Pensions Audit Sub Committee

2.00pm, Tuesday, 3 December 2024

Business Continuity Management

Item number 6.5

1. Recommendations

The Pensions Audit Sub Committee (Committee) is requested to:

1.1 Note the contents of this report.

Alan Sievewright
Chief Finance Officer

Contact: Nikola Brown, Business Continuity & Supplier Manager, Lothian Pension Fund

E-mail: companysecretariat@lpf.org.uk | Tel: 0333 996 1900

Business Continuity Management

2. Executive Summary

2.1 There are regulatory requirements to have business continuity management (BCM) in place as well as good business practice.

2.2 An Internal audit (conducted in 2023) identified widespread gaps in LPF's current arrangements.

2.3 LPF's BCM will align with the International Standard for Business Continuity (22301:2019). There are many benefits to this (see 4.6 and 4.7) including its use as a vehicle to achieve effective BCM.

2.4 A risk-based BCM Programme is now in place and will be managed by LPF's dedicated BC & Supplier Manager. See Appendix 1 for a programme summary.

2.5 The programme encompasses all 21 Audit recommendations (see Appendix 1 and Appendix 2).

2.6 Arrangements for all known critical services will be in place by December 2025.

2.7 Implementation of the full programme is expected to take between two to four years with clearer timeframes confirmed as implementation progresses (see Appendix 1 for programme summary).

2.8 The latter part of the programme focuses on embedding, consistency and improvement.

2.9 Implementing effective BCM will require a time commitment from colleagues. Resource requirements will be clarified as knowledge is gained during early stages of the programme.

2.10 The aim is to reflect good practice, yet be proportionate.

3. Background

3.1 LPF has a regulatory responsibility to have appropriate BCM arrangements in place as documented by the Pensions Regulator (TPR) and in the Financial Conduct Authority's (FCA) Handbook, for LPFI activities. The Handbook also contains additional guidance on business continuity which it recommends organisations should follow as good practice.

3.2 Robust BCM minimises the impacts of a disruption by enabling the organisation to respond and recover quickly and effectively. It enables service areas to continue delivery of their critical activities, supports effective risk management, provides

assurance to stakeholders and strengthens the organisation's ability to achieve its vision and values with confidence.

3.3 An internal audit of the Fund's business continuity arrangements was conducted in 2023, which used ISO22301:2019 as the benchmark for good practice. The Audit Report concluded that arrangements offered 'limited assurance' with 'significant gaps, weaknesses or non-compliance'. It contained a wide-ranging set of recommendations aimed at building effective BCM.

3.4 A new Business Continuity & Supplier Manager role has been created to help build robust BCM processes, meet regulatory requirements and embed a culture of resilience.

4. Main Report

How do we do enough, but not too much?

4.1 To determine the approach and future shape of LPF's BCM, we have clarified what we are aiming to achieve, namely:

- Ensure resilience of our critical services.
- Meet LPF's regulatory obligations.
- Support effective risk management.
- Represent good practice.
- Provide assurance and confidence to stakeholders.
- Be proportionate to the organisation's context, size, type and complexity.

4.2 The maturity model at Appendix 3 is a useful tool to determine what 'proportionate' looks like. In addition, it can reflect the realities of introducing change, avoid unrealistic 'big bang' planning and provides a way to manage effort in different areas aligned with risk-based prioritisation.

4.3 Using the maturity model in Appendix 3 as a guide, LPF is aiming to achieve Level 4 (*Established*) i.e. has robust arrangements in place but is not sector-leading. Our current state of readiness, indicated by the Audit Report, is Level 2 (*Developing*) with "some arrangements in place but key elements still to be developed".

How do we get there, and how do we know when we've arrived?

4.4 The FCA Handbook documents what the organisation must achieve (rules) only in general, high-level terms. It also contains some additional good practice guidelines, but does not provide detail on how to accomplish an effective BCM system or what it looks like.

4.5 LPF therefore plans to align with the International Standard for business continuity (ISO22301:2019) and use it as a 'vehicle' to provide concrete direction and clear standards.

4.6 ISO 22301:2019 is a whole system approach which will help develop appropriate arrangements and ensure they are maintained and continually improved. In addition:

- International Standards are recognised internationally across all business sectors providing assurance and confidence to stakeholders.
- ISO 22301 will support LPF to meet its regulatory requirements and is specifically recommended by The Pensions Regulator.
- Internal Audit recommends adopting the Standard and used it as a benchmark to conduct the audit.
- The City of Edinburgh Council is certified to ISO 22301 and LPF's alignment will ensure synchronicity and a consistent approach. This could be particularly beneficial in the event of a joint incident response.
- It supports good risk management by helping to identify potential threats and providing an effective control.

4.7 Alignment to the Standard, rather than formal certification, has a number of advantages including:

- No requirement for external audits to be undertaken, and no fees incurred.
- Less resource needed as a 'light touch' approach can be taken where requirements will not realise value for LPF.
- It is more proportionate to LPF's regulatory requirements, its size, complexity and range of services.

When will we get there?

4.8 Agreement was reached to address all 21 audit recommendations through the development of a phased implementation programme. The programme was approved by LPF's Risk Management Committee in October 2024 and shared with Internal Audit for tracking. A programme summary can be found at Appendix 1 and a summary of the report's findings and associated completion dates at Appendix 2.

4.9 The BCM programme (see Appendix 1 for programme summary) consists of four phases:

- Phase 1: Discovery and framework
- Phase 2: Process development and implementation
- Phase 3: Embedding
- Phase 4: Consolidation

4.10 Whilst these phases offer a general guide, the programme has been developed using a risk-based approach so areas of highest risk will be prioritised e.g. LPF's most critical services will be expedited through the phases.

4.11 The programme indicates arrangements for the known critical services will be in place by end 2025 with a full, established BCM system in place in two to four years noting:

- This is a wide timescale but will close as the implementation progresses and the programme will adapt to reflect this.
- Earlier phases will focus on development and implementation with later phases focusing on embedding, consolidation, continual improvement and demonstrating ongoing adherence to ISO22301.
- LPF's resilience will grow incrementally as the programme progresses and prevailing risk should start to reduce from early in the programme.
- The aspiration is for the programme to be at the lower end of the estimated time range. However, at this stage there are potentially many "unknown unknowns" and in general change often takes longer than envisaged to really bed in so milestones have been set accordingly.
- Expectation is that the schedule will firm up over time as knowledge is gained implementing early stages of the programme.

4.12 The full programme encompasses, and cross-references to, all 21 recommendations of the Internal Audit Report and has been shared with Internal Audit for tracking.

What will it take to get there?

4.13 Whilst there is no direct financial commitment required, it is recognised that a time resource is needed from various stakeholders to develop and maintain arrangements. This includes engagement with all teams in LPF, engagement with cross-Fund services, in particular IT, Risk & Compliance and HR, commitment and advocacy from senior management and joint planning with critical suppliers. The extent of this resource requirement will be better understood as implementation begins.

What governance will be in place?

4.14 LPF has a dedicated BC & Supplier Manager who will manage the BCM programme.

4.15 Phases 1 and 2 of the programme (due for completion Dec 2026) will be managed as a project and will adhere to LPF's project management process. As part of this process, LPFs Senior Leadership Committee (SLC) will provide governance and will consider and approve key BCM documentation and methodologies. Regular oversight will be provided by the Risk Management Committee (RMC).

4.16 Governance for phases 3 and 4 will be assessed on completion of phase 2 and will reflect the needs and circumstances at that time.

What are the first steps?

4.17 Develop a BCM Policy & Framework documenting LPF's approach to BCM, it's aims, objectives and the roles, responsibilities and authorities.

4.18 Review current incident management procedures, determine suitability for use in all types of incidents (not just IT-related) and deliver training and exercising, as appropriate.

4.19 Develop the business impact analysis (BIA) methodology.

5. Stakeholder/Regulatory Impact

5.1 The approach outlined in this report will enable LPF to meet it's BCM regulatory obligations in respect of TPR and FCA.

5.2 Effective BCM will help enable the continued delivery of our critical activities, including member payments, in the event of a disruption.

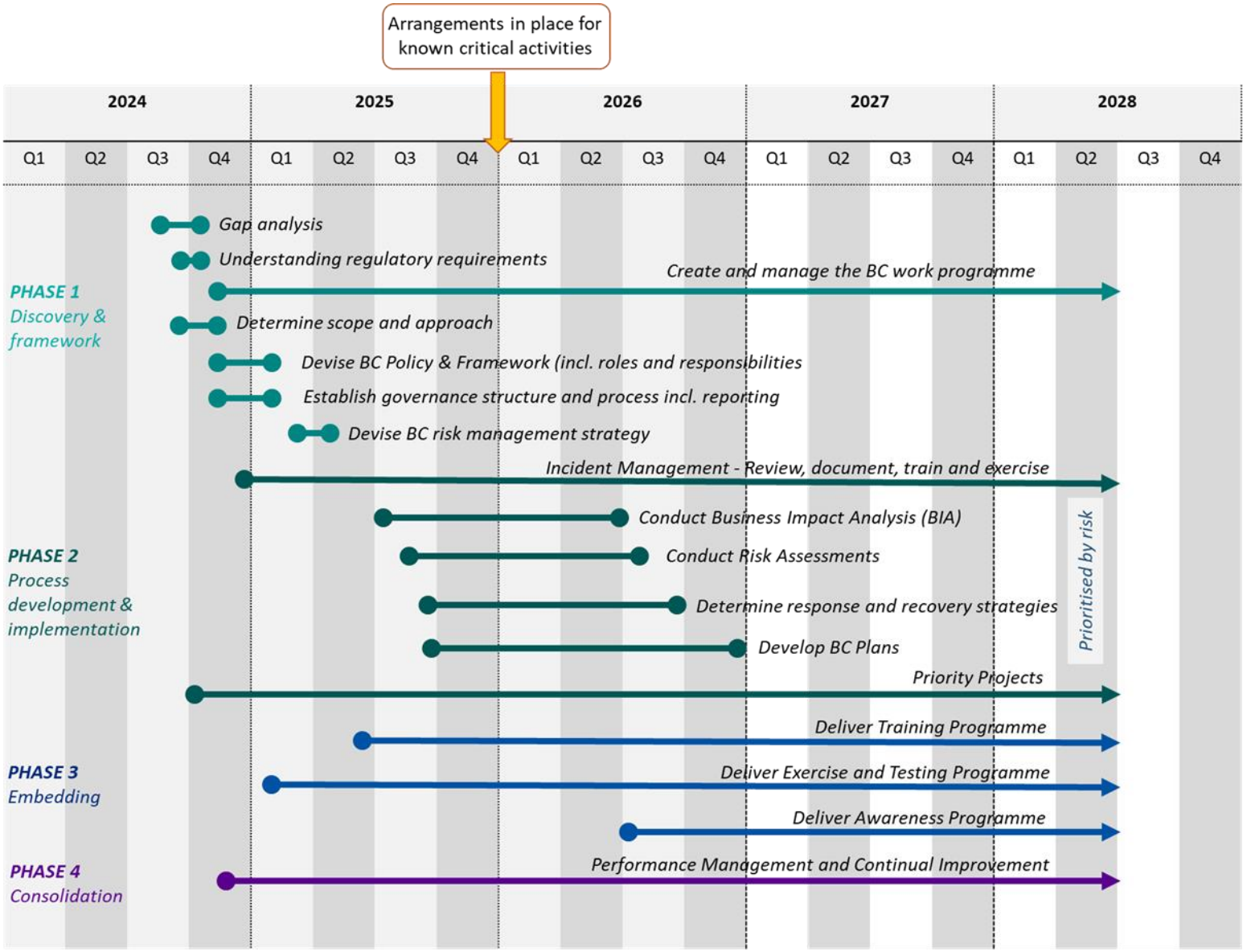
6. Background reading/external references

6.1 Internal Audit Report: Business Continuity Management (April 2024).

7. Appendices

Appendix 1 – Programme Summary
Appendix 2 – Internal Audit Findings – Summary
Appendix 3 – Business Continuity Maturity Model

Appendix 1 - Programme Summary



Appendix 2 – Internal Audit Findings – Summary

	Findings	Number of Recommendations	Priority	Agreed Completion Date
1	BCM experience, guidance and tools	6	Medium	April 2025
2	Business impact analysis (BIA)	2	High	October 2025
3	Business continuity plans	4	Medium	December 2025
4	Integration of BCM programme with wider business processes	3	High	December 2025
5	Exercising strategy and post-incident review process	4	Low	December 2025
6	Business continuity training and awareness programme	2	Medium	December 2025

Appendix 3 – Business Continuity Maturity Model