

AFFORDABLE HOMES STRONG COMMUNITIES

GOOD PRACTICE GUIDANCE

---

# Managing risk for smaller housing associations

---

March 2006



# Foreword

Risk management is central to the effective running of an organisation, and best practice risk management is simply good management.

A sample survey of smaller housing associations conducted as part of this project demonstrated that much progress has been made in risk management. However, more remains to be done.

Risk registers are a common problem in smaller associations. Often they are too long and do not focus on the key risks. Boards cannot give adequate time and attention to all the possible risks and should, instead, concentrate on the most significant areas. In practical terms, this means restricting board attention to high risks, of which there should be a manageable number. Management should consider lower-level risks in detail.

Smaller associations have limited resources and may not be able to implement ideal levels of control. The situation needs open recognition and to be dealt with transparently in order to manage the increased level of risk, particularly with regard to possible weakness in segregating duties. It is also sensible for the board to review arrangements periodically.

When resources are scarce, departures from best practice risk management should not compromise the rigorous identification and assessment of risks. Cutting back in these areas has more wide-ranging consequences than openly acknowledged deficiencies in control.

Implementing an effective assurance system, including monitoring the control systems, will help prevent nasty surprises and improve the overall effectiveness of management. Management assurance to the board on the effectiveness of controls needs to be embedded into the standard management reporting cycle. Small associations need to be imaginative in considering what information sources and activities can provide assurance to management and the board.

**Clare Miller**

Director of Regulation

# Contents

A systematic approach pays dividends	2
Risk practices in smaller associations	6
Roles and responsibilities	10
Risk identification and assessment	15
Responding to risk	25
Selective bibliography	35

# A systematic approach pays dividends

## Aim of this publication

In recent years, buckets of ink have been spilt on risk management and it is a legitimate question to ask what another publication might add.

The purpose of this publication is to answer the need of those busy executives, managers and board members of smaller housing associations who, whilst taking their responsibilities extremely seriously, have to cope with the realities of day to day work issues as well as a deluge of documents and other information. This publication aims to summarise but not over-simplify the vital topic of risk that affects all people working in organisations. The booklet is intended as a way to help them through the maze to worthwhile action.

In some senses, much of what follows is not rocket science and may well be quite familiar. The idea is to put some identifiable structure and process around many long-established practices and to introduce some new ideas. This actually contributes much to the effort because following a structured and systematic approach generally pays dividends.

## Smaller associations

Smaller organisations generally have less managerial time and other resources to devote to formal risk management. This requires careful assessment of the elements that are absolutely essential for good practice and to comply with regulations, and those that fall more into the ‘nice to have’ category.

As explained in the Risk identification and assessment chapter, small organisations have particular vulnerabilities and need a tailored approach. With limited resource it is important to use that resource cost effectively. This quite simply means focusing on the areas of highest risk.

Whilst this may seem obvious, it has an important implication. Namely there should be no compromise on the quality of risk identification and assessment. The risk areas must be clearly established to ensure that the main effort is directed to the riskiest areas. If compromises must be made in the light of reality, these must be in the full knowledge of the potential implications (i.e. the risks) and be completely open and transparent. For example, in an ideal world it is often desirable for one person to check

the work of another. If this is impractical it must be openly acknowledged as an increase in risk which it has been decided to accept. This approach, if carried out in the right way, may help address some of the difficult internal control issues smaller associations have wrestled with for some time.

The Housing Corporation's expectations on risk management are set out in Paragraph 2.8 of the Regulatory Code:

Housing associations must operate a framework that effectively identifies and manages risks:

- 2.8.1 Identifying all major risks that might prevent them from achieving their objectives;
- 2.8.2 with the necessary arrangements to manage risks and mitigate their effects.

Regulatory Guidance to Paragraph 2.8 of the Regulatory Code says:

- a The association's risk management framework highlights key risks and how they are to be managed;
- b The governing body regularly reviews activities and policies and all new business decisions and there is a

clear case for the proposed or existing direction of the association;

c Approved terms of reference for the governing body and other committees and delegated authorities for staff are in place;

d There are internal control systems. Their effectiveness is regularly reviewed by the governing body and reported in the annual report.

The emphasis in 2.8.1 and 2.8.2 is on identifying major risks and their management. It is also a major theme of this publication. What is important is to identify the largest risks and ensure vigilance in applying controls to manage those risks.

## Is the effort worth it?

A question often asked is, “What’s the point of all this new paperwork, risk registers, workshops and policies; we will continue to manage our risks as before and isn’t the only difference a lot more unnecessary work?”

In the main best practice risk management is nothing more or less than good management. The following areas are fundamental requisites:

- clarifying and recording what the key risks are;
- assessing and documenting the significance of the key risks; and
- evaluating the extent to which they are within tolerable limits.

People in positions of great trust in social housing must be able to account for their actions to boards, tenants, the regulator and the wider community.

This means required standards of probity and management are of necessity high. Lapses in control, if they occur, may have serious adverse consequences for people that are less able to bear them than others that are more fortunate. Therefore, the

need for high standards and also for a high degree of transparency and accountability is clear. And this in turn requires an appropriate level of risk management and documentation of how it works in practice.

In particular there must be ready answers to reasonable questions such as:

- How do you anticipate potential problems in achieving your plans?
- How do you ensure the ongoing viability of the association?
- What precautions do you take against the possibility of physical disasters in the properties you manage?
- How do you ensure you do not misspend money?
- How do you protect against fraud?

Risk management is used positively as a fundamental element in managing the achievement of planned business objectives. Good risk management starts with a consideration of business objectives and then considers the factors that may impede achieving them.

## Why document everything?

Much of the literature on risk places special emphasis on documentation. Simply doing things is not sufficient, there is also a requirement to set down in a written document what you have done and intend to do. The need for documentation is often questioned.

One of the key elements of good governance and management is audit trail. Not just of financial transactions but of all important decisions. It is often essential to understand how decisions were arrived at in the light of prevailing circumstances. These may well change after the decision is made. If things go wrong and questions are asked, documentation is also vital to ensure the right conclusions are drawn from the evidence. This is why emphasis is placed on documentation and the associated 'show me' test. For example, a risk policy formally adopted by the board with an appended risk and control register is far more convincing than a mere oral statement of what the procedures are.

# Risk practices in smaller associations

## The survey

A number of smaller associations (less than 1,000 units) were circulated with a questionnaire which was selectively followed up by an interview with the executives responsible for risk. The survey covered the following areas:

- responsibilities for collecting and receiving information on risk;
- the use of outside third parties as facilitators;
- a sample listing of the association's risks (the risk register).
- how probability/impact is assessed and how the risks are prioritised;
- periodic board and annual financial reporting on risk and sample reports; and
- details of the current risk management framework.

## Main things associations got right

The respondents to the survey generally followed at least the following good practices:

- most had a register of all the risks, though not all had assessed and prioritised them (see next section 'Common areas for improvement');
- the risk register had been reviewed and approved by the board by most of the associations; and
- some associations had risk policy documents.

## Common areas for improvement

Whilst most associations had, on the face of it, comprehensive risk registers, very few assessed the probability and impact of the risks. Of those that did, even fewer clearly prioritised the risks within the register. Many associations had long lists of 40 to 50 risks with little indication of how significant they were regarded. This makes it very difficult to ensure that appropriate focus is being given to the areas which most merit it.

A common mistake is to have too many risks listed on the register which makes it unwieldy and costly to keep up to date. Listing too many risks is counter-productive. It is essential to assess the probability and impact of the risks and prioritise them in order of significance. Many respondents to the survey did not list risks in order of significance and did not isolate the most major risks.

Not all the boards of the associations surveyed had carried out an annual review of risk and risk management.

Many of the documented risk-mitigating activities noted in risk registers were rather generic and too unspecific to be of help to the association. They seemed rather to be like quotes from text books on what might be expected rather than clear, specific descriptions of what is actually done. In addition, where actions to address issues were noted these were often incomplete, leaving out clear responsibilities for delivery of specific actions within a documented timescale.

## Some case studies

Good practice was identified as taking place in a number of the associations which responded to the survey.

### Case study 1: An association with 50% of its activities in general needs housing and 50% in supported housing

The approach to risk management is well developed and is taken seriously by senior management. The association has adopted a Risk Assessment and Internal Controls Policy which sets out the basis for risk management. This requires an annual review by the management committee of the risk map and also that the chief executive is to ensure that routine management reports confirm that internal controls and other risk management procedures are operating as intended. This latter requirement constitutes embedded internal controls monitoring and requires an appropriate infrastructure of reporting to implement.

The chief executive's report to the management committee on internal controls assurance has the risk map appended. The risk map is divided into three sections: external risks (where there is little power to prevent occurrence), internal risks

(generated from within the association) and internal/external bridging the two. Probabilities and impacts are assessed as high/moderate/low and for external risks alternative courses of action are documented, as well as consequences and current mitigation measures. For the other risks, the consequences and mitigation measures are set out.

### **Case study 2: An association with mixed housing activities covering general needs, special needs and shared ownership**

Whilst there is no formal risk policy, the chief executive reports annually to the board on internal control, appending the Risk Management Strategy which is essentially the risk map. The internal control report sets out overall internal control arrangements and notes any breakdowns in control or the absence of such breakdowns during the year. As part of the arrangements it is noted that the monthly management group meetings require formal consideration of risk management as an agenda item, including follow up of previously agreed risk mitigation actions. There is also formal consideration of the risks in any new initiatives requiring consideration of the risk implications of any organisational or

systems changes and the resources available to properly control the new activities.

The number of risks on the risk map reduced from 29 in 2003-04 to 13 in 2004-05, concentrating only on significant risks, giving good board focus on a manageable set of the most important risks.

The risk map sets out for each risk a 'score' which is categorised as: prevent/plan/control (indicating the type of mitigation action); control procedures in place; the lead officer; monitoring; and on-going actions. The clear allocation of management responsibility is an important plus point.

### **Case study 3: A provider of supported housing**

The association covers special needs almost exclusively in an ongoing risk management process and the plan is updated every six months. Risks are ranked according to an overall level, categorised as VHIGH, HIGH, MED and LOW.

There were 27 risks on the 2004-05 risk map compared to 44 on the 2003-04 risk map (called the Risk Plan). The risk map lists the risks in descending order of significance (highest first) and, interestingly, notes for

comparison the previous year's ranking of the risk. That way some basic trends can be noted in terms of risks deteriorating or becoming less significant. A separate priority risk report is prepared for the board containing only VHIGH and HIGH risks.

In addition to the level and ranking, the risk area is noted, classifying risks into one of ten discrete areas. Also, for each risk, current actions and progress in implementing actions as at the end of March is noted.

Being so involved in supported housing, the association also prepares a supporting people risk appraisal under the required headings.

Risk is an agenda item at monthly management meetings.

#### **Case study 4: An example of pooling resources**

Four housing co-ops in Leicester pool resources to approach risk in two ways, through the business planning process and through a specific risk mapping exercise. In 2005 an all-day event was held involving committee members of the four co-ops and staff of the agents. The risks faced and ways of mitigating them was part of the discussions which produced the draft

business plan for each co-op which was then written up and presented to a subsequent committee meeting

The chairs of the four co-ops met with the agency services manager and reviewed the risk map produced the previous year. A number of changes and additions were made.

The risk map includes a list of eight principles related to risk that the co-ops will comply with, there are then 12 categories of risk each identifying specific risks, impact, probability, mitigating factors/the controls in place and an overall measure of risk on a high/medium/low scale. The risk map is reviewed fully annually and once formally at the six-month stage by committee

The business planning day consisted of:

- an introduction to business planning;
- a focus on priority areas;
- a review of the existing business plan action plans and a range of other action plans;
- break-out sessions for each individual co-op to discuss its individual priorities; and
- an exercise pulling together all the priorities and objectives identified and recorded them onto a new business plan action matrix.

# Roles and responsibilities

It is important to understand the responsibilities of the different groups of individuals for the management of risk within an organisation.

## The board

The board carries ultimate responsibility for the success or failure of the association and for setting the strategic direction of the organisation. In addition the board is ultimately responsible for the system of internal control and managing risk including reviewing the effectiveness of internal control. It cannot devolve that responsibility to the executive (or senior management team).

The board does not manage the association on a day-to-day basis and delegates certain powers to the executive. This delegation of powers does not relieve the board itself of overall responsibility. The principal consideration is that all decisions involve a view on the acceptability of the assessed level of risk implied by the decision. Consequently, a balance needs to be struck between:

- too much delegation which gives rise to too little control over the executive and may result in an abrogation of responsibilities; and
- too little delegation prevents management from being properly able to exercise day-to-day control.

What is needed according to best practice governance principles is:

- appropriate delegation to the executive; and
- appropriate accountability by the executive to the board.

Put simply, this means that the board delegates the power to take decisions (but not all decisions) to the executive, which must account to the board for what they have done. The board's responsibilities require it to keep a careful eye on what the executive is doing, at a high, big-picture level.

In addition, there must be clarity about those decisions the board reserves to itself and those which it delegates to the executive. This may be set out in a Schedule of Decisions Reserved to the Board, as a companion document to the Delegated Authorities. These latter often provide for

all powers being delegated to the executive, other than those specifically reserved to the Board.

Housing Corporation Circular 25/01 'Internal controls assurance' requires the board to conduct an annual review of the effectiveness of the association's system of internal control.

## The audit committee

Where an association has an audit committee, the board will probably have delegated to it the task of carrying out the annual review of the association's risks and the internal control and risk management system, including ensuring there is adequate and appropriate regular reporting by management on the functioning of the internal control and risk management systems. Nevertheless, the ultimate responsibility for the system of internal control remains with the board. Additionally, the audit committee is likely to be given responsibility for reviewing the effectiveness of internal and external audit. The detailed responsibilities of the audit committee should be set out in its terms of reference and approved by the board. For a small association it might be regarded as

appropriate to operate a combined finance and audit committee.

## The executive

The executive, or senior management team, is accountable to the board within the terms of its delegated authorities for the day-to-day management of the association and, as such, for identifying, assessing and managing risks. This responsibility includes the design and implementation of the system of internal controls and regular reporting on its functioning to the audit committee or board. Whilst the executive may engage assistance in this task it cannot abrogate the responsibility.

Assistance in risk management may include internal and external audit. However, reliance on those functions for the fundamental operation of the internal control and other risk management systems is not appropriate and their role needs to be clarified in writing to ensure there is no possibility of confusion in this respect.

Circular 25/01 requires the chief executive or executive team to present the board (or audit committee) with an annual report on the effectiveness of the internal control system.

## Staff

Staff operate within the terms of their own job descriptions. All employees have some responsibility for internal control, in that all of them are accountable for achieving objectives. In order to embed risk management it is sensible to clarify within job descriptions the responsibility for identifying, assessing and managing risk. It is particularly important to clarify the risk decision making authority of the individual insofar as practical.

## Internal audit

Internal audit is essentially an independent function which reviews the operation of the association's internal control systems and other risk management processes and reports to the audit committee or the board.

Internal audit's basic role does not include designing, implementing or operating any of the association's controls or other business processes. It may not be relied upon as the primary risk management function. Neither may internal audit be relied upon as the embedded monitoring system for internal controls. Internal audit will only

review a specific area of internal control or risk management periodically, usually not more than once a year, yet important controls must be monitored on a much more continuous basis. Internal audit assessments of internal control gradually lose their relevance with the passage of time. Finally, it is not for the internal audit function to set out what should be the level of control to manage particular risks. The acceptability or otherwise of risk is the province of line management not internal audit.

The role of internal audit does include a review of management's own assessment of risks. Line managers who manage risks on a day-to-day basis and live with those risks can often benefit from the objective involvement of a third party such as internal audit, to ensure that risks are neither over-estimated or under-estimated.

In a sense, internal audit's job is done once it has reported appropriately. In other words, its role is to point out to line management, the executive and the board (depending on the level of risk concerned) the consequences in terms of potential risk of management's actions or inactions in managing the association's risks.

Once internal audit has reported its view of the risks the organisation runs it is up to the board and management to decide whether or not that risk is acceptable. However, if internal audit is asked for its advice on how to manage a risk it may provide that advice provided it is not seen as in any way mandatory on management or that internal audit is adopting an executive or operational role. In due course internal audit will follow up on the implementation of agreed action plans.

## Departure from the ideal

The description above is basically the ideal role of internal audit. However, in keeping with other aspects of the operation of a smaller association, resources may force a departure from the ideal. The approach to managing the additional risk created is the same as for any other risk. There must be open recognition of the situation and conscious adoption by the board and executive after a fair assessment of the potential problems.

In the final analysis, it is for the executive and the board to determine the role of internal audit, bearing in mind that its effectiveness as a check on the actions of

the executive and management depend crucially on its independence from them. For example, the independence of internal audit needs special consideration in the following situations:

- where the head of internal audit reports to a specific executive or manager (e.g. the finance director);
- where internal audit advises on the introduction of specific controls and assists in their design; and
- where internal audit is called upon to carry out specific line operations, such as managing the annual review of risk management and corporate governance.

## External audit

The role of external audit is principally to report on the association's financial statements and give an audit opinion. The external auditor also reports to the board on findings from the audit in a management letter. This letter provides a source of external assurance on the operation of internal control systems.

External auditors of housing associations are also required to report if the association has not maintained a satisfactory system of internal control. This requirement only applies to Industrial & Provident Societies and Charities (Housing Act 1996 Sch 1 Part III s18). However, reporting under this requirement is essentially a form of negative assurance that would report weaknesses if identified.

It must be remembered that the external auditor's work is not intended to provide assurance on all the controls that the board may be interested in. If small associations require assurance on specific areas they may request the external auditor to conduct assurance work in addition to the work required to reach an opinion on the financial statements.

# Risk identification and assessment

This chapter sets out basic guidance on how practically to identify and assess risks within an association.

## Types of risk

It is usually helpful to classify the types of risks faced by the association. The following scheme is by way of illustration of the type of framework which may help the identification process.

Risk area	Examples
Financial risks	Liquidity risk (inability to meet financial obligations as they fall due) Interest rate risk (arising from changes in interest rates)
Physical risks	Natural perils to office accommodation and housing properties – fire, flood, storms - resulting in loss of buildings, IT, phones or other facilities
Operational risks	Errors in processing data Project failure (e.g. developments) including mis-specification, late delivery, excessive cost or delivery not to specification Fraud Poor value for money in procurement Legal risk (unenforceable contract e.g. outsourcing or software contract, or misinterpretation of the law) Compliance (breach of regulation) Failure to deliver service standards as promised (e.g. emergency repairs) Failure to control costs Outsourcing (of IT, maintenance, internal audit etc.) risks e.g. quality of service and loss of control

Personal risks	Workplace stress Physical safety of front line staff Liability of directors
Strategic risks	Deterioration in economic environment Changes in regulations Changes in Government policy Increased competition
Reputational risk	Adverse publicity focusing on events at one of the association's developments or poor service delivery

## Risk management challenges in small organisations

Managing risk, including implementing controls, poses special problems for smaller organisations. These may be partly reduced by the principle of concentrating on the significant risks. Generally there are a manageable number of these that are more readily controlled.

In a smaller organisation the following areas are especially vulnerable:

- susceptibility to concentration of power;
- poor segregation of duties leading to less checking than ideal;
- inadequate time/resources to carry out comprehensive risk analysis;
- insufficient funding for fully effective internal audit; and

- sporadic monitoring of the internal control system.

Concentration of power may be a major risk for a smaller organisation which may not always be able to ensure there is adequate segregation of powers and duties, especially at the higher levels. Undue concentration of power may exist as a fact in spite of reasonable formal procedures, so that it is possible the chief executive may be unduly dominant and the board not sufficiently challenging to apply an effective check. Key segregation of duties, on paper, is the minimum requirement, and the 'four eyes' principle should apply (i.e. at least two people should take major decisions). The constitution and delegated powers of the organisation needs to be reviewed carefully to ensure the principle is enshrined. It is

important to keep sight of the fact that undue concentration of power may allow fraud on the association by senior executives and that segregation of duties and the checks and balances of good governance exist as much to prevent malicious actions as accidental mistakes.

In addition to all of this, smaller associations might consider engaging a trusted third party to assess the overall governance arrangements in practice and the effectiveness of the oversight of the executive by the board and any committees. This is a sensitive area because any issues there may be relate to individuals and in effect this is an assessment of individuals' behaviour and performance both in the executive and in the board and committees. However, as this is likely to be one of the biggest potential risks for a small association it is right that the issue should be dealt with in the open as a matter of course for the protection of all concerned.

If compromises need to be made in the extent of risk management activity this should not be in the area of risk identification and assessment. This is an absolute minimum on which all risk decisions are built and requires sufficient time and attention to ensure it is done

properly. Ignorance of the risks is not an excuse for inaction. The hard choices need to be made in the area of controls.

## Risk identification

Risk identification relies on people knowledgeable about the area of operations concerned considering potential downside scenarios and grouping them into sensible categories. It is often done in a workshop setting involving managers responsible for, and staff working in, the specific area being considered. Internal audit may often be involved to contribute additional objective input.

The following inputs may assist the identification process:

- past events within the association. Things which have gone seriously wrong in the past can be a useful pointer of what to avoid in the future;
- relevant external events, such as news stories or knowledge about other associations' issues. Learning from the mistakes of others is also important and helps put risks into better perspective. When trying to persuade sceptics of the possibility of a risk crystallising, the fact

it has already happened elsewhere can be helpful;

- current control processes. Internal controls are put in place to manage risk so consideration of controls can provide useful information about the risks. Careful consideration of what the controls actually achieve can also help eliminate unnecessary controls; and
- analysis of what needs to go right with a business process and looking at the threats to those factors. This can be done by considering what a process needs to function effectively under the following headings:
  - people;
  - physical resources i.e. buildings, computer hardware, telephones, desks/furniture;
  - organisation and management;
  - information management and communication.

By identifying threats to each of these factors useful information about risks to the process can be obtained. For example, threats to people might include dependence on key staff and difficulty in recruiting trained people. Threats to organisation and management might include unclear reporting lines, poor management and poorly defined business objectives.

## Identification and evaluation process

There are a number of possible approaches to risk identification and evaluation including:

**Workshop:** people with knowledge of the association's activities meet for a workshop session, possibly facilitated by a professional facilitator, independent of the subject of the workshop. It is important to ensure that the facilitation is effective and that the right people take part.

**Questionnaire:** specially designed questionnaires are completed by people with knowledge and understanding of the key business processes. The questionnaires require thoughtful design and evaluation.

**Interview:** one or more individuals undertake interviews of managers and others to obtain the list of risks and their evaluation.

All of the three methods have their plus and minus points and the actual techniques chosen usually depend on the available resources and expediency. Whichever method is employed, the results would then

be documented and subjected to critical review, possibly by an independent third party for example internal audit, in order to validate them.

## Likelihood and impact

There are two basic aspects of risk:

- the likelihood that an event occurs; and
- the impact, or consequences, if it does.

To quantify the risk therefore requires quantifying each aspect and a combination of these numbers to arrive at an overall risk assessment.

One complication is that events generally have a range of potential impacts, each with an associated probability of occurrence. For example, if there were a fire at the association's main offices the possible effects could range from a little smoke damage in a kitchen to total destruction of the building. In order to assess the significance of the risk it is necessary to choose an impact which is representative and estimate the probability of occurrence of that impact.

This can be done by considering the maximum probable loss (MPL), which is the maximum loss which could be reasonably foreseeable and not such a remote possibility that it may be discounted.

Once this is done the next step is to assign numbers representing probability and impact. These numbers are selected from a scale (for example, one to five, or one to ten) representing the severity of the impact of the MPL crystallising and its probability of occurrence.

For some risks the impact may not be quantifiable in monetary terms and this applies particularly to reputational risks whose effects may be difficult to assess. Some structured way of assigning numbers to probabilities and impacts needs to be used.

Example of an impact scale one to five

	<b>Monetary impact</b>	<b>Reputational impact</b>
<b>1</b>	£0 to £5,000	One or two customer complaints
<b>2</b>	£5,000 to £20,000	Many complaints, mention in news
<b>3</b>	£20,000 to £100,000	Local news headlines
<b>4</b>	£100,000 to £500,000	National news, not main item
<b>5</b>	More than £500,000	National headline news

If a monetary scale is used, the levels depend on the board's assessment of the differing levels of significance in the context of the association's business.

Probabilities need to be similarly categorised, for example.

Example of a likelihood scale one to five

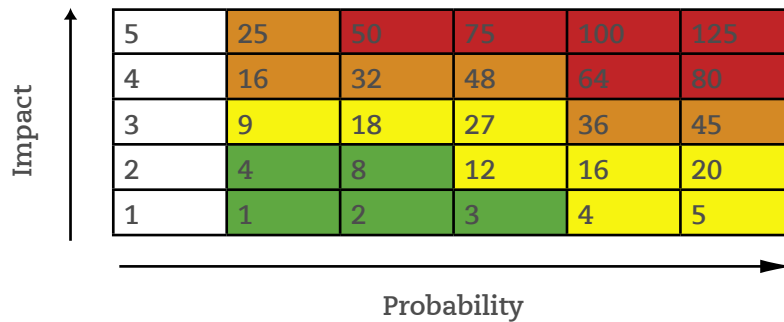
	<b>Likelihood</b>
<b>1</b>	Negligible likelihood of occurrence
<b>2</b>	Remote possibility
<b>3</b>	Possible but not likely
<b>4</b>	Moderately likely
<b>5</b>	Very likely

## Risk matrix

Once numbers have been assigned to the likelihood and impact of the risk, it may be plotted on the risk matrix to assign it a degree of significance, often indicated by colour coding.

Example risk matrix indicating the degree of significance of a risk

The numbers in the cells are explained later.



The colour codings have the following meanings

Very high	Potentially very high, possibly terminal impact on the association at an unacceptable likelihood. Urgent action needed to reduce the risk to acceptable levels.
High	Could be either a potential catastrophe with a very low likelihood of occurrence, or a major impact with a higher possibility of occurrence
Moderate	Moderate impact, and, depending on other activities, the association may decide to live with it or give actions lower priority.
Low	Not regarded as an issue.

Some schemes use only three levels (High, Moderate and Low). However this has the potential drawback that there is a temptation to put too many risks into the moderate category.

Sometimes the probability and impact scores are multiplied to get an overall risk score and rank risks accordingly. Care needs to be taken when using such an approach as it may give misleading results, e.g. such a methodology would rank equally (at an overall score of five):

- a catastrophic impact with a very low probability; and
- a negligible impact with a high probability.

These types of risk are completely different in nature. The first may represent an event such as total loss of IT and phones for a week, whereas the second is the repeated occurrence of something insignificant. In the latter case, action will be taken once management has been alerted to the issue, whereas in the former, if controls such as contingency and insurance are not in place, the association might not recover at all.

An alternative approach, as illustrated above in Example risk matrix indicating the degree

of significance of a risk, is to use the square of the impact multiplied by the probability.

## Gross risk and net risk

When discussing risk, it is important to be clear whether it is gross or net risk which is being referred to, according to the following definitions:

- gross risk (of an event) is the risk assessed on the basis that there are no controls or other risk mitigation in place; and
- net risk is the risk assessed on the basis that there are controls in place which are functioning effectively.

Gross and net risk are sometimes referred to as inherent and residual risk respectively. However, in this publication inherent risk signifies risks inherent in the business which cannot be mitigated.

Note that in the definition of gross risk, whilst there is the assumption of no risk mitigation in place, a rational and reasonably intelligent organisation is assumed, which even in the absence of formal controls would eventually take action to mitigate the adverse impact of an event.

Whilst the main concern of management may be the current level of residual risk exposure, gross risk is used to ensure due diligence is applied to monitoring those controls which address it. In other words, controls covering high gross risks require constant vigilance and a more rigorous monitoring procedure than others. This is the case even though the residual risk may be tolerable, or to put it another way, there are no problems at present. If things go wrong with high gross risk areas, the consequences, by definition, are much greater.

## Recording and reviewing the risks

Once all the risks have been identified and assessed, the results need to be documented and considered by the board. The risks may be recorded in a risk register containing the following information:

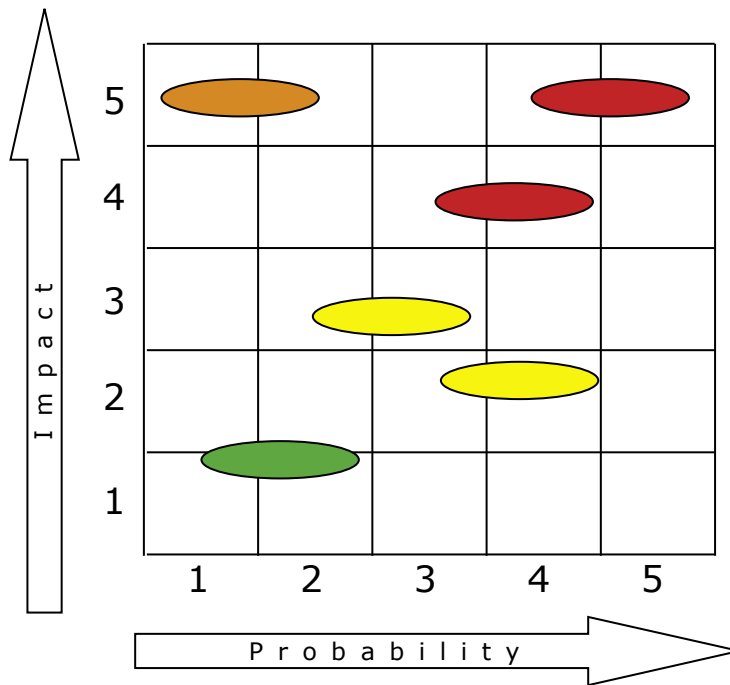
- the identifying title of the risk;
- the probability/impact score(s). It is most helpful if risks are listed in descending order of assessed significance;
- how the risk is managed (the combination of risk responses applied to the risk);

- high level summary of any actions needed to be implemented to mitigate the risk to acceptable levels. Actions must record deadlines for completion and who is responsible;
- the trend of the risk i.e. a comparison of the level of risk with that previously reported.

It is essential that the risk register, or similar document, is reviewed on a regular basis, possibly every quarter, but also whenever any aspect of operations changes, for example when considering:

- new development projects;
- new activities;
- major changes in the structure or organisation of the association; and
- new IT systems.

A supplementary, one-page summary is often found to be useful in reporting to the board. This is a 'bubble' report which shows the colour coded matrix of probability and impact, and lists all the identified risks in their appropriate position.



# Responding to risk

Of course, it is not sufficient merely to identify and assess risks. An organisation must also consider its response to those risks, both on a risk specific basis (whenever risk exercises are carried out, it almost goes without saying that any current areas of very high risk exposure should be dealt with immediately) and overall by setting out its overall approach to risk.

## Summarise in a risk policy statement

Good corporate governance and effective management require the association's policy on risk and risk management to be set out in a formal document for approval by the executive and the board. The policy needs to cover at least the following:

- a list of the main risks and a high level policy statement of how they are to be managed;
- procedures for the periodic review and refresh of the Risk Register;
- clear allocation of responsibilities for the management of each main risk;
- a system of delegated responsibilities for risk clarifying at what level decisions on acceptance of risk may be taken;
- a statement that the risk of failure of the organisation cannot be reduced to zero and a statement of what the corporate tolerance to overall risk is;
- details of the high level process in place to monitor the effectiveness of risk management including details of ongoing risk and internal control reporting procedures and the annual review of risk complying with regulatory governance requirements;
- terms of reference and membership of any specially constituted risk committee, or, if the audit committee is to take on the role, clarification of what its role is within the risk framework;
- clarification of the role of internal audit within the overall risk management framework and the main high-level procedures for internal audit; and
- definition of terms (risk language) to ensure there is common understanding of the concepts across the organisation.

## The three lines of defence

A model commonly applied in managing risk is known as the ‘three lines of defence’. These are:

- first, line management who are primarily responsible for identifying and managing risks and implementing and operating internal controls;
- second, any independent risk management function. Such departments are common in larger organisations, but unusual in smaller ones; and
- the last line of defence is internal audit, whose role is to review the operation of risk management arrangements and report to the board.

It is important to recognise that internal audit is not normally responsible for managing risks directly. It is helpful if there is a general understanding that managers’ responsibilities for risk and control cannot be devolved to internal audit, and this should be documented in the risk policies.

## Clear business strategy

Good risk management generally begins with a clear documented business strategy. Risks are possible events that may adversely effect the achievement of objectives.

So if there is ambiguity about what the association is trying to achieve, identifying and prioritising the potential risk is almost impossible.

This is not the place to detail what a good practice business strategy should look like. At the least it would need to contain:

- an overall summary of the aims of the organisation in a mission statement or something similar;
- a clear list of measurable targets and objectives;
- a list of actions and accountabilities of how it is intended to achieve the objectives; and
- a risk analysis of what might stand in the way of the strategy and a high level summary of the proposed approach to mitigation.

In broad terms the risks in the strategic plan are likely to be confined to the business and strategic risks. Detailed operational risks,

even if potentially large, would not normally find their way into the strategic plan.

## Clear operating policies

Good practice requires clearly documented delegation of authority from the board down through the executive and then to all levels in the organisation. There is also a need for clarity around what powers the board reserves to itself.

## Risk management responses – the four Ts

In terms of responses to specific risks these may be considered under four headings:

**Tolerate:** the risk is accepted as being within the organisation's risk appetite. For high risks this should be done formally and signed off by the Board as part of its overall risk management/corporate governance procedures;

**Transfer:** the association transfers the risk to another party. For example, the risk is insured, in which case, in exchange for the payment of the premium, the insurance company bears the risk. **Warning:** a serious

problem with risk transfer arises from the legal risk that in the event, the other party cannot, or will not meet its obligations. This may be particularly true of certain outsourcing contracts where the association may believe it has transferred risk, but in reality it has not;

**Treat:** treating a risk involves taking actions to mitigate the risk, both in terms of reducing the likelihood of its occurrence (preventive controls) or reducing the impact if it does occur. It includes putting in place operational controls and contingency arrangements; and

**Terminate:** an option sometimes overlooked is to terminate the activity that gives rise to the risk, equivalently not commencing the activity if the risk appraisal does not demonstrate that the benefits outweigh the risks.

Several of the most common types of control techniques and procedures are discussed below.

### **Authorisation controls – segregation of duties**

Authorisation controls are among the most basic and well known financial controls. These require one person to obtain authorisation for a transaction, or other action, from another person. The whole idea is that the authoriser is in a position to check the activities of the person requesting authorisation. The possibility of fraud or error is reduced as it would require either collusion or two people making the same mistake. The effectiveness of authorisation controls depends essentially on a segregation of duties between the person that initiates a transaction and the authoriser.

Authorisation is especially important in the area of procurement where ideally there should be segregation between:

- the person placing an order;
- the person approving the invoice; and
- the person authorising actual payment.

What can be done in a small organisation? A basic system of limits of authority is essential. These should be spelt out in the procurement policy so that while an individual may be allowed full control over

all aspects of some transactions up to a specified limit beyond that a second person must be involved.

For larger transactions the risk of fraud becomes significant. This places a considerable responsibility on the board when approving the delegated spending authorities. It is up to the board to approve a policy that fits its risk appetite. Board members must also consider carefully whether there is any question of undue influence by any of the executive. Conversely it is in executives' interests to ensure there is appropriate check and review of their activities for their own protection.

### **Reconciliation controls**

Reconciliation is another basic control procedure. It consists of making a comparison between two pieces of information drawn from different sources that are expected to be consistent.

Explanations must be obtained for any inconsistencies or differences.

The prime example of this control is the bank reconciliation. This compares the bank balance in the association's books with the bank statement and any differences are investigated and explained. Again, to be

effective, appropriate segregation of duties between staff keeping the records and those performing the reconciliation is vital.

Another key reconciliation control is the comparison of rent arrears in the nominal ledger with the sum of individual tenants' balances in the rent ledger.

Reconciliation controls are so important that their effectiveness must be monitored. Not only must the procedures require them to be done but there must also be regular review at a senior level to ensure that they are actually happening.

### **Financial risk management**

Sound planning, cash flow forecasting and professional management of liquid funds are fundamental to financial risk management.

It is unlikely that the use of sophisticated financial instruments, committed bank funding and so on would be required by smaller associations. Unless there are special circumstances many smaller associations would not rank financial risks as high on the risk map.

However, whilst an association may not have high financial risks, the operational risks associated with cash management may be

high. In other words whilst there may not be high exposure to interest rate movements, for example, investing cash in the wrong place or attempting something too exotic may lead to disaster.

### **Value for money controls**

A high cost base due to poor procurement processes is a key risk for smaller organisations. Value for money management follows well established principles including:

- competitive tendering;
- appropriate segregation of duties (ordering, invoice approval, payment); and
- value for money reviews.

### **Business continuity planning**

Sometimes it is not possible to prevent a potentially high impact event occurring. The question when this happens is to what extent it is possible to contain the impact, recover and carry on providing services afterwards. This is the province of business continuity planning (BCP), an often overlooked under-resourced activity.

Like many aspects of risk management this activity more often comprises the

application of common sense than rocket science. In a nutshell, as part of the risk identification and assessment process, disaster scenarios are prepared and consideration given as to what the association would actually do in the event.

A typical scenario might involve the total loss of all IT. As part of preparations against this possibility IT professionals have contingency plans which require daily backup of vital systems and data and the availability of contingency machines, either at an off-site location or more probably by agreement with a provider of such services.

BCP is just as necessary for small organisations as for large ones. Some important aspects of this area of risk management are:

- the business continuity plan needs to be tied in to and be an integral part of the overall process of risk management. It comprises after all just one element of the risk response to high impact, low probability events (other responses include insurance and other preventative control measures);
- the plan needs to be periodically tested to ensure it will work in the event it is called upon; and

- BCP covers all aspects of recovery after disaster, not solely IT recovery.

It is recommended that in drawing up business continuity plans, due attention is given to the framework and methodology published by the Business Continuity Institute.

### **Insurance**

Insurance is a standard response to many of the physical hazard risks and can be used to mitigate the impact of a high impact/ low probability event (after the event has occurred). All of the issues of legal risk apply to this and in the case of very large claims it is not necessarily a straightforward matter to recover large sums immediately.

If the expenditure on insurance is high it is worth reviewing the programme of insurance from a risk management perspective to make adjustments in the level of deductibles (i.e. insurance excess) in the light of the association's risk appetite. So by raising the level of deductible in a policy, and in effect self insuring, and possibly effecting additional control, it may be possible to save considerably. This needs to be done carefully as reduction in insurance cover clearly has the potential for serious consequences.

## **Outsourcing/partnering monitoring**

Small organisations are likely to be engaged in outsourcing services that are not economic to undertake internally. Examples include IT, maintenance and internal audit. There are many risks associated with such arrangements that generally revolve around the potential non-performance by the service provider or actions by the provider which are not considered helpful.

Approaches to this vary, but there are two main principles:

- ensure there is a clear service contract which provides sufficient rights to monitor performance and take action, and sufficient obligations on the provider to perform, and to provide regular information and allow necessary direct access to its records and systems by the association;
- put in the necessary time and effort to monitor performance and maintain the correct relationship with the provider. Outsourcing contracts do not take care of themselves and require continuous monitoring and vigilance. This may be done by identifying an accountable person internally who 'owns' the

contract and whose job is to oversee the delivery of the right quality of service.

The biggest mistake, and one commonly made, is to assume that once a service has been outsourced and commenced there is nothing further to worry about and responsibilities have been outsourced also. Nothing could be further from the truth. Without a good performance monitoring system and close attention to it things may well go wrong. If in addition, sufficient care and attention to the potential for things to go wrong had not been given to the contractual arrangements the association may also be left with no redress to add insult to injury.

## **Addressing compliance risk**

Compliance risk is an operational risk and as such is generally addressed by implementing the appropriate control systems. Many of the controls covering compliance risk are standard controls covering many other operational risks. In effect one control can cover many risks. However, how can associations be sure that all the regulations are covered?

In managing compliance risk, there is no substitute for a formal exercise listing

all applicable regulations, grading them according to the assessed level of risk and noting the controls in place to manage the risk of breach.

Following the principle of concentrating on areas of highest risk it is important to identify these in respect of compliance. This will narrow the area of focus to a manageable size.

## Assurance and monitoring of the internal control system

The principle of continuous monitoring should be applied to the whole system of internal control. Without continuous monitoring of key controls it is not appropriate to assume that everything is under control and operating as intended.

Whatever practical processes are put in place (and there need to be formal systems with a clear documentary trail to evidence performance) there should be two levels of assurance and monitoring:

- the continuous monitoring performed by management; and
- the board's (at least) annual review of the system of internal control.

Consideration should also be given to an independent review of the system of internal control e.g. by internal audit or other independent reviewer.

The obligations and responsibilities of directors and managers have become more extensive over recent years and the requirement now is for proactive monitoring of the control systems.

### Management reporting

The management reporting/performance monitoring system should cover the operation of the key controls which cover the areas of highest risk. That of course assumes the highest risks have been reliably identified.

To do this, an analysis of the key controls needs to be carried out to determine what would be the best way to monitor performance. One task which may be usefully allocated to the internal audit function would be to facilitate the development and introduction of this embedded monitoring of internal controls.

An approach that can be readily implemented is a monthly statement of a list of key controls, signed by the responsible

manager to confirm they have operated as intended during the month or details of any breakdowns in control and issues which have surfaced. The statement could be part of regular board/executive reporting. Obtaining confirmatory signatures on a document is in itself an important control.

Notification procedures may also be introduced to ensure that incidents and major adverse events (crystallised risks) are immediately reported to the appropriate level within the organisation

Where major issues have been reported under the association's notification procedures or through the review of the risk map it is essential that action plans are drawn up to deal with them. An appropriate action plan requires clearly allocated responsibilities and a stated deadline for the delivery of each action. Once the plan is in place for major issues of significance the board/audit committee should monitor progress, supported by appropriate verification work carried out by internal audit. It is important that the board obtains independent assurance that management has done what it promised to do to address the issue (i.e. risk exposure above the tolerable limit) and internal audit can be of assistance in this respect. Regular

progress reporting needs to be included in the embedded control monitoring system i.e. within the executive's regular monthly report to the board.

### **Board assurance**

The board must seek regular assurance from management on the state of the internal control system and the management of the major risks. The ideal is that this is built into regular monthly reporting so that discussions about risk and control can be held well before issues have built up.

The board's review of the system of internal control is covered in detail in the Housing Corporation's Circular 25/01, together with the accompanying guidance notes.

It is for the board of each association to decide how to obtain assurance on the effectiveness of the association's system of internal controls. Possible methods include the following (which should not be regarded as an exhaustive list):

- board/audit committee overview;
- management assurances on internal controls;
- management reports on operational and financial matters;

- risk management activities;
- internal audit;
- quality management systems;
- external audit;
- key performance indicators; and
- external regulatory reports and other external reports.

For a small organisation, where resource constraints are particularly tight, it is essential that imagination is used to exploit potential sources of assurance which are undertaken in the normal course of business and consequently do not involve the consumption of additional resource.

Circular 25/01 requires executives to carry out a review of the internal control system and report to the board annually. However, it is recommended that in addition, a brief quarterly or half-yearly update would be of benefit since with the rate of change in today's environment an annual gap between reviews is likely to be too long.

The review may be facilitated by internal audit and comprises obtaining management's assessment of the current risk exposures and the effectiveness of the associated controls. If management has implemented effective continuous monitoring systems there will be little to

do, other than review all the risks to ensure there are no new ones and the assessment of the levels of gross and net exposure have not changed.

Where there is no well developed monitoring system, a comprehensive review will need to be carried out.

In either case the executive needs to review the high level summary of risk and control and sign it off prior to submission to the board and/or audit committee. It is important to ensure that there is appropriate focus on the big risks. A multi-page report with many dozens of risks mixing significant and insignificant risks is very unhelpful.

## Reviewing the effectiveness of audit

Internal and external audit play key roles in the overall risk management system. As such it is helpful for the board/audit committee to implement formalised procedures for the annual review of the effectiveness of internal and external audit. The Corporation's guidance referred to above on external audit and internal controls assurance contain relevant sections on reviewing the effectiveness of audit.

# Selective bibliography

## Housing Corporation publications

The Regulatory Code

Managing Risk (collection of six papers)

- The quantification of risk
- Embedding risk management – some tips and tactics
- Monte Carlo simulation and the art of aviation
- Risk mapping – dilemmas and solutions
- A practical approach to identifying risk
- Reputation, risk and governance

A strategy for success: effective risk & business management

Circular 25/01 'Internal Controls Assurance' and accompanying guidance

Good Practice Note 7 External audit of housing associations

Housing association risk data sharing project

Improving the effectiveness of audit committees

## National Housing Federation

Competence and accountability 2004

A wider role for internal audit

## Housing Association Internal Audit Forum

Practical guide to risk management

# Our offices

Maple House  
149 Tottenham Court Road  
London W1T 7BN

For enquiries, contact us at:

Tel: 0845 230 7000

Fax: 0113 233 7101

E-mail: [enquiries@housingcorp.gsx.gov.uk](mailto:enquiries@housingcorp.gsx.gov.uk)

Internet: [www.housingcorp.gov.uk](http://www.housingcorp.gov.uk)

## **CENTRAL:**

Attenborough House  
109/119 Charles Street  
Leicester LE1 1FQ

31 Waterloo Road  
Wolverhampton

Trinity House  
Cambridge Business Place  
Cowley Road  
Cambridge CB4 0WZ

## **LONDON:**

Waverley House  
7-12 Noel Street  
London W1F 8BA

## **NORTH:**

4th Floor  
One Piccadilly Gardens  
Manchester M1 1RG

1 Park Lane  
Leeds LS3 1EP

St. George's House  
Team Valley  
Kingsway Trading Estate  
Gateshead NE11 0NA

## **SOUTH EAST:**

Leon House  
High Street  
Croydon  
Surrey CR9 1UH

## **SOUTH WEST:**

Beaufort House  
51 New North Road  
Exeter EX4 4EP

## The authors

Roger Lustig specialises in internal audit, risk management and financial investigations. He undertakes this work for housing associations through his practice based in central London. Roger is a chartered accountant with 15 years' experience in the housing sector. He also edited a series of papers for the Housing Corporation on risk management, published in 2004 as a booklet entitled *Managing Risk*.

Contact details:

[roger.lustig@lustig.co.uk](mailto:roger.lustig@lustig.co.uk)

Dr David Bobker is a chartered accountant and mathematician with 25 years' experience in the financial services sector covering internal and external audit, consulting and nearly three years with the Building Societies Commission. He was group head of internal audit for the Alliance and Leicester and later for Norwich Union. David has contributed to the development of internal audit and corporate governance through articles and conference talks and through his past participation in the internal audit committee of the Institute of Chartered Accountants in England and Wales. He is an associate of Lustig and Co.

Contact details:

[david.bobker@lustig.co.uk](mailto:david.bobker@lustig.co.uk)

For further copies of this publication please call 0845 230 7000 or e-mail [enquiries@housingcorp.gsx.gov.uk](mailto:enquiries@housingcorp.gsx.gov.uk). We can also provide versions in other languages, large print and audio cassette on request.

