RISK MANAGEMENT TOPIC PAPER No. 2

EMBEDDING RISK MANAGEMENT – SOME TIPS AND TACTICS

By Gill Bolton and Sarah Blackburn

INTRODUCTION

What do we mean by embedding risk management?

Risk has several wide-ranging definitions but is best understood as *'the chance of something happening that will have an impact on objectives. It is measured in terms of consequence and likelihood'* (Australia and New Zealand Standard on Risk Management).

Risk management is defined as *'…the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects'* (Australian Standard 4360).

Risk management has become a prominent area for management attention because of :

a) the corporate governance requirements affecting companies listed on the London Stock Exchange (LSE) as well as a range of other organisations;
b) the benefits that led many of those companies to implement a more formal approach to risk before it was a requirement; and
c) the benefits that other organisations (public sector bodies, private companies, unlisted companies) believe will accrue from managing their risks more proactively.

LSE-listed companies and other organisations are now required to take the actions detailed below. Anything demanded by regulation can degenerate into a half-hearted, just-enough-to-get-by, ticking-the-boxes exercise, so the Stock Exchange regulations stress the actions required as much as the public reporting element:

- The Board must implement policies on **risk** and control; i.e. the whole process of risk management must be driven from the top of the organisation through well-structured and clearly thought through strategies and policies.
- Internal control must be **risk-based;** i.e. it must be in place to manage the significant risks in the organisation. For these purposes, 'internal control' covers all aspects of risk management.
- The Board must report publicly that there is an ongoing process for identifying, evaluating and managing significant risks which it regularly reviews; i.e. the Board must be able to make regular statements on how well the significant risks in the organisation are being managed.

The aim of embedding risk management is to ensure that it is not seen as an additional set of layers and processes; rather it becomes part of the 'way we do business round here'. Many organisations have already been through the early stages of risk management implementation; i.e. they have developed processes for risk identification, risk assessment, monitoring and reporting. However, many are still struggling with the whole concept of 'embedding' risk management into the culture of their organisation.

EDITOR'S FOREWORD

This second paper on risk management is published as part of a short series sponsored by the Housing Corporation. The aim is to encourage development of best practice among housing associations. The papers follow on from previous publications that sought to introduce and develop effective risk management. In particular the publication in 2000 of Effective Risk and Business Management was designed to identify the elements of a risk management framework for housing associations.

The views expressed in these topic papers are those of their authors and not the Housing Corporation. It is hoped that they will stimulate discussion and the development of best practice in specific areas of risk management. Comments on the papers and suggestions for further topics would be welcomed. Roger Lustig

THE HOUSING CORPORATION

This paper aims to set out some ideas on how housing association might embed risk management. It also includes case studies showing how other organisations are tackling this issue. Some of the language of risk management is technical. A glossary is given in *Appendix 2*.

What are the benefits of embedded risk management?

The benefits are widely recognised and include:

- reduction in management time spent 'fire-fighting';
- fewer sudden shocks and unwelcome surprises;
- more focus internally on doing the right things in the right way;

and therefore

- more likelihood of achieving business objectives;
- more likelihood of implementing change initiatives;
- strategy being appraised more effectively, leading to calculated risk taking;

hence

- more confidence in moving into new areas;
- overall cost of risk is reduced.

What are the key success factors in embedding risk management?

As your organisation starts to implement its risk management strategy, or to enhance what is already in place, it is more likely to succeed if risk management is:

- supported by the Board, publicly and privately, and communicated to everyone in the organisation;
- sponsored by the senior management team and supported by experts in risk areas;
- business-led – in the ownership of management, rather than departments such as insurance, risk management or internal audit;
- linked to clear strategic objectives at the top level and to clear operational objectives throughout the organisation;
- a priority for everyone – because no matter what their job, everyone has some responsibility for risk management – and measured as a personal objective;
- built on business processes already in place such as strategy reviews, planning, budgeting, insurance reviews, project appraisal and performance appraisal;
- expressed in a common language accessible to all members of the organisation *see Appendix 2*;
- given quality time by key management, including reports to the Board;
- kept as simple and as concise as possible – risk management is not rocket science.

HOW DO WE EMBED RISK MANAGEMENT INTO OUR RSL?

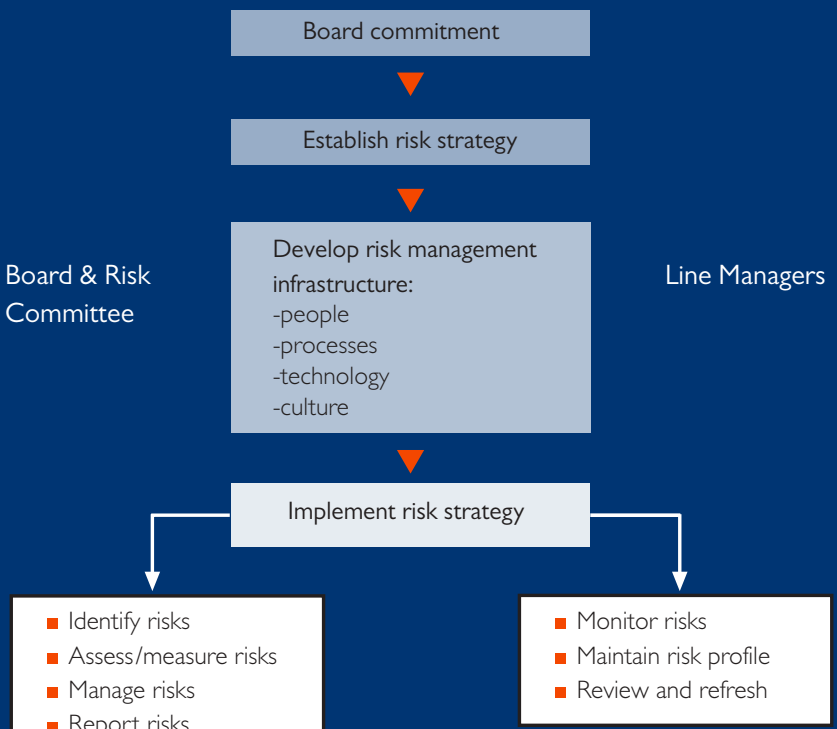
There is no single right way. What you choose to do and how will depend on a range of factors including:

- your risk management aspirations – i.e. why you are implementing risk management – is it merely for regulatory reasons or because you believe it is an essential part of good management?
- what you already have in place in terms of structures, processes and procedures – no organisation is likely to be starting from scratch in embedding risk management;
- your organisational culture – some approaches suit some organisations better than others.

The framework for implementing risk management shown in *Diagram 1* has been developed from leading practices in a wide range of organisations.

Each of the elements of the framework is described in more detail below. Following an approach as outlined here will help to embed the whole philosophy of risk management into your organisation.

Diagram 1
Framework for implementing risk management



Establish risk strategy

In the same way that organisations need a business strategy, business objectives and a business plan, the same is true for risk management. In its simplest form the risk strategy will focus on why you want to implement risk management, who is responsible and accountable for it, and the processes by which it will be embedded. This is illustrated by the approach adopted in the NHS set out at *insert 1*.

1 ***The NHS Risk Management Standard***
This standard ensures that all NHS organisations have the basic building blocks in place for managing risk by developing and implementing a comprehensive risk management system. The standard defines a set of generic principles for establishing risk management in NHS organisations. These principles deal with the management of risk from board responsibility to developing and communicating a risk policy, identifying accountability and implementation throughout the organisation. In this way risk is integrated into the organisation's philosophy, practices and business plans, rather than being viewed or practised as a separate programme. When this is achieved, risk management becomes the business of everyone in the organisation.

Develop risk management infrastructure

Risk management will become embedded in your organisation only if you have the right people, processes, technology and culture. You may need to build this infrastructure from scratch or, more likely, build on existing processes and structures. In the example in *insert 2* existing elements such as Board meetings, Audit Committee, and budget and strategy reviews were supplemented by a new Risk Committee and such processes as risk assessment and risk reporting.

2 *Roles and Responsibilities in Risk Management at Exel plc*

The Board
Agrees the risk management framework. Sets risk appetite. Directs risk strategy. Receives reports and demands action.

Operational Management
Owns the management of risks: assesses risks, reviews them twice yearly, confirms responsibilities.

Functional management (e.g. HR, Finance, IT, Property)
Provides technical support to manage risks. Responsible to line management.

Insurance and Risk Management department
Provides support for claims-related risks. Manages risk transfer to insurers.

The Risk Committee
Co-ordinates efforts of the above. Learns from risk occurrences and reports to the Board.

The Audit Committee
Satisfies itself of risk management process and reports to the Board.

Internal Audit department
Provides assurance of content to Risk Committee, and of process to Audit Committee.

Implement risk strategy

This stage involves risk identification, evaluation, management (tolerate, terminate, treat or transfer), monitoring and reporting; namely the key elements of a sound risk management process which are described in other guidance papers from the Housing Corporation.

KEEPING THE PROCESS ALIVE

Not being satisfied

Invariably, once all the structures and processes have been put in place, people tend to sit back and say: "we've arrived". But this is only the beginning, as risk needs continuous management.

Here are some processes and structures that will keep risk management alive and sustainable:

- Risks and their management should form an inherent part of any discussion at strategy reviews, budget approval meetings, performance reviews, project planning and review meetings. Consequently any reports to the Board on these topics will include an analysis of risk.
- The risk profiles should be regularly updated by the management responsible and accountable for managing them.
- Events and indications that risks are not sufficiently controlled need to be discussed in a constructive environment and the lessons learned shared within the organisation.
- Evidence of weaknesses in the control of risks must be addressed promptly.
- Risks and their management should be reviewed at the different levels of the operational hierarchy (regional and area meetings, divisional boards etc) and where common risks exist across the organisation they should be compared to share understanding and treatment.
- The Board should always assess the financial and non-financial risks when taking decisions.
- Responsibility and accountability for risks should be included in each manager's annual objectives.
- Insurance managers, risk managers and internal auditors should be asked to advise and check on the quality of risk management.

A chief executive was asked: "Are we risk free yet?" "I hope not," he replied, "because if we are not taking risks then we are not creating value."
The more that senior level people can 'live the vision' of risk management, the better the chance that it will become embedded. For an example of this, see *Insert 3*.

3 *Lex Service PLC – Demanding Directors*
"Whenever something happens, goes wrong, the Group Finance Director (he's the one responsible for the risk management process) always asks the managers: 'Did you have this in your risk assessment and risk management plan?'"

Improving Processes and Controls

The whole risk management process needs review at least once a year to ensure that:

- it still covers all the most important business risks;
- it retains management acceptance and buy-in at all levels; and
- people are refining their understanding of it, but without getting the process cluttered by excess detail.

Some have argued that a discrete risk assessment process should be unnecessary as risk management becomes embedded in strategy, capital expenditure and budget reviews, and in performance and project reviews. This may not be feasible in practice: processes without a tangible existence in an organisation soon get forgotten among the hundreds of other claims on management time.

As organisations become more mature in their risk management, they tend to shift from considering only hazards and interruptions in routine operations to identifying more sophisticated threats and opportunities for their business. Leading organisations constantly scan the horizons for:

- shifts in market and stakeholder expectations;
- forthcoming regulatory changes;
- models of best practice.

They continuously check:

- the robustness and completeness of the risk profile;
- whether risk treatment actions are reducing exposures;
- whether lessons from experience e.g. post implementation reviews of major projects are integrated into risk profiles, policies and guidelines;
- whether assurance is effective.

ORGANISATIONAL CULTURE

How an organisation implements and embeds risk management will depend on a wide range of factors, but culture is a key issue:

- Open or closed culture?
- Commitment to risk management
- Attitude to internal controls – things that constrain managers or things that can help the housing association achieve its business objectives?
- Governance – recognition of the expectations of the wider stakeholder community.

A culture of risk management comes from the chief executive, the senior management team and the Board. It stems from their actions, which will influence the way people behave towards risk throughout the organisation.

Some ways of embedding risk management in the culture include:

- aligning operational and individual goals with strategic goals;
- explicitly including risk management roles and responsibilities in job descriptions;
- establishing reward and recognition systems that acknowledge risk taking and problem prevention in practice;
- developing performance measures for effective risk management, ensuring that they are appropriate and sufficiently focused on future goals, and that they act as an early warning system;
- balancing individual responsibility with tolerating individual mistakes and learning from them for the benefit of the organisation as a whole;
- developing a common language for risk management and ensuring it is communicated effectively across the whole organisation (*see Appendix 2*);
- publicising success stories across the organisation, and also rewarding management for sharing lessons learnt from things that did not go according to plan.

CONCLUSION

This paper has demonstrated some of the elements of successfully embedding risk management into your organisation's culture. However, one single approach will not suit all situations, so it is essential to cherry-pick the elements that will work best in your own structure and culture.

APPENDIX 1
SOME FURTHER CASE STUDIES

These case studies show several of the issues highlighted in this paper.

CASE STUDY 1

Using a range of techniques to provide the necessary assurance on risk management and internal control

This large housing association clearly takes internal control very seriously. As well as having an internal audit function comprising three people, they also operate a robust self-audit programme.

Responsibility for gaining assurance about the operation of internal controls – and hence the management of significant risks – falls rightly on the shoulders of management and their staff rather than Internal Audit. This culture has been built up in the organisation over several years through education and by setting accountabilities and responsibilities through clear performance objectives.

The role of Internal Audit is to give independent assurance, while managers are responsible for gaining their own assurance through the 'self-audit' programme which focuses on compliance and quality-related issues. Within this programme managers and their staff must, every quarter, review the operation of the key controls in their area of business and report on them to the chief executive.

CASE STUDY 2

Making risk management a clear and robust management responsibility

This medium-sized housing asscociation, based in the Midlands, has appointed a part-time risk manager who is responsible for implementing risk management. His main role is to run workshops for all levels of staff and, based on what they say, to provide input to the overall risk management strategy.

Other key responsibilities include training and education of line management and their staff in the fundamentals of risk management as it affects their roles and responsibilities.

He is also responsible for ensuring that Internal Audit focuses on the issues that matter to the organisation, so that the risk profile affects the work of Internal Audit. However, Internal Audit is also encouraged to carry out its own audit needs assessment and not simply to focus on the organisational risk profile.

CASE STUDY 3

Risk management as part of sound management practice

This FTSE 100 plc implemented many risk management philosophies before the Turnbull requirements came into force.

At the heart of its risk management is the philosophy that managers and their staff are both responsible and accountable for risk management. As a result, the company set a strategy and clear policies for risk management but has allowed each area of the business to adopt approaches that suit them.

The company's risk management function has provided training and education for the different businesses and has also played a key role in reviewing and monitoring progress against the plan. However, it is clear to all that the purpose of the risk management group is to advise, educate and monitor progress – not to manage risks actively.

APPENDIX II
A COMMON RISK LANGUAGE

RISK
The threat that an event or action will adversely affect an organisation's ability to maximise stakeholder value and to achieve its business objectives. Risk arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.

External risks
External risks arise when there are external forces that could either put an organisation out of business or significantly change the assumptions that drive its overall objectives and strategies.

Strategic risks
Those risks which affect the organisation's ability to meet its strategy or which derive from the strategy.

Operational risks
The risks associated with all the ongoing day-to-day management of the business.

This will also include the risks around the business processes employed to meet the business objectives.

Information risks
Risks arising from the organisation making decisions, based on information which is in some way flawed.

People risks
Risks arising from the fact that people make both deliberate and inadvertent errors in carrying out their day-to-day tasks.

Financial risks
Risks related specifically to the financial aspects of the business and the underlying financial processes.

RISK MANAGEMENT
A logical and systematic method of identifying, analysing, assessing, treating, monitoring and communicating risks in a way that will enable organisations to minimise losses and maximise opportunities.

It consists of steps which, when undertaken in sequence, enable continual improvement in decision making.

RISK TREATMENT
The selection and implementation of appropriate options for dealing with risks. These may include:

- risk acceptance;
- risk transfer;
- risk elimination;
- risk increase;
- risk reduction;
- risk avoidance.

Risk acceptance
An informed decision to accept the likelihood and consequences of a particular risk.

Risk transfer
Shifting the responsibility or burden for loss to another party; for example, through insurance.

Risk elimination
Finding some means to eliminate a risk entirely because if it happened the consequences would be unacceptable.

Risk increase
Deciding to increase a particular risk, i.e. to reduce the risk management activities around it. This may be because the cost of managing the risk outweighs its possible impact, or simply that the risk currently being accepted is less than the determined risk tolerance of the organisation.

APPENDIX II
A COMMON RISK LANGUAGE (Cont'd)

Risk reduction
A selective application of appropriate techniques and management principles to reduce either the likelihood of occurrence or the impact, or both.

Risk avoidance
An informed decision not to become involved in a risk situation or to cease activities in a particular area because the risk is too high.

Residual risk
The remaining level of risk after risk treatment measures have been taken. If it falls within the organisation's risk tolerance, then residual risk is acceptable; if it falls outside, then other actions may be needed.

SUMMARY
Starting risk management and developing your risk profiles and risk registers is a relatively easy part of the overall risk management process. The key challenge is around embedding risk and control into the culture of your organisation. This paper sets out some of the fundamental elements to achieve this as well as providing some useful case studies.

The Authors

Gill Bolton is a freelance consultant specialising in internal audit and risk management. She has worked with a wide range of organisations including the Housing Corporation and a number of housing asscociations. Her work also includes a wide range of training courses which she runs to update people on what is happening with respect to best practice in risk management. She is running a series of courses with the National Housing Federation in 2002 to introduce board members to the new internal controls assurance requirements.

Sarah Blackburn is Head of Global Audit and Assurance at Exel plc. After her first taste of internal audit with Sainsbury's, Sarah headed up internal audit in Argos plc, Kingfisher plc and then audit and risk management at Lex Service PLC. She has specialised in re-establishing internal audit departments, bringing a risk-based approach and client-centred working. Sarah speaks regularly at conferences on risk management, corporate governance, and behavioural competence. She has written three books on internal auditing and risk management.

THE HOUSING CORPORATION

The Housing Corporation
Regulation Division
149 Tottenham Court Road
London W1T 7BN

Contact: Tim Jackson
tim.jackson@housingcorp.gsx.gov.uk

May 2002
©Housing Corporation

PLAIN LANGUAGE COMMISSION
Clear English Standard
WINNING DOCUMENT