Institute of Operational Risk
Operational Risk Sound Practice Guidance

**Operational Risk Governance**

September 2010
The Institute of Operational Risk Sound Practice Guidance

The IOR recognises that there is no one size fits all approach to the management of operational risk. However by drawing on the experience of practising risk professionals it is possible to identify examples of good practice described in this Guidance. Equally it is hoped that these guidance papers will facilitate a shared understanding of key operational risk concepts amongst risk management professionals, regulators and academics, thus contributing towards the further development of the discipline of operational risk.

This is one of a series of Sound Practice Guidance papers being produced by the Institute of Operational Risk (IOR) with the following objectives:

- Providing information on the practicalities and know-how necessary in order to implement the techniques that support a robust operational risk management framework;
- Empowering operational risk professionals to demonstrate the value of operational risk management to senior management in a practical rather than theoretical manner;
- Capturing the real experience of practising risk professionals, including the challenges involved in developing operational risk management frameworks.

This paper is available from the Institute’s website at www.ior-institute.org. If you have comments or suggestions on this paper please contact us on standards@ior-institute.org

The Institute of Operational Risk

The Institute of Operational Risk was created in January 2004 as a professional body whose aim is to establish and maintain standards of professional competency in the discipline of Operational Risk Management. It is an independent, not for profit, professional body designed to support its members. The stated mission of the Institute is to promote the development and discipline of Operational Risk and to foster and maintain investigations and research into the best means and methods of developing and applying the discipline and to encourage, increase, disseminate and promote knowledge, education and training and the exchange of information and ideas.
Table of Contents

1. Risk governance and culture ........................................................................................................... 1
   1.1. Risk culture ............................................................................................................................. 1
   1.2. Risk governance ...................................................................................................................... 1
   1.3. Risk leadership ........................................................................................................................ 2
   1.4. The ‘use’ test ........................................................................................................................... 2
   1.5. Incentivising good risk management ...................................................................................... 3

2. The risk governance framework ..................................................................................................... 3
   2.1. The three lines of defence ....................................................................................................... 3
   2.2. The board ................................................................................................................................ 4
   2.3. Risk oversight .......................................................................................................................... 5
       2.3.1. The risk management function ................................................................................ 5
       2.3.2. The operational risk management function ............................................................. 5
       2.3.3. Other risk oversight functions ......................................................................................... 6
   2.4. Independent assurance ............................................................................................................ 7

3. Operational risk policy .................................................................................................................... 7

4. Risk roles and responsibilities......................................................................................................... 8
   4.1. The chief risk officer (CRO) ................................................................................................... 8
   4.2. Operational risk roles and responsibilities .............................................................................. 8
   4.3. Committees ............................................................................................................................. 9
       4.3.1. Audit committee .............................................................................................................. 9
       4.3.2. Risk committee ............................................................................................................... 9
       4.3.3. Operational Risk Committee ........................................................................................... 9
   4.4. Operational risk reporting ..................................................................................................... 10

5. External stakeholders .................................................................................................................... 10
   5.1. Meeting regulatory expectations ........................................................................................... 10
   5.2. Meeting rating agencies’ expectations .................................................................................. 10
   5.3. Investors ................................................................................................................................ 10

6. Business benefits of good governance .......................................................................................... 10
1. Risk governance and culture

1.1. Risk culture

A firm’s organisational culture, its values and valued behaviours, will underpin its risk culture. It may be entrepreneurial; it may be risk averse and have a strong control element, or it will fall somewhere in between.

The valued behaviours which mark out a healthy corporate culture, supportive of good risk management, include: clarity, openness, trust and, importantly, honesty and integrity. Openness and transparency encourage comprehensive risk reporting and also encourage a challenging debate about risk at every level of the organisation. The challenge may come from the CEO and senior management but, equally, lower levels of the organisation should be encouraged to report or comment on risks they see or new and emerging risks of which they become aware.

Within such a culture, people will have an awareness of risk in what they do. They will understand their responsibilities and their levels and limits of accountability. At every level in the firm, they will be open to learning and open to challenge. A good risk culture will be supportive and not be one where blame is the name of the game.

Risk management is about opportunities as much as threats. It is also about being aware of the firm’s changing internal and external environment. The culture should therefore be one which is alive to change and to continuous improvement in all aspects of risk management.

1.2. Risk governance

Risk governance is the architecture within which risk management operates in a firm. It will reflect the firm’s risk culture. Since risk management is fundamental to running any business, risk governance is a fundamental part of corporate governance. The UK Corporate Governance Code states that ‘good governance should facilitate efficient, effective and entrepreneurial management that can deliver the long-term success of the company’. Similarly, good risk governance should result in risk being accepted and managed within known and agreed risk appetites. Risk management should be as much about identifying and taking opportunities, within agreed risk appetites, as it is about identifying and managing threats to the business which exceed those appetites.

Risk governance is not just concerned with risks internal to the firm, but must also cover the risks involved in, for example, outsourcing or wherever there is a third party dependency.

The risk governance framework should put in place a structure of risk responsibility throughout the firm. As a result, everybody in the firm will be aware of their own risk responsibilities and accountabilities and those of others with whom they work. Governance delivers effective accountability, including the accountability of the board to its owners.

Risk governance is an integral part of the day to day running of the business and is not about just complying with a set of rules. And since risk management, and especially operational risk management, involves everybody in the firm, the risk governance framework should encompass everybody. That means that it can only operate successfully if there are clear and effective lines of communication both up and down the firm and a culture in which good and bad news is allowed to travel freely.

Because governance is not a set of rules and will be influenced by the size, nature and culture of a firm, there is no ‘one size fits all’ template. However, in practical terms, the essential elements of risk governance will be established through:

- the firm’s organisational structure for risk management
- policies covering the various risks to which the firm is exposed, including its risk appetites (see IOR Sound practice guidance on Risk Appetite)
• clear statements of the roles and responsibilities of those involved in risk management, from the board down, including terms of reference of relevant committees or similar groups.

1.3. Risk leadership

As with any organisation, leaders set the standards by which the organisation operates. An effective culture, which supports good risk management, can only become part of an organisation if it is embraced by the board and senior executives, not only on paper but in their behaviour and decision-making. In this way, the core corporate values will be embedded in the behaviour of everybody in the organisation.

Risk management, and acceptance of risk against agreed risk appetites, should be at the heart of all decision-making processes, including discussions about strategy and other business initiatives, all of which will inevitably involve operational risk. Examples at a strategic level could be: acquisitions, new products, new distribution channels or changes in systems and resources, which might involve considering either the quantity or the quality and competence of staff.

If risk assessment and management are seen to be key elements of strategic decisions, it will also become a natural component of decisions at the process and activity levels. The ‘tone at the top’ will become the ‘tune in the middle’.

1.4. The ‘use’ test

It is important that risk management, including operational risk management, is not simply a group of policies which have been completed as a compliance exercise and rubber-stamped by the board. As has been stated above, it is fundamental to all business decisions. It should be demonstrable by involvement of staff at all levels in the decision-making process, from the board down as appropriate. Evidence that risk has been considered in business decision-making should be properly documented in board and meeting minutes, so that it can be made available to those responsible for internal oversight (e.g. board, audit committee, new product committee, internal audit, compliance), as well as external overseers such as external auditors and regulators. It should demonstrate how decisions are reached and that decisions are being made with due consideration of risk.

Where decisions have to be reviewed in future, proper documentation will also help executives understand the rationale for decisions made in the past, in the light of different circumstances and, quite possibly, in the absence of those who made those decisions.

With regard to operational risk management, evidence of the ‘use test’ will also come from the range of operational risk reports and the use being made of them. As regards these reports, a number of questions can be asked including, for example:

• Event reports. Is it evident that all material events are captured? Are reports thoroughly analysed for cause and the lessons which they provide?

• Risk and control assessments. Is their basis robust and consistently applied? Do they involve all the right people? Are those people regularly changed to ensure that a wide and changing range of views is included? Are the assessments challenged and peer reviewed to ensure consistency across the firm?

• Risk indicators. Are the values of indicators independently derived? Are the indicators agreed by line managers (the risk owners) as being the best for their purpose?

• Scenarios. Are they sufficiently broad? Are they sufficiently extreme? Are they nevertheless realistic?

All of this work, though, is of little use if it is not part of decision-making. All reports should lead to action. If they do not, they are probably not fit for purpose. Therefore, is there evidence that reports and what they show, especially about deteriorating risk exposure, are acted upon?

Finally, is the content of reports regularly challenged by recipients to ensure that they continue to be fit for purpose? Is the information presented sufficient for decision-making? Is the information
appropriate for the level of management to which it is addressed? Could some reports, or the information they contain, be dispensed with? It is easy to continue to provide reports ‘because that’s what we’ve always done’ rather than ask whether it is what we need to enable us to fulfil our risk management responsibilities.

1.5. Incentivising good risk management

Remuneration incentivises behaviour, which is at the heart of culture and governance. A key element of good governance and the application of the ‘use test’ is that remuneration should reward good risk management performance and should not be structured so that it encourages excessively risky behaviour or behaviour which exceeds a firm’s risk appetite.

Risk responsibilities should be an integral part of individual job descriptions and person specifications. Definitions of an employee’s risk responsibilities can be derived from risk and control assessments. These will highlight: risks to which members of staff are exposed or are responsible, controls for which they are responsible and indicators which show them how risks within their responsibility are developing.

This analysis will also help to identify the core competencies required by each member of staff, key aspects of their job descriptions, and also point to performance objectives.

Reward should therefore be a result of risk outcomes which accord with the firm’s risk strategy and appetite and should be clearly expressed in both performance objectives and appraisals.

Providing appropriate benchmarks or targets for good operational risk management is not easy. Where risk management relates to financial risks, such as market, commodity or credit risk, targets can take the form of hard numbers and be quantitative in nature.

With non-financial risks, such as operational risk, where targets involve good behaviours, such as team-work, leadership or acceptance of responsibility, or good service, setting quantitative targets can be harder. Risk indicators may form a basis, but for some behaviours which a firm wishes to incentivise, bands of achievement may well be expressed in qualitative statements.

But remuneration is not the only incentive. If there is a healthy risk culture, motivation for good risk management will come from the pride of doing a job well, in accordance with acceptable norms of behaviour and integrity, and of this being recognised through regular and positive appraisals and feedback.

All of the above underlines the importance of the risk function having a close relationship with the Human resource (HR) function, as well as HR’s role as an important element of risk oversight (see 2.1 below).

2. The risk governance framework

2.1. The three lines of defence

A comprehensive risk management framework will have clear risk roles and responsibilities at all levels. These roles can be represented by the ‘three lines of defence’ shown in the following diagram:
The first line of defence is the responsibility of senior management, the risk takers in the business. This involves day to day risk management, in accordance with agreed risk policies, appetite and controls, at the operational level.

The second line of defence concerns those responsible for risk oversight and risk guidance in the firm. For example: risk management function, compliance, legal and finance, but also health and safety, IT security and HR functions. As well as monitoring reports, they are responsible for risk policies and risk processes and controls.

The third line of defence is independent assurance to the board and senior management of the effectiveness of risk management processes. That assurance is the responsibility of the internal and external auditors and other external providers.

Finally, all three levels report through to the board and are all responsible to it, so that the fourth line of defence, in a sense, is the board.

2.2. The board

The board is responsible for the good governance of the organisation and ensuring that there is proper oversight over senior management. It sets the organisation’s strategy and objectives, which form the context within which risk is managed. It also ensures the firm’s corporate values are established.

Specifically in relation to operational risk, its key responsibilities are to:

- approve and periodically review the firm’s framework for managing operational risk, including:
  - satisfying itself that appropriate systems are in place to identify, evaluate and manage the significant risks faced by the firm, and
  - ensuring that staff throughout the organisation are clear as to their own roles and responsibilities,
- provide senior management with clear principles underlying the framework,
- approve the policies developed by senior management or, if appropriate, the firm’s Risk Committee, and set the risk appetites for the various operational risks,
- receive reports on operational risk exposure, including against risk appetites, as part of its oversight function, so that it can ensure appropriate action is taken.
• ensure that the operational risk framework and the processes within it are audited effectively by independent, appropriately trained and competent staff.

2.3. Risk oversight

2.3.1. The risk management function

Given the importance of risk management in any organisation, the risk management function should have a commensurate authority and stature. That will result in issues it wishes to raise being given appropriate attention by the board, senior executives, business lines and other functions.

The risk management and analysis function does not directly manage risk. Business line executives and managers do that and are clearly responsible for the risks they accept. The risk management function provides oversight of the business line’s risk activities and facilitates effective risk management throughout the firm, for which responsibility it is ultimately answerable to the board.

Its core responsibilities are to:

• Identify, assess and analyse key risks,
• Monitor risk exposures against agreed risk appetites,
• Ensure that risks are appropriately controlled and mitigated,
• Ensure that risk processes and policies are being adhered to,
• Report to the appropriate authorities on issues raised by the risk assessment process and make recommendations on those and other risk matters,
• Ensure appropriate risk behaviours are being demonstrated and facilitate training and awareness.

Since risk assessment should form part of all business decisions, the risk management function should be involved in strategy-making. It may also have the primary responsibility for assessing, and providing recommendations to the board on, the allocation of risk-based capital.

It should be independent when it comes to decisions on risk exposures. This is especially true for financial institutions where for risk types such as credit, market or similar risks, where the risk function may have a control function and a delegated risk authority and so should be independent of the front office or marketing activities. Risk management must be able to challenge, and where appropriate veto, decisions freely and be independent of the operating functions it reviews.

However, it should not be isolated from the business lines, geographically or otherwise so that it is unable to understand the business or the information it receives. It needs to interact freely with the business lines and other functions so that it can obtain or access the information it needs to fulfil its responsibilities. Too much independence may mean that it becomes divorced from the business which it is overseeing. In the case of operational risk, however, the practicalities of independence are not so clear-cut, as is discussed below (see 2.3.2. Operational risk management function).

2.3.2. The operational risk management function

2.3.2.1 Role and responsibilities

The operational risk function:

• provides the framework, infrastructure, tools and methodology to allow key decision-makers to manage operational risk as part of their overall portfolio of risks, in conformity with cost-benefit analysis, within the risk appetites agreed by the board,
• identifies, assesses and monitors key operational risk exposures and the information used to make those assessments, including event causal analysis, risk and control assessment, and risk indicators,
2.3.2.2. Operational risk control and mitigation

Operational risk management involves implementing and assessing the design and performance of controls, whether at the strategic, process or activity levels of the organisation.

Operational risk mitigation also involves activities such as business continuity planning, outsourcing, IT security and insurance, as well as actions taken to minimise the risk of the firm being subject to criminal activity. In many firms, these activities may be managed by separate departments. Given their importance in mitigating operational risk, it is beneficial for them to report to the operational risk function or, failing that, at least to work closely with that function so that operational risks are managed and mitigated appropriately and that operational risk is managed in a coherent way across the firm.

2.3.2.3. Independence

A debate in relation to the operational risk function concerns where it sits in the organisation and, in particular, whether it should be centralised or whether it should be decentralised and embedded in business lines. Establishing an operational risk management framework across a firm demands a central person and team driving the activity. That may be the CRO or CFO, or it may be the responsibility of a dedicated operational risk management function.

Once the framework has been established, a central function may be retained, reporting to the CRO, with operational risk managers being situated within business units. Here they will report on operational risk exposure, as well as acting in an advisory or consulting role for the business.

Another reason why operational risk may not be as ‘independent’ as other risk functions is that, unlike risks such as credit or market risk, where the risk function operates as a control function, at the apex of a hierarchy of authorities, operational risk is something to be dealt with on a day to day basis at an operational level. It is not always a risk which is proactively sought, but one to be actively managed whenever or wherever it appears. For this reason, once the discipline is established, operational risk managers tend to be appointed within business units, with a small central team reviewing policy and collating reports for the board.

However, the function nevertheless remains one of oversight, part of the second line of defence, and it is important that it is independent enough to be free to escalate reports of risks which exceed risk appetite to an appropriate independent authority such as the CRO. This will be in the expectation that decisions will be taken either to accept the exposure or to take action to bring it back within agreed risk appetite. Operational risk managers should not be so much part of a business unit that their independence for reporting losses or control failures is compromised.

2.3.3. Other risk oversight functions

As was shown in the diagram in 2.1, The three lines of defence, a number of functions have risk oversight roles. They may include finance, treasury, regulatory compliance, health and safety, IT security and human resources.

Of these, the risks of failure to comply with regulatory requirements, including health and safety, or the risks arising from people, are significant sources of operational risk. That is especially true of the human resources (HR) function. HR is often responsible for policy and its implementation relating to such key risk mitigation as selection, training, appraisals and remuneration. As such it is important...
that the risk function, and especially the operational risk function, maintains close relations with HR and works with it to identify good data and indicators which will highlight increasing people risk exposure, either in the firm as a whole or in individual departments or business units.

### 2.4. Independent assurance

Independent assurance is provided to the board, senior management and external stakeholders, such as regulators and investors, by internal audit (assuming there is such a function) and/or the external auditors.

Internal audit must be independent and should report, other than for pay and rations, to whoever is most appropriate, e.g. the chairman of the board audit committee, the senior independent non-executive director or the non-executive chairman. To fulfil its functions properly, it must be truly independent.

Internal audit provides assurance on:
- The risk governance and risk management processes from Board level down,
- The management and oversight process for risks, including the effectiveness of controls,
- The accuracy and reliability of the components of the risk assessment and reporting process.

External audit must also remain independent. Its role is to provide its opinion on the financial statements.

In some firms, compliance or internal audit report to the chief risk officer and form part(s) of an overarching risk function. Given audit’s responsibility to provide independent assurance, best practice demands that it should not report to the risk function, although it may, of course, report to the CRO (or others in the C-suite) for ‘pay and rations’. Where internal audit is involved in the risk management process, its independence will be compromised. Audit cannot provide independent assurance of what it has been a party to deciding.

### 3. Operational risk policy

The board should approve an operational risk policy which, typically, will cover the following:

- **Purpose and scope of policy.**
  
  The key component is to set overall risk objectives for the firm which will then cascade down to form objectives for each level – division, business unit, and employee.

- **Definitions**
  
  These will include definitions of the different risk groups, as agreed by the firm, e.g. credit, insurance/underwriting, market, liquidity, operational, and guidance as to how ‘boundary’ issues will be dealt with. When a credit loss is reported, will it be treated as such or will it be analysed to identify which part of it was purely down to poor credit risk management and which part was down to, say, operational risk, perhaps in the form of a failure to take collateral properly. Will the resultant loss be split, or will it be recorded as a credit loss and the operational risk element merely ‘noted’?

  This is also the section for other definitions which will help to establish a common risk language throughout the firm.

- **Operational risk structure and responsibilities** – see 4. Risk roles and responsibilities below.

- **Operational risk management process**
  
  This section will establish:
  - how the firm assesses its risks,
- the core elements of its risk management framework; how it will identify, measure, manage and report risks
- the principal sources of risk
- how deviations from policy will be authorised.

• Operational risk appetite and risk tolerance – see IOR practice guidance on risk appetite

• Ethical and behavioural guidelines. Since operational risk is very much concerned with people risk management and culture, this section will identify core values and acceptable behaviours, which are consistent with board strategy.

4. Risk roles and responsibilities

4.1. The chief risk officer (CRO)

Just as the risk management function should have authority and stature within the organisation, so the CRO should have similar stature and authority and the resources to fulfil their responsibilities. The CRO should also have direct access, whenever required, to the board and to the chairman of the risk committee, if there is one.

The role of the CRO, or whoever is responsible for risk at director level, is to:

• provide risk leadership, vision and direction,
• develop and review risk management policies,
• establish the risk management framework across the firm, including the various metrics, indicators and other data which will provide a basis for risk assessment, and
• develop a supporting infrastructure to ensure that risk policies are being implemented, to enable challenge to risk exposures and decisions and to provide appropriate reports on risk exposure against agreed risk appetites.

As such, a number of oversight functions, such as compliance, risk, insurance purchase, legal and the company secretary may report to the CRO.

Ultimate accountability for risk leadership and management, the first bullet, rests with the board. However, the CRO is its embodiment and has responsibility to ensure its implementation.

The CRO may be a full board director. If not, it is arguable whether the CRO should report to the CEO or CFO. Given the centrality of risk to business decisions, reporting to the CEO would seem appropriate but, since failures of risk management will almost all result in financial loss, there is a logic to reporting to the CFO. The important thing is to ensure that the CRO and risk function, especially if they have a control or authority function, should be independent of the business lines and sales functions. The Basel Committee’s consultation paper on corporate governance makes clear that senior executives, such as the COO or CFO, should not also double up as CRO or equivalent.

The Walker report, which was instituted by the UK government following the financial crisis, and the Basel Committee paper on corporate governance both recommend that the CRO should not be removed without approval of the board. The Basel Committee paper goes on to recommend that the remuneration of the CRO and risk management staff should not compromise their independence and be based principally on the achievement of objectives rather than ‘being substantially tied to business line revenue’.

4.2. Operational risk roles and responsibilities

Where there is one, the head of operational risk will be responsible for implementing the activities identified above (2.3.2. The operational risk management function).
However, unlike other types of risk, operational risk involves, and so becomes the responsibility of, every member of staff. For an operational risk culture to be implemented effectively, all staff must be clear about their roles as part of the risk management process and have a clear understanding of their responsibilities for operational risk. That will happen if there is clarity as regards a firm’s objectives and of its risk appetite and approach to risk.

Clarity of reporting lines and the responsibilities of senior management will ensure that ambiguities are avoided and risk reports are seen and acted upon by those responsible.

4.3. Committees

4.3.1. Audit committee

The Audit Committee needs to be truly independent, so that it can fulfil its investigative work on behalf of the board, and so its members will be the independent non-executive directors. All financial services firms and public companies will have an audit committee, a sub-committee of the board. This forms part of the codes of corporate governance in many countries.\(^9\)

The audit committee’s principal responsibilities are to:

- ensure that the firm’s financial reporting and controls are appropriate and effective;
- appoint the external auditors and ensure that the quality of their work is in accordance with the terms of their engagement; and
- oversee the work of the internal auditor.

However, according to the UK’s Combined Code, and especially in the absence of a formal risk committee, the audit committee has an important role in relation to risk management by satisfying itself that the firm’s processes for risk assessment and risk control are appropriate and being implemented effectively.

4.3.2. Risk committee

The increasing responsibility of boards for risk management means that a significant part of the board’s oversight of risk falls to a specially appointed sub-committee of the board, the risk committee. It is important to recognise that it is the board’s risk committee, and not a meeting of executives apart from the board. Its membership may comprise executives but, because its primary responsibility is to fulfil the board’s risk oversight responsibilities, it should be chaired by an independent non-executive director and have a majority of non-executive directors as members.\(^10\) It should oversee and provide advice to the board on all risk types and not just those which do not have their own specialist committees.

The advice it provides to the board should cover:

- current risk exposure and future risk strategy, including strategy for capital and liquidity management,
- risk appetite, tolerance and related strategy,
- reputation risk management,

and may also cover advice on the risk aspects and due diligence in respect of strategic transactions. It should also advise the board on the extent to which the risk culture is embedded in the firm.

4.3.3. Operational Risk Committee

The Operational Risk Committee, chaired by the head of operational risk, provides a focus for implementing the operational risk framework consistently throughout the firm and for reviewing reports from the various business units and divisions and taking action where appropriate.
4.4. **Operational risk reporting**

Effective reporting of risk exposure up and down the firm, including operational risk exposure, is a key element of risk governance. Reporting is described in more detail in a number of the other Sound Practice Papers.

5. **External stakeholders**

5.1. **Meeting regulatory expectations**

So far as financial services firms in the UK are concerned, the FSA clearly states that all regulated firms must have:

‘robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, and internal control mechanisms, including sound administrative and accounting procedures and effective control and safeguard arrangements for information processing systems.’ (FSA Handbook, SYSC 4.1.1)

Other regulators have similar requirements as regards risk management.

From a regulatory point of view, the key point is that a firm must be able to evidence that it fulfils the requirements, both on paper, i.e. unless it is documented it does not exist, and through the ‘use test’. (see 1.4 above)

5.2. **Meeting rating agencies’ expectations**

Rating agencies have always claimed that the quality of management and, by extension, the quality of risk management in a firm, has always formed an integral part of their overall assessment of a firm. However, in recent years, they have begun to formalise their assessment of the quality of a firm’s overall risk management and operational risk management in particular. At present Standard & Poor’s evaluates on a 4 point scale – excellent, strong, adequate (subdivided into tending to strong and tending to weak) and weak.

5.3. **Investors**

Good risk management should mean that the interests of the business are allied to those of investors, who require profits (and therefore dividends) and acceptably low volatility in performance.

Providing information to investors on a firm’s risks and how it manages them is not just a compliance requirement, but something which should form part of the ongoing communication with investors to assure (or reassure) them that their investment is being protected.

Good governance should also mean that the communication is a dialogue. Mechanisms should be in place to enable investors to raise issues and concerns with the company they have invested in, and to be able to suggest sustainable improvement in the performance of the company.

6. **Business benefits of good governance**

Good governance from the board down, in which everybody in the firm is clear about their roles and responsibilities for operational risk, is essential to good operational risk management. Good governance therefore brings with it the principal benefit of risk management which, essentially, is that effective risk management and reporting will lead to informed decision making.

The principal activities of operational risk management described in this paper all produce direct benefits to the business. For example, analysis of operational risk exposures and events leads to fewer losses; effective assessment of controls and scenario planning lead to optimisation of resources and reduced costs. Good people management, an essential part of operational risk management, leads to
improved risk management and increased staff retention. Intelligent operational risk management also helps to instil a culture of continuous improvement and business optimisation.

All of this is possible only if it operates within a sound governance framework and a risk culture which is embedded throughout the organisation and involves everybody in it.

---


2 For the purpose of this paper, the term ‘board’ is used to describe the principal decision-making body of an organisation.


6 Basel Committee (2010), para 69.

7 Walker (2009), Recommendation 24; Basel (2010), para 72.


9 See the European Corporate Governance Institute website for comprehensive details of arrangements in all countries, www.ecgi.org.

10 Walker (2009) recommends that the risk committee should have a majority of non-executive directors.