Appendix 4

1. Audit Summary – IT Resilience

Background and Context

1.1 The Covid-19 pandemic represents the largest disruption to day to day operations that has been seen in years. It has meant that some of the services of the local authorities have been suspended, reduced, or put on hold. It has also resulted in the Council having to adapt to new ways of working and implement business continuity plans and incident response teams.

1.2 Bristol City Council (the Council) holds a large amount of information across a wide range of IT systems, hosted on three different environments: council's two local data centres, Azure cloud and by the third-party providers. IT resilience is crucial to ensure that IT operations, systems and applications continue to operate efficiently and effectively. To achieve this, IT processes must operate consistently and proactively to avoid recovery situations. However, contingencies should be in place to ensure that the Council can continue operating should a failure occur.

1.3 It is important that the Council has robust processes and controls in place for IT resilience. Critical IT functions and business processes should be well-defined; key risks, required dependencies and potential impacts of disruptions should be identified and well understood. IT processes should maintain continuity of operations to meet business needs.

Scope and Objectives

1.4 The scope of the assignment included the following areas:

a) **Leadership and Governance:** we reviewed relevant policies, standards, and procedures in place to assess the accountability and ownership for IT business continuity management across the Council. We reviewed the Business Impact Assessment (BIA) and whether it adequately identified the Council's key/core critical services, work streams and supporting resources.

b) **Back-ups and Recovery:** we reviewed policies and procedure to ensure that back-ups are in place for all key systems. We selected a sample of internally and externally hosted applications and reviewed arrangements that are in place for regular (ideally weekly, no less than monthly) off site back-ups. We also assessed the key dependencies of the externally hosted applications and impact of the key dependencies on the continuity of operations.

c) **Incident Response Planning:** we reviewed the incident response plan for critical applications to ensure rules and responsibilities are defined for reporting, managing, and resolving incidents.

d) **Remote Working:** we reviewed the policies and procedures around remote working and assessed whether the Council has arrangements in place to provide workers with the equipment required to perform their role from a remote location (e.g. Laptops, mobiles). Furthermore, we assessed whether the Council has arrangements in place to allow employees to connect remotely to systems and applications if necessary (e.g. the use of a VPN to connect to the intranet), and that these arrangements are suitably resilient and are tested regularly.

Audit Opinion

1.5 Overall, Internal audit obtained **limited assurance** that effective internal control and risk management measures were in place.

Key Messages and Findings:

1.6 We carried out a high-level review of IT resilience controls operating within corporate IT Services and also for core IT applications managed by other Council Departments. Our main findings of in scope areas were as follows:

1.7 We raised 6 high priority and 2 medium priority findings. These have been grouped as follows:

1.8 **Leadership and governance:** The Council's Business Continuity Plan is currently out of date, and last reviewed in 2015. Our review of the policies and procedures noted that there is no consistently applied process in place to ensure policies and procedures are reviewed periodically. We inspected the Business Continuity Plan and noted the plan in place does not specifically address the IT related aspects of business continuity. Furthermore, no Council-wide business impact assessments have been carried out to identify critical systems and their inter-dependencies.

1.9 **Back-ups and recovery:** There are legacy weaknesses in design and implementation of IT resilience controls in place which remain after the IT Transformation Programme. The Council has two main data centres and we noted there are applications/services that are not replicated across both data centres, which means in the event of a data centre failure, these systems will not be available. There has not been any assessment of how many systems or services are currently relying on only one data centre.

1.10 From our discussions with senior management, we noted that the Council's policy is to move to cloud-based software as a service (SaaS) solution, and we confirmed the recent ITTP programme has moved most of the corporate systems / applications to a cloud-based hosting solution. However, there are legacy systems that could not be moved to cloud hosting due to operating on older operating systems and databases, and these are not directly managed by the Corporate IT team. Furthermore, where some applications/services identified as critical are replicated, the resilience of these systems is not tested regularly, and some have been found, during recent outages, to not be resilient.

1.11 Additionally, some externally hosted third party applications, which rely on the Council's Active Directory (AD) authentication (or other services), may not be consistently configured to use cloud-based authentication as well as on-premise authentication, and may therefore not be resilient.

1.12 We noted that at the time of our review the Council did not have a fully documented IT Disaster Recovery Policy, however, there were supporting and instructional documentation available. The lack of a formal plan may increase the risk of delay in recovering IT systems and infrastructure from an IT outage/disaster.

1.13 **Incident response planning:** the corporate Incident Response Plan in place at the Council does not include IT services. There is no separate Incident Response Plan owned and managed by the IT Department.

1.14 **Remote Working:** Testing of the resilience of the remote working infrastructure has not been carried out, and the ability of Council employees to work remotely may be impacted by the configuration of the Council's domain controllers.

Management Overall Comments

1.15 The findings from the review are accepted and an implementation plan has been developed that will ensure the agreed management actions are fully implemented within the agreed timelines. Some of the key actions being taken to address the findings can be summarised as follows:

- An application/system risk log is currently being developed in the same format as the Corporate Operational Risk Register, and in direct response to the Corporate Risk "Suitability of Line of Business Systems". When complete, this will be reviewed and the risk owners known, scale of risk known, and potential mitigation costs/approaches advised. It will then be for service areas to undertake activity as part of their service plans.

- Engaging with a third party to perform a full audit and assessment, and to devise a rectification plan

- Adding IT related scenarios to the existing Business Continuity Policy

- Undertaking a group wide Business Impact Assessment and incorporating the information into the Business Continuity Plan.

- The Incident Response Plan will be amended to include IT Incidents and also consider temporal aspects based on anticipated outage periods which will change the response IT Resilience and Business Continuity Planning Project.

- Establishing a Disaster Recovery Plan and run document

- As part of service planning 2022/23, the IT Team will review and put into place an appropriate replacement contract that meets current needs and enables effective testing.

- Performing a review of systems, backup/resilience methods and locations of backups. Recovery times will form part of Business Continuity planning.

- Undertaking periodic reviews of all relevant polices and ensuring good liaison between all service areas.