Are schemes ready for the new governance requirements on risk management?

April 2021

What are the new requirements on risk management?

In a nutshell, this is the translation of the EU's IORP II Directive to the UK, now forming part of TPR's consultation on the consolidated Code of Practice. It requires schemes to have **effective governance** that enables them to be sustainable in the long term. Part of that is **risk management**, proportionate to their complexity and risk profile.

The focus is on all risks faced by a scheme; the material, strategic, financial, external and reputational risks as well as operational risks, particularly those relating to outsourcing and cyber; the latter being key given the highly outsourced nature of pension scheme delivery.

One important new requirement is for trustees to complete an **own-risk assessment (ORA).** These should consider how well governance systems are working and the way potential risks are managed in the short-, medium- and long-term. Associated with this, is a requirement for schemes to have risk management and internal audit functions.

What is an ORA?

Any private sector scheme with 100 or more members will be required to conduct an ORA, within one year of the code coming into force. It starts with the **ORA policy** which will be approved by the trustees. This will cover, amongst other things:

- The scheme's risk profile, including its risk objectives; risk tolerance limits; consideration of the membership structure, funding requirements and recovery plan where relevant; information on outsourced activities and conflicts of interest.

The **assessment of risks** follows, which looks at the internal and external risks likely to affect the scheme from funding, investment, administration and strategic through to operational, compliance and expense risk. The focus is on forward-looking oversight - understanding what might change the risk profile of the scheme through future developments and emerging risk - as well as what's happening now.

The output of the assessment is the **results and action plan**. The results will provide a statement on the effectiveness of the scheme's risk management, looking at lessons learned during the exercise and providing forward-looking actions to improve risk management. The aim being to **improve governance** and inform the trustees' **strategic decision making**.

TPR expects the first ORA to be a considerable amount of work for trustees, after which it will become an annual process of review. TPR's consultation provides some clarity on what will be expected and we strongly suggest that trustees turn attention to this sooner rather than later.

It's not just spreadsheets and RAG status

Trustees should use risk management as an integral part of informed and effective decision making. It's key to good governance: understanding risks informs the strategy, helps clarify roles, responsibilities and delegations and enables trustees to seek and receive focused information and assurance that helps fulfil their oversight responsibilities. Risk management is about understanding what will hinder or prevent you getting to where you want to be and thus improving member outcomes.

A risk culture embedded into processes, ways of working, behaviours and decision making is what makes risk management effective. Strategic decisions are made in the context of risk and what's happening around you and coming towards you. Those operating the scheme should live and breathe it, as it's just part of the way they do their jobs. It's no longer just a risk register and an annual tick box exercise. There are some key things that trustees can do now to tackle risk effectively and be ready for their ORA:

- Agree risk objectives; what does risk management mean to you?
- Be clear on where you're heading as a scheme; your objectives and strategy so that you can identify risks that might prevent you from getting there;
- Determine how much risk you're prepared to take to get there; set your risk appetite;
- Agree risk materiality limits and define impact classification to support incident reporting and escalation;
- Set tolerances – parameters within which the scheme is operated;
- Assess risks and existing controls to test whether or not they are within appetite and if controls are effective;
- Agree risk ownership – clarify who is accountable for what;
- Align operational risks with strategic and 'top-down' risks, so that what's happening on a day-to-day basis supports the trustees' long-term aims;
- Ensure that you have policies in place that are key to integrating risk assessment and mitigation into management and decision-making processes (covering areas such as knowledge and understanding, identifying and assessing risks, internal controls and their assurance, managing conflicts of interest, continuity planning, stewardship etc.);
- Define the reporting necessary for oversight, to hold outsourced providers to account, and information required for decision making.

You might look at the list above and baulk at the idea of risk appetite and tolerance, uncertain of how to tackle these or what they mean. What's important is that trustees decide what these things mean to you. A good way to do that is to use examples from your own scheme and bring to life where your risks are, how you know you're mitigating them and how you know what you might be faced with in the not too distant future.

Risk management is often seen as too difficult, with lots of complex metrics and confusing terminology, because the focus for too long has been almost solely on financial risk management led by investment experts. Risks to members from an outcomes perspective and operational risks haven't been given the airtime they deserve. Risk management doesn't need to be difficult. If you make it about what matters to the trustees and members, what helps trustees make decisions and what keeps you out of trouble, you can make it quite simple.

Rosanne Corbett, Muse Advisory