AUDIT AND STANDARDS COMMITTEE

26 September 2018

Title: Progress update on actions arising from the Internal Audit report for the IT Security Framework.	
Report of the Chief Operating Officer	
Public Report	**For Information**
Wards Affected: None	**Key Decision:** No
Report Author: Paul Ingram IT Strategy Lead	**Contact Details:** Tel: 07455 168555 E-mail: paul.ingram@lbbd.gov.uk
Accountable Director: Claire Symonds Chief Operating Officer & Deputy Chief Executive	
Accountable Strategic Leadership Director: Claire Symonds	
Summary Update on the Council IT Disaster Recovery arrangements.	
Recommendation(s) The Audit and Standards Committee is recommended to: (i) Agree that the proposed updates will provide a suitable level of assurance around Council IT disaster recovery. (ii) Note the work underway to assure the Council has a fit for purpose IT disaster recovery capability.	
Reason(s) The Committee requested an update following the earlier Internal Audit report.	

1. Introduction and Background

1.1 The Council historically had a disaster recovery contract for key IT infrastructure with a 3rd party organisation.

1.2 During 2014/15 the Council moved away from it's on premise data centre (Dagenham Civic Centre) and move to a Infrastructure As A Service (IAAS) arrangement with Agilisys. It was recognised that this type of service was capable of delivering a high level of resilience between sites and that the existing Disaster recovery arrangement would not deliver a meaningful level of protection to the

Council with an IAAS based service. As a result, the existing Disaster recovery contract was ceased.

1.3 In February 2018, Cabinet approved a budget to deal with historic under investment in ICT within the Council. Part of this budget was specifically intended to implement and deliver a fit for purpose IT disaster recovery arrangement that meet's the Council's current and emerging needs and risks.

1.4 In March 2018, an internal audit report around IT security gave limited assurance with the main finding being the lack of an ICT Disaster recovery capability.

1.5 In April 2018, a paper was presented to the Council's Assurance Group highlighting the key risks and a proposed approach to delivering a suitable ICT DR service.

1.6 In June 2018 Audit & Standards Committee reviewed the findings of the security audit and requested an update on the work being carried out to meet the Council's IT Disaster Recovery need.

2. Proposal and Issues

2.1 Approach to mitigation

Since 2016, the Council has preferred where economically, operationally and technically reasonable to procure IT systems as services rather than as applications that the Council then hosts. This effectively moves the risk from the council and Elevate to the application provider who have DR processes in place. This has a number of benefits, including reduced dependency on IAAS and so over time is managing down the risk from a business failure from its single provider, Agilisys.

Below are some of the applications now being delivered or moving to hosted or "delivery as a service" type approach whcih all include an availability based contract and / or DR. These include:

- Liquid Logic
- Email
- Sharepoint
- Abitras
- Oracle
- Case Management
- Integration

Some of the key applications remaining on IAAS or Hosted with Agilisys for a significant number of years include

- Revs & Bens (Acadamy)
- Income management
- Housing (Capita Housing and Capita Open)
- Our various asset systems
- Information @ work
- Key parts of GIS systems
- Planning (IDOX)
- School enrolment (CACI)
- Legal system (IKEN)

- Oracle Archive (R11)
- Confirm
- Council Website
- Telephone system
- Contact Centre telephony including voice recording
  Total of 185 servers

Mitigation for IAAS dependent systems and workloads

Proposed mitigation

Technical approach
The proposed mitigation for this risk is to create a maintained data copy of all the data and applications currently in Agilisys IAAS into Microsoft IAAS (Azure).

The Microsoft Azure services are costed by a number of parameters but this means that we can maintain storage copies of our systems and server configurations ready to run whilst incurring very low levels of cost for server capacity.

In the event of a failure leading to us needing to invoke, the server capacity can be started up rapidly ie: during working time, minutes to hours.

This approach has benefits outside of the pure Disaster Recovery risk mitigation:

- We can choose to run test and development environments in Azure instead of IAAS.
- The Azure data can (subject to governance controls) be more easily cloned and accessed for data mining
- At the end of the Elevate contract, a path will exist and be well tested to allow the Council to migrate services from IAAS

In addition to the contingency provided by creating a copy and instance of our environment in Azure, it is necessary to seek assurance from other service providers that their DR arrangements are tested and that they work.

Commercial approach

The cost for this activity has been estimated at £100K of manpower in 2018/19 to implement the required services and a further £100K per annum on a revenue basis for subscription and manpower to maintain the regime going forward to the end of the Elevate Contract.

After the end of the Elevate contract, costs for DR will be included in the ongoing IT costs for Core. These are currently under development with a full business case expected to go forward to Cabinet in Sept / Oct 2018.

The proposed costs above are included in the February forward budget forecast now approved by Cabinet.

3. Options Appraisal

3.1 A number of options and approaches were considered in the development of this approach including:

- No Action: Rejected as it leaves the Council exposed to an unacceptable risk and does not conform to good practice from a business continuity or IT Security standpoint.
- Normal DR contract: Rejected as it is expensive and complex to deliver and would not be the best strategic fit for Council ICT strategy.
- Creating additional resilience capacity within Agilisys IAAS: Rejected as it doesn't address the key risk around a business failure of Agilisys.

4. Financial Implications

None

5. Legal Implications

None

6. Other Implications

None

List of appendices:
None