

# Getting ready for the Code: The risk management function and the use of internal audit

Welcome back to the Muse series **Getting ready for the Code**, where we are sharing tips and tools to help you navigate the Code. Get in touch to find out more at [governanceservices@museadvisory.com](mailto:governanceservices@museadvisory.com).

In this update we'll look briefly at how the risk management function can add value to your scheme, and the potential value of independent sources of assurance on controls, such as internal audit.

We will put out a further article once the Final Code is published, as TPR will say more about how they expect Trustees to take a proportionate approach on the risk management function and internal audit.

Currently the Final Code is expected to be laid in September when Parliament is in session, coming into force after 40 sitting days so we expect mid-November to mid-December – barring a snap UK election!

As we always flag, TPR say in the introduction to the Draft Code and have stressed since: "Governing bodies need to use their judgement as to what is a reasonable and proportionate method of ensuring compliance ...". In the legislation, proportionality relates to scheme size, scale, complexity and resources.

August 2022







## What do we know so far about the risk management function?

The Code says that it needs to be in place for schemes with 100 members or more and it:

- Should be proportionate to the scheme's size and internal organisation, as well as nature, scale and complexity of their activities.
- May be a committee of the governing body, or an independent body that facilitates reporting to the whole governing body or the relevant sub-committee.
- Might be given delegated responsibility for identifying and evaluating risks and/or internal controls.
- Should be structured in such a way as to enable the scheme to adopt strategies, processes and reporting procedures necessary to identify, measure, monitor, and manage risk.
- Should also regularly review the risks, at an individual and aggregated level, to which the scheme is or could be exposed, and the interdependencies of such risks.

### **How can the risk management function help?**

-  *It can provide an objective view of your risk management approach*
-  *It can check that the risks you are spending time and effort on are the right ones*
-  *It can help you understand your risks and the impact they'd have on your scheme, so that you can check your controls are good enough and are working well*
-  *It can ensure the right issues are escalated and that important things stay on the radar and don't get missed*
-  *It can give you meaningful reporting to oversee BAU and keep decisions on track to meet your objectives*

## On the risk management function and getting value from it

The central idea behind the risk management 'function' is to help trustees govern scheme risk well and know where the accountability for mitigating risk lies. The trustee board will always be responsible overall for risks the scheme is running.

### **A delegated function?**

In more complex schemes with committees and/or those with some trustee pensions management resource, the way the board oversees risk and what risk work is delegated will vary. The risk management 'function' aims to bring some structure, to help boards be clearer about risk delegations and reporting.

If the risk management function is delegated then this needs a clear remit, with the aim of ensuring the board is well sighted and advised on risk, board level risk reporting is fit for purpose, risk is linked to decision making and it is clear where the day to day work on areas of risk and controls is being done.

If the risk management function sits within a committee (such as Audit & Risk or Governance), there will be a co-ordinating role to avoid gaps and overlaps in risk governance and to maintain an overview, so the committee can advise the board on how risks are trending and ensure the risk escalation policy to the board works effectively e.g. on flags for investment triggers, serious data events, TPR breach reports.

### **A simpler function that stays at the board?**

Equally many scheme Trustees, perhaps especially at the mid to smaller end, will mainly want to ensure that their risk register is relevant and manageable as it's the key document on risk that they regularly review. In these situations the function typically stays with the board to ensure risk reporting and the ways risks are identified and being managed stay fit for purpose, with providers and advisers aligned to this.

### **Getting value from what you do on it – focusing on the right risks**

Starting with the end in mind enables you to get value from how you identify and manage risk and helps you to judge what's proportionate for the risk management function you need and who operates it.

Considering these three questions gives you a top-down perspective on where your main risks really lie and helps to check the regulatory 'musts' are covered in a sufficient way for the scheme to be compliant.

**What MUST we do for compliance**  
**What, for our situation, is a proportionate response?**



Having a good sense of where you are going with your scheme is important – you may have set objectives, you may have an overall view of where your course lies with the sponsor and be working on your long term DB funding and scheme data journey, or for DC, on your future plans with the sponsor.

That middle question ‘what could knock us off course’ is the key one here: risks are events that, should they occur, will lead to different outcomes and/ or timings, with knock on effects elsewhere.

So ‘risks’ can be problems that get in the way, delay things, or make things a lot worse than you expect. Risks can also be opportunities that could speed things up or improve things. It’s not all downside.

The point is how well the trustee board stays sighted on these, how well risks are mitigated, and how ready the board is to respond when something unexpected (inevitably) happens.

Working out whether you’ve got the right major risks reflected in your risk register and how well you and the sponsor (and for some risks, the scheme members) could tolerate those risks is important. It can prove to be very insightful work, and helps the board to ensure all parties are on the same page.

This approach also helps the board scan the horizon on risk more effectively engaging on this well with the sponsor/ Company, and as relevant in your work with scheme members.

You will typically find your board risk register becomes a lot shorter and that you can also have a better conversation with advisers and service providers about scheme aims, key risks and how to manage them.

You can then be clearer on what information is most useful to you to fulfil your oversight responsibilities and take decisions: advisers and service providers can help you to do the heavy lifting on risk with papers for meetings clearly linked to the key risk/s that are being addressed, with timely updates and escalation.

This way risk becomes a backbone of how you run the scheme and make progress for members. And risk is not ‘the boring report with too much in it’ (sic!) you look at after lunch just before the meeting ends.

## Independent assurance on controls and use of internal audit

On internal audit (IA) and a functional IA role, TPR does not expect an appointed internal auditor per se, and again we anticipate the Final Code will be a bit clearer on this. Many schemes will have good existing sources of assurance on controls, including service provider AAF reports, to evidence and review as BAU.

There will be a need to consider if there are specific areas where it would be of benefit to get independent assurance to give the board additional comfort on important aspects of the system of internal controls. One example might relate to digital and cyber risks and controls as it’s a fast moving and technical area, which is on TPR’s radar and features in the Code.

Most trustees will seek to rely on their service providers’ AAF01/20 assurance reports and related internal audit work commissioned by the provider. TPR wants trustees to understand and use these. Our recent articles in this series on assurance and on reporting considered more on this area of oversight assurance.

The available sources of IA assurance could reasonably differ depending on the subject matter – TPR are looking for independence, pensions expertise and a lack of role conflicts in IA assurance work. This is why TPR don’t want trustees to primarily rely on a sponsor’s IA team/ service or a Trustee’s statutory auditor.

Some large, complex schemes will choose to put an IA service in place to review controls on a rolling basis in line with an agreed IA plan (in a similar way to IA plans for a corporate sponsor). The very largest schemes are likely to have IA resource in a Trustee-facing role in-house.

Trustee practice in these Code areas will evolve and over time TPR’s expectations will become clearer. We would also expect more services providing independent pensions IA to trustees to become available.



## Muse Advisory's 'Getting Ready for the Code' series

Contact Rosanne, Jo, Julia or Barry for practical help and independent advice at [governanceservices@museadvisory.com](mailto:governanceservices@museadvisory.com)

Our next article will look at Contingency and Continuity planning.

