Getting ready for the Single Code: Continuity and contingency planning

How resilient are you?

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

This eighth article is a practical look at continuity and contingency planning, how to plan for and respond when things go wrong.

Most schemes will have tested their business continuity planning and revised it during the COVID-19 pandemic. The ability to work and access systems remotely remains a way of working for many schemes.
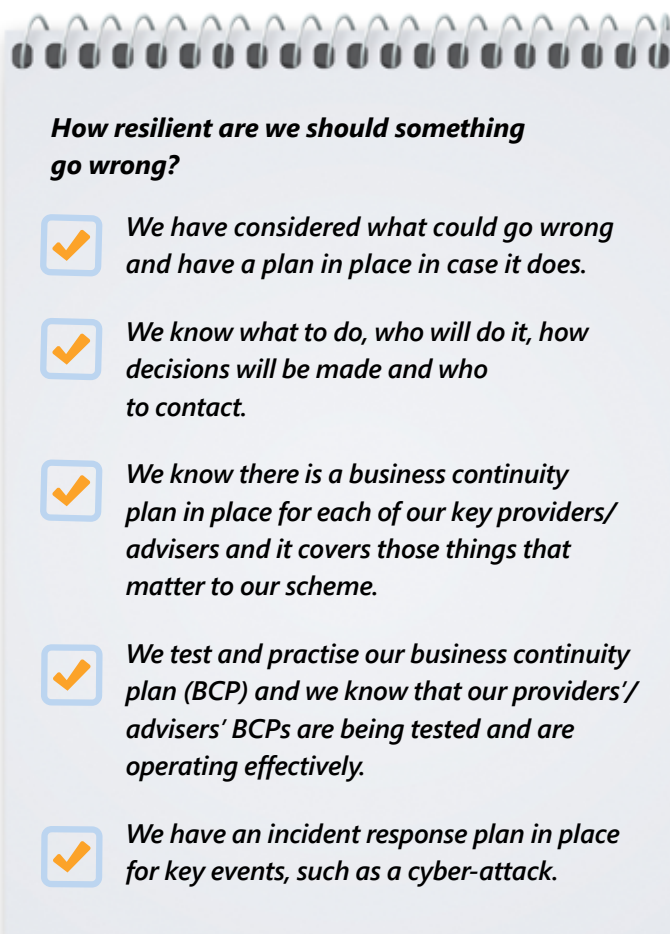
Business continuity plans are a requirement of an Effective System of Governance (ESOG).

What is business continuity planning?

Business continuity planning is being proactive to ensure critical scheme operations are maintained during a serious event/ significant disruption. Resilience is key.

It is being prepared for incidents that could jeopardise the trustee's ability to meet critical activities, such as payroll, or making time-sensitive strategic decisions.

It is distinct from disaster recovery, which looks at re-establishing vital infrastructure and systems, focusing on IT, to support critical scheme functions.

How resilient are we should something go wrong?

☑ We have considered what could go wrong and have a plan in place in case it does.

☑ We know what to do, who will do it, how decisions will be made and who to contact.

☑ We know there is a business continuity plan in place for each of our key providers/ advisers and it covers those things that matter to our scheme.

☑ We test and practise our business continuity plan (BCP) and we know that our providers'/ advisers' BCPs are being tested and are operating effectively.

☑ We have an incident response plan in place for key events, such as a cyber-attack.

What does a BCP look like?

A BCP can be comprehensive, or principles-based. It should set out what to do when faced with a variety of incidents, who will be responsible for which activities and contact information.

It might also have an escalation plan and decision tree to assess the impact of an event and agree immediate actions.

What do we need to think about when drafting our BCP?

Trustees are most likely acquainted with administration BCPs which focus on recovery of IT systems and data to maintain administration services, critically payroll.

A trustee-specific BCP focuses on the trustee's own governance arrangements, particularly those that will be relied upon in an emergency, e.g.:

- Remote working of Trustees and pensions support
- Quorum for decision making at short notice
- Trustee and resource availability and roles in different scenarios
- Succession planning
- Ability to sign documents in short timeframes
- Reliance on advisers/providers and support provided.

Those schemes impacted by last year's 'Mini-budget' and the liability driven investment (LDI) fall-out may have had to consider the above at an unprecedented pace.

In your BCP, you will want to consider:

- What decisions are needed?
- What advice is required before a decision can be taken?
- When does a decision need to be taken by?
- What are the appropriate delegations to aid speed of decision making?
- Who else needs to be communicated to e.g. TPR, HMRC, the Company, members?
- Who needs to be involved to implement the decisions?

What about providers and advisers?

BCPs of advisers and providers should set out how they would provide ongoing services and support and be able to provide appropriate resources to the scheme.

How often are the BCPs of other providers, investment managers, custodians, and advisers reviewed and checked for efficacy?

Trustees, as part of their ORA, will want to understand what assurance they receive that BCPs are not just tested regularly, but lessons learned implemented and circumstances relating specifically to the scheme factored in.

How does a BCP help us know we are resilient?

Resilient schemes have considered how they will prevent and prepare for an event and will be able to recover if/when it occurs. Some schemes have crisis management plans in place or material events guidelines, which are broader and include business continuity and response plans for a range of events. Others have plans specific to their risk exposure, e.g. a weak covenant and vulnerable employer, whatthey would do if the sponsor failed overnight.

The BCP is an opportunity to look for any potential vulnerability and manage it effectively.

Scenario testing and planning with advisers and providers is a good way to test 'what-if' situations.

Going back to the LDI situation, many trustees will have tested investment strategy sensitivity to market changes. However, only a few scenario tested for a 1 in 300 year event. How many, though, would have tested the governance and operational aspects when needing to take such quick action.

Contingency planning

Investment and funding contingency planning is common place for defined benefit schemes as part of long-term strategy setting.

Less scenario testing is undertaken in respect of governance and Trustees being able to operate and make decisions. It can be a helpful exercise to think about events that could occur, the impact they would have and the mitigations required to limit the impact.

Trustees also might benefit from considering how they would communicate in these different situations, to whom and when. Some schemes undertake 'war game' scenarios, collating a bank of template communications ready to use.

The governance benefits

- Being equipped to respond to an event immediately in the right way, with the right support, with no unintended consequences.

- Being able to maintain ongoing services to members with as minimal disruption as possible.

- Learning lessons and applying them for the future, to be more resilient.

Whilst the scenario testing might not match what actually happens if/when an event occurs, trustees practising what to do if business is disrupted will be much better placed than those who have never thought about it.

What is the Pensions Regulator looking for?

Schemes should develop and implement continuity plans to ensure that operations can be maintained in the event of a disruption to activities. Governing bodies should:

- seek to ensure continuity and regularity in the performance of the activities in the scheme

- have a resilient business continuity plan (BCP) that sets out key actions in case of a range of events occur that impact the scheme's operations

- make sure member data and general scheme administration are included in the BCP

- ensure advisers and service providers also have a BCP in place to maintain services to the scheme

- choose how to rely on reports and information about their service providers' BCP arrangements

- set out roles and responsibilities within the plan, and agree these with service providers

- regularly review process documents and maps, particularly after system or process change

- prioritise scheme activities in the event of the BCP being triggered, for example pensioner payments, retirement processing and bereavement services

- ensure continued access to resources, services and communications with key parties

- have an awareness of the timeframes required to bring new resources on board

- understand what contingency is in place to mitigate any under-resource due to, for example, increase in work volumes or the loss of staff

- seek to identify any events which may reasonably occur that may require additional resources.

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

Contact Rosanne, Jo, Hana or Barry for practical help and independent advice at **governanceservices@museadvisory.com**

Effective continuity planning is a key part of the ORA and Code requirements.

Our next article will look at completing the ORA and using the ORA findings.

Gap analysis of Trustee policies, scheme docs and processes

Completing the ORA and using the ORA findings

Identify and understand your risks

Contingency and continuity planning

Trustee Objectives and Strategy

ORA toolkit

Understand your controls and their effectiveness

Risk Management Function and Internal Audit

Know your sources of assurance

Reviewing the ESOG

Effective reporting and taking action