Slough Borough Council

Report To:	Cabinet
Date:	15th January 2024
Subject:	Procurement of a managed IT cloud-based back-up and disaster recovery solution
Lead Member:	Councillor Chandra Muvvala, Cabinet member for customer service, resident engagement, digital, data and technology.
Chief Officer:	Sarah Hayward, Executive director, strategy and improvement
Contact Officer:	Simon Sharkey Woods, Associate director, chief digital and information officer
Ward(s):	All
Key Decision:	YES as it is likely to result in the council incurring expenditure in excess of £500,000.00
Exempt:	No
Decision Subject To Call In:	Yes
Appendices:	None

1. Summary and Recommendations

1.1. In 2022, three audits of the council's cyber security and resilience capability highlighted that should the council undergo a cyber-attack, the risk of loss of service or data would be high. One area identified as needing urgent updating was the council's IT back-up and disaster recovery capability.

1.2. Officers have considered several options to address this risk, and the preferred option that most closely meets the council's needs is to engage a specialist partner to provide a managed service. This approach provides a solution that can scale to the council's needs, is designed and managed by the supplier, and run on reputable cloud platforms such as Microsoft's Azure or Amazon Web Services.

1.3. To achieve this, the council will undertake a procurement exercise using an existing Crown Commercial Service Framework Agreement to identify an appropriate provider and contract with the supplier for a maximum period of four years, with an initial period of three years, and the option to extend the contract for a further year. The likely cost of the service is in the region of £1.3m to £1.5m over the duration of the contract term (four years)

Recommendations:

1.4. It is recommended that Cabinet:

a) Approve the commencement of a procurement exercise using an existing Crown Commercial Service Framework Agreement for the provision of a cloud-based IT back-up and disaster recovery solution by a specialist service provider;

and,

b) Delegate the decision to award and enter into the contract to the Executive Director of Strategy and Improvement in consultation with the Cabinet Member for customer service, resident engagement, digital, data and technology.

Commissioner Review

No specific comments. Commissioners are fully supportive of the approach.

2. Report

Introductory paragraph

2.1. This report outlines the requirement to carry out a procurement exercise to contract with a reputable supplier for the provision of a cloud-based IT back-up and disaster recovery solution.

2.2. Partnering with a supplier for a secure, scalable, and flexible back-up and disaster recovery solution will enhance the council's cyber security and resilience capability, reducing the impact of a data breach following a cyber-attack and strengthen the council's business continuity capability.

Options considered

2.3. The council's high-level requirements for a back-up and disaster recovery solution are:

- A secure cloud-based backup and disaster recovery solution with an assured high level of operational performance.
- A flexible solution which can scale to the council's changing needs.
- A solution which meets (and exceeds) the National Cyber Security Centre (NCSC) cloud security standards.
- Data is secured within EEA based data centres, preferably UK data centres.
- A solution that maintains the integrity of the council's data and provides a replicated copy of the council's systems in a public cloud with the ability to recover to on-premises or run in the cloud as required.
- A solution which can provide and guarantee the appropriate Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for council systems in the event of an incident.

2.4. Based on these requirements, three options have been considered:

a) Procure an externally managed back-up and disaster recovery service – **recommended**.

Using the council's requirements, summarised above, a competitive procurement exercise will be undertaken using an existing framework agreement.

This will allow the council to select an appropriate partner that can meet the council's requirements with a value for money solution.

It is expected that the contract will be for an initial three-year period and include the option to extend the contract for a further year.

b) Implement an in-house back-up and disaster recovery solutions – not recommended

This option was the council's original preferred solution. The council would buy separate cloud-based back-up and disaster recovery solutions and manage the

service through internal resource. However, market research and the recent experiences of other local authorities have highlighted that this option is:

i. Resource intensive – the council would need to employ additional resource to manage the solution;
ii. Typically, total cost of ownership is more expensive that a managed solution; and,
iii. Requires additional on premises infrastructure to support management of the solution, at a time where the council is seeking to reduce its IT infrastructure footprint.

c) Do nothing – not recommended.

The cyber security audits highlighted an urgent need to improve the council's cyber security resilience and disaster recovery capability. 'Doing Nothing' does not address these issues.

2.5. The table below outlines the key stages in the process:

Activity	**Date**
Requirements gathering	Complete
Undertake market research with service providers and other councils	Complete
Prepare tender documentation	December 2023
Cabinet approval to proceed	January 2024
Issue tender	January 2024
Clarification and evaluation of tender returns	February 2024
Award contract	March 2024
Implement chosen solution	TBC

2.6. The evaluation panel will consist of key members of the ICT&D service, supported by procurement and finance as required.

3. Background

3.1. The council's cyber-security capability was assessed three times in 2022. Two assessments were undertaken as part of the council's internal audit function and a third assessment by the Department of Levelling Up, Homes and Communities (DLUHC).

3.2. Across all three audits, 33 recommended actions were identified to bring the council's cyber security capability up to an acceptable standard. These actions were grouped into ten projects which are in various stages of delivery through the modernisation programme.

3.3. Two recommendations covered the council's back-up and disaster recovery capability. The audits outlined a risk to the council that unless it updated its back-up and disaster recovery capability there was an increasing risk that should the council experience a cyber-attack, a loss of access to IT applications or a loss of data was likely.

3.4. The council's recent move to the ARK data centre facilities is providing better security, resilience, flexibility and availability, thereby improving the council's cyber resilience. However, the decision to move to the new data centre was predominantly an economic one, it did not address the issues outlined in the audits. It was cheaper

and the ‘pay-as-you-go’ consumption model aligned to the council’s future expectation that more of the council’s infrastructure is cloud-based.

3.5. In 2022 the council’s contract for external procurement expertise expired and the service was brought in-house. During this time the necessary strategic expertise to run a complex technology procurement was lost. Whilst draft specifications for both the back-up and disaster recovery services were prepared it was not possible to progress the procurements without procurement subject matter expertise, especially in developing a robust commercial model.

3.6. In September 2023 an interim resource, with recent expertise in procuring cloud-based back-up and disaster recovery solutions, was brought into the modernisation programme to deliver five complex IT procurements – back-up, disaster recovery, council-wide wi-fi refresh, security incident and event monitoring, and review and updating of audio-visual capability in Observatory House.

3.7. Research was undertaken into the technology solutions available which included: discussing the direction of travel for cloud-based solutions, the pros and cons of a council-managed versus externally managed solution and the recent experiences of other local authorities.

3.8. The research findings support the recommendation to seek an external partner to deliver this service on behalf of the council.

Implications of the Recommendation

Financial implications

3.9. The current estimate for the cost of these services is in the region of £1.3m – £1.5m over 4 years. This has been factored into the conversations taking place around the medium-term financial strategy and growth has been factored into the draft budget for 2024/25 which will be presented to Cabinet on the 18th December and finalised in March 2024. The Associate Director Chief Digital & Information Officer has been clear that the risk versus cost business case is compelling and that this is an important investment for Slough to prevent severe operational difficulties in the future. However until a decision is made on the final budget for 2024/25, whilst procurement activity can take place, a contract cannot be awarded until budget has been approved.

3.10. From a financial perspective, the necessary groundwork has been laid out within the budgetary framework to support this initiative. The allocated funds have been earmarked to cater precisely to this strategic endeavour, ensuring that the implementation of these services remains on track without compromising other essential financial commitments.

3.11. Furthermore, it's imperative to recognise that this allocation isn't solely about immediate expenditures; rather, it's an investment in our future operational efficiency. It is anticipated that long-term benefits, including improved service delivery, streamlined processes, and potential cost efficiencies that align with our overarching financial goals may be achieved. It will be important that cost efficiencies are identified as soon as possible and it cannot be assumed that these can be used within the service, given the need to identify further actions to increase the council’s financial sustainability these will need to be considered at a corporate level in future budget setting processes over the medium term of the council.

3.12. Moving forward, diligent monitoring and evaluation of the project implementation will be in place. This includes rigorous financial oversight to measure the return on investment and ensure that the expected outcomes and efficiencies are realised as

planned. The relevant members of the finance team will need to be involved in the monitoring process.

Legal implications

3.13. The UK GDPR and the Data Protection Act 2018 place a statutory obligation on the council to keep data securely by means of appropriate technical and organisational measures. This requires the council to consider things like risk analysis, organisational policies, and physical and technical measures. The measures must ensure the 'confidentiality, integrity and availability' of the council's systems and services and the personal data processed within them. The measures must also enable the council to restore access and availability to personal data in a timely manner in the event of a physical or technical incident and must ensure that the council has appropriate processes in place to test the effectiveness of the measures and undertake any required improvements. The council can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to the council's circumstances and the risk the processing poses.

3.14. Failure to implement an appropriate solution may place the council at risk of breaching this obligation.

3.15. The procurement strategy outlined in this report is compliant with The Public Contracts Regulations 2015 (PCR). Regulation 33 of the PCR provides for and regulates the compliant use of Framework Agreements. The Crown Commercial Service Framework Agreement G-cloud 13 RM1557.13 is current, the council is identified as a potential call-off party, and the services required are in scope and within budget under the Framework Agreement, so the council can lawfully call-off the services from the Framework in accordance with the Framework rules. The proposed procurement route is also compliant with the council's Contract Procedure Rules set out in the council's constitution.

3.16. Any call-off contract can initially last for a maximum of up to 36 months, with the option to extend once by up to 12 months but the council must specify this in the initial contract terms. Legal advice should be sought on the contract terms.

Risk management implications

3.17. The table below details the four main risks within the project:

Status	Risk description	Mitigation
Amber	Cost of service is greater than expected	• Review service requirements and identify any services which are driving costs upwards.
Green	Insufficient interest from the market	• Mature marketplace and call off from a framework will support supplier involvement
Amber	Delay in completing procurement process	• A project plan will be developed and proactively managed.
Green	Procurement result is challenged	• The procurement will follow the terms and conditions of further competition for the framework. • A standstill period may be enacted to allow supplier response. • All information, including evaluation reports will be retained.

Status	Risk description	Mitigation
		• Legal and procurement advice will be sought and followed throughout the procurement process

Environmental implications

3.18. None.

Equality implications

3.19. None.

Procurement implications

3.20. The application will be procured from a Crown Commercial Service's framework agreement – G-cloud 13 RM1557.13. The procurement will follow the standard call-off procedures for the framework:

- A set of requirements/ specification is developed.
- A split between price and quality is agreed by the project team – mostly likely weighted in favour of quality on this occasion.
- A key word search undertaken, shortlisting appropriate service offerings.
- A detailed review of the requirements against each vendors' service description is undertaken.
- The vendors' standard pricing is evaluated against the council's requirements.
- Any areas of uncertainty are followed up through clarification questions.
- The successful vendor is chosen.
- A call off contract based on the framework's standard terms and conditions and the vendor's contract are signed.

3.21. Evaluation of the service description will be undertaken by panel drawn from ICT&D, procurement (external resource) and finance as required.

3.22. The contract will be for an initial three-year period with the option to extend the contract for a year. The likely contract value will be between £1.3-£1.5m over the full term of the contract (four years).

3.23. The project implementation costs will be met from the modernisation programme budget and the annual cost of service will be met from existing budget available within the service area.

3.24. The chosen procurement strategy is appropriate and complies with the council's Contract Procedure Rules and Public Contracts Regulations 2015.

Workforce implications

3.25. None.

Property implications

3.26. None.

4. Background Papers

4.1. None.