



IT Audit Findings

Coventry City Council

Year ended 31 March 2025

Issued 27 May 2025

Nerys Bint

Director, IT Audit

T: +44 (0)20 7383 5100

E: Nerys.Bint@uk.gt.com

Molly Chen

Assistant Manager, IT Audit

T: +44 (0)20 7865 2077

E: Molly.Chen@uk.gt.com

Saif A Ahmed

IT Auditor, IT Audit

T: +44 (0)20 7865 2225

E: Saif.A.Ahmed@uk.gt.com



Contents

| Section | Page |
|--|------|
| 1. Executive summary | 3 |
| 2. Scope and summary of work completed | 4 |
| 3. Summary of IT audit findings | 5 |
| 4. Detail of IT audit findings | 7 |

Section 1: Executive summary

01. Executive summary

02. Scope and summary of work completed

03. Summary of IT audit findings

04. Detail of IT audit findings

To support the financial statement audit of Coventry City Council for year ended 31 March 2025, Grant Thornton has completed a design and implementation review of the IT General Controls (ITGC) for applications identified as relevant to the audit.

This report sets out the summary of findings, scope of the work, the detailed findings and recommendations for control improvements.

We would like to take this opportunity to thank all the staff at Coventry City Council for their assistance in completing this IT Audit.

Section 2: Scope and summary of work completed

01. Executive summary

02. Scope and summary of work completed

03. Summary of IT audit findings

04. Detail of IT audit findings

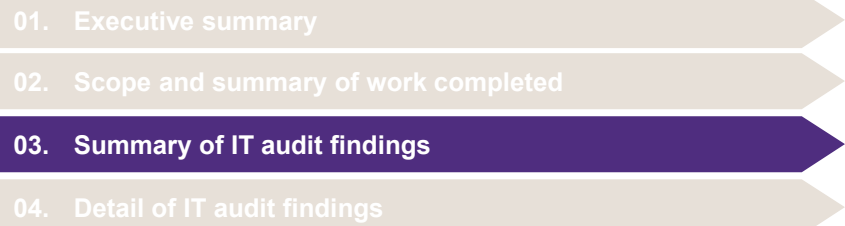
The objective of this IT audit was to complete a design, implementation and operating effectiveness controls review over Coventry City Council's IT environment to support the financial statement audit. The following applications were in scope for this audit:

- Business World

We completed the following tasks as part of this IT Audit:









- Evaluated the design and Implementation effectiveness for security management and change management controls
- Performed high level walkthroughs, inspected supporting documentation and analysis of configurable controls in the above areas
- Documented the test results and provided evidence of the findings to the IT team for remediation actions where necessary.

Section 3: Summary of IT audit findings





- 
- 01. Executive summary
 - 02. Scope and summary of work completed
 - 03. Summary of IT audit findings**
 - 04. Detail of IT audit findings

Other findings – IT audit

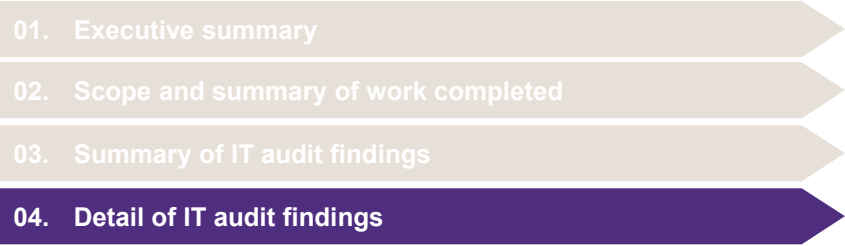
This section provides an overview of results from our assessment of the relevant Information Technology (IT) systems and controls operating over them which was performed as part of obtaining an understanding of the information systems relevant to financial reporting. This includes an overall IT General Control (ITGC) rating per IT system and details of the ratings assigned to individual control areas.

| IT system | Level of assessment performed | Overall ITGC rating | ITGC control area rating | | |
|-------------------------|---|---|---|---|---|
| | | | Security management | Technology acquisition, development and maintenance | Technology infrastructure |
| Business World | Detailed ITGC assessment (design and operating effectiveness) |  |  |  |  |
| Active Directory | Detailed ITGC assessment (design and operating effectiveness) |  |  |  |  |


Assessment

-  Significant deficiencies identified in IT controls relevant to the audit of financial statements
-  Non-significant deficiencies identified in IT controls relevant to the audit of financial statements / significant deficiencies identified but with sufficient mitigation of relevant risk
-  IT controls relevant to the audit of financial statements judged to be effective at the level of testing in scope
-  Not in scope for testing




Section 4: Detail of IT audit findings

- 
- 01. Executive summary
 - 02. Scope and summary of work completed
 - 03. Summary of IT audit findings
 - 04. Detail of IT audit findings**


IT general controls assessment findings

| Assessment | Issue and risk | Recommendations |
|--|--|--|
| 1.  | <p>Inadequate Specification and Approval of User Access Requests</p> <p>During our audit, we noted that user access requests for Business World were required to be raised and approved via the Motion Ticketing Tool or emails. However, for a selected sample, the specific details of the required user access were not provided.</p> <p>Furthermore, permissions were granted before approval was given by the designated approver, based on the Finance Systems Team's experience and the user's position.</p> <p>Additionally, for another selected sample, the user access request was approved by the system user himself, who was also the budget holder and designated approver. No independent approval was obtained for this case.</p> <p>In response, we have verified with the Lead Finance Systems Accountant and confirmed the permissions provided to these users were appropriate and aligned to their job responsibilities.</p> <p>Risk These observations present several risks:</p> <ul style="list-style-type: none"> Without specifying the required user access details and approval, there is a risk that users may be granted permissions beyond their job requirements, leading to unauthorised access to sensitive financial data. Allowing a system user to approve their own access request compromises the principle of segregation of duties. This increases the risk of fraudulent activities and unauthorized transactions, as there is no independent review or approval. | <p>It is recommended that Management should consider the following:</p> <ul style="list-style-type: none"> Establish a formal document that outlines the levels of access and roles to be assigned to users based on their specific levels and grades. This document should include detailed information on data and menu permissions required by budget holders. Establish a policy that prohibits users from approving their own access requests. Ensure that all access requests are reviewed and approved by an appropriate independent individual who is not the requester or the associated user. Ensure that all user access requests are fully documented and approved by the designated approver before any permissions are granted. <p>Management response</p> <ul style="list-style-type: none"> Document Access Levels: Create a detailed document showing the levels of access and roles for different type of Business World users Independent Approval Policy: Set a policy that stops users from approving their own access requests. All requests will be reviewed and approved by their line manager or equivalent Approval Process: Make sure all user access requests are fully documented and approved before any permissions are given. This includes a detailed specification of the required access. We've already improved the new user request form on our IT support ticketing system, which now documents the access requirement and needs approval from the line manager. |

Assessment

-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

IT general controls assessment findings

| Assessment | Issue and risk | Recommendations |
|--|--|---|
| 2.  | <p>Password requirements on Active Directory and Business World are not aligned with the Council's password policy</p> <p>During our audit, we noted that password requirements on Business World and Active Directory were not aligned to Council's password policy.</p> <p>Please refer to Appendix A for details.</p> <p>Risk</p> <p>The misalignment between the password requirements set in the network and the system, compared to the Council's password policy, poses several risks:</p> <ul style="list-style-type: none">• Shorter passwords are easier to guess or crack using brute force attacks.• Weak password history policies allow users to reuse old passwords, making it easier for attackers to gain access | <p>It is recommended that Management consider the following:</p> <ul style="list-style-type: none">• Review and update the password policies in Active Directory and the system to ensure they comply with the entity's established password standards. This includes setting minimum password length and enforcing password history requirements• Conduct regular audits of password policies to ensure ongoing compliance with the entity's standards and to identify any discrepancies promptly.• Review the Council's password standards to ensure they are up-to-date and align with industry best practices <p>Management response</p> <ul style="list-style-type: none">• We agree that there are some minor differences between the Council's password policy and the password requirements for users. We don't believe this creates a significant risk but will be reviewing updated password guidance from the NCSC and aligning the password policy and password requirements in the near future. |

Assessment

- Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
- Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
- Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

Appendix A: Password Policies

| Parameter | Policy | Active Directory | Business World (Note 1) |
|------------------|---|---|--|
| Minimum Length | 12 characters (general users) 16 characters (high privilege) | 12 characters (default domain policy) 15 characters (administrator accounts) | 0 character |
| Complexity | No complexity enforced | Password must meet complexity requirements | User advanced combinations of numbers and characters |
| Password Expiry | 365 days | 365 days (default domain policy) 90 days (administrator accounts) | 30 days |
| Password History | Previous 25 passwords are blacklisted | 24 password remembered | 5 passwords |

Note 1: Although Business World uses single sign-on with reliance on Active Directory for user authentication, some users were not configured to authenticate through domain accounts. These users had to set up their passwords according to the password policy configured in the system.

Assessment

- ✓ Action completed
- X Not yet addressed

