Getting ready for the Code: sources of assurance

How much assurance do you need?

Welcome to the Muse series Getting ready for the Code, where we are sharing tips and tools to help you navigate the Code and Own Risk Assessment (ORA) requirements. Get in touch to find out more at governanceservices@museadvisory.com.

This fourth article is a practical look at your sources of assurance.

Why does assurance matter?

Having identified the controls you need to manage your risks; the next step is to determine how you gain confidence that those controls are in place and are effective. Being able to answer the "how do you know?" question, is really what assurance is about – knowing the right question to ask and seeking the right information to answer it well.

Assurance tells you the extent to which your controls are effective at managing your risks, helping demonstrate that controls have been designed well, implemented and are operating as expected.

Receiving appropriate and timely assurance means you can take action when things aren't working quite as they should be, or ask questions to get a better understanding of the controls in place, particularly where they sit within outsourced providers.

Good assurance will:

- reduce the likelihood of surprises, financial shocks or operational errors
- enable increased levels of delegation
- demonstrate compliance with legislation and regulations.

April 2022

How will we know we have an effective system of assurance?

- ✔ *We know who is managing each of our controls*
- ✔ *We know each of our controls is effective and has been implemented*
- ✔ *We know how the control owner will demonstrate the controls are being practiced on a day-to-day basis*
- ✔ *We know how and when the effectiveness of our controls will be independently reviewed*
- ✔ *We know the strength of assurance provided*
- ✔ *We receive regular reporting on the effectiveness of the management of our controls*
- ✔ *We know our assurance gaps and what we need to do to plug gaps*

If you don't have assurance that a control is being applied and is effective, you may be exposed to more risk than you realise and more risk than you want.

So, how much assurance do you need?

Understanding the amount of risk each control is managing, and the type and purpose of controls you have in place (e.g. manual versus automated), allows you to be proportionate in the level of assurance you seek around each control's effectiveness.

Where do I get assurance? When might I need more assurance?

Your trustee 'first line of defence' is the management controls put in place by the team or provider you've identified as the risk control owner. Trustees need to consider whether the information received from them gives sufficient comfort i.e. assurance, that controls are fulfilling their purpose and are adequate in mitigating risk to an acceptable level: what is and isn't working well that we need to know?

For example, whether the information demonstrates a documented process is in place, being followed as designed and having the expected impact and whether it is identifying when things are going wrong. Administrators and fund managers have many such processes, and provide AAF 01/20 assurance reports.

Where assurance is sourced by the risk control owner is it enough, to give the trustees comfort that things aren't going wrong and to answer your scheme's own control questions? Does it tell you enough about the specifics or is it blanket information in an AAF 01/20 designed for assurance on the provider's main systems and processes, rather than those used for your scheme e.g. if you are on an older administration system. Then what else might you need to know about your key controls and how can you find out?

This is where a third party such as internal audit can be useful, helping to lift up the bonnet on controls. And external audit can give assurance on key financial reporting controls. We look at 'third line' roles below.

Do I also have any 'second line' assurance? What is it and how do I use it?

You have a second line if you have roles in your governance structure that are separately responsible for overseeing the system of controls operating in their function – heads of risk, legal, governance, compliance are typical examples in large schemes, with independent reporting lines into trustee committees and the board. The Secretary is an example of a second line role most schemes have in place.

The trustees can place reliance on the additional level of assurance reporting these roles provide, on keeping their function's risk framework up to date and overseeing operation of the function's controls.

TPR envisages a risk management function as part of the ESOG under the Single Code and this will form a second line role in your structure, depending on where you decide to assign the role.

We have limited resources, is internal audit necessary? When is a 'third line' used?

Internal audit provides independent and objective assurance on the effectiveness of controls. It is part of the 'third line of defence', as is external audit. TPR will not make internal audit 'compulsory' in the Code. Some schemes already use internal audit and we anticipate more will as they review risk management.

Management controls, however well intentioned, aren't independent or without bias; it's like marking your own homework. When a team or provider is too close to the detail, they may have blind spots, be overconfident, or they may miss opportunities for improvement. Providing assurance, finding weaknesses to rectify in key controls, or identifying opportunities for improvement, are the benefits of using an independent party such as internal audit, to assess and report on those controls.

Looking at controls in key areas of risk on a cyclical basis is a typical way of planning internal audit work.

A number of trustee service providers operate internal and/or external audits over their key controls. The extent to which these can also provide your trustees with assurance will depend on the remit of any internal and external audits your providers undertake, in particular:

- whether the processes and systems used by your own scheme are covered within those audits, and
- the extent providers are willing to share the relevant aspects of audit reporting with their clients.

On that second point, it can be the case that bundled service providers used by smaller schemes limit the extent to which you can 'get behind' their standard stewardship reporting. TPR's view appears to be that the existence of standard assurance reporting and evidence you show of working with it and monitoring risk trends for your own scheme should be sufficient for the ESOG and ORA, to stay proportionate.

Do check whether scheme processes, especially any bespoke or scheme specific requirements, will be covered by the provider's audit scope with findings automatically reported to the Trustee.

I've heard of assurance maps – what are they? Do I need one to keep track?

Done well, assurance mapping brings together the different assurances received for a risk and control area. An effective assurance map will tell you where key controls are being managed, the assurance you receive and the sources of that assurance, as we've touched on above.

The map doesn't need to be overly complicated or cumbersome to set up or to maintain. It can be a high level RAG-rated table on one or two pages, or something more granular depending on your needs. It's something you can develop over time.

An assurance map helps you focus on key risks you have less appetite for, such as payment errors or misdirected investment instructions, and where things are changing such as in areas of scheme operations or cyber controls, when the trustee board will typically want increased comfort and sometimes expert independent assurance that the right controls are in place and working as needed.

A good assurance map will also allow you to identify gaps or weaknesses and also eliminate assurance activities that add little or no value, thereby saving cost and keeping things proportionate. Where a committee is owning the oversight of the system of controls to report on to the trustee board, such as an audit and risk committee typically might, an assurance map can become a central committee tool.

The governance benefits

You want to have effective and timely assurance around your controls, so that you know that your controls have been implemented, are being used in practice and are effective in managing your risks.

Assurance reporting enables you to be on the front foot in identifying gaps and addressing issues.

The ORA is an assessment of your system of governance – assurance helps you determine whether your controls are in place, being followed, and are effective in managing your risks.

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**

Knowing your sources of assurance and getting the right information to know that your specific risks are being managed is a key part of the ORA and Code requirements.

Our next article will look at effective reporting and taking action.