

Information / Discussion Paper

Overview and Scrutiny Committee – 15 January 2024

Business Continuity

1. Why has this come to scrutiny?

- 1.1 This item has come to scrutiny at the request of the committee.
- 1.2 The purpose of this discussion paper is to enable the committee to understand the council's approach to business continuity and any key risks.

2. Summary of the Issue

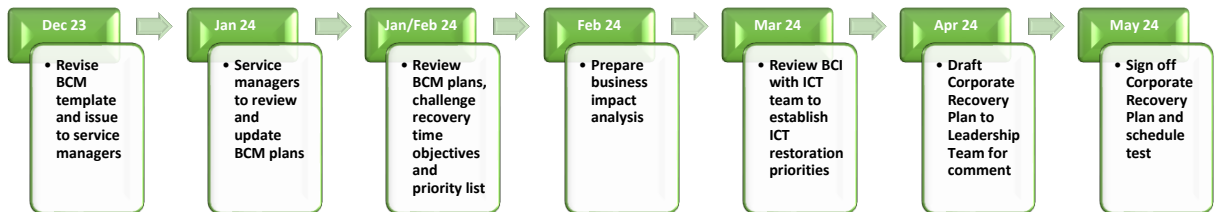
- 2.1 Business continuity is the council's ability to maintain critical business functions during a disaster and after it has occurred. Business continuity planning establishes processes and procedures that aim to prevent interruptions to critical services and re-establish full day-to-day function to council services as quickly and smoothly as possible.
- 2.2 Business Continuity plans are vital in terms of the council's preparedness. They provide a framework for considering potential events and threats such as fires, pandemics, supply chain disruptions, and cyber-attacks. It is the responsibility of each service manager to have an up-to-date plan for their service area.
- 2.3 Building on the service level plans, the council should have a corporate recovery plan. This plan sets out the way that the council would respond to an incident which impacts on multiple services or the council as a whole. It is created by using data from the service plans to produce a business impact assessment and enables some early decisions to be taken around service priorities and failover mechanisms that need to be activated.

3. Summary of evidence/information

- 3.1 Ensuring business continuity plans are up to date and work effectively is best done outside of a live incident. Therefore, officers have recently embarked on a complete review of the councils' arrangements.
- 3.2 This review will retain the relevant parts of the historic plans around building loss etc but will have a much stronger focus on loss of ICT and will enable us to capture any lessons learned from the pandemic or other council's cyber incidents. By way of example each plan owner will be asked to identify, where possible, manual workarounds which could be applied in the event of a cyber incident and how data will be input back into systems once they are recovered.
- 3.3 The committee may also wish to note that the Council recently received substantial assurance from internal audit in relation to ICT business continuity and disaster recovery.

4. Next Steps

4.1 The following timeline sets out the next steps to be taken in this important piece of work:



Background Papers	None
Contact Officer	Claire Hughes, Corporate Director and Monitoring Officer claire.hughes@cheltenham.gov.uk
Accountability	Councillor Martin Horwood, Cabinet Member for Customer and Regulatory Services