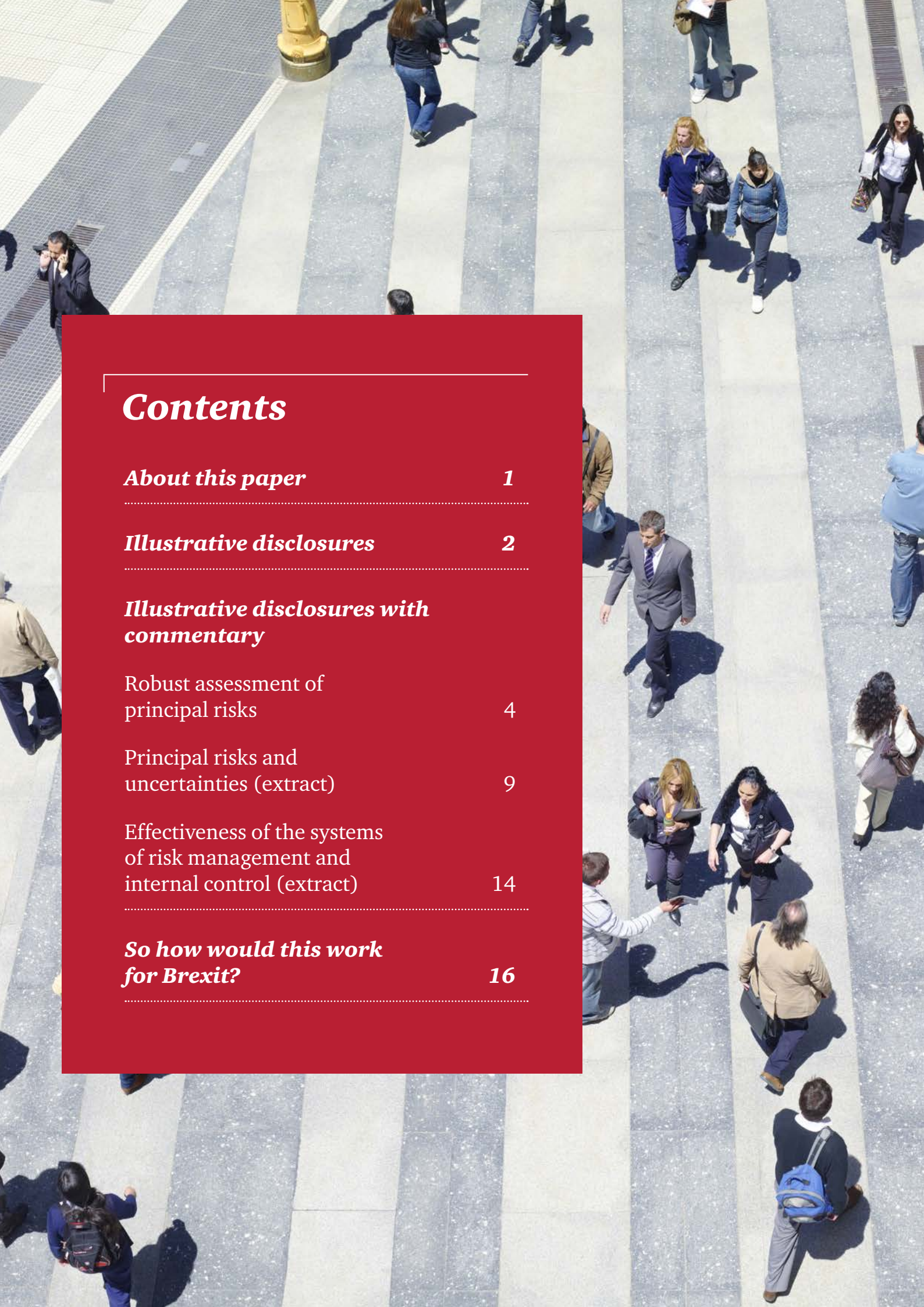
www.pwc.co.uk

Tackling risk reporting

Practical suggestions, positive thinking

September 2016

pwc



Contents

About this paper

The 2014 UK Corporate Governance Code ('the Code') may well be remembered as the one that introduced the viability statement – certainly, of all the changes to the Code, the viability statement had the most obvious impact on 2015-16 annual reports. In contrast, although we know that there has been lots of focus within companies on the underlying risks and risk management systems, there is much less evidence of this coming through into annual reports. The 2015/16 PwC corporate reporting survey shows that the steady improvement in risk disclosures has continued, but it has been very much a slow ongoing evolution, and there has been no revolution as a result of the advent of the new Code.

In many ways, this is understandable. Other than the new confirmation that the directors have carried out a 'robust assessment' of the principal risks, there is little to drive change in risk disclosures in either the Code itself or in the FRC *Guidance on risk management, internal control and related financial and business reporting* ('the Guidance' or 'the FRC Guidance') that was issued alongside it. Risk reporting remains a challenging area where a natural conservatism holds sway: companies tell us that their priority is to avoid giving away anything that is commercially prejudicial and that the rewards of breaking free from the pack are just not there. Risk professionals can find their insights being toned down by compliance or legal management – or the board. They don't believe there is a commonly understood language in which to talk about risk, so giving real insights into their own company-specific risks would actually be a risk in itself: too many shareholders (and other stakeholders) would be likely to take away the wrong message.

We hope the proposals in this paper will help to move risk reporting forward[1]. What we are suggesting is intended to be challenging. It has to be, because we know from our engagement with investors and other stakeholders that the state of risk reporting today does not meet their needs. But it is also intended to be practical: it should not add pages and pages to an average annual report – indeed it could save some space – and it does not include anything that we see as potentially prejudicial. Our proposals are based on a few simple ideas:

- **Risk reporting is an opportunity to show how an organisation is on top of its risks** – that management and the board/board committees understand what the risks are and why they're taking them, have considered what they need to do about them, and know whether they are being managed according to plan.
- **Risk reporting could be better integrated** with other related parts of the annual report, including the business model and strategy and – flowing from the previous point – the effectiveness of the systems of risk management and internal control.
- **Risk reporting would benefit from a robust, consistent framework** on which to base the identification and assessment of risks; risk specialists clearly have their own frameworks to manage risk but our focus in this paper is on how to generate meaningful disclosures and the language we have used reflects the Code and FRC Guidance rather than any particular methodology.

As with our previous publication on the viability statement[2], we have put our heads above the parapet and included illustrative disclosures to show what we have in mind (pages 2 to 3). As always, these are not intended to be templates, and our thoughts continue to develop. From page 4 onwards we comment on the various parts of our proposals – it's important to read the comments as well as the illustrative disclosure. We also include published examples where companies have already moved in the direction that we are advocating. At the end of the document we include some specific suggestions around reporting on Brexit as that will be a key issue for many. Overall, though, what is in this document is a prototype that we will continue to work on and we would be delighted to receive your feedback on it.

[1] Companies in the financial services sector and SEC registrants have a number of specific additional challenges that we have not attempted to address here. We believe that the underlying concepts are still relevant for them, however.
[2] Tackling the viability statement: practical suggestions, positive thinking and the update on this.

Illustrative disclosures

Set out below are illustrative disclosures for a company with a December year end with proposals for three key areas of risk-related reporting: the robust assessment of risks, the principal risks and the review of effectiveness of the systems of risk management and internal control. We have illustrated only one principal risk for this purpose, but comment on how it relates to our wider thinking from page 4.

1) Robust assessment of principal risks

The audit committee received a report from management at its meetings in [May] and [November] setting out an update on the principal risks and uncertainties arising from the group's business model and strategy. The report was derived from the group's systems of risk management and internal control and was used as the basis for the robust assessment of principal risks. The audit committee also considered the effectiveness of the systems, and has reported on this below (see page 3).

The report set out the judgements made by management in selecting the principal risks and uncertainties from the underlying [risk register/ other appropriate source], using a consistent set of criteria for each potential risk on the register.

These criteria included:

Focus

- Is the risk clearly identified and expressed?
- Is it tailored to the circumstances of the group, including why it is being incurred?

Relevance and materiality

- How does the risk relate to the business model and/or strategy?
- Would the consequence(s) be direct and/or indirect and what would they be?
- Would the consequence(s) be short-term, medium-term or long-term?
- Which stakeholders are interested?

Status

- What is being done about the risk in terms of active management or other mitigation?
- Is the risk currently within the risk appetite parameters? Specifically:
  - Are there any failings or weaknesses of risk management or internal control in connection with the risk? Are they significant?
  - What has changed in relation to the assessment and management of the risk, and what is expected to change going forward?

Note: *The criteria that management has used have been listed out for ease of reference and to allow us to comment on them later. They could be omitted from a published disclosure, or boxed out if included.*

The audit committee assessed management's judgements in relation to whether the right risks had been selected and their status, based on the information and assurance provided to them and their own involvement where applicable. The results of the management and audit committee process are set out below in the disclosure of the principal risks and uncertainties.

The audit committee also held a session at its meeting in [November] to consider the completeness of the risk register on a top-down basis.

The committee reported on their work to the board at its meeting in [February] to support it in making its confirmation that it had carried out a robust assessment of the principal risks.

2) Principal risks and uncertainties (extract)

The risk

Failure in the continuity of supply of key components and reputational damage arising from the use of subcontractors in the supply chain.

The risk > relevance and materiality

- Following the decision to restructure the supply chain, as set out on pages [x] to [y], the group during the year entered into contracts for the manufacture of certain products in its [x] range with organisations that utilise major subcontractors. Two of these subcontractors, based in [territory x], have been the subject of negative reports from certain NGOs as to the terms and conditions of their employees.
- These matters could expose the group to short-term failures in the continuity of supply of key component [z] for the [x] range of products and also make the supplier relationship unsustainable in the medium-term.
- This could result in direct financial penalties under our contracts with those organisations if our ability to supply customers [x] and [y] is affected. It could also affect our ability to do business with customers [x] and [y] in the future; currently they represent [50]% of the revenue from the [x] range and [25]% of overall revenues.

- Even if the direct financial effect of the risks outlined above is limited, there could still be a significant impact on the reputation of the group from negative publicity (whether or not an incident occurs). A number of other stakeholders monitor the involvement of companies in the [x] industry in relation to the terms and conditions of workers in their supply chain.

Management's response > status

- The group took the decision to enter into these supplier contracts following formal tender processes including significant due diligence on their arrangements in the areas discussed above.
- The contracts were specifically drawn up to include arrangements for regular reports to the group on how the suppliers are monitoring working terms and conditions at third parties, and allow for supplier audits that include the third parties. The reports provide data on a number of indicators designed to identify where the risk might be increasing, including matters such as employee turnover and training records, breaches of policies on working hours, and lost-time accidents.
- Reports on these 'key risk indicators' and supplier audits are monitored at the weekly supply chain meetings chaired by the Operations Director.
- They have not so far indicated any incidences where the subcontractors appear to be moving outside of the anticipated parameters.

The audit committee's view

- The audit committee assessed management's analysis of these supplier relationships and the role of third parties in them, including the status of the key risk indicators, at its meeting in [November]. It had also reviewed the proposed reporting and supplier audit arrangements prior to the contracts being entered into.
- The strategic change was discussed when last year's results were announced and explained in the annual report. The management and governance arrangements around it have also been addressed at the meetings held with a number of institutional investors during the year.
- The committee consulted an external expert on the risks associated with the use of third parties in the supply chain and considered the specific factors that they advised should be taken into account. The expert had also advised management when the supplier contracts were being drawn up.
- The committee reviewed how management had engaged with the relevant civil society stakeholder groups on an ongoing basis, and considered whether any specific matters raised had been appropriately addressed.
- The committee was satisfied based on its review that this risk is currently being managed within the anticipated parameters, and that it is not currently likely to affect the group's delivery of its strategy.

3) Effectiveness of the systems of risk management and internal control (extract)

The audit committee reviewed the effectiveness of the group's systems of risk management and internal control. In doing so, it focused on the following areas in particular:

Risk appetite and corporate culture

- The change in strategy to restructure the supply chain involved a decision to take on a new principal risk based on the criteria explained above.
- In considering the change of strategy the board's appetite for matters of this kind was established and this has now been formally documented to allow future decisions to be considered against the same parameters, which include payback periods and return on investment.
- The board has also now set formal parameters for its appetite in relation to customer contracting. This is seen as particularly important to ensuring that the appetite for risk is embedded in the day-to-day decision making of employees and management.
- The board will continue to consider creating formal statements of risk appetite and company policy in other areas, but believes that other areas of risk are appropriately handled by management and the board on the current, less formal basis.

Illustrative disclosures with commentary

1) Robust assessment of principal risks

Illustrative disclosures

The audit committee received a report from management at its meetings in [May] and [November] setting out an update on the principal risks and uncertainties arising from the group's business model and strategy.

The report was derived from the group's systems of risk management and internal control and was used as the basis for the robust assessment of principal risks. The audit committee also considered the effectiveness of the systems, and has reported on this below (see page 3).

Commentary

We have assumed that the audit committee is taking the lead in both the robust assessment of the principal risks and the review of effectiveness of the systems of risk management and internal control, and that it is covering operational and compliance as well as financial matters. This is not always the case, and it may be that the whole board or a risk committee leads in relation to a number of areas of risk and internal control.

The outcome of the work of the audit or risk committee would of course have to be communicated to the whole board as it is the board which has the responsibility for reporting on these provisions of the Code.

The reporting from management that we refer to here would be part of the annual cycle of work for the audit committee, contributing to the ongoing monitoring of the systems of risk management and internal control that is now required under provision C.2.3 of the Code.

The report set out the judgements made by management in selecting the principal risks and uncertainties from the underlying [risk register/other appropriate source], using a consistent set of criteria for each potential risk on the register. These criteria included:

The idea here is to have a **robust framework on which management can base its judgements**. The precise criteria should be tailored to the circumstances – these are not meant to be definitive for every situation.

As noted earlier, risk specialists have their own frameworks to identify and manage risk – our focus is on how to generate meaningful disclosures and our language reflects the Code and FRC Guidance rather than any particular methodology. We also make no systematic distinction between the terms 'risk' and 'uncertainty' in this paper though we believe that a risk can be defined as 'a future event that could affect an organisation's ability to achieve its objectives'.

Illustrative disclosures

Focus

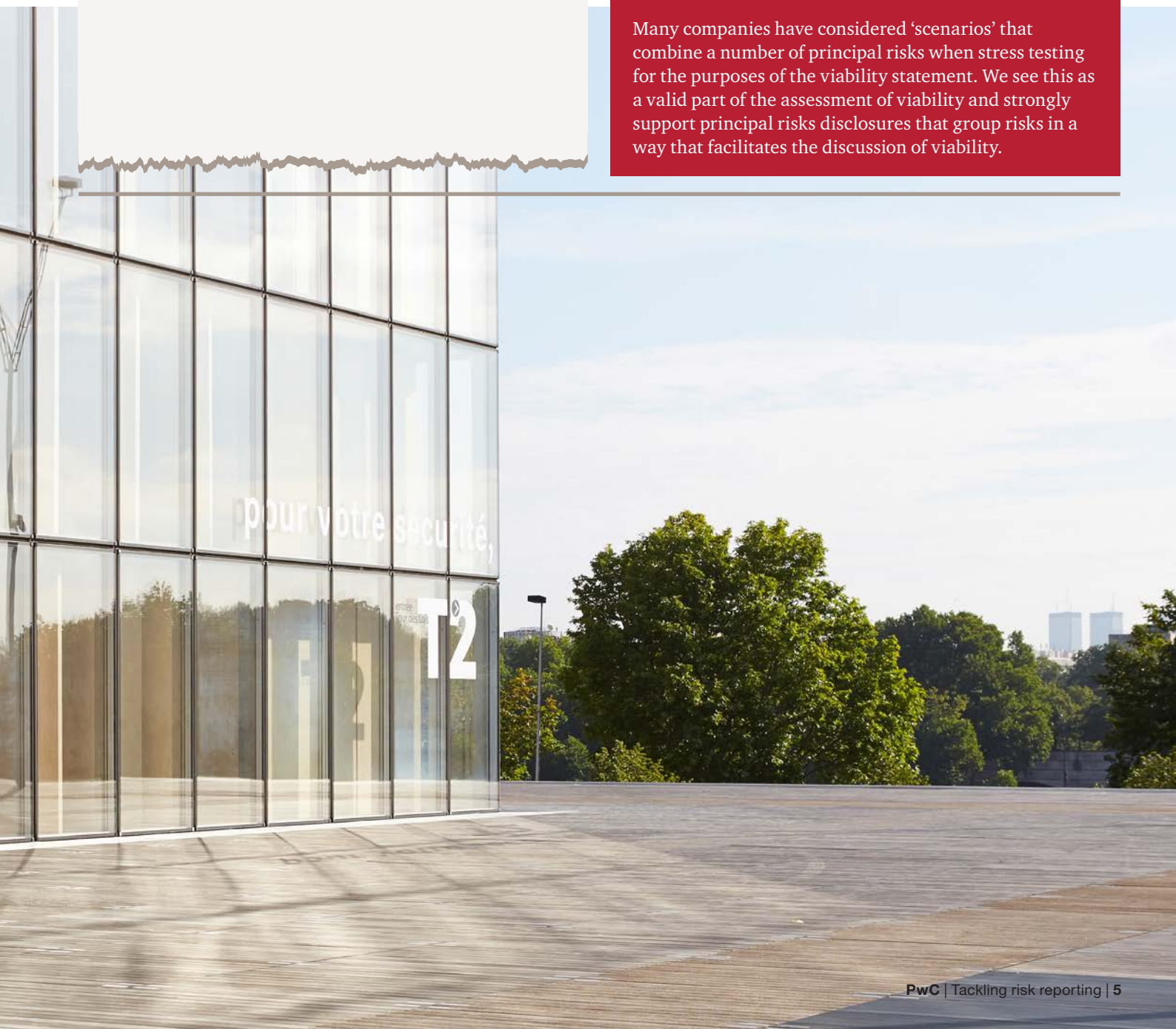
- Is the risk clearly identified and expressed?
- Is it tailored to the circumstances of the group, including why it is being incurred?

Commentary

Too many of the principal risks in annual reports are very generic, barely change year on year and could be applied to almost any company. And if the risk itself is not rigorously thought through afresh each year, the rest of the disclosure will almost always be generic too.

There can also be various relationships between risks. Where they are genuinely inter-related, we would usually see them as elements of one combination risk that should be dealt with together.

Many companies have considered 'scenarios' that combine a number of principal risks when stress testing for the purposes of the viability statement. We see this as a valid part of the assessment of viability and strongly support principal risks disclosures that group risks in a way that facilitates the discussion of viability.



Illustrative disclosures with commentary (Contd.)

1) Robust assessment of principal risks

Illustrative disclosures

Relevance and materiality

- How does the risk relate to the business model and/or strategy?
- Would the consequence(s) be direct and/or indirect and what would they be?
- Would the consequence(s) be short-term, medium-term or long-term?
- Which stakeholders are interested?

Commentary

There is still a tendency for there to be too many principal risks in annual reports. The regulator is clear that principal risks should be limited to those that are considered by management to be '…material to the development, performance, position or future prospects of the entity' [*FRC Guidance on the strategic report*, paragraph 7.24]. We think that using questions such as those opposite would help management to make these judgements more rigorously and consistently.

The first question on our list deals with how the issue relates to the business model and/or strategy. This is because we think that a genuine principal risk will almost always relate to an aspect of the business model and/or a strategic direction. To take one example: being able to hire and retain good people is important for any business but it is strategically vital (and therefore a principal risk) for a business where the model is built on the creativity of a few individuals.

We have not focused on the likelihood of a risk crystallising because we believe that the experience of the financial crisis and other major 'black swan' events in recent years has resulted in a shift away from likelihood to a greater weighting being placed on the potential impact/effect of risks.

The right approach to reputational risk is often debated. In our principal risk illustration we have envisaged a potential breach of working conditions having both a direct effect on the company's relationship with its civil society stakeholders and an indirect effect on its relationships with customers through discontinuity in the supply chain.

*Based on the first **288** FTSE 350 companies to report against the 2014 Code…*

12 *principal risks on average are disclosed by FTSE 100 companies.*

10 *principal risks on average are disclosed by FTSE 250 companies.*

Illustrative disclosures

Status

- What is being done about the risk in terms of active management or other mitigation?

Commentary

We are suggesting that the information generated in this part of the disclosure should focus on activities at the management level; the audit committee/board level input is dealt with below.

The activities described should be the key ones and be as directly related as possible to the risk, not a restatement of the overall risk management system. We would also use active language to describe management's contribution: so, 'management took steps to address the group's reliance on…' rather than (as we often see) 'the group is naturally hedged against…'.

- Is the risk currently within the risk appetite parameters? Specifically:
  - Are there any failings or weaknesses of risk management or internal control in connection with the risk? Are they significant?
  - What has changed in relation to the assessment and management of the risk, and what is expected to change going forward?

We are focused here on the status of the risk against management's plans rather than what management's plans were. **So we are not necessarily advocating that the appetite for every principal risk is disclosed,** but we would expect an explanation where the current position is outside the planned parameters.

Such exceptions or issues could relate, as the questions suggest, to failings or weaknesses in risk management or internal control and/or to situations where there is a change in the extent to which the risk is being controlled or mitigated. Remember however that risk management is a dynamic process and such changes can be positive as well as negative.

Note: notwithstanding the approach we have taken in our illustrative disclosure, we think it is often useful to include commentary on the appetite for risk at a risk-by-risk (or equivalent) level.

*Of the first **288** FTSE 350 companies to report against the 2014 Code…*

Only ***11%*** *disclosed qualitative information on risk appetite.*

*Of the first **288** FTSE 350 companies to report against the 2014 Code…*

Only ***1*** *definite significant failing or weakness was disclosed.*

Illustrative disclosures with commentary (Contd.)

1) Robust assessment of principal risks

Illustrative disclosures

The audit committee assessed management's judgements in relation to whether the right risks had been selected and their status, based on the information and assurance provided to them and their own involvement where applicable.

The results of the management and audit committee process are set out below in the disclosure of the principal risks and uncertainties.

Commentary

The principal risk and risk management disclosures are generally included in the strategic report and reflect the fact that the executive takes day-to-day responsibility for these areas. We think it makes sense to **integrate the audit committee's independent check on these activities with the underlying processes and risks** to give the complete picture as to how the group deals with the relevant matters.

The combined disclosures could either be in the strategic report or the governance report, with cross-references as necessary to indicate where the necessary content is situated. We can see a strong argument for pulling everything together in the strategic report as it can also be provided to shareholders on a standalone basis.

The audit committee also held a session at its meeting in [November] to consider the completeness of the risk register on a top-down basis.

It is important that the audit committee is given an opportunity to step back and use its combined knowledge and experience as a completeness check on the risks identified through management's processes.

The committee reported on their work to the board at its meeting in [February] to support it in making its confirmation that it had carried out a robust assessment of principal risks.

We always recommend that the board makes its formal statement (which is not shown here) in proximity to the principal risk disclosures, using wording that mirrors the Code provision to make it clear that the requirement has been met. Reporting by the audit committee alone does not meet the requirement for a formal statement.

*Of the first **288** FTSE 350 companies to report against the 2014 Code...*

Only ***234*** *provided an easily identifiable robust risk assessment statement.*

2) Principal risks and uncertainties (extract)

Illustrative disclosures

The risk

Failure in the continuity of supply of key components and reputational damage arising from the use of subcontractors in the supply chain.

The risk > relevance and materiality

- Following the decision to restructure the supply chain, as set out on pages [x] to [y], the group during the year entered into contracts for the manufacture of certain products in its [x] range with organisations that utilise major subcontractors. Two of these subcontractors, based in [territory x], have been the subject of negative reports from certain NGOs as to the terms and conditions of their employees.

Commentary

This is an illustrative example of a principal risk disclosure made using the criteria above. It could also be presented as a table, though we find a narrative format to be more flexible and suited to telling a coherent story and making connections.

The principal risk disclosure starts by indicating how the risk arises from a strategic decision made in the year – so this is a matter of strategic importance, representing a significant change in the overall risk profile of the group.

As noted on page 1, in our illustration we are advocating a substantial level of detail to make the description of the risks really specific and tailored.

We would give the names of the relevant subcontractors if this has been cleared with them (potentially through the suppliers) as part of the contractual arrangements.

Example 1> Sage Group > September 2015 annual report and accounts > Page 40

Good linkage between strategy and risk

Principal Risk	Risk Background
2. Licensing Model Transition	
Sage does not successfully move to a target subscription licensing model, and adapt its customer approach to reflect the change to this model Primary strategic alignment: Customers for Life	Sage wishes to continue to shift its licensing model towards subscription, where customers pay a monthly charge to use a licence, and in doing so are entitled to upgrade to the most recent release. Subscription licensing is perceived as beneficial within the software industry for a variety of reasons, including increased customer contact and predictability of cash flow. Any transition process must, however, be controlled in order to manage potential impacts, including short term revenue figures. This risk is an evolution from 2014. Through 2015, a dual approach has been followed to ensure achievement of revenue figures, while moving towards subscription. In parallel to these activities, the first of a number of Customer Business Centres have been opened for global products, which co-locate teams (digital marketing, sales, service operations) enabling them to operate collaboratively and serve customers quickly and efficiently.

*Of the first **288** FTSE 350 companies to report against the 2014 Code...*

Only **34%** *disclosed the links between principal risks and strategic objectives.*

Illustrative disclosures with commentary (Contd.)

2) Principal risks and uncertainties (extract)

Illustrative disclosures

- These matters could expose the group to short-term failures in the continuity of supply of key component [z] for the [x] range of products and also make the supplier relationship unsustainable in the medium-term.

Commentary

This sets out the time horizon(s) over which the risk is most relevant. Where it is possible to be even more specific, we would be.

- This could result in direct financial penalties under our contracts with those organisations if our ability to supply customers [x] and [y] is affected. It could also affect our ability to do business with customers [x] and [y] in the future; currently they represent [50]% of the revenue from the [x] range and [25]% of overall revenues.

We now set out the direct and indirect consequence(s) that the risk might have for the group itself. As well as direct financial penalties, there could also be reputational damage affecting the future relationship with these important customers.

Note: we are starting with the gross risk and will move on to management and mitigation and its net effect below.

- Even if the direct financial effect of the risks outlined above is limited, there could still be a significant impact on the reputation of the group from negative publicity (whether or not an incident occurs). A number of other stakeholders monitor the involvement of companies in the [x] industry in relation to the terms and conditions of workers in their supply chain.

The strategic decision noted above means that the group's operations are now particularly relevant to the concerns of certain stakeholder groups. Their activities also have the potential to impact the group in a direct manner.

*Of the first **288** FTSE 350 companies to report against the 2014 Code...*

56% *described the movement in principal risks.*

But only **31%** *disclosed more than just directional arrows.*

Illustrative disclosures

Management's response

- The group took the decision to enter into these supplier contracts following formal tender processes including significant due diligence on their arrangements in the areas discussed above.
- The contracts were specifically drawn up to include arrangements for regular reports to the group on how the suppliers are monitoring working terms and conditions at third parties, and allow for supplier audits that include the third parties. The reports provide data on a number of indicators designed to identify where the risk might be increasing, including matters such as employee turnover and training records, breaches of policies on working hours, and lost-time accidents.

Commentary

The disclosure now moves to how the risk is being managed or mitigated. The measures described here are very specific to the risk and reflect active measures taken by management.

The reports to the group from the suppliers are envisaged as including a number of **'key risk indicators'**. These are increasingly being used to give early warning to management and boards. The focus here is on reporting where matters are moving outside the parameters (rather than where those parameters are set).

- Reports on these 'key risk indicators' and supplier audits are monitored at the weekly supply chain meetings chaired by the Operations Director.

Organisations are starting to provide more **information on where the responsibility for particular risks and risk management sits;** here we have suggested extending this to include the relevant process.

- They have not so far indicated any incidences where the subcontractors appear to be moving outside of the anticipated parameters.

Where matters are outside the anticipated parameters we would expect disclosure as to what is being done, or can be done, to bring them back within the acceptable range. This could easily be relevant to the judgement as to whether the annual report is **'fair, balanced and understandable'**.

Illustrative disclosures with commentary (Contd.)

2) Principal risks and uncertainties (extract)

Illustrative disclosures

The audit committee's view

- The audit committee assessed management's analysis of these supplier relationships and the role of third parties in them, including the status of the key risk indicators, at its meeting in [November]. It had also reviewed the proposed reporting and supplier audit arrangements prior to the contracts being entered into.

Commentary

We are placing as much emphasis in our illustrative disclosure on the independent check and exercise of its own judgement by the audit committee as we are on management's assertions about the management and mitigation activities.

This allows for some discretion in the discussion of how the risk is being managed (the detail of which is potentially sensitive). Instead, we are shifting the focus on to how more independent observers with access to all the relevant information assessed management's approach and conclusion.

- The strategic change was discussed when last year's results were announced and explained in the annual report. The management and governance arrangements around it have also been addressed at the meetings held with a number of institutional investors during the year.

A reminder has been included here that the restructuring of the supply chain was communicated and the group engaged with shareholders and analysts on it. As well as the direct financial risk, many institutions have regard for such non-financial and corporate social responsibility issues and some investment manager mandates specifically refer to them.

Example 2 > GSK > December 2015 annual report > Page 88

Good detail in audit committee report on the committee's involvement with a number of principal risks

Novartis integration

Oversight of the Novartis transaction has been a key priority for the Committee, given the importance of the success of the transaction to the Group. The Committee has received regular reports and presentations on the integration and management of the acquired Novartis businesses from an operational, internal control accounting and risk management perspective both in the run up to the close of the transaction in March 2015 and regularly throughout the year as the integration and associated restructuring programmes began to be implemented. In addition, on-boarded Novartis employees have successfully completed the mandatory training on our Code of Conduct, ABAC, and Corporate Integrity Agreement obligations.

Illustrative disclosures	*Commentary*
• The committee consulted an external expert on the risks associated with the use of third parties in the supply chain and considered the specific factors that they advised should be considered. The expert had also advised management when the supplier contracts were being drawn up.	Even if the expert here is not fully 'independent' (in that they also advised management), it is helpful to know that the audit committee had the opportunity to ask its own questions and form its own views.
• The committee reviewed how management had engaged with the relevant civil society stakeholder groups on an ongoing basis, and considered whether any specific matters raised had been appropriately addressed.	Back on the theme of engagement, this time with other stakeholders. Making this disclosure could give those stakeholders some comfort that their agenda is recognised in the boardroom – which it should be for such a strategically important matter.
• The committee was satisfied based on its review that this risk is currently being managed within the anticipated parameters, and that it is not currently likely to affect the group's delivery of its strategy.	It is currently unusual to find **a clear conclusion as to the status of the risk management over a particular risk.** We think it is useful to make an explicit statement of this kind – it is an opportunity to spell out what is and is not being said. *Note: this risk could well be relevant for the viability assessment in our example due to the importance of this area for the group's customers and society more broadly. This could be indicated here in the principal risks or in the text of the viability disclosure.*

Illustrative disclosures with commentary (Contd.)

3) Effectiveness of the systems of risk management and internal control (extract)

Illustrative disclosures

Commentary

Paragraph 43 of the FRC Guidance on risk management, internal control and related financial and business reporting sets out a number of areas that *should* be considered in the review of effectiveness. Provision C.2.3 of the Code requires a report on that review. **Our view is that it would therefore make sense to report on the relevant aspects of paragraph 43 in the annual report.**

The audit committee reviewed the effectiveness of the group's systems of risk management and internal control. In doing so, it focused on the following areas in particular:

Although we advocate bringing the 'robust assessment' and governance over the principal risks into the strategic report, we would not make the same recommendation for the overall review of effectiveness as it covers matters not directly relevant to the principal risks. We would, however, **deal in the strategic report with any aspects of the review of effectiveness that are directly related to the principal risks**, in the way that we have shown below. We would also shift the overall balance of disclosures around the risk management and internal control systems (and their effectiveness) towards the elements that relate to the principal risks; currently we see too much detail focused on relatively low-level matters.

Note: as suggested earlier, cross-references can be used to ensure that both the strategic report and governance report are technically complete if this becomes an issue.

Illustrative disclosures

Risk appetite and corporate culture

- The change in strategy to restructure the supply chain involved a decision to take on a new principal risk based on the criteria explained above.
- In considering the change of strategy the board's appetite for matters of this kind was established and this has now been formally documented to allow future decisions to be considered against the same parameters, which include payback periods and return on investment.
- The board has also now set formal parameters for its appetite in relation to customer contracting. This was seen as particularly important to ensuring that the appetite for risk is embedded in the day-to-day decision making of employees and management.
- The board will continue to consider creating formal statements of risk appetite and company policy in other areas, but believes that other areas of risk are appropriately handled by management and the board on the current, less formal basis.

Commentary

The change in strategy in connection with the supply chain has driven the board to formalise relevant aspects of its approach to risk appetite, including some quantification of the benefits that it would look for in future.

It has done the same in one other area but does not believe this to be necessary elsewhere. It does not, therefore, regard this as a failing in its systems of risk management or internal control, but it is being clear about its approach.

Example 3 > Smith and Nephew > December 2015 annual report > Page 42

Provides an unusual level of insight into risk appetite for categories of risk

Our risk appetite

The Group operates in global markets with long-term high growth potential. We are pursuing ambitious growth targets and are prepared to accept a certain level of risk to remain competitive and to continue operating in an ever-changing world. We are very clear about the specific risks our businesses face and the level of risk that we are prepared to accept in each part of our business. We have put in place robust plans for managing those risks, through elimination, avoidance or mitigation.

Our approach to each risk varies depending on the circumstances and we accept that over time, our approach towards each risk might change as our business or the external environment evolves.

During the year, the Board took the opportunity as part of our Strategy Review to review our risk appetite in respect of our principal risks. The results of our deliberations can be summarised in the adjacent table.

CATEGORY OF RISK	RISK PARAMETERS
Strategic Moderate to high	In acquiring and developing new products and business models, moving into adjacent markets and technologies, organically or through acquisitions, and implementing innovative pricing strategies, we have a moderate to high tolerance for risk. We are willing to take certain risks in pursuit of innovation and new business.
Operational Low to moderate	In operating our business, managing our suppliers, keeping control of inventory and managing our talent and our facilities, we have a low to moderate tolerance for risk. We aim to be as efficient as possible and adopt a cautious approach, but recognise that we need to take certain risks in order to take full advantage of the opportunities open to us.
Financial Low	We recognise that sound financial controls are necessary in order to manage our business as effectively as possible. We therefore have a low tolerance for risk relating to financial controls and require all our operations to comply with our minimum acceptable practices.
Compliance Extremely low	In complying with laws and regulations and in matters relating to bribery and corruption, product safety and patient and employee safety, we have an extremely low tolerance for risk. Whilst we attempt to eradicate this risk completely, we recognise that, as in any human system, compliance failures may occur. We will respond to issues as they arise and will reassess our business scope where needed, if we judge there to be risk in these areas, which we can't manage.

So how would this work for Brexit?

Where companies made any disclosures during the main 2015-16 reporting season of risks in relation to the referendum on the UK's membership of the EU, they were generally dominated by talk of uncertainty and volatility affecting the whole economy. Now that the vote has happened we are one step closer to the risks crystallising, but the situation is still just as unclear as it was – if not more so.

So how does our proposed framework cope with discussing the implications of Brexit? Here's what it might look like if we overlay it on the basic fact pattern in our illustrative example – that is, a company which has restructured its supply chain to involve subcontractors in overseas territories.

Note that we have chosen to treat Brexit as an additional principal risk for the purposes of this disclosure, partly because it has a number of significant direct impacts on the company. In practice these impacts could also be reflected in amendments to existing principal risks. Note that Brexit is not automatically a principal risk and needs to be considered on a case-by-case basis, but that most companies are currently choosing to explain why it does not affect their risk profile significantly where the board believes this to be the case.

1) Robust assessment of principal risks

As part of the group's ongoing system of risk management, the audit committee received a report from management at its meeting in [July] updating the analysis of the group's principal risks using the same criteria used at the year end. The committee agreed that the result of the EU referendum affected a number of the existing principal risks so has added a new principal risk to summarise the situation.

2) Principal risks and uncertainties

Implications of the UK's referendum on EU membership

The risk > relevance and materiality

- The result of the recent referendum will trigger political and regulatory change affecting the whole of the UK economy in the medium to long term. Although the nature of the changes to come is currently very unclear, it has already created uncertainty in the financial markets, a significant fall in the value of sterling and a downgrading of the UK's credit rating by a number of agencies.
- The short to medium term effects of this for the group are additional risks to margins caused by higher costs in the supply chain, and a knock-on effect on the group's bank financing arrangements, as explained below.
- The group's contracts with its suppliers of the [x] range of products expose it to currency risk through the suppliers' subcontracting arrangements because the subcontractors buy and sell in US dollars, but the group pays its suppliers in sterling (so cannot hedge the currency exposure). Given the high-volume low value nature of the end product, a relatively small change

in the US dollar/sterling exchange rate has a significant impact on the group's margins and could ultimately make the contracts unsustainable. Contractual penalties would apply if the contracts were exited and the arrangements are a key part of the group's revised supply chain strategy.

- The group's bank debt is subject to covenants including interest cover and EBITDA multiples (see also page [x] in the financial review). A fall in the gross margin could affect the group's ability to comply with these covenants and any re-financing, if available, may be on less favourable terms if UK interest rates increase.

Management's response > status

- The financial monitoring of product range [x] has been extended to include sensitivity analysis whereby the impact on EBITDA of changes in the US dollar/sterling exchange rate and sales volumes are modelled, down to a $[x] to £[y] exchange rate. Currently, this modelling indicates that the exchange rate would need to move well beyond the parameters seen so far since the referendum, and to a level not seen for several decades, before the financial viability of the contract comes into question.
- Management has also begun discussions with a number of potential providers of finance as a contingency plan, as the supplier contracts recently entered into are seen as strategically important for the group's long-term plans.

The audit committee's view

- The audit committee reviewed management's analysis of the financial position on product range [x] at its meeting in [July] and was satisfied with the format and content.
- The committee also encouraged management to continue to develop its contingency plan in relation to financing, and recommended management look again at a number of other possible areas of cost control.
- Overall, the committee was satisfied that the risk was being managed within the parameters established through the reassessment of the group's risk appetite set out below.

3) Effectiveness of the systems of risk management and internal control

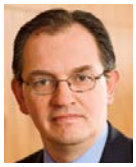
As part of its ongoing monitoring of the group's risk management systems the audit committee reassessed the group's appetite for risk in relation to its supply chain arrangements in light of the new principal risk:

- Based on the data provided by management and quality and innovation available from the new suppliers of product range [x], the committee agreed with management's view that the strategic benefits still outweighed the increased currency risk. The group continues to focus on the longer term benefits of the supply chain arrangements rather than the risk of short-term volatility.
- As noted in the description of the principal risk, the group cannot hedge its currency risk because it pays its suppliers in sterling, though they pass on the currency impact from their subcontractors to the group in the sterling price. The committee considered whether this justified a change to the group's existing policy of not engaging in currency speculation. It was agreed that the policy would not be changed at the moment but that the appetite for this would continue to be reassessed as the market position develops.

In summary the key message is that shareholders don't need to be reminded of the general uncertainty and volatility: they want reassurance that management and the board have thought through the specific implications for their particular business and are dealing with the situation as effectively as possible in the circumstances.

Contacts

We would very much like to hear what you think of our suggestions. We're conscious that we have not included some of the emerging practices we see in risk reporting, such as risk matrices and heat-maps. This is because, although we see the potential in those tools, we think the focus at this point needs to be on bringing more rigour and insight to the underlying risks themselves. We have collected plenty of examples of the current state of the art in risk reporting, however. To discuss them, the proposals in this document, or any other area of risk and governance reporting, please get in touch with your usual PwC contact or one of the central team listed below.



John Patterson

T: +44 (0)1223 552413
E: john.t.patterson@uk.pwc.com

Mark O'Sullivan

T: +44 (0)20 7804 3459
E: mark.j.osullivan@uk.pwc.com

Patrick Leach

T: +44 (0)20 7804 0315
E: patrick.m.leach@uk.pwc.com

*For more on how to implement the risk, viability and going concern aspects of the 2014 UK Corporate Governance Code, visit our **website***

160810-174223-PL-OS