Slough Borough Council

Information needed	Details
Report To:	Audit and Corporate Governance Committee
Date:	10 December 2024
Subject:	Digital, Data and Technology Internal Audit Recommendations – Update
Chief Officer:	Will Tuckley – Chief Executive
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 reported outstanding to the November 2024 Audit and Corporate Governance Committee. For recommendations not yet closed, it sets out the plans and target date for closure.

Recommendations:

Committee is recommended to:

a) Note the contents of this report;

b) Seek ongoing assurance that the outstanding actions are being delivered in accordance with the plans set out;

c) Agree the proposed revised target dates for closure of the outstanding recommendations

Commissioner Review

Commissioners have reviewed the report and made no comments.

2. Report

Background

2.1 The outstanding recommendations relate to two audits. The first of these was a Cyber Essentials audit in 2021/22. This made 19 recommendations. In the November 2024 report, three of these were outstanding. Two of these have since been closed, so that – at the time of writing – one remains open; specific action on this is in hand. Detail is given at Appendix 1.

2.2 The second audit was a follow-up audit of IT Business Continuity and Disaster Recovery. This made nine recommendations of which one has been closed. 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 has been delayed, primarily because of procurement issues but also because of a lack of dedicated project management resource. Two steps have been taken in this quarter to accelerate delivery of this overdue project:

- The procurement has been relaunched using a revised route to market. At the time of writing, longlisting has been completed following a healthy response from the market, and the procurement is on track for contract signature at the end of January 2025.

- A recruitment process has 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.

2.4 Details of the actions planned to address the remaining audit recommendations are set out at Appendix 1, together with proposed revised dates. The Committee is recommended to note the planned actions and agree the revised target dates.

3. Implications of the Recommendation

3.1 Financial implications

Funding for the one-off costs of the disaster recovery and backup project has been allocated within the budget for the Digital & ICT Modernisation Programme which was agreed by Cabinet in March 2022 and funded through IT Transformation.

The ongoing revenue costs of the solution are already contained within the service budgets for 2024/25 and beyond.

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, controkl 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 November 2024 Audit and Governance Committee.

Audit / Area	Recommendation	Target Date	Revised 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	30/06/23	28/02/25	**Update:** It has been established that there is no automatic means of identifying shared accounts. A manual review to identify all shared accounts has been completed. These accounts are now being analysed to determine which can be deleted, which can be retained, and which can be replaced by the use of alternative approaches. For example, where there are shared accounts for generic mailboxes, it is now possible instead to allow the mailbox in question to be shared across individual accounts, removing the need for the shared account. Such cases require individual change to business practice and technical configuration and it is this which drives the revised target date. Where a shared account is still required, the justification is being captured in the central register. A process will be put in place for maintaining that list, although it is expected that it will only be in exceptional circumstances that new shared accounts would be needed.	Open

Audit / Area	Recommendation	Target Date	Revised Target Date	Update and action plan to discharge recommendation	Status
Cyber Essentials Medium Risk 2021/22	The Council will document a user account access management procedure covering areas.	30/09/22	N/A	**Update:** This policy has been created and approved by the Information Governance Board. Internal Audit confirmed closure of the recommendation on 5 November 2024.	Closed
Cyber Essentials Medium Risk 2021/22	The Council will document an administrator account management policy/procedure covering areas.	30/09/22	N/A	**Update:** This policy has been created and approved by the Information Governance Board. Internal Audit has confirmed closure of the recommendation on 5 November 2024.	Closed
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.	31/03/23	27/01/25	**Update** – Work on this action had been paused because of its interlinkage with the project to procure Disaster Recovery as a Service and Backup as a Service (DRaaS/BaaS). That project has launched its procurement and work on this action has restarted with renewed urgency. The same update applies to other outstanding actions relating to this audit. The target date for the award of the DRaaS/BaaS contract is 27 January 2025 and, given the need for policy and contract to align, the target date for this action is aligned to this. **Action Plan** – 1. Work with Emergency Planning to agree DR governance and responsibilities	Open

Audit / Area	Recommendation	Target Date	Revised Target Date	Update and action plan to discharge recommendation	Status
				2. Update content of policy to reflect DRaaS/BaaS requirements 3. Ensure appropriate linkages between policy and DRaaS/BaaS contract	
Follow Up IT Business Continuity and Disaster Recovery Medium Risk 2022/23	IT Business Continuity Plan	31/05/23	30/05/25	**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 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 (which, subject to agreement with the supplier, is planned for end May 2025).	Open
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.	29/12/23	31/05/25	**Action Plan** This action will be discharged as part of the reworking of the IT Business Continuity Plan described in the previous action	Open

Audit / Area	Recommendation	Target Date	Revised Target Date	Update and action plan to discharge recommendation	Status
Follow Up IT Business Continuity and Disaster Recovery Medium Risk 2022/23	IT DR & BCP Testing, including Testing of Backups	29/12/23	30/09/25	**Action Plan** 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
Follow Up IT Business Continuity and Disaster Recovery Medium Risk 2022/23	Business Impact Analysis (BIA)	29/09/23	31/05/25	**Action Plan** 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
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	29/09/23	20/12/24	**Action Plan** The review focused on the fact that there were inconsistencies between different application lists. Work to consolidate these into a single central register and ensure this is up to date is well advanced. The acquisition of new applications requires approval by the Technical Design Authority, and the Expenditure Control Panel process has been updated to include a check that such approval has been gained. This enables the register to be kept up to date.	Open