

Codes-related guidance

Internal controls

Complying with the obligation to
establish and operate internal controls

To be read in conjunction with
the Pensions Regulator's code of
practice no. 9 - Internal controls

February 2007

Contents	page
An example of the scheme risk-management process	2
Set objectives	3
Identify risks	4
Define success criteria	6
Assess risks	7
Produce action plan	9
Implement action plan	11
Monitor and review	11

Internal controls

Complying with the obligation to establish and operate internal controls which are adequate for the purpose of securing that the scheme is administered and managed in accordance with:

- the scheme rules; and
- the requirements of the law.

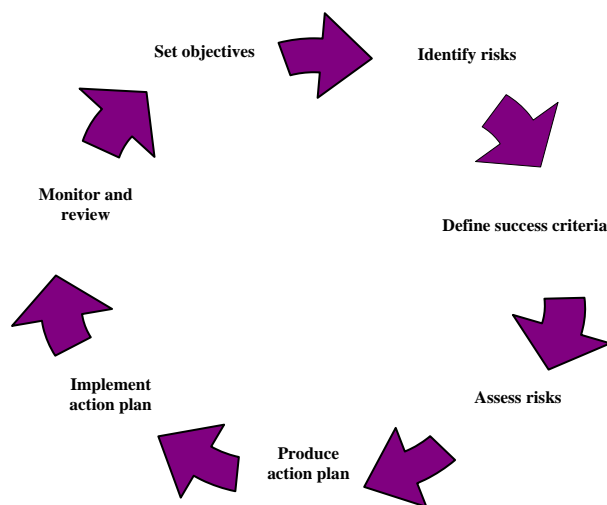
This guidance is designed to complement the code of practice on internal controls and should be read in conjunction with the code.

It expands upon the concept discussed in the code that the establishment of adequate internal controls depends upon a robust risk-management approach and provides an example of how a risk-management process might work in practice.

The guidance will be of interest to trustees and managers of all occupational pension schemes, especially to trustees of smaller schemes and to fully insured schemes.

An example of the scheme risk-management process

The code of practice recommends a risk-management approach as a means of meeting the requirements set out in the regulations (The Occupational Pension Schemes (Internal Controls) Regulations [SI 2005/3379]). The risk-management process you use, and the steps followed to identify key risks, will probably look similar to this:



This guidance provides:

- an explanation of the purpose of each step;
- a description of the activities that you might need to carry out at that stage; and
- details of the likely outcome you will need to carry forward to the next step in the process.

You may want to tailor the process to suit your scheme, taking advice if appropriate from those with experience in implementing systems of internal control. If you are involved with a larger scheme, you may already have worked closely with internal and external advisers to make sure that the systems put in place are fit for purpose.

We recognise that smaller schemes may benefit from some guidance on risk management procedures and we have produced this guidance accordingly.

Set objectives

Purpose

The purpose of setting objectives is to identify the activities that you believe are fundamental to the good running of your scheme and decide what the desired outcome is for each activity.

They will also allow you to measure whether the internal controls you set up are adequate for the purpose of securing that the scheme is administered and managed in accordance with the scheme rules and the requirements of the law.

Description

You will need to look at the activities of the scheme that you consider to be fundamental to its good-running and then think about what the desired outcome is for each activity.

Many schemes will not have an existing risk-management policy. However, if your scheme does, this should be the starting point for setting objectives. Where a scheme has identified objectives from a previous review, these should be updated and any new objectives added.

For most schemes the overarching objectives are likely to be linked to:

- safeguarding scheme assets;
- maintaining suitable funding levels;
- securing the payment of adequate contributions;

- correct levels of benefit are being paid to bona fide members; and
- ensuring that the scheme operates within the law and in accordance with the scheme's trust documentation.

As an example, the desired outcome for the objective of safeguarding scheme assets could be that this prevents any misappropriation of funds.

Once agreed, existing and new objectives, together with the desired outcomes, should be recorded in a clear statement of risk-management objectives.

Outcomes

A robust set of documented risk-management objectives have been agreed which can be used in the next stage of the process to help identify the specific risks to the scheme.

Identify risks

Purpose

Using the risk-management objectives defined in the previous step, the purpose of this stage is to assemble a full list of the risks to which the scheme is exposed.

Description

The agreed risk-management objectives should be used to help you focus on the key activities of the scheme. You should then look in detail at the activities and identify the risks involved with each activity.

At this stage, you are trying to identify all the risks applicable to each activity and are not attempting to do any assessment of the likelihood and impact of the risk. It is important that as many risks as possible are identified and it will be helpful to get input from all the trustees and others representing the main activities carried out by the scheme (managers, administrators etc).

External risks that may affect its good running must also be considered. The risk of delegated services, such as third-party administrators, failing to deliver is one which will affect the majority of schemes. Even if you are involved in a scheme that uses in-house services, you are still likely to use external investment management or insurance companies.

As outlined in the code, when identifying the risks, you may find the categories below helpful.

Once you have identified the risks, these should be collated and recorded. The conventional way of recording identified risks is through the use of a listing known as a **risk register**. You can view and download an example risk register on our website. The register schedules the identified risks and has additional columns for:

- the risk assessment that follows;
- the controls to be put in place; and
- the residual risks.

It also provides the basis for identifying the responsibilities, monitoring procedures and follow-up action required to make the risk-management process effective.

Outcomes

A complete list of all the risks affecting the key activities of the scheme has been agreed. This has been recorded as a schedule in a risk register.

Categories of risk

Operational

These risks are linked directly to the operational processes of the scheme and involve day-to-day activities where error can occur. Even when controls exist, there are also risks associated with those cases where individuals are determined and able to circumvent the internal controls in place and, in those cases, the most appropriate control may be one of detection rather than prevention, eg peer reviews, reconciliation processes.

Should significant data be lost, either through accident or through malicious damage, the ramifications could be widespread and financially very costly, so this is a key area for trustees to consider. Failures in the administration system could affect amongst other areas, the payment of benefits, the calculation of benefits, or the correct allocation of contributions received. Scheme documents and member information often go back a number of years and capture details of former schemes, those subject to legacy arrangements, alternative benefit structures etc, information which may be almost impossible to recover without some kind of contingency plan.

A proportionate approach needs to be taken at all times. For example, security of assets and safe custody arrangements need tailoring to the scale, nature and importance of the assets in question. Those schemes using third-party administrators will require particular procedures in place to maintain and monitor and review this relationship and to ensure they receive information from the provider to ascertain if controls exist and work. For instance, those schemes relying on the employer to supply payroll services must also ensure that there is adequate reporting to trustees or managers, although the logistics may be different from those schemes relying on a third-party provider. An in-house arrangement should not lead to a weakening of internal controls.

Financial

This could refer to the scheme itself or to the sponsoring employer where either party suffers financial loss. In particular trustees may wish to consider the likelihood of the employer company failing or having insufficient cash to fund contributions and the effects this may have and the risks this creates. In

a unitised money purchase arrangement, the allocation of contributions to the correct investments and accurate allocation of units poses a potential risk to administrators and, clearly, adequate internal controls are critical.

Funding (defined benefit schemes)

The risk here is that the combination of the two factors of funding levels and employer financial ability to make good any deficits, leaves an exposure to a reduced entitlement for members and, in extreme cases, a call upon the Pension Protection Fund (PPF).

A regular, structured and open dialogue with the employer is an essential characteristic of a well governed scheme. It is important that the trustees have an understanding and appreciation of the financial position of the sponsor. The extent to which trustees or managers are able to do this will depend on their own skills and the willingness of the employer to engage in open dialogue with them. Regular reviews of the sponsoring employer's covenant and a suitable make-up of the trustee board may help to provide the environment for adequate control in this area.

Regulatory

A framework exists (reinforced by provision for trustee knowledge and understanding) to help protect the interests of members. This covers disclosure and other requirements in respect of funding, investment etc and prescribe those actions that constitute a notifiable event or require clearance or disclosure. The risk of operating outside the regulatory framework leaves trustees (and ultimately the members) open to undue risk.

Compliance

Trustees are responsible for identifying control weaknesses and for implementing and maintaining systems of control, as appropriate, which are sufficient to enable them to discharge their legal duties.

An important scheme objective is to ensure that their actions comply with legal or regulatory requirements so the risk that they might fail to do so either through ignorance or deliberate action must be considered. The trustees are also bound by the scheme's trust deed and rules as well as by their fiduciary duties to members.

The risk of breaching legislation or the provisions of the trust deed and rules for a scheme could, in more serious cases, result in court action, fines, loss of reputation and potential compensation.

Define success criteria

Purpose

The purpose of this stage is for trustees to determine the levels of risk that they consider to be acceptable to the scheme in light of the desired outcomes

established earlier in the process. This will provide an effective means of recognising whether the controls they put in place in future are being successful in mitigating the targeted risks.

Description

Before you can assess and prioritise the list of risks held on the risk register you need to establish what level of risk is acceptable to the scheme. You cannot mitigate all risk completely and accepting a degree of risk is a valid outcome from the risk-management process.

Setting the level of acceptable risk will provide the threshold above which you may need to establish internal controls when you come to assess the risks in the next stage of the process. It will also provide a measure for establishing the success of the internal controls you put in place to see whether the risk has been sufficiently mitigated.

It may be helpful to consider the acceptable level of risk in terms of its impact on:

- the security of members' benefits;
- disruption to the smooth running of the scheme; and
- direct financial cost to the scheme.

At this stage you will also need to establish who 'owns' the risks you have identified. The owner of the risk is the person with primary responsibility for managing it. The ownership of each risk will need to be communicated to the relevant person.

You will need to record the agreed success criteria and risk owners on a risk register.

Outcomes

The scheme's acceptable risk levels and risk owners have been agreed and communicated, and success criteria have been recorded in the risk register.

Assess risks

Purpose

The purpose of this stage is to assess each risk on the risk register and categorise it depending on its impact and likelihood of occurring. This assessment will help inform your subsequent decisions on whether an appropriate control needs to be established to mitigate that risk or whether improvements need to be made to existing controls.

Description

You will need to take each risk recorded on the risk register and make an assessment of its severity in order to decide which ones require mitigating action.

There are a number of ways of categorising a risk. One method is to consider each identified risk and decide what the likelihood is of the risk occurring along with the severity of the impact on the scheme's objectives (as defined at the beginning of the risk-management process) if it did occur.

It can help to use a chart, such as below, when making the risk assessment.

Likelihood of occurrence (Chance of happening)	High likelihood Low severity of impact (A)	High likelihood High severity of impact (R)
	Low likelihood Low severity of impact (G)	Low likelihood High severity of impact (A)
	Level of severity of impact on the scheme (for example, the financial cost to the scheme)	

This chart attempts to map risk using the likelihood of an undesirable outcome and the impact that an undesirable outcome will have on the scheme's ability to achieve its operational objectives. This process enables the trustees to identify those risks which fall into the major risk categories. Our example has only two divisions on each axis, low and high, but you may choose to have more.

Risks are categorised into red, amber and green (R, A, G). In the green zone, the exposure to risk is considered to be within the acceptable level (as established at the previous stage of the process).

A risk falling into the amber zone is not considered to be one that is an immediate threat to members' interests. However, this does not mean that no action need be taken as it is important that amber risks are monitored and prevented from becoming red risks.

Those falling into the red zone are thought to provide a critical exposure to risk requiring immediate action. Red risks have a high likelihood of occurring, and when they do, would have an impact on the operational performance, objectives or reputation of the scheme. They may also involve a breach of legal requirements.

Having assessed each risk against this chart, you will need to update the risk register with your assessment.

Outcomes

Each risk has been assessed for likelihood and impact and then classified as either red, amber or green. This will provide the foundations for preparing an effective action plan. The assessment has been recorded in the risk register.

Produce action plan

Purpose

Having identified the major risks, a decision needs to be made how to manage them. The purpose of this stage is to agree controls and to produce a plan setting out the responsibilities and timescales for implementing the controls to ensure that the required changes in procedure do indeed take place.

Description

In the previous stage of the process you assessed the risks for likelihood and impact and classified them as red, amber or green. You will now need to take each risk and, based on the classification, decide whether:

- a control already exists to mitigate the risk;
- any existing control is adequate; or
- a new control is needed.

Generally, if a risk is classified as green a control will not be necessary. If it is amber, although there may not be an immediate risk, some control will be necessary to reduce exposure. Any risk classified as red will require the implementation of one or more controls immediately.

You will need to consider what actions need to be taken to mitigate the red and amber risks. The action you decide to use may reduce the likelihood of the event occurring, or limit its impact if it does. Existing controls may need to be replaced or augmented if they are not thought to be working adequately.

Controls can be categorised in the following ways:

- *Preventative*: eg segregation of duties, password protection or restricted access
- *Detective*: eg exception reporting, reconciliations
- *Deterrent*: eg disciplinary procedure, supervisory checks
- *Corrective*: eg back-up procedure

An effective control will fit into one of these categories. To be adequate it will need to ensure that the scheme is administered and managed in accordance with the scheme rules and the requirements of the law.

The following are examples of the type of actions that may be needed to implement the controls:

- the risk may need to be avoided by that activity (eg closing the scheme to new entrants);
- the risk could be transferred to a third party (eg a third-party administrator);
- the risk could be shared with others (eg a fully insured scheme);
- the pension scheme's exposure to the risk can be limited (eg in relation to a particular section of the scheme);
- the risk can be reduced or eliminated by establishing or improving control procedures (eg internal financial controls, controls on recruitment, personnel policies);
- the risk may need to be insured against (this often happens for residual risk, eg employers' liability, third-party liability, theft, fire); or
- the risk may be accepted as being unlikely to occur and/or of low impact and therefore will just be reviewed annually (eg earthquake damage in the UK or loss in transit of a one-off contribution).

In assessing actions to be taken, the costs of mitigation or control will generally be considered in the context of the potential impact or likely cost that the control seeks to prevent or mitigate. The cost of mitigating a risk needs to be proportional to the potential impact. A balance will need to be struck between the cost of further action to mitigate the risk and the potential impact of the residual risk.

You will need to produce an agreed action plan to cover all the new controls you intend to introduce as well as any changes you want to make to inadequate existing controls.

The plan will need to be agreed with and communicated to all the risk owners, acting as a point of reference when implementing their controls.

The plan will need to specify the priority order for carrying out the work, the owner of each risk, the accountabilities and responsibilities for action in the plan (ie introducing the controls), timescales for completion, resources and costs.

You will also need to update the risk register to include details of the control relevant to each risk and the risk owner.

Outcomes

All risks have been categorised and the highest risks have an appropriate control identified. Accountability for implementation of the controls has been agreed and outlined in the completed action plan.

Implement action plan

Purpose

The purpose of this stage is to ensure that those people accountable for activities in the action plan carry out the plan in accordance with the agreed timescales.

Description

You will need to take responsibility for making sure that all aspects of the action plan are implemented. This means chasing risk owners and others responsible for actions in the plan to ensure they comply with the agreed timescales for implementation and to ensure that the correct controls are being put in place as agreed.

During implementation, the action plan will need to be constantly reviewed to ensure that it is still fit for purpose. For example, risk owners may have identified new risks during the course of their work, or they may have decided that the wrong risks have been identified. Similarly it may become clear during implementation that the proposed control is no longer appropriate or effective. You will also need to ensure that the action plan and, if necessary, the objectives are updated.

Outcomes

The primary outcome is the fulfilment of the steps set out in the action plan in a competent and timely manner. This means that the scheme has agreed and appropriate internal controls in place to mitigate its main risks.

Monitor and review

Purpose

The scheme will now have agreed internal controls in place to mitigate its main risks. The purpose of this stage is to monitor the effectiveness of the controls and to make changes to the controls if they prove inadequate or if new risks arise.

Description

A review of scheme risks and internal controls should not be seen as a one-off exercise. You will need to review the risks on a regular basis to ensure that changing circumstances have not altered any of the existing risks or introduced new risks that now need mitigation.

The circumstances you might need to consider include changes to:

- legislation, eg changes to disclosure requirements;

- scheme membership, eg bulk transfer in due to a scheme merger;
- key staff including scheme administration, eg a change of pension manager;
- delegated services such as third-party administrators;
- scheme structure, eg the introduction of a defined contribution section;
- the trustees' view of acceptable risk and its success criteria; and
- the scheme's operational objectives.

You will also need to consider whether the controls you have in place are still adequate. You should consider whether the control is still mitigating the risk to an acceptable level. The success criteria established earlier in the risk-management process should be used to help make this judgement.

If you use third-party administrators you will need to review their control reports to ensure that their controls are adequate enough not to subject your scheme to unacceptable risk.

Larger schemes are likely to have an internal audit function, an audit committee and structures already in place to mitigate risk. Nevertheless, even the largest schemes can benefit from including a wide ranging review of their risk management policy on a periodic basis.

Outcomes

Regular monitoring and reviewing will ensure that the scheme can be confident that all risks are identified and that major risks are mitigated down to an acceptable level by the implementation of suitable internal controls.

The scheme now complies with the regulatory obligation to establish and operate internal controls which are adequate for the purpose of securing that the scheme is administered and managed in accordance with the scheme rules and the requirements of the law.
