“Need to knows” from the General Code

January 2024

1. What’s changed from the draft Code

“Our new general code is an opportunity for governing bodies to make sure their schemes meet the standards of governance we expect, and savers deserve. It means there is no excuse for failing to know what TPR expects of them.” Louise Davey, TPR’s Interim Director of Regulatory Policy, Analysis and Advice.

As expected, the final Code closely resembles the draft in terms of scope and structure, consolidating 10 existing codes of practice. At 171 pages it is designed for online use. The Code remains in five sections (the governing body, funding and investment, administration, communications and disclosure, reporting to TPR), with some existing codes of practice sitting outside it and continuing to apply – including funding.

Governing bodies will need to consider what information to provide to members about the findings of the ORA, ESOG links are clearer, risk modules are better organised. The ORA will not need to be completed in one go, it can be done in stages, provided it is carried out in its entirety at least every 3 years.

The ORA purpose has been made clearer - it can, where applicable, build on existing processes, pointing to existing material to avoid duplication.

Schemes that started with an ESOG gap analysis based on the draft Code will find that work remains valid.

2. Key points

General

- Trustees should regularly carry out a skills audit to inform training and recruitment needs.
- The requirement to publish the remuneration policy has been removed. The policy should cover costs for activities that are paid for by the governing body, e.g. remuneration of service providers, but not be explicit on levels of remuneration.
- The risk management modules have more clarification, with the link between strategic objectives and risks being made a bit more clearly. Operational resilience is also introduced.
- The inclusion of E,D&I in places, e.g. recruitment and appointment to the governing body and in investment decision making.
- TPR also now refers to a requirement to invest mainly in regulated markets, rather than having any specific expectations on unregulated investments.
- Governing bodies are expected to identify the rights attached to their investments and consider their approach to voting and engagement, be familiar with their investment manager’s stewardship policies, monitoring and reviewing these regularly, as well as seeking to influence them, as appropriate, and seeking to establish engagement approaches with investee companies either directly or via their investment managers.
- Climate-related risks and opportunities should be assessed, even if reporting isn’t necessary.
- Cyber security remains important with a cyber incident response plan being required, with governing bodies having clearly defined roles and responsibilities for identifying and responding to cyber incidents. There is an expectation for governing bodies to understand their cyber risks, which means understanding and assessing vulnerabilities within the scheme and with service providers.

ESOG, risk management function and ORA

- The risk management modules have more clarification, with the link between strategic objectives and risks being made a bit more clearly. Operational resilience is also introduced.
- All pension schemes must operate an ESOG, including internal controls (the relevant section of the Pensions Act 2004 does not apply to some schemes e.g. public sector, master trusts and CDC).
- The ESOG covers the aspects identified in the table below, which should be subject to regular, timetabled internal review. This review may be carried out as part of the ORA. Otherwise, each element should be reviewed at least every three years, but not necessarily all at the same time.
- Schemes with 100+ members should have a risk management function, which facilitates the identification, evaluation, recording, monitoring, managing and reporting on risks.
- Governing bodies are free to choose who will perform the risk management function role.
- Schemes with 100+ members must complete a triennial ORA. The timing of the first ORA is within 12 months after the end of the first scheme year following the Code taking effect.
- A sub-committee of the governing body, the risk management function, or a third party can perform the ORA. Conflicts of interest should be effectively managed by those carrying out the ORA.
- It is not necessary for all elements of an ORA to be assessed at the same time. This can be done over the three-year period to the next ORA, as long as there have been no updates or changes to the system of governance or risk management and/ or no material changes to risks, which would require earlier assessment.
- Governing bodies who already undertake aspects of the ORA, e.g. risk assessment, will not need to duplicate this work. The ORA may refer to other relevant documents recording these assessments.

3. ESOG requirements

All pension schemes need to have systems of governance and internal controls that:

- provide the governing body with oversight of the day-to-day operations of the scheme
- include any delegated activities for which the governing body remains accountable
- provide the governing body with assurances that their scheme is operating correctly and in accordance with the law.

The system of governance must be proportionate to the size, nature, scale, and complexity of the activities of the scheme.

A system of governance includes anything that can reasonably be considered part of the operation of a pension scheme, a key feature of which is internal controls. Here TPR focuses on scheme administration and scheme management, how these are monitored and the safe custody and security of the scheme assets.

All pension schemes must operate an ESOG, including internal controls (the relevant section of the Pensions Act 2004 does not apply to some schemes e.g. public sector, master trusts and CDC).

The ESOG covers specific requirements included in 18 modules. 8 additional modules on internal controls and administration and management also apply to schemes required to maintain an ESOG, as shown in the table below. The elements of the ESOG should be subject to regular, timetabled internal review. This review may be carried out as part of the ORA. Otherwise, each element should be reviewed at least every three years, but not necessarily all at the same time.

The governing body should establish and maintain policies for the review of each element of the ESOG. These policies should be established before any review is carried out and reviewed at least every three years.

Management of activities	Organisational structure
• Role of the governing body • Meetings and decision-making • Remuneration and fee policy • Knowledge and understanding • Governance of knowledge and understanding • Dispute resolution procedures • Scheme continuity planning	• Appointment and role of the chair • Conflicts of interest • Managing advisers and service providers • Risk management function
Investment matters	**Administration and management**
• Investment governance • Investment decision-making • Investment monitoring • Stewardship • Climate change • Statement of investment principles	• Financial transactions • Record-keeping • Data monitoring and improvement • Receiving contributions • Monitoring contributions • Maintenance of IT systems
Internal controls	**Communications and disclosure**
• Identifying, evaluating and recording risks • Internal controls	• General principles for member communications

3.1. Internal review

The Governance Amendment Regulations 2018, which implemented IORPII into UK legislation watered down the requirement for an explicit internal audit function. Instead, they refer to: "the function which internally evaluates adequacy and effectiveness of the system of governance".

The Code says that governing bodies should ensure that the elements of their ESOG are subject to a regular internal review, according to an agreed timetable, which should assess whether each element is functioning as intended, and whether changes are required. This review may be carried out as part of the ORA. Otherwise, each element is to be reviewed at least every three years, but not necessarily all at the same time.

TPR does not expect schemes to have an internal audit function, but points to internal audit or independent/third-party assurance about controls where the governing body might consider it necessary.

4. Risk management function

As with the system of governance, the risk management function should be proportionate to the size, nature, scale and complexity of the activities of the scheme. In practice, the degree of separation between the risk management function and the governing body will be influenced by the size and internal organisation of the scheme and participating employer(s).

Schemes with 100+ members should have a risk management function, which facilitates the identification, evaluation, recording, monitoring, managing and reporting on risks. The function should also regularly review key risks, at an individual and aggregated level, and the interdependencies of those risks.

Governing bodies are free to choose who will perform the risk management function role. The person(s) can carry out any other key function of the scheme or be involved with the scheme in any other role.

Risks should be considered from the member perspective, particularly where members and beneficiaries bear risks.

5. ORA requirements

5.1. Requirements

The Trustee should prepare and document its first ORA within 12 months after the end of the first scheme year following the Code coming into force. Each subsequent ORA should be carried out and documented triennially. It should also be reviewed whenever there is a material change in the risks facing the scheme or updates or changes to its governance and/ or risk management processes.

The governing body should record the date of the ORA, the date of the next ORA and details of any interim reviews or updates that the governing body has carried out or plans to carry out.

The ORA may be carried out by a sub-committee of the governing body, the risk management function, or a third party. Those carrying out the ORA should effectively manage any actual or potential conflicts of interest between themselves, the governing body, employers, and service providers.

The ORA should be in writing, provided to all members of the governing body, who should consider what information should be provided to members about the findings, and signed off by the Trustee Chair.

The ORA is an assessment of how well the ESOG is working and the way potential risks are managed.

5.2. Assessment

It is not necessary for all elements of an ORA to be assessed at the same time, however each element covered by the ORA should be assessed according to a timetable. This can be done over the three-year period to the next ORA, as long as there have been no updates or changes to the system of governance or risk management and/ or no material changes to risks, which would require earlier assessment.

Governing bodies who already undertake aspects of the ORA, e.g. risk assessment, will not need to duplicate this work. The ORA may refer to other relevant documents recording these assessments.

Where services or functions are outsourced, governing bodies may choose to incorporate assurance reporting supplied by service providers into their ORA.

The ORA does not need to document the steps taken to mitigate identified risks. However, appropriate records of mitigations should be maintained as part of ordinary risk management processes.

As the ORA will identify the key governance risks facing the scheme, the governing body should incorporate the findings into its management and decision-making processes. The findings may be used to adjust or create new processes or procedures.

5.3. ORA documentation

The ORA documentation should cover:

- how the governing body has assessed the effectiveness of each of the policies and procedures covered by the ORA, and
- whether the governing body considers the operation of the policies and procedures to be effective and why.

Trustees should ensure that their ORA covers the effectiveness of, and risks arising from, each element listed below:

Policies for the governing body

- How the governing body is integrating risk assessment and mitigation into its management and decision-making processes, and
- The operation of policies relating to the role of the governing body, knowledge and understanding and governance of knowledge and understanding.

Risk management policies

- The operation of policies to identify and assess risks facing the scheme,
- The internal control policies and procedures for the scheme,
- Management of potential internal conflicts of interest, and those with participating employers and service providers,
- The prevention of conflicts of interest where the employer and governing body use the same service provider, and
- Continuity planning for the scheme and, where applicable, how it has performed.

Investment

- The Plan's investment governance processes,
- How investment performance is reviewed and monitored,
- How the governing body assesses investment risks relating to climate change, the use of resources and the environment,
- How the governing body assesses social risks to the Plan's investments,
- How the governing body considers the potential for depreciation of assets arising from regulatory or societal change,
- How the governing body assesses the protection mechanisms available to the Plan, including how these might apply and the risks of them not functioning as intended,
- How the governing body ensures the security of assets and their liquidity when they are required, and
- How the governing body assesses the protection of member benefits in the event of the insolvency of a sponsoring or participating employer, or a decision to discontinue the scheme.

Additional investment matters for DB schemes

- How the governing body assesses the scheme's funding needs with reference to its recovery plan, and
- How the governing body assesses the specific risks relating to the indexation of benefits provided by the scheme.

Administration

- How the governing body assesses the risks associated with the scheme's administration, with particular reference to financial transactions, scheme records and receiving contributions,
- Action the governing body takes to manage overdue contributions, considering the degree to which they represent material amounts or delays, and
- Risks posed by legal and regulatory change and court decisions.

Payment of benefits, where applicable

- How the governing body assesses operational risks, focusing on the risk to members and beneficiaries relating to record-keeping and payment of benefits,
- The governing body's management of risks relating to circumstances where accrued pension benefits may be reduced, under which conditions and by whom,
- The governing body's management of the risk of member benefits being reduced or altered, including on the insolvency of a sponsoring or participating employer or the cessation of the scheme, and
- Scams and the risk of members making poor choices.