INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	System Ownership and Management
TO:	Head of Customer and Digital Services	**DATE:**	29 January 2024
C.C.	Chief Executive Deputy Chief Executive Head of Finance 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 Corporate IT systems and business applications are critical assets that should be managed effectively to ensure they continue to support the Council’s objectives. Clear lines of accountability and responsibility should exist for all IT business applications.

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. No details are maintained on key line of business IT systems and their owners.
2. Roles and responsibilities for managing IT systems are not clearly defined between Digital Services and service areas.

3. Service areas do not have the skills to manage IT systems in accordance with corporate policies.
4. There is no structure in place to review IT system issues and development opportunities.

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 area was last audited in 2018-19. However, as the scope of this audit differs from the last one a follow-up of previous recommendations has not been undertaken.

4.2 Potential Risks

4.2.1 Potential Risk: No details are maintained on key line of business IT systems and their owners.

Digital Services maintain a list of all current IT business applications on SharePoint. The details held about each IT business application include name, hosting location i.e. on-premise or cloud, name of supplier, system owner, system owner delegates (for when the system owner is not available) and system administrators. Sample testing confirmed that these details are held for the following three key IT business applications:

- Acolaid (which includes Planning, Building Control and Land Charges);
- ActiveH Housing; and
- Civica Revenues.

Details start to be collected when systems are under development so that they are in place for when the system goes live. This was confirmed for the TotalMobile solution which is currently being developed.

A review of all system owners and reaffirmation of their roles and responsibilities should be performed annually. However, for the sample of three IT applications tested, Acolaid was last reviewed in September 2020, ActiveH in January 2022 and Civica in March 2022.

Recommendation

A review of all system owners and reaffirmation of their roles and responsibilities should be performed annually.

IT business applications are prioritised for recovery purposes but we found the details are out-of-date.

Recommendation

The priority level of IT business applications should be reviewed.

4.2.2 **Potential Risk: Roles and responsibilities for managing IT systems are not clearly defined between Digital Services and service areas.**

System owner responsibilities are documented within section 6.7 of the Information Security and Conduct Policy. Further details, based on the policy, are published on the Intranet. As part of the annual review of system owners, they are emailed the role and responsibilities from the service desk and are required to formally acknowledge them.

Digital Services have a dedicated Application Support team that help support all corporate business IT applications. The team comprises of a team leader and five lead analysts. Responsibilities are documented in job descriptions.

4.2.3 **Potential Risk: Service areas do not have the skills to manage IT systems in accordance with corporate policies.**

Service areas are responsible for ensuring their system administrators are suitably trained. System administrators should receive formal training when new IT business applications are implemented, or on the job training if there are any changes to staff roles. For the three IT business applications tested, Acolaid, ActiveH and Civica, the Digital Services Application Support Team Leader confirmed there are proficient system administrators within service areas. We confirmed the same for the finance system when completing the recent finance IT application audit.

Each IT business application has a nominated lead analyst in the Digital Services Application Support Team. The lead analyst is the person with the greatest knowledge and experience of the IT application.

Each service area is responsible for managing user access to their IT business application. System owner responsibilities include ensuring the principle of least privilege is followed, removing accounts for staff leavers and performing an annual audit to validate existing user rights.

HR circulate details of starters, leavers and movers to service areas / teams for them to take the appropriate action. A review of the distribution list found it includes 16 service areas / teams in total. For the three IT business applications tested, the distribution list includes service areas using ActiveH Housing and Civica Revenues but not the Acolaid application.

Recommendation

The HR distribution list for starters, leavers and movers should be reviewed to ensure it includes service areas / teams of all key IT business applications.

4.2.4 **Potential Risk: There is no structure in place to review IT system issues and development opportunities.**

Prior to the pandemic, there was an ICT Steering Group that was attended by Digital Services, Deputy CEO and Heads of Service. In 2021, the group merged with a HR group to form the Workforce Steering Group (WSG). The WSG focusses more on HR matters than ICT. Also, as the WSG is attended by Heads of Service, who are not involved in the day-to-day operational management of IT systems in their areas, it cannot be used to discuss / review specific IT system issues or development opportunities.

Discussions have been held about creating a new Transformation Steering Group, which would include Digital Services and service area representatives who have operational IT responsibilities. This type of group would provide a more effective governance structure for managing IT business applications and help ensure closer working between Digital Services and service areas on IT matters.

Recommendation

An IT working group containing Digital Services and service area IT representatives should be established.

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:

- Risk 1 – No details are maintained on key line of business IT systems and their owners.
- Risk 3 - Service areas do not have the skills to manage IT systems in accordance with corporate policies.
- Risk 4 – There is no structure in place to review IT system issues and development opportunities.

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 System Ownership and Management 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 System Ownership and Management – January 2024

Report Ref.	Risk	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.2.1	No details are maintained on key line of business systems and their owners.	A review of all IT system owners and reaffirmation of their roles and responsibilities should be performed annually.	Medium	Application Support Team Leader	System Owner review tasks will be revisited and brought up to date. This will be done on a month-by-month basis for our business applications. Thus, spreading the reviews out over the year to ensure they don't all fall at the same time.	Ongoing
4.2.1	No details are maintained on key line of business systems and their owners.	The priority level of IT business applications should be reviewed.	Medium	Application Support Team Leader	Old priority recovery list will be reviewed and brought up to date. Will also published in a more accessible place.	April 24
4.2.3	Service areas do not have the skills to manage IT systems in accordance with corporate policies.	The HR distribution list for starters, leavers and movers should be reviewed to ensure it includes service areas / teams of all key IT business applications.	Low	Application Support Team Leader	Will review current list and liaise with HR to amend where appropriate. Notifications to key services areas when people start, leave or change roles has also been covered in the Identity and Access Management Policy that was approved by SLT.	April 24

Report Ref.	Risk	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.2.4	There is no structure in place to review system issues and development opportunities.	An IT working group containing Digital Services and service area IT representatives should be established.	Medium	Head of Customer & Digital Services	The formation of an ICT Steering Group will be discussed with the Senior Leadership Team in March for implementation during April 24.	May 24

* 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.