The road to General Code

With most journeys, we usually have a clear idea of our destination, and how to get there. However, there are often challenges along the way. The road to the General Code is no different

The General Code of Practice (the code), formerly known as the Single Code, has suffered many delays. Originally expected in spring 2023, it's still yet to arrive. When it's published the code will be one of the most significant changes in occupational pensions in decades with new requirements around cyber security, so trustees must understand its requirements and get prepared.

Create a road to effective governance:
Even the most well-governed schemes will need some work to prepare for the requirements of the code, but complying with it shouldn't be rocket science; it's simply a redesign of the governance structure, including the introduction of a self-performed audit function.

Though implementing the code may appear daunting, it's crucial to remember the purpose behind it: **delivering enhanced governance that adds value and makes you think at the right times.** Enhanced governance translates to better outcomes for members, so it's important to not simply develop a system that leads to an annual box-ticking exercise. For example, a poor system may simply ask if there's a risk register in place. Meanwhile, a good system will stipulate when the risk register should be reviewed; ensuring all key risks are covered and mitigated as far as possible.

Get prepared:
To best prepare your scheme for the General Code, you can start by reviewing where it currently is. By assessing your current scheme's practices against the **effective system of governance** (ESOG) guidelines, you'll:

- understand how well your pension scheme already complies
- identify areas that need improvement; and
- pinpoint where a new policy or procedure is necessary.

Such analysis will also help guide you as the trustee, on where to prioritise and channel your efforts effectively. This is particularly important, given The Pensions Regulator's (TPR) guidelines stating that trustees must implement an ESOG that aligns with the size, nature, scale, and complexity of their scheme's activities.

While size shouldn't be a barrier to good governance, trustees of smaller schemes may understandably have concerns about addressing similar challenges with limited resources. However, they can take comfort that proportionality must be considered.

Speak to a professional:
It's the responsibility of pension trustees to ensure that their scheme is in compliant with the law and governed effectively. Seeking professional guidance can make this process more manageable offers trustees increased confidence.

At Vidett, our unique 'toolbox' can assist our clients in complying with the code, including:

- **Gap analysis** – our compliance review tool allows us to present initial results and an action plan to clients.
- **Template policies** – to comply with the draft code; implementing new policies and processes, which once drafted, accompany our progress summary report.
- **An ESOG planner** – to ensure each policy (once in place) is reviewed at appropriate times, including a risk register and dashboard to highlight key risks.
- **Training guides** – we've developed some for new trustees on key areas they should know about. Our equity, diversity and inclusion (EDI) guide is a prime example, it's not currently an area covered in the code but is something we want embedded to help optimise all trustee boards; building on existing work embracing TPR's EDI guidance to take the lead in conversations on EDI supporting our clients.

Prioritise essential policies and processes:
The General Code has been delayed, but there is still plenty that trustees can do in preparation for it. We recommend putting in place top priority policies and processes, such as a cyber security and incident response plans.

The high-profile cyber issues that impacted Capita's systems earlier this year were a timely reminder for all pension trustees and trustee boards to take stock of their IT security and data protection policies.

The loss of personal member data from a cyber-attack or denial of services through disruption to systems can be costly to members through the inability to settle benefits or pay pensions, as well as to trustees through potential fines from the Information Commissioner's Office (ICO) or TPR.

Pension trustees, as data controllers, have a legal duty under the UK General Data Protection Regulation (GDPR) to have 'appropriate technical and organisational measures' in place to process data securely. This 'security principle' extends to the processing of data by each of a pension scheme's data processors. **A cyber security policy setting out cyber risks and the management of them, is therefore the bare minimum required by trustees to put in place.**

TPR requires trustees to build cyber resilience into their systems to protect members against cyber risk. Their guidance on cyber security requires trustees to assess and understand the risks; putting controls in place; monitoring and reporting on those risks and controls. TPR also urges pension trustee boards to understand the potential cyber risks faced by their scheme; putting in place appropriate measures to assess and manage cyber risks.

If a cyber incident or data breach occurs, regulations require data controllers (trustees) to take immediate action and report matters to the ICO (within 72 hours), TPR and affected members without delay. To do so, trustees will need their policies and procedures in place.

Improve cyber security:
Here are our top tips to start doing right now:

- Assess and understand your scheme's 'cyber footprint' and any vulnerabilities
- Ensure roles and responsibilities of trustees, data processors and scheme managers are clearly defined and understood
- Speak to your sponsor as it's important to understand their cyber security and you may want to align your plans with their cyber policies
- Add cyber risk to your scheme's risk register and review it regularly
- Have back up plans in place e.g. in relation to the operation of pensioner payroll
- Ensure your data processors have robust internal controls in place to deal with cyber incidents and data breaches
- Put in place and test your incident response plan so that any cyber incidents or data breaches can be dealt with and how/when operations can resume
- Ensure reporting deadlines and processes are known so any incidents can be reported
- Record cyber incidents and data breaches so action can be taken to mitigate, reduce and learn from them
- Undertake regular training for all staff to understand cyber risks, new regulations and guidance

Reach the finish line
TPR's new code will introduce a new module relating to internal cyber controls, that will sit alongside the ESOG that trustees need to have in place and demonstrate compliance with. With the new code expected to be published soon, we can help you navigate and review your existing cyber security policies; ensuring they're appropriate and meet the code's requirements as you arrive at your final destination.

Written by Vidett client director, Simon Riviere