1. **Introduction:**

In February 2022 PwC concluded an audit of Business Continuity which resulted in limited assurance and listed several recommendations to improve strategy, operating model, and corporate impact analysis and planning.

The Council’s cyber security maturity and ability to respond effectively to an attack has a critical dependency on business continuity plans (BCPs). To expedite and provide assurance on progress, the high risk (RED) elements of that audit will be delivered via a Cyber Security and Information Risk Programme, supporting Business Continuity to respond to the increased risks because of the war in Ukraine.

There are three elements of the February 2022 audit listed as high risk:

1. Out of date Corporate Business Continuity Management Policy Statement, Strategy, and Plan
2. Lack of Strategic Business Impact Analysis (BIA) and criticality matrix
3. Minimal integration with wider business processes and third-party suppliers

Working with and funded by the CSIR team, Business Continuity has developed an Improvement Programme that will deliver a series of projects to address the high-risk elements outlined above. To deliver these outcomes, business continuity needs additional specialist resources to advise on strategy and the corporate business impact analysis and engage with the priority service areas to improve or create new plans.

The Council has an existing Business Continuity Management software package called Clearview that corporate and business area specific plans should be created and managed on. Clearview will need optimising as part of this engagement.