Slough Borough Council

Report To:	Audit and Corporate Governance Committee
Date:	30 April 2025
Subject:	Digital, Data and Technology Internal Audit Recommendations – Update
Chief Officer:	Annabel Scholes – Executive Director, Corporate Resources
Contact Officer:	Martin Chalmers – Director of Digital, Data and Technology
Ward(s):	All
Exempt:	No
Appendices:	Appendix 1 - Finance and Commercial Internal Audit Recommendations – action plan

1. Summary and Recommendations

1.1 This report sets out status and progress for the Internal Audit recommendations relating to Digital, Data and Technology that were outstanding at the time of the last update on this matter, which was tabled at this Committee on 10 December 2024. For recommendations not yet closed, it sets out the current status.

Recommendation:

1.2 Committee is recommended to note the contents of this report and seek a further update on delivery at the June 2025 Committee.

Commissioner Review

This report is outside the scope for pre-publication commissioner review; please check the Commissioners' instruction 5 to CLT to sign off papers for further details.

2. Report

Background

2.1 The outstanding recommendations as at December 2024 related to two audits. The first of these was a Cyber Essentials audit in 2021/22. One item on that report remained outstanding. At the time of writing this report, the final stages of work on that action remain in progress (detail at Appendix1); a verbal update will be provided at the Committee meeting.

2.2 The second audit was a follow-up audit of IT Business Continuity and Disaster Recovery. Six recommendations from that report remained open in December 2025. The outstanding recommendations (detailed in Appendix 1) are all being addressed by a project, within the Digital & ICT Modernisation Programme, which is procuring new cloud-based services for backup and disaster recovery. Intrinsic to that project is the review and updating of policies, plans and processes for backup and disaster recovery to align with the services that are being procured.

2.3 Initiation of the project's procurement was approved by Cabinet in January 2024 but the project had been delayed, primarily because of procurement issues but also

because of a lack of dedicated project management resource. We reported in December 2024 that two steps had been taken in to accelerate delivery of this overdue project:

- A recruitment process had been launched for an interim project manager, with relevant domain experience, to focus on delivery of the project. That project manager will have responsibility for both managing the incoming supplier and for working with Emergency Planning and services across the Council to complete the review of policies, plans and procedures that will satisfy the outstanding recommendations.

  Current position: The recruitment process was challenging but an individual has now been in post since 17 February 2025

- The procurement had been relaunched using a revised route to market and longlisting had been completed. At that point, contract signature was forecast for end January 2025.

  Current position: The procurement took significantly longer than had been planned because of the scale of the clarification process that was required, and the consequent need for multiple rounds of evaluation. Contract award was confirmed on 18 March 2025 and, at the time of writing, contract finalisation discussions are in progress involving the supplier and the SBC legal team. A verbal update will be provided at the Committee meeting, by which time it is expected that the contract will have been signed and sealed.

2.4 Details of the current status of the actions planned to address the remaining audit recommendations are set out at Appendix 1..

3. Implications of the Recommendation

3.1 Financial implications

The total one-off cost of delivering the Disaster Recovery and Backup solution is up to £100,000. This cost is being met through a combination of funding sources:

- £40,000 from the MHCLG Cyber Security Grant
- The remaining £60,000 from the IT Transformation budget.

These funding arrangements are in place and do not require additional resources beyond those already allocated.

The ongoing revenue costs associated with the new solution have been identified and are fully contained within existing service budgets from 2025/26 onwards. No additional growth or virement is required to support the sustainability of the solution in future years.

In terms of financial risk, delays in procurement and implementation have not led to increased cost exposure, but any further slippage will be closely monitored to ensure that planned funding remains sufficient and that any contractual dependencies are managed within existing financial controls.

3.2 Legal implications

A failure to complete the actions proposed could impact the ability to secure compliance with the UK GDPR and the Data Protection Act 2018, which place a

statutory obligation on the council to keep data securely by means of appropriate technical and organisational 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 Audit and Accounts Regulations 2015 requires the Council to undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance. These standards require an effective system to monitor progress and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

The Council has been found to have failed to comply with its best value duties under Part I of Local Government Act 1999. The best value standards and intervention guidance confirms that to demonstrate effective use of resources, authorities should respond to audit recommendations and address issues in a timely way and that as part of good governance, internal audit functions should be challenging, robust, valued and contribute to efficient delivery of public services.

3.3 Risk management implications

The internal audit recommendations have been evaluated by Internal Audit as either high, medium or low risk; the risk level for each outstanding recommendation is given at Appendix 1. Management are aware of their responsibilities in ensuring that action is taken to respond and close out the recommendations.

3.4 Environmental implications

There are no direct environmental implications from this report.

3.5 Equality implications

There are no direct equality implications arising from this report.

4. Background Papers

None

Appendix 1 – Digital, Data and Technology Internal Audit Recommendations

The table below sets out the status of the recommendations that were reported as outstanding to the December 2024 Audit and Governance Committee. The target dates stated are those that were agreed at that Committee.

Audit / Area	Recommendation	Target Date	Update and action plan to discharge recommendation	Status
Cyber Essentials Medium Risk 2021/22	The Council will retain a central register of all shared accounts in use, with the justification for this recorded. This will then be subject to periodic review with a view to remove shared accounts where possible	28/02/25	**Update:** The identification and review of shared accounts has proved to be a resource-intensive manual exercise as there is no automatic way of identifying them. Furthermore, review is not purely technical: it also requires investigation with services of how accounts are being used. A central register of accounts has been established and an initial review of that list completed. As a result of that review, the majority of shared accounts have been deleted. The remaining accounts are subject to further investigation. These will either be deleted or the confirmed justification for their retention recorded on the central register. This work will also confirm that appropriate management processes and access controls are in place to minimise the risk from these accounts. A verbal update on the progress of this will be provided at the Committee meeting. A process for the management of shared accounts has been established. This includes a requirement for the creation of any new shared	Open and overdue

Audit / Area	Recommendation	Target Date	Update and action plan to discharge recommendation	Status
			accounts – expected to be exceptional – to be authorised by the Technical Design Authority body.	
Follow Up IT Business Continuity and Disaster Recovery High Risk 2022/23	DR Policy The Council will document a Disaster Recovery Policy, independent of the Disaster Recovery Plan.	27/01/25	**Update:** A draft of the policy is in review, and is expected to be signed off by the Corporate Leadership Team by the end of April. A verbal update on progress will be provided at the meeting.	Open and overdue
Follow Up IT Business Continuity and Disaster Recovery Medium Risk 2022/23	IT Business Continuity Plan	30/05/25	**Update:** Work is in progress in line with the Action Plan below. There are two risks: • Action 3 is dependent on wider service engagement at a time of intense pressure. This will be mitigated by focusing initially on the areas of manifest high criticality. • Action 4 will depend on the agreement of the supplier implementation plan. **Action Plan** 1. Work with Emergency Planning to agree scope of plan, relationship with other business continuity plans, and governance 2. Rework draft plan in parallel with DRaaS/BaaS procurement	Open (not yet due)

Audit / Area	Recommendation	Target Date	Update and action plan to discharge recommendation	Status
			3. Engage with business to agree recovery priorities. This process will inform individual business areas' thinking about their own business continuity plans for dealing with ICT unavailability. 4. Finalise plan with selected DRaaS/BaaS supplier and test as part of service launch of the Backup element of the solution.	
Follow Up IT Business Continuity and Disaster Recovery Medium Risk 2022/23	Roles and Responsibilities / Training The Council will outline the key responsibilities of each area of The Incident Hub as part of the IT Business Continuity Plan.	31/05/25	**Action Plan (unchanged from December 2025)** This action will be discharged as part of the reworking of the IT Business Continuity Plan described in the previous action	Open (not yet due)
Follow Up IT Business Continuity and Disaster Recovery Medium Risk 2022/23	IT DR & BCP Testing, including Testing of Backups	30/09/25	**Action Plan (unchanged from December 2025)** This action will be discharged as part of the implementation of DRaaS/BaaS. The revised target date aligns to the provisional date for implementation of the Disaster Recovery element of the solution (which will follow implementation of the Backup element) and is subject to confirmation following the procurement process.	Open (not yet due)
Follow Up IT Business Continuity and Disaster Recovery Medium Risk 2022/23	Business Impact Analysis (BIA)	31/05/25	**Action Plan (unchanged from December 2025)** This action will be discharged as part of the reworking of the IT Business Continuity Plan described above, with step 3 of its action plan being particularly relevant	Open (not yet due)

Audit / Area	Recommendation	Target Date	Update and action plan to discharge recommendation	Status
Follow Up IT Business Continuity and Disaster Recovery Medium Risk 2022/23	Applications List The Council will ensure that a central register of all applications is retained with priority of recovery for applications, either individually or by group	N/A	**Update** The process of reconciling applications lists into a single Master Applications List has been completed and Internal Audit has confirmed that this resolves the acquisition.	Closed