The Pensions Regulator's General Code of Practice - Own Risk Assessment

In Depth

February 2024

Contents

Background

For nearly three years the pensions industry has known that the General Code of Practice (formerly known as the Single Code of Practice) is on the horizon. Following delays caused by the global pandemic and UK political developments in 2022 and 2023, the Code was laid before parliament in January 2024 and is expected to be effective by end March 2024.

Since the consultation on the General Code of Practice (the "Code") was launched in March 2021, we have been working with trustee boards to prepare for the Code, assessing existing practice against the requirement to have an "Effective System of Governance" (ESOG) and supporting the preparation for compliance with some of the new and enhanced requirements set out in the Code.

This In Depth considers the risk management aspects of the Code and the requirement for trustee boards to prepare an "Own Risk Assessment" (ORA).

1 In a nutshell

Governing Body

The Code applies to occupational, personal and public service pension schemes. As a result of this, the Pensions Regulator (TPR) has introduced a new term of "governing bodies". The term Governing Body refers to:

"Trustees or managers of occupational pension schemes, managers of personal pension schemes, and the scheme managers and/or pension boards of public service schemes that we regulate."

Throughout this document we have used the term trustees or trustee board.

As a result of requirements set out in EU Pensions Directive prior to Brexit, the Government laid down new governance regulations. All schemes are required to have effective systems of governance and internal controls, although the standards of governance required by law depends on the type of scheme.

This raised the bar for pension scheme governance as previous requirements under the Pensions Act 2004 required trustees of occupational pension schemes to have "adequate" internal controls. The governance regulations also provided that TPR must change existing codes of practice, incorporating the new governance requirements, and it prescribed a range of matters that the Code should cover.

The Code is a consolidation of ten existing codes of practice, incorporating the governance regulations in a streamlined online format.

Some existing Codes of Practice (in particular, the codes relating to Notifiable events (2), funding defined benefits (3), modification of subsisting rights (10), the material detriment test (12), the authorisation and supervision of master trusts (15) and CDC schemes (unnumbered)) will sit outside of the Code and continue to apply.

The Code divides its contents into 51 modules under 5 key headings.

- The governing body
- Funding and investment
- Administration
- Communication and disclosure
- Reporting to TPR

Status of Codes of Practice

The Code provides clarity on TPR's expectations in relation to the risk management of pension schemes, with risk management covered in seven modules of the Code. The Code introduces the requirement for trustees of occupational pension schemes with 100 members or more to produce an Own Risk Assessment ("ORA").

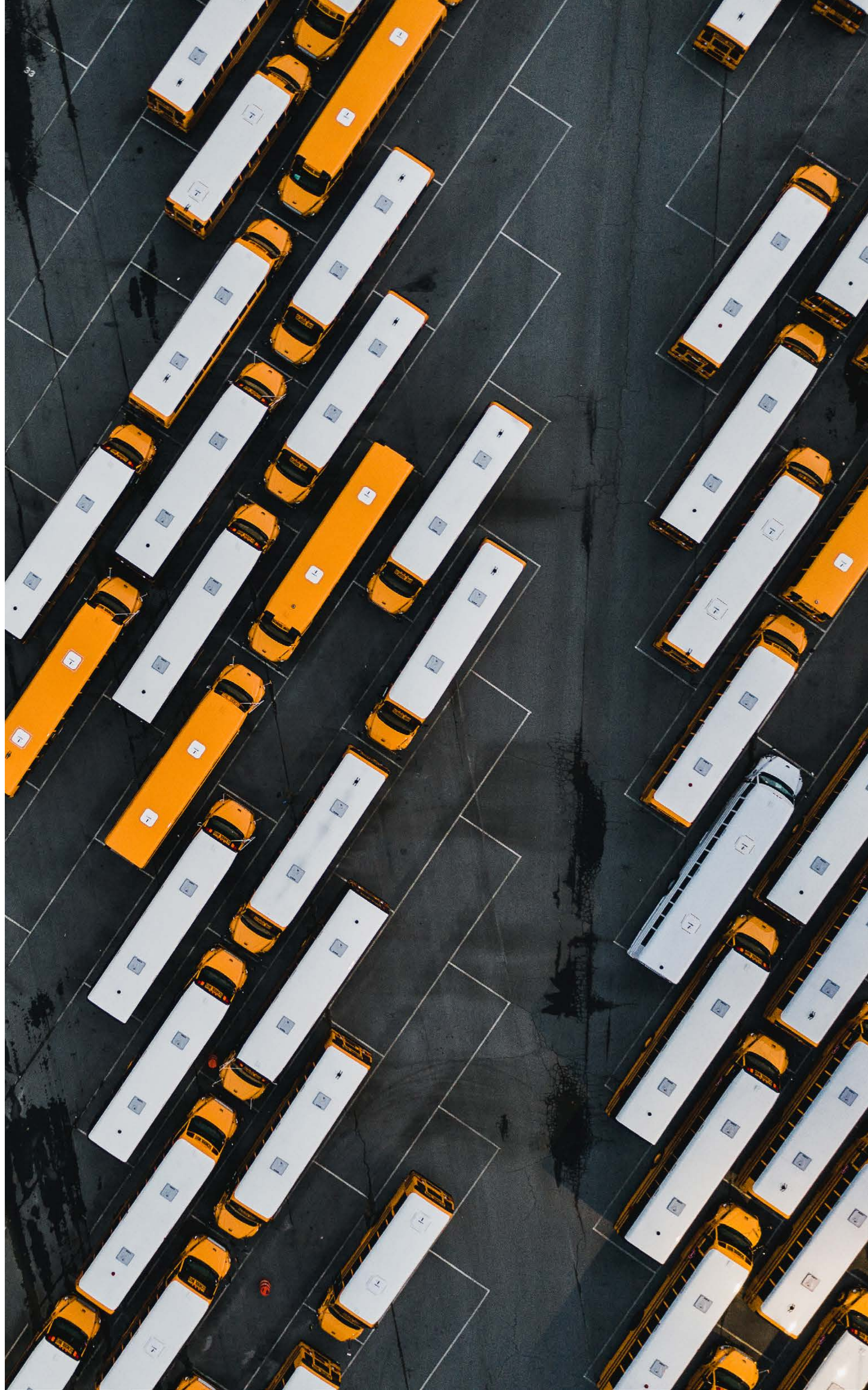
The requirements were adopted in Europe in 2019 and European pension funds of the EU Directive have now established their Effective System of Governance ("ESOG") and their ORA. We are able to draw on the experience of our EMEA colleagues in preparing UK pension schemes for the requirements of the Code.

Codes of practice are not statements of the law and there is not usually a direct penalty for failing to comply with them, but the General Code does set out TPR's expectations of how Governing Bodies should comply with their legal duties.

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 the Code of Practice will need to meet the underlying legal requirements, and a penalty may be imposed if these requirements are not met.

When determining whether the legal requirements have been met, a court or tribunal must take any relevant provisions of a Code of Practice into account.

If there are grounds to issue an improvement notice, or a compliance notice, TPR may direct a person to take, or refrain from taking, such steps as are specified in the notice. These directions may be worded by reference to a Code of Practice issued by TPR.



2 Preparing for your ORA

The following is a summary of the key aspects of the ESOG as they relate to the risk management framework and the ORA.

Requirements – Effective System of Governance

One of the primary aims of the Code is to improve the governance of pension schemes and have more consistent standards across different types of pension scheme, for example occupational DB and DC, personal pension arrangements and public service schemes.

The governance regulations introduced the requirement for trustee boards to establish and operate an ESOG. The ESOG includes anything that can reasonably be considered part of the operation of a pension scheme, including policies, processes and procedures in place to manage the scheme.

Each element of the ESOG should be reviewed to assess whether the policy is functioning as intended, according to a timetable established by the trustees. It isn't necessary for all elements of the ESOG to be reviewed at the same time, but reviews on each element should be carried out at least every three years.

The Code sets out that trustees should establish a plan for reviewing each element of the ESOG.

The ESOG should be proportionate to the size, nature and complexity of the scheme.

Aon recommendations

- Compile a checklist of the policies and procedures you have in place which form your ESOG.
- Understand whether you have any undocumented practices and supplement your current policies to fill any gaps in documentation.
- Consider when your policies and procedures were last reviewed and if necessary, review them to ensure they are up to date and reflect your current practices.
- Establish a rolling review programme for policies and procedures and include this in your annual calendar of activity.

Requirements – Managing risk using internal controls

Over the past few years, we have seen a growing focus on internal controls from scheme auditors.

A scheme's internal controls should be reviewed at least every three years, in line with the ESOG and ORA requirements. In addition, the Code requires trustees to undertake reviews of internal controls if there are substantial changes to the scheme or where it is identified that the control is not working to the standard required by law.

Trustees should document their internal controls and ensure that they:

- Include a clear separation of duties for those performing them, and processes for escalation and decision-making; and
- Require the exercise of judgement where appropriate, in assessing the risk profile of the scheme and in designing appropriate controls.

TPR notes that an internal controls framework isn't infallible and will not eliminate all risks of a pension scheme (for example, some investment risks may be accepted by trustees in their desire to seek returns on assets).

Internal controls

- **Arrangements and procedures to be followed in the administration and management of the scheme.**
- **Systems and arrangements for monitoring that administration and management.**
- **Arrangements and procedures to be followed for the safe custody and security of the assets of the scheme.**

Trustees should also understand that where functions or activities are delegated to advisers or service providers, the trustees retain legal responsibility for the scheme's internal controls. Trustees should seek assurances from their third parties that they are meeting their own standards for internal controls.

Aon recommendations

- Understand the internal controls you have in place and ensure they are documented in your risk register.
- Seek assurances from third parties associated with the scheme in relation to their own internal controls.

Requirements – Assurance of governance and internal controls

Assurance reporting is the process through which different processes and procedures of third parties are assessed. Trustees may obtain assurances from their third parties to assess whether they meet the legislative requirements, and the schemes own internal controls. The Code acknowledges the various assurance frameworks that may be suitable for pension scheme operations. The trustee board should understand the limits of the assurance and the scope of the assurance process relating to its internal controls.

Assurance reporting to the trustee may be provided by:

- Statutory audit.
- Internal audit (eg. via sponsoring employers).
- Assurance reports directly from service providers.
- Assurance reports commissioned by the trustee from an independent third party.

Aon recommendations

- Document the assurances relied upon in your risk register.
- Review the assurance reports provided by the third parties you have appointed.
- Follow up on any relevant actions arising from the assurance reports.

Requirements – Risk management function

Occupational pension schemes with 100 members or more should have a "risk management function" in place. The risk management function may be a sub-committee of the trustee board or an independent body that facilitates reporting to the trustee board. The Code states that 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 trustee board will therefore depend on the nature of the scheme (and the participating employers).

The risk management function is responsible for identifying, evaluating and recording risks and for the operation of the internal controls to monitor and manage scheme risks.

Aon recommendations

- Review your risk appetite and document in a risk statement.
- Identify and document the party which will carry out the risk management function.
- Document the terms of reference and reporting for the risk management function.
- Review your risk management framework to ensure it supports the risk management requirements under the Code.
- Review your risk register to ensure it captures the agreed risk tolerances and an audit trail to support the preparation of the ORA.

3 What is an ORA?

Under the governance regulations, schemes with 100 or more members that are required to establish and operate an ESOG must carry out and document an ORA. The ORA is an assessment of how well the ESOG for your scheme is working and the way that potential scheme risks are managed. This does not replace any of your existing risk management processes and is not intended to duplicate the processes already in place.

The ORA acts like a self-assessment by trustees of the various parts of their scheme governance and risk management framework. The ORA doesn't need to include detail of the steps taken to mitigate identified risks, but trustees are expected to ensure they maintain appropriate records of mitigations as part of its ordinary management processes. The ORA should document how trustees have assessed the effectiveness of their ESOG, whether the trustees consider the operation of their policies and procedures to be effective and the risk arising from each element of the ORA.

In order to meet the requirements of the Code and fulfil the expectations for the ORA, trustees may need to expand their existing risk management processes, but it is expected that most trustees will already undertake some of the aspects of the ORA as part of existing scheme governance.

The ORA should be proportionate to the size, nature and complexity of the scheme and should be documented, in writing and signed off by the chair of the trustee board.

Documenting the ORA

Schemes must prepare their first ORA within 12 months beginning with the last day of the first scheme year that begins after the Code becomes effective (expected March 2024). The ORA may be prepared by a sub committee of the trustee board, the risk management function or a third party and must be signed off by the Chair and made available to TPR on request.

The ORA is then required to be completed at least every 3 years.

The ORA does not need to be submitted to TPR, but TPR may ask trustees for a copy of their ORA as part of other TPR engagement with the scheme. TPR may consider failure to complete an ORA as an indicator of poor governance and it is possible that we will see auditors requesting to see the trustees' ORA as part of statutory audit processes.

There is no requirement for trustees to share the ORA with their membership. However, the Code says that trustees should consider what information to provide to scheme members about the findings of the ORA.

4 Risk Management cycle

Risk Management is an ongoing process requiring input from various parties connected to the scheme with oversight and overall management delegated to the risk management function under a terms of reference.

Typically, we would expect a risk management cycle to consist of the following stages:

Risk Management Function

Objectives and Risk Statement

Strategic and Operational Risks

Project risks

Emerging risks

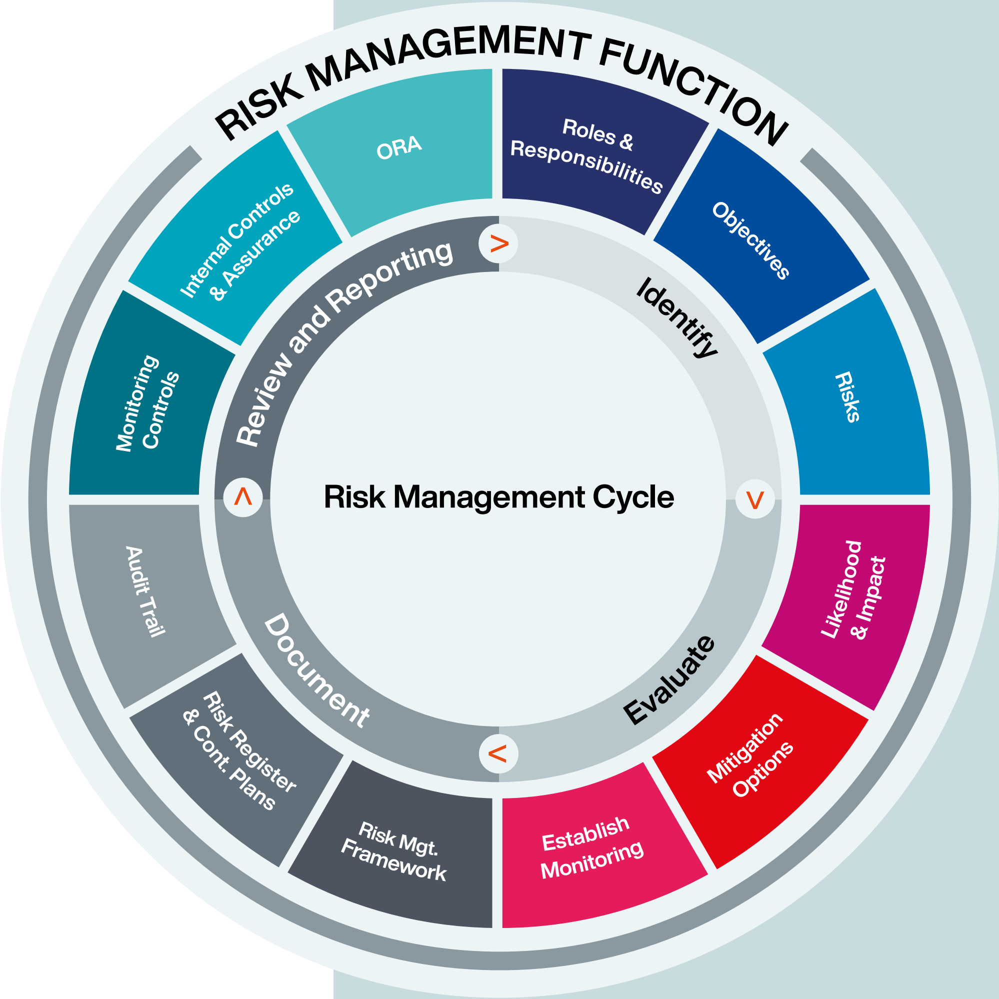
1. Identify

When considering risk, it is important to understand your objectives (strategic & operational) and to agree the trustee board's risk appetite and tolerances in relation to the key risks. This can be captured in a Risk Statement.

This stage also involves capturing the key parties involved in managing risk and how they will operate in practice, that is, your Risk Management Function. For example, will risk be managed at a Board level, will risk management be delegated to a committee or in-house resource?

Importantly within this section you will also undertake the process of identifying risks the scheme is exposed to. These risks should include all the key risk headings not just those that you feel able to quantify or mitigate. Consideration should be given to those risks associated with particular strategic projects the scheme is running and risks that could emerge in the future.

It is important that you are able to group your risks into themes to avoid an over lengthy document that becomes unwieldy.



Likelihood and impact of risks

Consider options for mitigation

Establish monitoring control

2. Evaluate

Once the risks have been identified then it is important to quantify those risks so that the exposure is understood. This can be done in a number of ways, whether through a risk register, modelling or other means, and it is likely to include a combination of likelihood and impact. Once you have this information you will be able to then cross reference and identify interdependencies between different risks.

Now for each risk you will want to consider whether there are mitigating actions that you could consider. Mitigating actions will include:

- Insurance, to pass on part or all of your risk to another party; examples include trustee indemnity insurance to mitigate individual trustee exposure.
- Protections to reduce the impact of a risk; examples include a contingent asset introduced to give trustees access to more security in the event of insolvency of the sponsoring employer.
- Detective measures to provide an early warning that a risk event may be materialising; for example, SLAs provided regularly to demonstrate that service levels are being met.

In many cases mitigating actions will be core to the running of a scheme. However, they will change over time as risks and scheme circumstances change, therefore it is important that trustees review these regularly as well as establishing monitoring controls.

Risk Management Framework

Risk Register

Contingency plans

Audit trail

3. Document

This stage is about creating the written summary of how risk management is run for your scheme. The risk management framework captures the roles and responsibilities and how risk is reported within the scheme structure. This includes who is involved at each stage of the risk cycle and how the trustees get comfortable that risk is being managed appropriately.

Contingency plans should also be put in place to ensure the trustees are able to respond quickly in the event that a key risk event materialises. The key risk events will vary by scheme. Common events include, but are not limited to, a cyber incident, a data breach, or a covenant event.

Each time the trustees complete a loop of the cycle the risk register should be updated to provide a clear audit trail on how risks are changing over time and evidence that they are being considered regularly. Creating an audit trail at this stage will make your ORA much easier to complete.

Some schemes will consider utilising risk software to make this stage of the process less time consuming.

Monitoring control (e.g. IRM dashboard)

Internal Controls

Assurance Reporting (incl. audit, provider reporting)

ORA (3 yearly)

4. Review & Reporting

Stages 1 to 3 of the risk management framework are intended to be sufficient and appropriate to manage the risks that the scheme is exposed to. Provided that they operate as planned, they should be sufficient. Stage 4 is essentially the additional level of oversight to ensure that Stages 1 to 3 are operating effectively.

The existence of this stage should not, and is not, used as a reason to cut corners within the previous 3 stages.

This part of the process brings together the risk management tools such as integrated risk management dashboards and internal control reports. This function may be delegated, via your risk management framework, to risk committees or others with the right credentials for the job.

You are also likely to want to utilise some form of assurance reporting to provide comfort in key functions, such as administration and systems. For those requiring additional assurance, here you can consider whether to employ an external auditor or whether the sponsor has an internal audit function that you can utilise to provide additional assurance reporting.

The final piece of this stage, is your look back and ORA of how well your governance systems are working and how potential risks have been managed. This is your opportunity to reflect and set out key areas to focus on for the following 3 year period.

Risk Management Function

As part of your risk management framework, clear roles and responsibilities should be established.

The Code sets out that schemes with 100 or more members should have in place a risk management function. This may be in the form of a sub-committee or an independent body that facilitates the reporting of risk management to the trustees. Responsibilities for identifying and evaluating risks may also be delegated to the risk management function.

The structure of your risk management function should be proportionate and appropriate for your scheme, to enable you to adopt strategies, processes and reporting procedures necessary to identify, measure, monitor and manage your risks effectively.

Clear levels of oversight should be in place, although for proportionality for the smallest schemes it is likely that the risk management function will involve all or most of the trustee board.

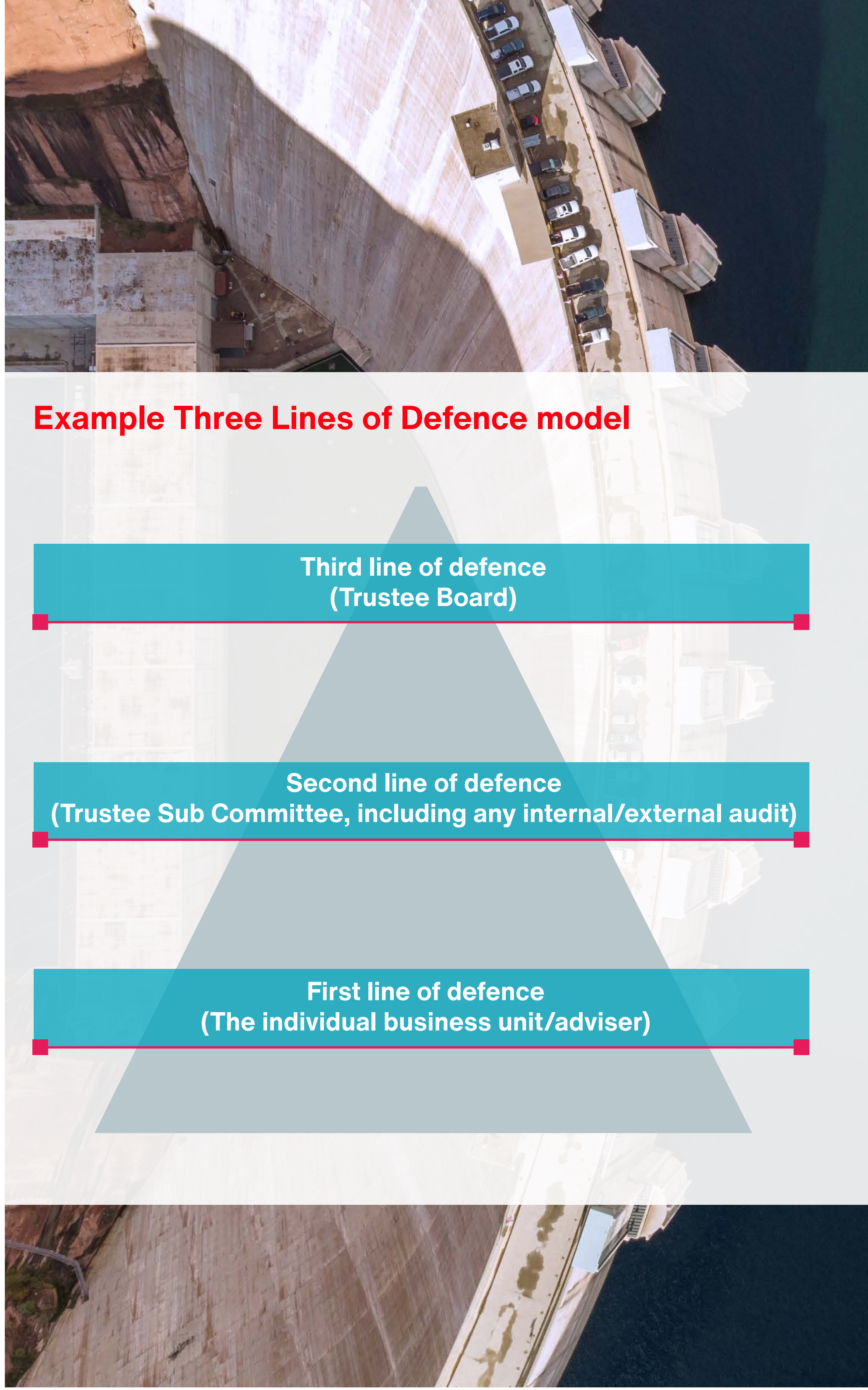
Our research shows that for the largest schemes it is more likely that individual roles are defined, and it may follow the "Three Lines of Defence" model to clearly identify the reporting lines for scheme risks. The diagram shows an example three lines of defence:

- **1st line of defence** usually sits with the owners of the specific areas who are closest to the detail of the process and activities;
- **2nd line of defence** is typically the risk management function which has oversight of all scheme risks; and
- **3rd line of defence** is the trustee board obtaining assurance that the 1st and 2nd lines of defence are effective.

In smaller schemes it is more usual to have 2 lines of defence. This usually consists of the 1st line of defence as the owners of the specific areas, followed by the 2nd line of defence which usually consists of the trustee board.

It is not necessary, nor possible, to eliminate all risks from a pension scheme. Trustee boards should have in place a risk management framework that allows them to identify risks and develop appropriate internal controls. As part of their risk management approach, trustee boards should assess all the risks faced by their scheme and define acceptable parameters for each by setting acceptable risk tolerances.

The range of risks will vary from scheme to scheme and may include matters such as investment, employer covenant, funding, administration, climate change, operational resilience, cyber security, communication, fraud and pension or decumulation options. Some investment risks may be accepted by trustees in their desire to seek greater returns.



Example Three Lines of Defence model

Third line of defence
(Trustee Board)

Second line of defence
(Trustee Sub Committee, including any internal/external audit)

First line of defence
(The individual business unit/adviser)

5 ORA checklist

The Code specifies the requirements for the ORA. This checklist will help to ensure you have covered everything.

		Complete
1.	**Documentation Format** • written assessment • date of assessment • date of next assessment • date of any interim reviews carried out or to be carried out in future • signed by the Chair	
2.	**Content** • how have you assessed effectiveness of the policies and procedures under the ESOG? • does the trustee believe the operation of the policies and procedures is effective and why?	
3.	**Risk management policies** • assess the effectiveness and risks arising from the following: • how the risks affecting the scheme have been identified and assessed • the effectiveness of internal controls and reliance on assurance reporting • management and prevention of conflicts of interest • the effectiveness of continuity planning for the scheme	

		Complete
4.	**Investment** • the investment governance process • how performance is monitored and reviewed • how have climate change and environment risks been assessed? • how have social risks been assessed? • assessment of potential depreciation of assets due to regulatory or societal change • how the protection mechanisms available to the scheme have been assessed and the risks of them failing • how is the security and liquidity of assets assured? • how is the protection of member benefits assessed in the event of insolvency of a sponsoring or participating employer or the decision to discontinue the scheme?	
5.	**Funding (DB Schemes)** • how do the trustees assess scheme funding needs with reference to its recovery plan and sponsor covenant? • how are risks associated with indexation of member benefits managed?	

		Complete
6.	**Administration** • how are the risks associated with the scheme administration assessed? including: – financial transactions, – scheme records and – receipt of contributions • how are overdue contributions managed? • How are risks posed by legal & regulatory change and court decisions assessed? • how are the operational risks relating to record keeping and payment of benefits assessed? • management of the risk of circumstances where benefits may be reduced • how are risks from scams and members making poor choices managed?	

AON

About

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Our colleagues provide our clients in over 120 countries and sovereignties with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.

Follow Aon on LinkedIn, X, Facebook and Instagram. Stay up-to-date by visiting Aon's newsroom and sign up for news alerts here.

aon.com

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

All rights reserved. aon.com. Aon Wealth Solutions' business in the UK is provided by Aon Solutions UK Limited (registered in England and Wales under registration number 4396810) and Aon Investments Limited (registered in England and Wales under registration number 5913159). Registered office: The Aon Centre, The Leadenhall Building, 122 Leadenhall Street, London EC3V 4AN. Tel: 020 7623 5500. Aon Investments Limited is authorised and regulated by the Financial Conduct Authority.

Contact Us

Lynsey Harri

+44 (0) 1372 733166

lynsey.harri@aon.com

Aon
3rd Floor
Epsom Gateway
2 Ashley Avenue
Epsom
Surrey
KT18 5AL