

Regulatory code of practice no. 9

# Internal controls

# Contents

Paragraph		Page
1	<b>Introduction</b>	3
5	The status of codes of practice	3
6	Other regulatory requirements	3
7	Terminology	4
9	Other relevant codes	4
10	To whom does this code apply?	4
13	Exemptions	5
	<b>At a glance</b>	6
	<b>The code of practice</b>	7
14	Obligation on trustees	7
16	What are internal controls and why have them?	7
18	A proportionate approach	8
21	The assessment of risk	8
28	The exercise of judgement	11
30	The need to review risks and internal controls	11
32	Limitations	11
33	Governance	11
36	Reporting	12
38	The Pensions Regulator's powers	13
	<b>Annex A: Corresponding Northern Ireland legislation</b>	14

## **Introduction**

1. Codes of practice are issued by The Pensions Regulator (the regulator), the body that regulates work-based pension arrangements (occupational pension schemes and certain aspects of stakeholder and other personal pensions). The regulator has issued this code under section 90(2)(k) of the Pensions Act 2004.
2. The regulator's statutory objectives are to protect the benefits of pension scheme members, to reduce the risk of calls on the Pension Protection Fund, and to promote the good administration of work-based pension schemes.
3. The regulator has a number of regulatory tools, including issuing codes of practice, to enable it to meet its statutory objectives.<sup>1</sup> The regulator will target its resources on those areas where members' benefits are at greatest risk.
4. Codes of practice provide practical guidelines on the requirements of pensions legislation and set out the standards of conduct and practice expected of those who must meet these requirements. The intention is that the standards set out in the code are consistent with how a well-run pension scheme would choose to meet its legal obligations.

### **The status of codes of practice**

5. Codes of practice are not statements of the law and there is no penalty for failing to comply with them. It is not necessary for all the provisions of a code of practice to be followed in every circumstance. Any alternative approach to that appearing in a code will nevertheless need to meet the underlying legal requirements, and a penalty may be imposed if these legal requirements are not met. When determining whether legal requirements have been met, a court or tribunal must take any relevant codes of practice into account.

### **Other regulatory requirements**

6. There is no explicit legislative requirement to report a lack of adequate internal controls. However, persistent failure to put in place adequate internal controls may, for example, be a contributory cause of an administrative breach or, in more extreme cases, result in the reduction or loss of scheme assets. Where the effect and wider implication of not having in place adequate internal controls are likely to be materially significant, the regulator would expect to receive a report, commonly referred to as a 'whistleblowing' report, outlining

---

<sup>1</sup> Section 5 (1) of the Pensions Act 2004

relevant information in relation to the breach. Detailed guidelines on whistleblowing reports are published in the regulator's code of practice No. 1 (Reporting breaches of the law).

## **Terminology**

7. In this code, legislative requirements are indicated by 'must' and code guidelines by 'should'.

8. 'Trustees' and 'managers'

The legislation refers to the duties imposed upon either a scheme's trustees or managers. Unless it is otherwise stated, all the references to 'trustees' in this code also apply to managers.

## **Other relevant codes**

9. The regulator issues codes of practice relating to a number of its activities. The following codes are likely to be most relevant to the application of this code:

- Reporting breaches of the law;
- Notifiable events;
- Funding defined benefits;
- Reporting late payment of contributions to occupational money purchase schemes, and
- Trustee knowledge and understanding.

## **To whom does this code apply?**

10. This code should be read and acted upon by trustees, both individual and corporate, and managers of occupational pension schemes.

11. The regulator also recommends the code to a wider readership including:

- scheme advisers (including professional advisers);
- participating employers;
- service providers such as fund managers, custodians and administrators; and
- others involved with the management and administration of occupational pension schemes.

12. This code is applicable to all occupational pension schemes, except those detailed below, regardless of size, structure or circumstance. Adequate internal controls are equally important whether a scheme is newly established, mature, closed or in wind-up.

## Exemptions

13. In accordance with section 249A(3) of the Pensions Act 2004, the following occupational pension schemes are exempt from the requirements of this code:

a) a scheme which —

(i) is established by or under an enactment (including a local Act), and

(ii) is guaranteed by a public authority;

(b) a pay-as-you-go scheme;

(c) a scheme which is made under section 2 of the Parliamentary and Other Pensions Act 1987 (c.45) (power to provide for pensions for Members of the House of Commons etc).

## **At a glance**

- This code sets out the regulator's expectations of how occupational pension schemes should satisfy the legal requirement to have adequate internal controls in place.
- The ultimate responsibility to establish and operate internal controls rests with the trustees.
- This code provides guidelines in terms of how the regulator views the implementation of adequate internal controls by trustees.
- It is not the intention for the code to provide a prescriptive list of internal controls.
- The code provides a high level, risk based approach which trustees may wish to follow when assessing the adequacy of their internal controls environment.
- A risk based approach enables trustees to focus on the key risks requiring adequate internal controls.

**In this code of practice, references to the law that applies in Great Britain should be taken to include corresponding legislation in Northern Ireland; an annex lists the corresponding references.**

# The code of practice

## Obligation on trustees

14. Section 249A of the Pensions Act 2004<sup>2</sup> gives effect to the requirement under Article 14(1) of the European Directive 2003/41/EC<sup>3</sup> that schemes should have adequate internal control mechanisms in place. There is therefore a legal requirement in the Pensions Act 2004 that trustees of an occupational pension scheme must establish and operate adequate internal controls.

15. The Regulations<sup>4</sup> state that:

“The trustees or managers of an occupational pension scheme must establish and operate internal controls which are adequate for the purpose of securing that the scheme is administered and managed:

- (a) in accordance with the scheme rules, and
- (b) in accordance with the requirements of the law.”

## What are internal controls and why have them?

16. Internal controls are:

- (a) arrangements and procedures to be followed in the administration and management of the scheme;
- (b) systems and arrangements for monitoring that administration and management, and
- (c) arrangements and procedures to be followed for the safe custody and security of the assets of the scheme.

17. The implementation and application of internal controls will therefore help trustees monitor the management and administration of their schemes. Internal controls will also improve the safe custody of assets and help protect the scheme from adverse risks which could be detrimental to the scheme had those risks not been mitigated.

---

<sup>2</sup> As inserted by the Occupational Pension Schemes (Internal Controls) Regulations 2005 (SI 3379)

<sup>3</sup> Directive 2003/41/EC on the Activities and Supervision of Institutions for Occupational Retirement Provision

<sup>4</sup> The Occupational Pension Schemes (Internal Controls) Regulations 2005 (SI 3379)

## **A proportionate approach**

18. All schemes, unless exempt, are required to have adequate internal controls. Trustees must decide what internal controls are needed to satisfy themselves that the scheme is being well managed in accordance with the law and the scheme rules.
19. Not all risks will have the same potential impact or the same likelihood of materialising. Trustees will need to look at both these areas and assess which risks the scheme can absorb without the need to take further action, and which risks require adequate internal controls to reduce their incidence and impact.
20. When considering risk, trustees should be mindful of the nature of their scheme and the risks which are inherent in a particular structure. Smaller schemes may require less formalised controls than more complex larger schemes, but regardless of size, key risk areas will still need to be adequately controlled.

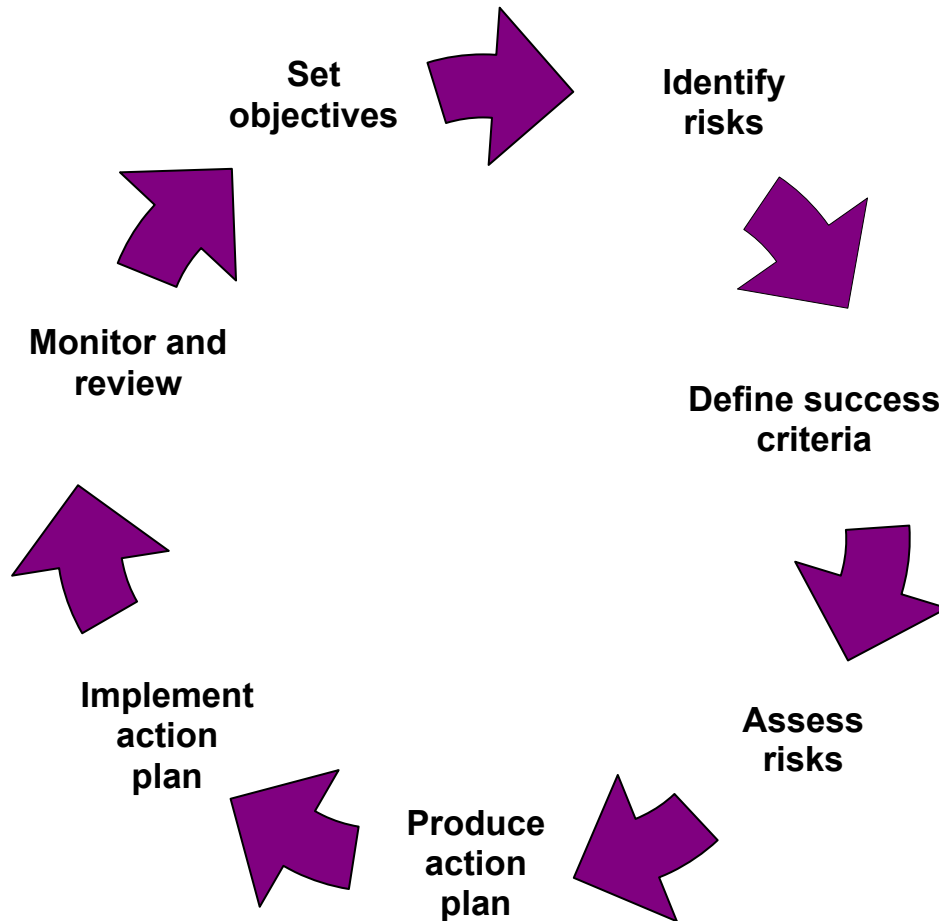
## **The assessment of risk**

21. Before implementing an internal controls framework, we recommend that the trustees should determine the various functions and activities carried out in the running of the scheme and then identify the key risks associated with those functions and activities.
22. The extent to which schemes are exposed to risk will vary from one scheme to another. To help identify areas where the scheme is exposed to undue levels of risk, and to enable trustees to establish and examine the adequacy of existing key internal controls, the trustees may wish to consider undertaking a risk review.
23. An effective risk review will assist trustees in identifying a wide range of both internal and external risks affecting the scheme and will provide a mechanism to detect weaknesses at an early stage. Internal controls will help mitigate risk to members' benefits and will also provide a framework against which compliance with the scheme rules and legislation can be monitored. Adherence to these controls will help ensure that risks are identified and addressed before affecting another part of a process or jeopardising the achievement of the schemes objectives. Implementing adequate internal controls will therefore assist the trustees in achieving these objectives.
24. The regulator recommends that trustees carry out a risk based review. It recognises that such an approach will initially focus on those areas where the impact and incidence of a failure relating to internal controls is high. Many trustees already use risk based methodology as a tool for highlighting exposure to risk and to help develop an adequate internal controls framework. Therefore, many schemes may already have adequate internal controls.



25. The diagram below provides one approach to the risk review process and summarises the stages involved in establishing and operating an adequate internal controls environment.

## The scheme risk management cycle



Source: based on Watson Wyatt business management cycle

26. Whilst not intended to be an exhaustive list, detailed below are some key risks which might be identified from a risk review exercise together with examples of adequate control procedures:

<b>Risk</b>	<b>Possible types of control</b> (where appropriate)
Risk that existing controls are not operating effectively	Periodic control reviews with changes made on a timely basis
Risk of fraud (misappropriation of assets and fraudulent financial reporting)	Segregation of duties; frequent reconciliation procedures for cash and investment balances
Corporate risk (risk of deterioration in strength of employer covenant and ongoing funding)	Monitor financial performance and corporate risk (e.g. inability of employer to fund scheme); procedures in place to detect corporate transactions in the public domain and assess impact on the scheme
Funding/investment risk (inappropriate investment strategies)	Reconciliation procedures; review of investment strategies; independent peer review of funding advice
Compliance/regulatory risk (failure to comply with scheme rules and legislation)	Compliance audits; stewardship and compliance reports from third parties
Non-compliance or maladministration by administration team or third party advisers, e.g. outsourced administrators (poor record keeping)	Peer review of key controls by administration team; authorisation procedures; periodic meetings between trustees and provider (when required); service level agreement reviews; performance appraisal of providers; internal quality review procedures by third party administrators (i.e. independent control reviews – “Assurance Reports”)
Computer system and database failures	System recovery plans; data back-up procedures; password controls
Poor scheme management (ineffective stewardship by those with delegated responsibility)	Regular trustee meetings; decisions taken within the formal structure of trustee meetings; minutes prepared for all meetings; sub committees; manage conflicts of interest

27. Linking internal control to a risk management framework will help trustees to focus on significant risk areas. The code addresses risk areas and considers risk as it applies to various types of scheme. Trustees should set up adequate internal controls which enable them to react to significant operational, financial, funding, regulatory and compliance risk.

### **The exercise of judgement**

28. Trustees should, having considered the nature and circumstances of their scheme, decide what internal controls are appropriate to mitigate the key risks they have identified and how best to monitor them. This requires them to exercise judgement, both in assessing the risk profile of the scheme and in designing appropriate controls.
29. The extent to which the trustees seek professional advice in this area will again be a matter requiring judgement. The regulator would expect advice to be taken when trustees feel they have insufficient knowledge to complete a risk review.

### **The need to review risks and internal controls**

30. Trustees should be prepared to monitor, challenge and review their risk assessment process and outputs. As referred to above, trustees should also ensure that they can recognise when professional advice is required.
31. Risk assessment is a continuous process and must take account of a changing environment. It is not simply concluded when an internal control is implemented. Internal controls should be reviewed periodically, at least on an annual basis, or sooner if substantial changes take place, such as a deterioration in funding, change in investment manager, or where a control has been found to be inadequate.

### **Limitations**

32. Trustees should be aware that an internal controls framework is not infallible and will not eliminate error or fraud from pension schemes. At any stage in a process where judgement is involved, the possibility of error remains. Similarly, the failure to understand how or why a particular control is operating, or more seriously, collusion to circumvent a control, will always be a risk that cannot be eradicated entirely.

### **Governance**

33. In both the corporate and not-for-profit sectors, the assessment of risk and the attention given to internal controls are seen as important features of good governance. Trustees may wish to demonstrate their own good practice in this area by making a positive statement (in their Trustees' Annual Report, for example), confirming that they have considered the key risks affecting their scheme together with the effectiveness of controls implemented to mitigate these risks.
34. The extent to which internal controls are documented will be a matter for the trustees to consider. The regulator would recommend that arrangements and procedures in respect of key internal control systems are documented as part of the routine business processes of

the scheme but recognises that the formalisation of controls will vary from scheme to scheme.

35. A number of third party administrators are obtaining independent reviews of their internal controls and are actively providing their clients with copies of the assurance reports. Trustees should read and understand these reports to establish the adequacy of controls used by the organisations to whom they outsource various functions. This will also include assurance reports produced by the scheme's investment manager and custodian.

## Reporting

36. There is no explicit statutory requirement to report a lack of adequate internal controls. However, persistent failure to put in place adequate internal controls may, for example, be a contributory cause of an administrative breach or, in more extreme cases, result in the reduction or loss of scheme assets.

37. Where the effect and wider implications of not having in place adequate internal controls are likely to be materially significant, the regulator would expect to receive a whistleblowing report. We would therefore expect users of this code to have a working knowledge of code of practice No. 1 (Reporting breaches of the law) which gives specific guidelines on reporting.

## **The Pensions Regulator's powers**

38. The regulator's principal aim is to prevent problems from developing and, where possible, provide support and advice to trustees where potential problems are identified. The regulator also has at its disposal a number of powers or regulatory tools that may be used in circumstances where serious internal control failings occur.
39. Regulatory action would have regard to the circumstances of the scheme and any use of powers would be proportionate.

## Annex A: Corresponding Northern Ireland legislation

GB Legislation	NI Legislation
The Pensions Act 2004	The Pensions (Northern Ireland) Order 2005 (S.I. 2005/255 (N.I. 1))
The Occupational Pension Schemes (Internal Controls) Regulations 2005 (SI 3379)	The Occupational Pension Schemes (Internal Controls) Regulations (Northern Ireland) 2005 (S.R. 2005 No. 567)
Section 90(2)(k) of the Pensions Act 2004	Article 85(2)(k) of the Pensions (Northern Ireland) Order 2005
Section 249A of the Pensions Act 2004	Article 226A of the Pensions (Northern Ireland) Order 2005