



EXECUTIVE BOARD DECISION

REPORT OF:	Executive Member for Digital and Customer Services
LEAD OFFICERS:	Director of Finance
DATE:	Thursday, 9 March 2023

PORTFOLIO/S AFFECTED:	Digital and Customer Services
WARD/S AFFECTED:	(All Wards);
KEY DECISION:	Y

SUBJECT: Procurement of new Backup Solution

1. EXECUTIVE SUMMARY

The purpose of this report is to seek approval to procure a new range of security and recovery facilities for corporate data that will provide greater capability of recovery from a cyber-attack or other significant data loss.

2. RECOMMENDATIONS

That the Executive Board:

- Approves the procurement of the new solution through the Crown Commercial Services (CCS) framework RM6068 lot 1 for a 3 year period with a 1 year extension.
- Approves the increase to the department's annual revenue budget from the 2023/24 financial year of up to £130k.
Approves a supplementary capital estimate of £150k to be funded from grant received from Department for Levelling Up, Housing and Communities Cyber Support Team to fund the initial capital costs of the project.
- Notes that the existing £80k of capital funding for backup held with the transition to the cloud programme is transferred back into ICT earmarked capital reserves.

3. BACKGROUND

Currently the department is using an on premise backup technology that was procured 4 years ago. Over that time the council has had challenges with functionality and the reliability of backups, this needs to be improved in order to provide the required capacity and performance levels for safeguarding the Council's critical data. The Exec Board previously approved in October 2021 that the department will commence a transition to the cloud over a 5 year period. Part of this paper included implementing an element of cloud backup with the associated funding. The existing backup and recovery systems are unable to recover the council from the type of ransomware attack techniques that are now prevalent in the digital sphere. These attacks have transformed in recent years and are undertaken by professional digital teams who seed attacks in average 210 days before attack. The attackers monitor organisations during that period and attack when they business is most vulnerable and least able to respond. A new approach is essential to protect against this very real threat, which

is likely to materialise during the planning horizon.

The department has recently undertaken a horizon scanning exercise which involves a systematic examination of information to identify potential risks, threats and emerging issues for better preparedness and the incorporation of mitigation to ensure we are in a position to deliver our Digital Strategy in a secure manner. We are clear that the Cyber Security threat is something we will always need to account for, this identified that the department needed to expand beyond the planned backup solution that was previously approved due to changes in the area over recent years, this will place the Council in the best possible position to protect against cyber threats in the future. As we are currently working on our journey to the cloud we will require a toolset that works across both cloud and our own facilities platforms, we will need to be able to protect data that migrates between these environments. We are most aware of the threats associated with Ransomware, as such we are looking to implement facilities that will play a key role in our strategy for threat hunting, protection and remediation of any threats that may present themselves. The solution would respond to and keep pace with the very quickly changing external threat environment, and be additional to but work in tandem with the cloud migration programme. It would include a new Security Information and Event Management facility a 24 hour Security Operations Centre, new security systems, new backup, recovery and business continuity facilities.

An evaluation of suitable frameworks was carried out with the G-Cloud framework and NHN SBS framework being rejected as they were more geared to cloud only solutions. The department are therefore seeking approval to tender this through CCS which is an executive agency and trading fund of the Cabinet Office. This will be tendered through their framework RM6068 lot 1 for technology products and associated services. Conversations with them have identified that this is a suitable route to market for a solution which covers both onsite and cloud solutions. The tender will be scored in accordance with the following weightings;

Social Value – 15%

Price – 20%

Quality – 65%

We will be looking for a partner that can provide active practical support in the cyber security domain and be a dependable part of our high availability response plan associated with cyber risks.

The proposed new backup and recovery system will safeguard the Councils critical data, delivering:

- Enhanced protection for the Councils critical data
- Enhanced reliability of the backup hardware and software
- Enhanced performance of backup and recovery
- Improved provision for Disaster Recovery
- Protection against Ransomware

4. KEY ISSUES & RISKS

- The departments existing backup technology is not sufficient to protect our data moving forwards.
- Recent years have seen a significant rise in cyber security related incidents affecting the public sector across the globe, as well as a marked increase in the number of attacks targeting national infrastructure including local government.
- The department requires additional systems hardening and attack prevention work to introduce the capability to quickly recover from a criminal attack in the shortest possible time.

5. POLICY IMPLICATIONS

Having an appropriate contract for backup hardware and software in place will assist us to comply with the Civil Contingencies Act and ensure the Authorities data is efficiently and safely backed up and is quickly available in the event of a recovery or a disaster. Public organisations face the likelihood of an attack within the planning horizon. Should a successful attack take place lack of the

capability that is sought will mean the Council's priorities would all be substantially undermined.

6. FINANCIAL IMPLICATIONS

Revenue implications

From market research it is estimated that the annual revenue cost for the new solution will be up to £165k per annum. The department already holds revenue of budget of £35k as part of the cloud business case to fund this leaving a shortfall of up to £130k per annum. This has been factored into the Council's budget for 2023/24.

Capital costs

The capital costs for the new solution are likely to be up to £150k for the equipment, installation and transition costs, this will be funded through the grant that the department has received to improve cyber security in the Council. As part of the original transition to the cloud approval there was £80k allocated to the capital costs of a new backup solution that will be transferred back into ICT capital reserves.

7. LEGAL IMPLICATIONS

The procurement process complies with the regulations of the Council's Contract and Procurement rules and the Public Contract Regulations 2015. All contracts and contract variations will be in a form approved by legal officers in the Commissioning and Procurement team.

8. RESOURCE IMPLICATIONS

IT resources for the new solution will be built into existing works plans.

9. EQUALITY AND HEALTH IMPLICATIONS

Please select one of the options below. Where appropriate please include the hyperlink to the EIA.

Option 1 Equality Impact Assessment (EIA) not required – the EIA checklist has been completed.

Option 2 In determining this matter the Executive Member needs to consider the EIA associated with this item in advance of making the decision. *(insert EIA link here)*

Option 3 In determining this matter the Executive Board Members need to consider the EIA associated with this item in advance of making the decision. *(insert EIA attachment)*

10. CONSULTATIONS

None with this report

11. STATEMENT OF COMPLIANCE

The recommendations are made further to advice from the Monitoring Officer and the Section 151 Officer has confirmed that they do not incur unlawful expenditure. They are also compliant with equality legislation and an equality analysis and impact assessment has been considered. The

recommendations reflect the core principles of good governance set out in the Council's Code of Corporate Governance.

12. DECLARATION OF INTEREST

All Declarations of Interest of any Executive Member consulted and note of any dispensation granted by the Chief Executive will be recorded in the Summary of Decisions published on the day following the meeting.

VERSION: 1

CONTACT OFFICER:	Peter Hughes
DATE:	20/02/2023
BACKGROUND PAPER:	Exec Board Decision, Transition to the cloud – 14/10/2021