IT Application Change Management

Final Internal Audit Report

Date of issue: 28 May 2025

Audit reference: 11.24/25

Contents

This document has been prepared for Slough Borough Council ("SBC") and is only for SBC management and staff. SBC must consult with Internal Audit ("IA") (pursuant to part 3 of the Secretary of State Code of Practice issued under section 45 of the FOI Act) before disclosing information within the reports to third parties. Any unauthorised disclosure, copying, distribution or other action taken in reliance of the information contained in this document is strictly prohibited. The report is not intended for any other audience or purpose, and we do not accept or assume any direct or indirect liability or duty of care to any other person to whom this report is provided or shown, save where expressly agreed by our prior consent in writing.

Executive Summary

Partial

Overall Audit Opinion

Partial Assurance

This rating signifies that: “There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.”

Internal Audit has completed a review of Slough Borough Council’s (“SBC”) IT Application Change Management processes, as included in the approved Quarter 4 Internal Audit Plan presented to the Audit & Governance Committee on 20th February 2025.

The audit focused on assessing the effectiveness of governance, control, and oversight over changes to IT applications used by the Council excluding applications that are externally hosted and fully managed by third-party vendors. In 2024, there were 25 application-related change requests recorded, of which a sample of 7 was selected for detailed review.

The audit identified significant weaknesses in key areas of the IT Application change management process, including:

- The absence of a formal policy and procedure, resulting in inconsistent practices and unclear responsibilities.
- Inadequate approval controls, with several changes lacking proper pre- and post-implementation sign-offs from business units or application owners.
- A lack of formal documentation and evidence for testing, raising concerns over the quality and reliability of deployed changes.
- Incomplete audit trails in the Astro system, with critical data such as testing results and approvals not consistently recorded.

These weaknesses expose the Council to operational, compliance, and reputational risks, including the potential for unauthorised changes, disruptions to critical applications, and difficulty in tracing accountability.

The Digital, Data and Technology (“DDaT”) team has acknowledged the findings and committed to implementing corrective actions within defined timeframes. Internal Audit will follow up on the implementation of these actions as part of its ongoing assurance activities.

The following is a summary of the recommendations emanating from the audit. Details of these recommendations are provided in the FINDINGS section of this report (below):

	High	Medium	Low
Recommendations	3	1	0

Introduction

Slough Borough Council ("SBC") currently uses approximately 143 applications, the majority of which are Line-of-Business (LoB) applications provided by external vendors and tailored to meet the Council's specific operational needs. There are 4 service delivery models for the Council's application:

1. The application is hosted internally and managed by the IT team, with support and testing carried out by the Application Support team. The vendor is responsible for managing the release cycles.
2. The application is hosted externally and managed by the vendor, while business-as-usual (BAU) support is provided by the internal IT team.
3. The application is hosted internally, with operating system patching and server management handled by the internal IT team. Application management and support are provided by the vendor.
4. The application is hosted externally and is fully managed and supported by the vendor, with no involvement from internal IT for business-as-usual (BAU) support.

Internal Audit conducted a review of the Council's IT Application Change Management processes, focusing on the first three application hosting models only. The fourth model, which is mainly managed by the vendor, with no involvement from Internal IT for BAU was excluded from this review. According to change request records, there were 25 application-related change requests submitted in 2024.

The objective of this audit was to assess the effectiveness and robustness of the Council's application change management processes to evaluate whether application changes are properly reviewed, approved, and implemented in accordance with defined controls and governance frameworks, thereby ensuring system integrity and minimising risk.

This audit was conducted as part of the approved Quarter 4 Internal Audit Plan, which was presented to the Audit & Governance Committee on 20th February 2025. Due to the involvement of IT staff in intensive year-end activities, the audit reporting was delayed, as agreed by Director of Digital, Data and Technology with Head of Internal Audit. Fieldwork was subsequently carried out between late February and April 2025, involving sample-based testing and review of documentation.

Findings

Findings are exceptions-based and are designed to communicate key issues identified during the audit, together with suggested actions for improvement. They are detailed below, together with details of the potential / theoretical risk (Assessed risk).

Assessed risk 1: Changes to IT applications are not properly authorised.
Assessed risk 2: Changes result in IT applications that do not meet the Council's requirements.
Assessed risk 3: Changes are not managed in accordance with expected processes.

No	Expectation	Finding	Cause	Implications	Recommendation and Priority
1	A formal IT Application Change Management Policy and Procedure should be in place to guide and standardise how changes are initiated, approved, tested, and implemented.	**Lack of Formal IT Application Change Management Policy** We noted that the Council does not currently have a documented policy or procedure in place for managing changes to IT applications.	The development and formalisation of Application Change Management policies may not have been prioritised due to competing operational demands.	The absence of a documented change management policy increases the risk of inconsistent practices, unauthorised changes, and lack of accountability, potentially leading to application disruptions or security vulnerabilities.	Develop and implement a formal IT Application Change Management Policy and Procedure that clearly defines roles, responsibilities, and required steps in the change process. 🟥 High
Management Response		Digital, Data and Technology ("DDaT") will write a formal IT Application Change Management Policy and create a Standard Operating Procedure for Application change management.		Responsible Individual	Rifhat Ahmed
				Date for Implementation	30th June 2025
No	Expectation	Finding	Cause	Implications	Recommendation and Priority
2	1. All application change requests should be formally reviewed and approved by relevant business units and application	**Inadequate Application Change Approval Process and record** In our review of change request cases, we observed the following:	Lack of standardised approval workflow or documentation process within the current application change management process.	Failure to obtain proper application owner approval may result in changes that do not meet business needs or that negatively affect application functionality.	1. Implement a formal and standardised approval process that ensures all application changes are reviewed and approved by the appropriate business units, application owners before implementation. (Pre-Implementation Approval)

	owners before implementation (Pre-Implementation Approval). 2. All application changes must undergo review and receive formal approval from the relevant business units and application owners prior to deployment to the production environment from testing environment. (Post-Implementation Approval) 3. ICT Change Advisory Board (CAB) review and approval record for change case should be recorded in Astro. (Pre-Implementation Approval). 4. Application change requests should only be raised or approved by the designated Application	1. Approval for Application Change request from business units or and application owners before implementation were not documented. (Pre-implementation approval) 2. Approval for Application Change result from business units and/or application owners before deployment to production environment were not documented. (Post-implementation approval) 3. The Change Advisory Board (CAB) decision and approval on each change case are not recorded in the Astro System. 4. Change requests can be initiated by any user or IT specialist working with the application, even if they are not officially authorised by the business management or application owner. 5. IA randomly selected 7 samples from a total of 25 cases in 2024. We noted that for 3 samples, approvals for application changes were not consistently provided in			2. Implement a formal and standardised approval process must be implemented to ensure that all application changes are reviewed and approved results based on User Acceptance Testing (UAT) by the appropriate business units or application owners. This is to confirm that the changes meet requirements and are satisfactory before deployment from the testing environment to the production environment. (Post-Implementation Approval) 3. Decisions made by the Change Advisory Board (CAB) should be clearly documented and linked to the respective change records in the Astro system to create an audit trail and improve accountability. (Pre-Implementation Approval) 4. Maintain and regularly update a delegated List/register to ensure that only Application Owners or their formally delegated authorities can initiate or approve application change requests. 5. ICT should establish defined timelines or service-level targets for the review and approval of application change requests to ensure timely completion.

	Owner or a formally delegated authority. 5. An authorised representative from the Digital, Data, and Technology team shall review and approve the completion of the change request in a timely manner.	a timely manner. In these cases, approvals were granted 7 to 10 months *after* the changes had already been completed in the Astro system.			🟥 High
Management Response		DDaT will update its master applications list identifying owners to applications. This will be added to the Commitments Register to ensure its reviewed quarterly. The approvals workflow through the ITSM will be configured to ensure approvals are sought by application owners prior to any changes. Decision made at CAB will be recorded in the RFCs Service level will be defined in the IT Application Change Management Policy		Responsible Individual	Rifhat Ahmed / Alex Cowen / Colin Watson
				Date for Implementation	30th September 2025
No	Expectation	Finding	Cause	Implications	Recommendation and Priority
3	All changes to applications should undergo documented testing to verify functionality and avoid disruptions or errors in the production environment.	**Lack of Formal Testing Documentation for Application Changes** Internal Audit reviewed 7 randomly selected application change requests out of 25 made in 2024. Of these, 3 included only high-level references to completed testing in the Rollout Plan section, with no detailed documentation	Testing activities are being conducted informally without a structured requirement for documentation results or obtaining formal approval before deploying to production.	Lack of formal testing documentation and audit trail increases the risk undetected errors or system issues being introduced into the production environment. Also, reduces traceability and auditability of change activities.	Establish and enforce a formal testing process that requires documented evidence before any application change is deployed to the production environment. This documentation should include at a minimum: • Test results (pass/fail outcomes). • Test details, date of test, application version.

		or supporting evidence. The remaining 4 had no testing records at all. No test results, no indication of the testing environment, and no sign-off by IT or the application owner. The absence of formal test documentation makes it unclear whether the changes met their intended objectives, or the requirements outlined in the Rollout Plan.			- Details of the testing environment used. - The identity of the user performing test. - Formal Sign-off or approval from the responsible tester and/or application owner (post-implementation approval) High
Management Response		The Internal Audit recommendation is accepted. DDaT will ensure testing evidence is provided for all applications changes. These will be attached to RFC as evidence of testing completed following the change. This process will be included in the Standard Operating Procedure.		Responsible Individual	Rifhat Ahmed / Sarah Power
				Date for Implementation	30th June 2025
No	Expectation	Finding	Cause	Implications	Recommendation and Priority
4	All application change requests should be fully documented in the Astro system including key details such as Business Unit/Application Owner approval, ICT pre-approval, testing results, and final sign-off.	**Incomplete Logging of Application Change Information in Astro** During the review, we noted that only 3 cases results were logged in Astro. However, for the other 4 cases only recorded entries captured basic details such as the requester's name, ticket properties, and change description, they lacked critical supporting information including Business Unit or Application Owner approvals, ICT pre-	The Astro system's current change request form lacks structured fields for entering all required approvals and test documentation. Additionally, the Council There is also no enforced requirement or checklist to ensure comprehensive recordkeeping.	Incomplete documentation of application changes negatively impacts controls by: - Reducing accountability and transparency, - Increasing the risk of unauthorised or untested changes being deployed, - Weakening the Council's ability to demonstrate control over the change management process. - Limiting traceability for audit and compliance purposes, potentially undermining post-implementation reviews and assurance efforts.	It is recommended that the Astro application change request form be enhanced to ensure comprehensive documentation of each change will be recorded in Astro for audit trail. The mandatory fields/information should be recorded at Astro system such as: (Pre-Implementation Approval) - Business Unit or Application Owner approval record stated in recommendation 2. - ICT CAB approval record stated in recommendation 2. (Post-Implementation Approval)

		approvals, change result and test results or evidence of test sign-off.			- Business units, application owners formal approval before deployment to production environment. stated in recommendation 2. Testing - Testing details and result stated in recommendation 3 Medium
Management Response		DDaT will update the RFC form on Astro as appropriate based in the IT Application Change Management Policy and SOP.		Responsible Individual	Rifhat Ahmed
				Date for Implementation	30th June 2025

Annex 1: Objective, scope and limitations

Objective

The audit will assess the adequacy of arrangements in place to ensure that changes to Council's IT application systems are properly authorised, documented, tested, approved, and implemented.

Scope and limitations

The review will be designed to assess the effectiveness of controls in place to ensure that the following risks are mitigated:

- Changes to IT applications are not properly authorised;
- Changes result in IT applications that do not meet the Council's requirements; and
- Changes are not managed in accordance with expected processes.

The scope of this review is limited by the following:

- Testing will be undertaken on a sample basis;
- In addition, our work does not provide any guarantee against material errors, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist; and
- The results of our work are reliant on the quality and completeness of the information provided to us.

Distribution

Colin Waston, Head of Technology (Infrastructure & Platforms), Digital, Data and Technology

Martin Chalmers, Director of Digital, Data and Technology (Final only)

Annabel Scholes, Executive Director Corporate Resources and S151 Officer (Final only)

Ian Kirby, Interim Head of Internal Audit

Annex 2: Our classification systems

Substantial	**Substantial Assurance** The framework of governance, risk management and control is adequate and effective.
Reasonable	**Reasonable Assurance** Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Partial	**Partial Assurance** There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
Minimal	**Minimal Assurance** There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

Recommendation

Priority	Definition	Action required
High	Significant weakness in governance, risk management and control that if unresolved exposes the organisation to an unacceptable level of residual risk.	Remedial action must be taken urgently and within an agreed timescale.
Medium	Weakness in governance, risk management and control that if unresolved exposes the organisation to a high level of residual risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
Low	Scope for improvement in governance, risk management and control.	Remedial action should be prioritised and undertaken within an agreed timescale.