means of providing shareholders with confidence that robust risk management procedures are in place. The company should seek to determine the efficiency and effectiveness of existing controls to decide whether there is an urgent need to design further controls. The underlying approach that should be reported is that the company is seeking to achieve greater and greater significance.**

In order to help to provide confidence that further improvements are being continuously sought, a good standard of risk reporting will be achieved when information is provided on actions that had been taken to improve the controls. The extract from the BT annual report and Form 20-F set out below illustrate

that proactive actions have been taken to improve the controls related to cyber attack. This is a good standard of risk reporting that will provide added confidence to shareholders.

#### **BT: Our principal risks – security and resilience**

Certain of our customers require specific, highly sophisticated security provisioning which we are contractually obliged to meet if we are to continue to be able to differentiate our offerings from those of our competitors. Reports of and attention paid to computer hacking incidents have increased concerns about the likelihood of a cyber attack. Enhanced laptop encryption and significant improvements in the protection and segregation of credit card data are some measures which we have taken to manage this risk. We continue to evolve our strategy and capabilities to seek to protect our business against the threat of attacks.

(Edited extract from BT Annual Report and Form 20-F 2012)

The extract below from the Rexam annual report provides information on the specific approach that is taken in the company. The description of the use of a risk mitigation evaluation tool represents a good standard of risk reporting because it provides extra confidence for shareholders that a proactive or performance risk agenda is being pursued.

#### **Rexam: Development**

We are looking continually to improve our risk management process and, during 2012, the process was further enhanced with the implementation of a new tool which requires risk owners to allocate a traffic light status against each mitigation. This tool categorises mitigations between those which are in place and effective, those under development and those which may not currently be functioning as intended. Categorising in this way helps to identify and follow up on outstanding actions.

(Edited extract from Rexam Annual Report 2012)

## **5.4 Responding to operational disasters**

**All well-managed companies have shown a greater awareness of business continuity management in recent times. The components of business continuity management are disaster response and business continuity planning. Ensuring that adequate attention has been paid to business continuity management will enable the company to become more resilient. Shareholders should be given confidence in the level of resilience displayed by the company and this can be achieved by a good standard of risk reporting.**

Events can occur that will cause significant disruption to the normal routine efficient operation of the company. The company will need to have plans in place to ensure an immediate and appropriate response to a disaster. Although it is impossible to identify all the sources of significant disruption, the ability to respond appropriately to a disaster starts with an analysis to understand

the potential source of disasters that could disrupt the company. The extract from the Sainsbury annual report and financial statements describes how the planning of suitable responses to potentially disruptive events is undertaken in the company.

#### **J Sainsbury: Business continuity and major incidents response**

Sainsbury's has detailed plans in place, supported by senior representatives who are trained in dealing with major incidents and have the authority levels to make decisions in the event of a potentially disruptive incident. The business continuity steering group meets quarterly to ensure that the business continuity policy and strategy is fit for purpose. In addition, it oversees the mitigation of all risks associated with business continuity and IT disaster recovery. In the event of any unplanned or unforeseen events, the business continuity management team is convened at short notice to manage any associated risk to the business.

(Edited extract from J Sainsbury plc Annual Report and Financial Statements 2012)

In addition to identifying the sources of potential disaster, a company will also need to anticipate how it will maintain normal routine operations immediately after the disaster struck. This is described as a business continuity plan and shareholders should be given confidence that the company has identified the actions that it will take to ensure routine activities continue after the disaster. The extract from Debenhams annual report and accounts helps to provide confidence for shareholders that this company has adequate business continuity plans in place.

#### **Debenhams: Business Continuity Planning**

The objectives of this committee are to ensure that potential threats to the group and the impact that those threats might cause have been identified, that a framework to build organisational resilience to known threats is in place and that the framework is capable of providing an effective response to safeguard the group. The committee undertakes a number of key activities. These are to review and agree: the business continuity management policy and how it will be managed and communicated; the risks and threats facing the group and prioritise them based on the evaluation of their severity and likelihood; the business continuity management strategy; the business continuity management response and its implementation; the process for exercising, maintaining and reviewing business continuity management arrangements; and the mechanisms to embed business continuity management in the group culture.

(Edited extract from Debenhams plc Annual Report and Accounts 2012)

## 5.5 Commentary on risk response disclosures

**Although the main reason for undertaking a risk assessment is to identify whether further controls are required, there is a tendency in some companies to treat the risk assessment exercise as an end in itself. Companies that have a good level of risk reporting provide information on how they use the outcomes from a risk assessment exercise to make decisions about the adequacy of the existing risk response arrangements.**

An appropriate level of confidence will be provided to shareholders when information on risk response procedures is provided by the company. These procedures will include reference to the arrangements for deciding how to respond to each individual risk. Many companies provide this level of confidence for shareholders by ensuring a good quality of risk reporting on the arrangements for determining the efficiency and effectiveness of existing controls, as a means of deciding whether there is an urgent need to implement further controls.

Increasingly, shareholders should seek confidence in the fact that the company has achieved an appropriate level of resilience in its operation. Resilience will be based on appropriate business continuity management, including established disaster response arrangements and associated business continuity plans. Companies that achieve a good standard of risk reporting provide information on the business continuity management arrangements in place.

The important issues when looking at the level of risk reporting in relation to the risk response component are the methodology for deciding how to respond to each individual risk and the means by which existing controls are tested. Companies that demonstrate a good level of risk reporting were able to deliver confidence to shareholders that there was an appropriate focus on the efficiency and effectiveness of existing controls. The importance of business continuity management as a means of increasing company resilience was recognised by companies achieving good standards of risk reporting in relation to risk response.

### Checklist for Risk Response

1. Decision on whether the level of risk identified during the analysis is tolerable, including consideration of whether the controllability of the risks should be recorded.
2. Description of the nature and type of the proposed additional control should be developed, ensuring that the implementation of the new control is fully auditable.
3. Deadline for completion of implementing the additional control, including details of how progress with the implementation will be monitored.
4. Responsibility for implementing the additional control, including details of how the resources that will be required to design and implement the control should be recorded.
5. Details of how the efficiency and effectiveness of the additional control will be monitored should be developed.



## 6. Component 4: Risk Communication

---

The company should provide information on risk and risk management responsibilities and describe arrangements for risk communication, including how risk information is recorded and risk action plans are developed.

---

### 6.1 Scope of risk communication

Communication of risk information is essential if the company is going to fulfil the aims and objectives for risk management set out in the risk agenda. In fact, risk communication extends to the reporting of risk information in the annual report and accounts. In order to help to provide confidence for shareholders, the company should provide a description of the risk architecture and protocols, the risk documentation, as well as the risk reporting arrangements. The factors that are relevant to risk communication are set out in Part 4 of Appendix B and the features of good reporting in relation to risk communication are:

- Description of the risk architecture and protocols, including information on risk management roles and responsibilities
- Information on risk management recordkeeping, including risk communication in risk training documentation
- Evidence that risk reporting, risk escalation and appropriate whistleblowing arrangements are in place in the company.

### 6.2 Risk architecture and protocols

**In order to achieve successful and effective risk communication, the structure of the risk management roles and responsibilities, together with the structure of the committees with risk management responsibilities, needs to be established. This structure of the roles and responsibilities is often referred to as the risk architecture or the risk management framework of the company. As well as the risk architecture, the company will need to establish the risk management policies and procedures.**

As part of the risk reporting by the company, details of the risk architecture and protocols should be included. This will help to provide shareholders with the confidence that the company has made appropriate provision for effective communication of risk information throughout the organisation. This will avoid the existence of a risk management glass ceiling in the company. The example below is an extract from the BT annual report and Form 20-F, and it provides information for shareholders on the way in which risk information is managed within the company.

### **BT: Risk management framework**

Our risk management framework is explained below:

- The board has overall responsibility for ensuring that our risks are managed appropriately.
- The operating committee is responsible for identifying, evaluating, responding to and monitoring risks.
- The board and the operating committee are supported in their oversight of risk management by the group risk panel.
- Each line of business and service unit operates a risk management process as part of our enterprise risk management framework.

(Edited extract from BT Annual Report and Form 20-F 2012)

Many companies establish a risk committee and this will be a key component of the risk architecture for the company. Information should be provided to shareholders on the role and responsibilities (or terms of reference) for the risk committee, if well established. An understanding of the activities of the risk committee provides information to shareholders on the means by which the company avoids the existence of a risk management glass ceiling. The example from the Invensys annual report and accounts set out below is a brief, but informative, account of the terms of reference of the risk committee.

### **Invensys: Responsibilities and Actions**

Risk Committee

- Formulates strategy and policy based on risk appetite and risk exposure.
- Develops risk framework, receives reports from divisions, reviews risk management structures and compiles the group risk register.
- Prepares reports and recommendations for the board through the audit committee.
- Monitors and coordinates actions to address key risks.

(Edited extract from Invensys plc Annual Report and Accounts 2012)

## 6.3 Risk documentation and records

**Although risk management should not be considered to be a bureaucratic exercise, there is a need to keep appropriate risk documentation. This will include records of risk assessments, risk communication arrangements and the requirements for risk training, and all of this may be consolidated into a written risk management manual. Information concerning the existence and contents of a risk management manual will help to provide shareholders with confidence that adequate risk management records are created and maintained in the company.**

Perhaps the most important document related to the management of risks is the risk register. Most companies produce a risk register and this normally records the outcome of the risk assessment undertaken in the company. It is important that the risk register does not become a static snapshot of the significant risk factors facing the company. In order to be effective, the risk register should be constructed so that the relationship between the risks and the strategy, tactics and operations of the company is obvious. The risk register should also operate as a risk action plan that will accompany and keep a record of the completion of risk improvement recommendations. The extract from the J Sainsbury annual report and financial statements set out below describes the role of the corporate risk register in the successful management of risk.

### **J Sainsbury plc: Risk Management**

Accepting that risk is an inherent part of doing business, the risk management system is designed to identify key risks and to provide assurance that these risks are fully understood and managed. The effectiveness of the process is reviewed twice a year by the audit committee. The board carries out an annual review of the significant risks facing the business. The operating board maintains an overall corporate risk register which is reviewed twice yearly by the audit committee and formally discussed with the board. The risk register contains the significant risks faced by the business and identifies the potential impact and likelihood at both a gross level (before consideration of mitigating controls) and net level (after consideration of mitigating controls). This gives the board the opportunity to review the level of risk that the business is prepared to accept. The register also contains the assurance provided over current key mitigating controls. Where further actions have been identified to mitigate risks to a level deemed acceptable, these are agreed with specific timelines for delivery and are monitored closely until fully implemented.

(Edited extract from J Sainsbury plc Annual Report and Financial Statements 2012)

The extract below from the Rexam annual report provides a further example of the extent of risk management recordkeeping that is kept by certain companies. The overall objective is to ensure that records of risk management activities are maintained. This is often achieved by use of a risk management information system software package.

#### **Rexam: risk management software system**

A new risk management software system was developed together with an external provider. The new system will be used as a platform and database for the risk management process. The benefits this will provide include improved reporting, easier analysis of risk information across Rexam to support best practice sharing, easier identification of key risk themes to input to the internal audit plan and improved analysis of risk interconnectivity.

(Edited extract from Rexam Annual Report 2012)

### **6.4 Arrangements for risk reporting**

**An important part of risk communication are the arrangements for the reporting of risk information, both internally and externally. Protocols should be established to monitor the progress with risk action plans, as well as providing details of risk escalation procedures and, as necessary, whistleblowing arrangements. Some companies will establish a separate disclosures committee, whilst the audit committee will fulfil the function of ensuring that all disclosures from the company are accurate.**

Details of the internal and external risk reporting arrangements within the company will help to provide shareholders with confidence that information related to risk management issues is properly managed within the company. For example, the extract below from Petrofac annual report and accounts explains the role of the audit committee in the company.

#### **Petrofac: Assurance and reporting**

The audit committee has continued its work in relation to the group risk management framework during 2012. Its primary areas of focus were developing further the assurance program for the group enterprise risk management system and ensuring the clarity and appropriateness of risk reporting through the chain of command. Group internal audit has focused on providing assurance regarding financial and regulatory controls and therefore continues to report solely to the audit committee.

(Edited extract from Petrofac plc Annual Report and Accounts 2012)

An increasingly important part of risk management and governance arrangements is related to the opportunity for whistleblowing within the company. The purpose of setting up whistleblowing arrangements is to ensure that lines of communication are open for individuals who are concerned about aspects of the way in which the company is managed. The example below sets out the whistleblowing arrangements for Debenhams as set out in the annual report and accounts.

### **Debenhams: Whistleblowing**

All Debenhams employees are required to adhere to the code of business conduct and the anti-bribery and corruption policy, with senior employees required to confirm compliance in writing. These policies set out the ethical standards expected and include details of how matters can be raised in strict confidence. Two main routes are available to employees to raise concerns over malpractices. The first, “Employees’ guidelines to problem solving”, encourages employees to talk to their line manager, their manager’s line manager or, if still concerned, to call the central human resources team directly. The second route is a confidential reporting line through which employees can speak to the group anti-fraud team. If an employee feels that the matter is so serious that it cannot be discussed in any of these ways, s/he can contact the company secretary or the director of internal audit and risk management.

(Edited extract from Debenhams plc Annual Report and Accounts 2012)

## **6.5 Commentary on risk communication disclosures**

**The importance of risk communication cannot be overstated in terms of arrangements for ensuring successful management of risk. It is the risk communication arrangements within the company that give rise to the reports on risk and risk management that are included in the annual report and accounts for the company and this emphasises the importance of these arrangements.**

However, it is often the case that the overall risk communication arrangements within the company are not disclosed to the extent that would be helpful shareholders. The means by which risk information is collated within the company, scrutinised and presented to the board are vital aspects of ensuring that the board fully understands the risk profile of the company. In order to make decisions about risk appetite, risk tolerance and risk exposure, the board requires risk information that has been objectively compiled and presented to the board in a relevant and easy to understand manner. The board will then be able to decide whether the information that is presented is relevant to the risk agenda of the company and delivers the aims and objectives for risk management that have been established.

In some of the report and accounts reviewed, insufficient information was provided about the arrangements for risk but detail was often given about the level of risk management expertise available to the company. However, many reports would have benefited from a better explanation of internal communication processes. Many of these processes involved the most senior risk management practitioner in the company, but may not be led or co-ordinated by that individual. .

### **Checklist for Risk Communications**

1. Details of risk management roles and responsibilities, including setting risk standards, implementing standards and monitoring compliance should be established.
2. Details of relationships between individuals and/or committees with risk management responsibilities, including reporting structures should be developed.
3. Information on the recordkeeping requirements in relation to procedures and records of incidents, performance and assessments should be recorded.
4. Information on the internal risk communications, including risk escalation procedures and risk training, information and instructions should be recorded.
5. Details of the external risk reporting, especially status reports, reports to regulators and the arrangements for whistleblowing should be established.

## 7. Component 5: Risk Governance

---

The company should provide information on the procedures in place to provide risk assurance to stakeholders and provide details of the governance processes for the management of existing and emerging risks.

---

### 7.1 Scope of risk governance

**Risk governance arrangements within a company are vitally important. The various risk management aims and objectives, systems and procedures, and reporting requirements will have been established in almost all companies. There is a need to evaluate compliance with these various systems and procedures, and the arrangements for undertaking this evaluation represent the risk governance arrangements for the company. The factors that are relevant to risk governance are set out in Part 5 of Appendix B and the features of good reporting in relation to risk governance are:**

- Description of the arrangements for risk governance, including responsibilities for establishing, implementing and monitoring risk performance
- Information on the means of providing risk assurance and the internal and external risk indicators that are utilised
- Description of the arrangements for the management of emerging risks and how the required additional information is obtained.

### 7.2 Procedures for risk governance

**The starting point for risk governance procedures is the production of the risk agenda for the organisation. The risk agenda will set out the arrangements for deciding acceptable levels of risk, as well as allocating responsibility for implementing standards and defining the arrangements for monitoring compliance with the established standards. In most companies, it is for the top management of the company, including the board and executive committee, to establish the risk agenda. Evaluation of the appropriateness of the risk agenda and the fulfilment of the risk agenda will often be the responsibility of the audit committee.**

In addition to scrutiny of the risk agenda, arrangements will also need to be in place for monitoring risk performance. This will include monitoring the risk performance of the company, together with the review of the level of compliance with risk management systems and procedures. Monitoring of performance and review of procedures are both required. The example below from the Rexam annual report describes the key role played by the various committees in the company that have risk and risk management responsibilities.



### **Rexam: Risk Monitoring**

The group level risk register is monitored by the board through a monthly report which updates on the trend of the key risks and mitigations. The executive leadership team, the audit and risk committee and the board all review the output from the risk management process on a periodic basis. The audit and risk committee also reviews the overall risk management process itself. The main mitigation activities for key identified risks are used as an input to determine coverage under the annual internal audit plan.

(Edited extract from Rexam Annual Report 2012)

Monitoring of performance and review of procedures can be an expensive activity. However, it is only by providing information to shareholders on the extent of the monitoring and review activity that the shareholders will gain confidence that appropriate attention is paid to risk and risk management in the company. The extract below from the J Sainsbury annual report and financial statements provides a full and helpful description of the risk monitoring and review work activities that take place in the company.

### **J Sainsbury: Internal controls**

The system of internal control encompasses all controls including those relating to financial reporting processes, operational and compliance controls and those relating to risk management processes. It also includes the controls over the bank and property joint ventures. The audit committee assesses the effectiveness of the internal controls systems on an ongoing basis, enabling a cumulative assessment to be made. The processes used during the year to support this assessment are as follows:

- discussion and approval by the board of the company strategy, plans and objectives and the risks to achieving them;
- review and approval by the board of budgets and forecasts, including those for both revenue and capital expenditure;
- regular reviews by management of the risks to achieving objectives and mitigating controls and actions;
- regular reviews by the audit committee of the scope and results of the work of internal auditors and the external auditors and of any significant issues arising;
- regular reviews by the audit committee of accounting policies and the levels of delegated authority; and
- regular reviews by the board and the audit committee of material fraudulent activity and any significant whistleblowing, and actions being taken to remedy any control weaknesses

(Edited extract from J Sainsbury plc Annual Report and Financial Statements 2012)

## 7.3 Sources of risk assurance

**In addition to monitoring and review, the means for providing assurance regarding the management of significant risk factors should be reported. This will include arrangements for challenging the assurances and details of the risk indicators that are of fundamental importance to the company. The company will need to decide on the sources of assurance that will be provided for the audit committee and the board. Information on the sources of risk assurance that are relied upon will enable shareholders to decide the level of confidence that they have in the risk management arrangements within the company.**

The scope of the risk assurance available within the company should be very wide. Shareholders will be interested in the internal risk indicators that are used within the company to monitor progress with the management of risk and the delivery of the risk agenda. These internal indicators will include improvements in risk performance and the information should be provided in a way that is relevant to the strategy, tactics and operations of the company. These internal indicators will often be lagging indicators that report historical performance. However, it is also important that the company makes use of leading indicators there are relevant to the risk agenda for the company. These may include financial market indicators, such as inflation, exchange and interest rates. The extract below from the Johnson Matthey annual report and accounts illustrates the scope of the corporate governance report prepared by the company.

### **Johnson Matthey: Corporate Governance Report**

The board, through setting its own annual agenda plan and in approving that of the audit committee, defines the process to be undertaken for the review, including the scope and frequency of assurance reports received throughout the year. The board and audit committee agenda plans are designed to ensure that all significant areas of risk are reported on and considered during the course of the year.

(Edited extract from Johnson Matthey Annual Report and Accounts 2012)

An increasingly common structure for providing risk governance, especially in energy and financial companies, is the three lines of defence model. If a company uses this model, the report to shareholders should indicate that this model has been adopted. This will help to provide additional confidence to shareholders that a well-structured risk governance structure has been designed and implemented in the company. The example from the Standard Chartered annual report describes the three lines of defence model that has been implemented in company.

### Standard Chartered: Risk Governance

Roles and responsibilities for risk management are defined under a three lines of defence model. Each line of defence describes a specific set of responsibilities for risk management and control.

- The first line of defence is that all employees are required to ensure the effective management of risks within the scope of their direct organisational responsibilities. Business, function and geographic governance heads are accountable for risk management in their respective businesses and functions, and for countries where they have governance responsibilities.
- The second line of defence comprises the risk control owners, supported by their respective control functions. Risk control owners are responsible for ensuring that the risks within the scope of their responsibilities remain within appetite. The scope of responsibilities of a risk control owner is defined by a given risk type and the risk management processes that relate to that risk type.
- The third line of defence is the independent assurance provided by the group internal audit function. Its role is defined and overseen by the audit committee.

(Edited extract from Standard Chartered Annual Report 2011)

## 7.4 Governance of emerging risks

**An increasing concern for all companies and their shareholders is the management of emerging risks, including details of the nature of emerging risks facing the company and the actions being taken to obtain more information and/or reduce exposure to these emerging risks. It is generally accepted that the phrase emerging risks refers to those risks where inadequate information is available to the company on the potential impact of risks and the anticipated consequences.**

Information on the arrangements for the management of emerging risks should be included in the risk report from the company. It is often the case that the emerging risks facing the company are the most unpredictable, but the most significant of the significant risk factors. The way in which the company addresses the governance of these emerging risks will provide shareholders with valuable insight into the attitude of the company to these emerging risks. The example below from the Petrofac annual report and accounts is a comprehensive view of the attitude of the company to emerging risks and how the consideration of digit risks is embedded within the achievement of strategy.

### **Petrofac: Risk Appetite**

As part of the review of our risk management framework, the committee continued to believe that it should not apply a single aggregate risk appetite for the group as a whole. In terms of concentration risk, our country entry assessments control entry into new territories. Business plans quantify maximum exposures in those territories through measures such as backlog, revenue and net income. Other risk appetite statements are embedded within our approach to issues such as:

- earnings volatility – focusing on the deviation from expectations
- credit headroom – for assessing liquidity risk
- deterministic scenarios focusing on specific project based opportunities
- reputation – focused on impact on stakeholders

(Edited extract from Petrofac plc Annual Report and Accounts 2012)

In addition to providing information on the overall risk governance structure in the company, there is also a need to provide information on the extent of corporate governance arrangements. The extract below from the Johnson Matthey annual report and accounts provides an example of the overall assurance to shareholders regarding the governance arrangements and the company.

### **Johnson Matthey: Corporate Governance Report**

The board, in part through the audit committee, has conducted a review of the effectiveness of the risk management and internal control systems, covering all material controls, including financial, operational and compliance controls, for the year ended 31 March and up to the date of approval of this annual report. The review process accords with the revised Turnbull Guidance. Following this review, the group is enhancing and standardising the stock take procedures across its gold and silver refineries.

(Edited extract from Johnson Matthey Annual Report and Accounts 2012)

## **7.5 Commentary on risk governance disclosures**

**Governance disclosures are vitally important in relation to arrangements for the management of the significant risk factors within the company. Information on the risk agenda that the company follows, the risk assessment and risk response procedures that it has in place, as well as details of the risk communication arrangements, can only act as a source of assurance if there are adequate risk governance procedures in place.**

Shareholders will be interested to know that the arrangements are in place to validate that all of the aims, objectives, systems, procedures, roles and

responsibilities described in earlier parts of the risk report are actually deliberately practiced. For the energy and finance sectors, the three lines of defence model has become standard practice in relation to risk governance arrangements. Many other companies have arrangements in place that are similar to the three lines of defence model, but are not as clearly defined.

When a company cannot report that it has fully implemented the three lines of defence model, it will need to provide shareholders with other forms of assurance that adequate risk governance arrangements have been designed, implemented and maintained. In general, the level of reporting observed in the selected companies was found to be satisfactory, with many examples of good practice, as illustrated by the edited extracts.

There was considerable variation in the way that different companies structured their risk reporting. In almost all cases, risk governance disclosures were found in the corporate governance section of the report. In about a quarter of the reports studied, all of the information provided on risk management processes was set out in the corporate governance section. This resulted in the table of key risk factors and mitigating actions being somewhat separated from the remainder of the report. The result was often that the links and relationships between risk factors and the strategy, tactics and operations of the company were not clearly defined.

#### **Checklist for Risk Governance**

1. Details of the risk assurance requirements of stakeholders, including shareholders and regulators should be established.
2. Information on sources of assurance, including those related to risk performance and leading / following indicators should be developed.
3. Details of the governance structure, including availability of specialist expertise and arrangements for independent auditing of performance should be established.
4. Information on risk performance, including how standards are set, implemented, monitored and challenged should be provided.
5. Details of risk reports and the stakeholders for whom they are intended should be documented, to ensure that statutory reporting requirements are fulfilled.

## 8. Commentary by sector, analysis and conclusions

### 8.1 Chemicals / Pharmaceuticals

**All of the selected companies displayed some aspects of risk disclosure that were excellent. All companies provided detailed lists of risk factors, together with information on the impact of risks occurring. However, the amount of detail provided on the risk management process within each company varied considerably.**

GlaxoSmithKline went into considerable detail, with a good focus on changing or emerging risks and the controls that were in place to mitigate these risks. GlaxoSmithKline and AstraZeneca provided considerable detail on procedures for reporting the assessment of risks and how these reports were presented to the relevant committees and the board.

Johnson Matthey provided a good overview of the risk framework and the procedures for risk identification and assessment. Information was also provided on the mitigation steps for each identified risk. The company also provided detail on the role of the board and the steps that had been taken to review the effectiveness of the risk management system.

### 8.2 Energy / Mining

**There are a number of similarities between the chosen reports for this sector. Primarily, all strongly focused on developments made over the previous year. For example, in the disclosures of key risks, as well as describing the risk factors, impact and mitigation steps, the reports clearly expressed how the risks and the relevant controls had altered or progressed over the previous year.**

Continuing this theme, within the sections on corporate governance, all reports devoted a section to changes in the risk management process made over the previous year, and also disclosed specific activities undertaken by the risk committee over the period. The disclosure of the risk management process was less detailed on average when compared with other sectors, with most focusing mainly on risk governance / monitoring and the roles and responsibilities of different committees / departments, whilst having limited information on day-to-day risk identification and evaluation, and how this related to the strategy, tactics and operations.

Tullow Oil provided some information on the improvements that had been made in relation to the control of each of the significant risks, as well as information on improvements that had been made to the overall risk management process.

### 8.3 Engineering / Manufacturing

Overall, the engineering / manufacturing sector provided excellent disclosure on risk management. All selected companies presented information on the significant risk factors and provided details of the impact of each risk on the strategy, tactics and operations of the company. Additionally, information was provided on the mitigation actions that had been taken.

The selected companies provided excellent sections describing the roles and responsibilities of the board and the various committees that had responsibility for risk management. All selected companies described the key risk actions that had been taken during the year to review and improve the effectiveness of the risk management process.

Together with the retail sector, this sector provided the best description of the risk assessments that had been undertaken, and all companies in the engineering / manufacturing sector described the identification and evaluation of risks. The emphasis in the Petrofac report was on the role of internal audit and the audit committee, whereas Rexam and Invensys provided more detailed information and a broader perspective.

### 8.4 Financial Institutions

**As would be expected, the information provided on risk management for financial institutions contained much more detail than for other business sectors. For example, the risk management section for Barclays was more than 100 pages long. Overall, the risk management descriptions provided by the three selected companies were extremely comprehensive.**

There were some very good examples of descriptions of the risk agenda and the arrangements for risk governance. These reports included details of the aims, resources and the alignment of risk management activities with other business operations. In fact, so much information was provided by the financial institutions that it has proved difficult to extract good practice lessons for other business sectors. The report produced by Barclays was extremely well structured and described the identification, assessment and control strategies separately for each of the significant risks identified.

This was an extremely comprehensive report that indicated that risk management played a significant role in the strategy, tactics and operations of the company. Risk management was also described in terms of the compliance obligations placed on financial institutions.

### 8.5 Food / Drink

The information provided on risk management by the companies selected in the food / drink business sector

was less detailed than for most other business sectors. The reports for the three selected companies were very similar in structure and content, and only provided limited information on the risk processes and systems in place and the arrangements for risk governance.

All of the selected companies provided a list of the key risks, together with some information on the impact and mitigation, although the information was not particularly detailed. SAB Miller provided some information on the link between each risk and the strategic objective that would be impacted, in order to give context to each of the significant risks identified.

## 8.6 Media / IT / Telecoms

The media / IT / telecoms sector was extremely diverse and so a wide variation in the amount of detail reported was observed. Although some of the reports were quite short, most of them were very clear and easy to understand. Nevertheless, a limited amount of detail was provided by this sector compared to the other business sectors that were investigated. In particular, there was little information on the roles of the different committees and no specific information on risk communication.

Despite the limited information provided by many companies in this sector, BT provided an excellent description of the risks faced, with a meaningful description of the changes to the risk profile that had occurred over the previous year. Also, details of the mitigations that were in place were provided.

De La Rue provided simple, clear flowcharts describing each step of the risk management process and the role of each business unit, committee and the board, as well as the roles of each business unit / committee / board. ITV provided a very informative table that mapped each of the risks to the strategic priorities for the company. This was one of the best examples of how to link risks to strategy.

## 8.7 Retail / Leisure

Overall, the companies selected in the retail / leisure sector provided the best sections on risk management. Each of the three companies selected in this business sector provided information on risk agenda, risk assessment, risk response, risk communication and risk governance. Extensive information was provided by each of the companies, with IHG and Debenhams providing extensive, yet easy to follow

information.

Sainsbury provided a similar amount of information, but it was split across the risk report and corporate governance statement, and this made it more difficult to follow. In particular, the selected companies in this sector were very good at reporting information on risk communication, and the other business sectors did not meet this high standard.

The IHG report, in particular, devoted a separate section to the risks that it believes are changing, with detailed information provided on associated mitigation steps. This demonstrated a dynamic risk management process that was closely and specifically aligned to the delivery of strategy, tactics and operations.

## 8.8 Support Services / Transport

The support services / transport sector comprises a wide variety of companies that are quite dissimilar. Nevertheless, the three companies selected all achieved good standards of risk disclosure. Serco gave details the risk management framework and provided a good summary of each stage of the risk management process in place in the company.

Serco, together with Wolseley and National Express, gave detailed overviews of the risk management process in place in the company, as well as details of the risk management framework and descriptions of the internal audit activities designed to provide assurance, as part of their risk governance arrangements. Wolseley provided information on the steps that had been taken to improve the governance arrangements in place in the company.

National Express gave a short description of the arrangements in place to ensure adequate risk governance, but the information provided by Serco included a slightly greater level of detail.

## 9. Keeping risk management reporting relevant

**In summary, disclosure helps the board to demonstrate that it is leading the organisation and it also provides evidence that the company has the systems and capability in place to deliver the strategy and business to increase and protect value over the long term. Keeping risk management reporting relevant enhances shareholder confidence.**

It is therefore in the best interests of the board of the company to provide full disclosure on risk management activities. If the company is undertaking effective risk management actions that are aligned with the success of the organisation and the delivery of the required strategy, tactics and operations, then it is in the best interests of the board, the company, the shareholders and other stakeholders to make this clear.

The contribution of the risk manager is to support the delivery of an effective set of risk management activities, as defined by the risk agenda, risk assessment, risk response, risk communication and risk governance components of an effective risk management structure. Additionally, the risk manager should ensure that the reports provided for the board on risk management activities are fully aligned and embedded within the issues that represent the priorities for board members.

By providing a robust structure and aligning risk management activities with the strategy, tactics and operations of the company, the risk manager will be able to demonstrate the relevance of risk management to the success of the company, as well as demonstrating the importance of the risk manager role.

Most companies recognise the benefits of having explicit risk management arrangements in place. Reporting on the nature and extent of these risk management activities will deliver further benefits. In summary, there are several reasons for reporting in full on risk management activities within the company, as follows:

- The overall intention is to make the company look good and thereby help to give shareholders confidence in the management of that company.
- If the company is doing risk management well, the disclosures will contain that message and show that risk management is dynamic and comprehensive.
- At the same time, if the company has decided to do risk management, then reporting on these activities will bring discipline to those risk management procedures.
- Good disclosures will give insight into the culture of the company and demonstrate the maturity of the management, specifically with regard to risk management.
- Efficacy of strategy, effectiveness of projects and efficiency of operations result in a resilient company that deserves stakeholder support.



The extract from the IHG annual report and financial statements is a good example of risk management efforts aligned with strategy, tactics and operations. This demonstrates that the company does risk management well, and is proud to report on its risk management activities and the fact that they are embedded into the management of a successful company. The risk management information published by companies such as IHG helps to provide confidence to shareholders and other stakeholders.

#### **IHG: Comprehensive and accurate risk content**

Risk management is about managing uncertainty and IHG seeks to develop comprehensive and accurate risk content through risk assessments. This enables us to have better informed decision-making, which when implemented in the right cultural context, greatly improves performance at the strategic, tactical and operational levels of the business. We therefore categorise our risks in this way to ensure that we consider the relevant risks and have in place appropriate oversight roles:

- strategic and market risks: arise from changes in the external environment and can impact on our vision, ambitions and strategy over the long-term
- tactical and project risks: the risks that impact the delivery of IHG key initiatives and projects
- operational risks: wide spectrum of risks that can affect the resilience, continuity or performance of IHG internal operating systems or hotels

(Edited extract from IHG Annual Report and Financial Statements 2012)

## Appendix A: List of business sectors and companies selected

Business Sector	Company and report studied
<b>1. Chemicals / Pharmaceuticals</b>	GlaxoSmithKline – GSK Annual Report 2012
	Johnson Matthey – Annual Report and Accounts 2012
	AstraZeneca – Annual Report and Form 20-F Information 2012
<b>2. Energy / Mining</b>	Centrica plc – Annual Report and Accounts 2012
	SSE – Annual Report 2012
	Tullow Oil plc – 2012 Annual Report and Accounts
<b>3. Engineering / Manufacturing</b>	Rexam – Annual Report 2012
	Petrofac plc – Annual Report and Accounts 2012
	Invensys plc – Annual Report and Accounts 2012
<b>4. Financial Institutions</b>	Standard Chartered – Annual Report 2011
	Barclays PLC – Annual Report 2012
	Man SE – 2012 Annual Report
<b>5. Food / Drink</b>	SAB Miller plc – Annual Report 2012
	Tate & Lyle PLC – Annual Report and Accounts 2012
	Dairy Crest Group plc – Annual Report 2012
<b>6. Media / IT / Telecoms</b>	ITV plc – Annual Report and Accounts 2012
	BT Group plc – Annual Report and Form 20-F 2012.
	De La Rue – Annual Report 2012
<b>7. Retail / Leisure</b>	IHG – Annual Report and Financial Statements 2012
	J Sainsbury plc – Annual Report and Financial Statements 2012
	Debenhams plc – Annual Report and Accounts 2012
<b>8. Support Services / Transport</b>	Serco Group plc – Annual Report and Accounts 2012
	Wolseley plc – Annual Report and Accounts 2012
	National Express Group PLC – Annual Report and Accounts 2012

# Appendix B: Scope and extent of good risk management disclosure

## Part 1: Risk Agenda

The company should provide information on the agenda for risk and risk management, including why it undertakes risk management activities, the resources allocated and the main features of those risk management activities.

- |     |   |
|-----|---|
| 1.1 | Description of the assurance reasons for undertaking risk management, including activities undertaken because it is mandatory, to help to provide assurance to stakeholders and in order to collect information for better informed business decisions. |
| 1.2 | Description of the performance reasons for undertaking the risk management activities, including improving the efficiency and effectiveness of the design and implementation of the business strategy, tactics and operations.                          |
| 1.3 | Description of the resources allocated to risk management that are proportionate to the level of risk, but sufficient to embed assessment, response, communication and governance of significant risks into company processes.                          |

## Part 2: Risk Assessment

The company should provide information on the extent and methodology for undertaking risk assessments, as well as details of the key risk factors with the potential to have a significant impact on the success of the company.

- |     |   |
|-----|---|
| 2.1 | Description of the risk assessment procedures, including details of the risk classification system, who is involved in the risk assessment activities, the information that is required and how the information is collected. |
| 2.2 | Description of the level of impact that is significant for the finances, infrastructure, reputation and marketplace, and the anticipated consequences for the strategy, tactics and operations of the company.                |
| 2.3 | Description of the efficiency and effectiveness of the existing controls, in order to decide whether the current level of risk is acceptable and within risk appetite, taking into account business and legal requirements.   |

## Part 3: Risk Response

The company should provide information on how it evaluates the efficiency and effectiveness of existing risk controls, how it decides whether additional controls are required and how it designs suitable disaster response and business continuity plans.

3.1	Description of the methodology for deciding how to respond to each risk in terms of the willingness to tolerate the risk; the desire to further treat the risk; the availability of suitable risk transfer; and the desire to terminate the risk.
3.2	Description of the means for determining the efficiency and effectiveness of the existing risk controls in order to decide whether there is a business or compliance need to design and implement further controls.
3.3	Description of the existing arrangements to evaluate the potential for major disruption to business operations and confirmation of the existence of up-to-date disaster response and business continuity plans.

## Part 4: Risk Communication

The company should provide information on risk and risk management responsibilities and describe the arrangements for risk communication, including how risk information is recorded and risk action plans are developed.

4.1	Description of the risk architecture and protocols, including information on the risk roles of individuals; the terms of reference for committees with risk responsibilities; and the risk management policies and procedures.
4.2	Description of the risk documentation, including records of risk assessments, risk communication arrangements, the requirements for risk training and the existence of a written risk management manual.
4.3	Description of the risk reporting arrangements, including details of progress with risk action plans, details of risk escalation procedures, external risk reporting procedures and, as necessary, whistleblowing arrangements.

## Part 5: Risk Governance

The company should provide information on the procedures in place to help to provide risk assurance to stakeholders and provide details of the governance processes for management of existing and emerging risks.

5.1	Description of the arrangements to ensure adequate governance of significant risks, including how acceptable levels of risk are decided; responsibility for implementing standards; and how achievement of standards is monitored.
5.2	Description of the means for providing assurance regarding management of significant risks, including arrangements for challenging the assurances and details of the risk indicators that are used to determine performance.
5.3	Description of the arrangements for the management of emerging risks, including details of the emerging risks facing the company and the actions to obtain more risk information and/or reduce exposure to emerging risks.

## Notes





6 Lloyds Avenue  
London  
EC3N 3AX  
Ph. +44 207 680 3088  
Fax. +44 20 7702 3752  
email: [enquiries@airmic.com](mailto:enquiries@airmic.com)  
[www.airmic.com](http://www.airmic.com)

Together Leading in Risk

