INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Finance IT Application
TO:	Head of Finance	**DATE:**	10 January 2024
C.C.	Chief Executive Deputy Chief Executive Head of Customer and Digital Services Principal Accountant (Systems) Application Support Team Leader Portfolio Holder (Cllr Harrison)		

1 Introduction

1.1 In accordance with the Audit Plan for 2023/24, an examination of the above subject area has recently been completed by Jot Bougan, IT Internal Auditor, and this report presents the findings and conclusions for information and, where appropriate, action.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and cooperation received during the audit.

2 Background

2.1 The Council went live with the new Technology One finance application in November 2021. Technology One is an integrated solution that replaced a number of legacy systems. It is a cloud-based system that has modules for core finance, contract management and reporting and analytics.

3 Objectives of the Audit and Coverage of Risks

3.1 The management and financial controls in place have been assessed to provide assurance that the risks are being managed effectively. It should be noted that the risks stated in the report do not represent audit findings in themselves, but rather express the potential for a particular risk to occur. The findings detailed in each section following the stated risk confirm whether the risk is being controlled appropriately or whether there have been issues identified that need to be addressed.

3.2 In terms of scope, the audit covered the following risks:

1. System errors are not detected or resolved, resulting in financial loss.
2. Budget monitoring is impacted by system or interface failures.
3. Loss of data.
4. There is no accountability for changes made to the system or data.

5. Weak logical security leading to unauthorised access.
6. User access is not correctly defined, leading to unauthorised changes to data.
7. System administrator access is not restricted.

3.3 These were drawn from a combination of risks identified in the Significant Business Risk Register, the departmental risk register, and discussion between the Internal Auditor and the Head of Customer and Digital Services.

3.4 The work will help to ensure the Confidentiality, Integrity, and Availability of the Council's data. Whilst this does not directly help the Council to achieve any specific objectives, it has a cross-cutting impact on several internal themes and objectives as set out in the Business Strategy.

4 Findings

4.1 Recommendations from Previous Report

4.1.1 The Technology One finance application has not been subject to previous internal audit review.

4.2 Financial Risks

4.2.1 **Potential Risk: System errors are not detected or resolved, resulting in financial loss.**

Users report system issues to the Principal Accountant (Systems) or the Systems Officer. A log of reported issues is not maintained and hence no details are available on what is reported, materiality and resolution. To be clear, there is no expectation that every minor issue is logged, only those that are key and significant.

Recommendation

All key issues reported by users should be logged. The log should include the date it was reported, name of user, description of issue, resolution and date resolved.

Issues or errors that cannot be resolved by the Systems Officer are reported to the supplier using their support portal. Only the Principal Accountant (Systems) and the Systems Officer log issues with the supplier. A review of the supplier's support portal found there are thirteen open support cases, eleven of which are service requests for system enhancements and two which are incidents. The oldest incident was logged on 31 August 2023, is not a priority and was last updated on the day of the audit. The last critical incident was logged by the Principal Accountant (Systems) in May 2023 and was resolved by the supplier in one day.

4.2.2 **Potential Risks: Budget monitoring is impacted by system or interface failures.**

The Systems Officer maintains a log of key changes to the system. The log includes a description of the change, module impacted, sign-off, date into test and date made live. The Systems Officer stated that changes are tested but this is not documented and hence cannot be confirmed. For system upgrades, a documented test plan is developed and executed. When all tests are successfully passed, the Principal Accountant (Systems) authorises the change being made to the live environment.

Recommendation

Change control procedures should be documented detailing the process for making changes to the system. The procedures should clearly outline the type of changes subject to the procedure, any exceptions, testing requirements and signoffs.

The contract with the supplier makes no reference to the disaster recovery arrangements in place for the system.

Recommendation

The disaster recovery plan for the system should be confirmed, including the recovery time objective and details of when it was last tested.

4.3 Legal and Regulatory Risks

4.3.1 Potential Risk: Loss of data.

As the system is hosted in the cloud, the supplier is responsible for taking backups of programs and data. A review of the contract for the system found that it does not include any details of the backups taken.

Recommendation

Confirmation should be sought on what backups are taken, including frequency, retention, testing, recovery point objective and storage of backup copies. Storage should include an offline copy for protection against ransomware attacks.

4.4 Reputational Risk

4.4.1 Potential Risk: There is no accountability for changes made to the system or data.

There is an audit trail on the system which logs user activity. A review of the audit trail confirmed that high-level activity reports are available and more detailed information is shown at a record level, including a history of all changes. The audit trail was configured by the supplier and no details are available on how it is setup i.e. what is / isn’t audited, ability to change the level of auditing, retention period for log data and reporting capabilities.

Recommendation

Further details on the operation of the audit logging system should be confirmed with the supplier.

4.5 Fraud Risk

4.5.1 Potential Risk: Weak logical security leading to unauthorised access.

Access to the Technology One Finance system is subject to Single Sign On (SSO), which utilises the Windows Active Directory username and password for user authentication.

As the system is cloud-based, it can be accessed off network i.e. from a computer that is not connected to the corporate network. It was tested and confirmed that off network access is subject to multi-factor authentication in accordance with good practice.

A review of the Windows Active Directory password policy found that passwords are required to be a minimum of eight characters and expire every 90 days. Changes are being proposed to this policy that will see the minimum password length for standard users increased to fourteen characters and password expiry to 180 days. These changes reflect current good practice and is something we support, apart from the expiry period. The National Cyber Security Centre now recommend that passwords are not expired.

Recommendation

The new password policy being proposed should be implemented, apart from the expiry period which should be reconsidered.

User accounts are locked for 30 minutes after five invalid logins to prevent brute-force attacks. A password protected screensaver is enabled after ten minutes of no user activity.

We tested the security of the networking protocol (SSL) that is used for securing remote connections over the internet and identified no issues. The web server only supports TLS (Transport Layer Security) 1.2 or later in accordance with recommended best practice.

4.5.2 Potential Risk: User access is not correctly defined, leading to unauthorised changes to data.

All requests for a new user account are made using an online form that is available on the intranet. The form requires line manager details and the request is automatically sent to the line manager for approval. Once approved, the form is emailed to the finance inbox for processing. A review of seven recent requests for a new account found they have all been appropriately authorised.

As the system uses SSO, a user's access is revoked when their network account is disabled by Digital Services as part of the corporate leaver's procedure. In addition, the Systems Officer receives a notification of staff leavers from HR and expires the user's account on the system.

User access within the system is defined using profiles. Each profile has a number of roles which provide access to functions. There are five standard profiles, five finance profiles, three procurement profiles and one system administration profile.

The profiles are bespoke to the Council and only a small number have been created to make them easier to manage. The reason behind this is that the previous finance system had a large number of profiles which became difficult to administer.

Generally, each category of profile e.g. finance, standard, procurement etc, provides the same level of access and the only major difference is the approval limit. The consequence of this is that users have a greater level of access than they need for their role. We understand that in finance, the small size of the team means that users are expected to cover other roles and need access to do this. Whilst this is accepted, the risk should be formally assessed and managed. It is also important that key activities are restricted as far as possible. For example, we found that the audit team have access to change supplier bank details, whereas this should be limited to designated users only. An annual review of user access rights was performed on the previous system but the exercise has not been completed since Technology One was implemented.

Recommendation

The following is undertaken:

- **A risk is added to the Finance risk register for the way access profiles are setup.**
- **Key / sensitive functions, such as changes to supplier bank details, are limited to designated users.**
- **An annual documented review of Finance user access is performed.**

Testing confirmed that users cannot approve their own requisitions.

4.5.3 Potential Risk: System administrator access is not restricted.

There are seventeen users with system administrator access. Four of these users are in Finance, six in the Digital Services Applications team and the remainder are all supplier accounts. The supplier accounts were enabled at the time of the audit as they are doing some work on the system. We are informed that these accounts are made inactive when they are not being used. The users in Finance and Digital Services were confirmed as requiring privileged access by the Systems Officer and Principal Accountant (Systems).

5 Summary and Conclusions

5.1 Section 3.2 sets out the risks that were reviewed as part of this audit. The review highlighted weaknesses against the following risks, with some of the findings covering more the one risk:

- Risk 1 – System errors are not detected or resolved, resulting in financial loss.
- Risk 2 – Budget monitoring is impacted by system or interface failures.

- Risk 3 – Loss of data.
- Risk 4 – There is no accountability for changes made to the system or data.
- Risk 5 - Weak logical security leading to unauthorised access.
- Risk 6 – User access is not correctly defined, leading to unauthorised changes to data.

5.2 In overall terms, therefore, we are able to give a MODERATE degree of assurance that the systems and controls in place in respect of the Finance IT Application are appropriate and are working effectively to help mitigate and control the identified risks.

5.3 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

6 Management Action

6.1 The recommendations arising above are reproduced in the attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit and Risk Manager

Appendix A

Action Plan

Internal Audit of Finance IT Application – November 2023

Report Ref.	Risk	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.2.1	Financial Risks: System errors are not detected or resolved, resulting in financial loss.	All key issues reported by users should be logged. The log should include the date it was reported, name of user, description of issue, resolution and date resolved.	Low	Systems Officer	A log is now in place.	Completed
4.2.2	Financial Risks: Budget monitoring is impacted by system or interface failures.	Change control procedures should be documented detailing the process for making changes to the system. The procedures should clearly outline the type of changes subject to the procedure, any exceptions, testing requirements and signoffs.	Low	Systems Officer	Change control procedures are now in place.	Completed

Report Ref.	Risk	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.2.2	Financial Risks: Budget monitoring is impacted by system or interface failures.	The disaster recovery plan for the system should be confirmed, including the recovery time objective and details of when it was last tested.	Medium	Principal Accountant (Systems)	The disaster recovery plan will be confirmed with Technology One. The Principal Accountant (Systems) will liaise with ICT colleagues to establish how to use the Council's cloud security questionnaire to address this.	End of January 2024
4.3.1	Legal and Regulatory Risks: Loss of data.	Confirmation should be sought on what backups are taken, including frequency, retention, testing, recovery point objective and storage of backup copies. Storage should include an offline copy for protection against ransomware attacks.	Medium	Principal Accountant (Systems)	The backup processes will be confirmed with Technology One. The Principal Accountant (Systems) will liaise with ICT colleagues to establish how to use the Council's cloud security questionnaire to address this.	End of January 2024
4.4.1	Reputational Risk: There is no accountability for changes made to the system or data.	Further details on the operation of the audit logging system should be confirmed with the supplier.	Low	Principal Accountant (Systems)	The configuration of audit logging reports will be confirmed with Technology One. The Principal Accountant (Systems) will liaise with ICT colleagues to establish how to use the Council's cloud security questionnaire to address this.	End of January 2024

Report Ref.	Risk	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.5.1	Fraud Risk: Weak logical security leading to unauthorised access.	The new password policy being proposed should be implemented, apart from the expiry period which should be re-considered.	Medium	Head of Customer and Digital Services	The revised password policy will be sent to SLT for approval and implementation by 02/02/2024. The policy will then be applied to all users of T1 via the Council's single authentication mechanism. Feedback regarding password change frequency will be noted for discussion with SLT accordingly.	2 February 2024
4.5.2	Fraud Risk: User access is not correctly defined, leading to unauthorised changes to data.	The following should be undertaken:	Medium			
		- A risk be added to the Finance risk register for the way access profiles are setup.		Head of Finance and Audit and Risk Manager	This will be flagged to be considered as part of the next review of the Finance risk register.	End of March 2024
		- Key / sensitive functions, such as changes to supplier bank details, be limited to designated users.		Systems Officer	This has been completed.	Completed
		- An annual documented review of Finance user access be performed.		Principal Accountant (Systems) and Systems Officer	An email will be sent to the relevant Finance section heads on an annual basis to confirm that users with the Finance profile still require this level of access.	End of March 2024

* The ratings refer to how the recommendation affects the overall risk and are defined as follows:

High: Issue of significant importance requiring urgent attention.
Medium: Issue of moderate importance requiring prompt attention.
Low: Issue of minor importance requiring attention.