2024 INTERIM REPORT

Brisbane City Council

4 June 2024

Queensland Audit Office
Better public services

Queensland
Audit Office
Better public services

The Right Honourable the Lord Mayor of Brisbane
Councillor A Schrinner
Brisbane City Council

Dear Lord Mayor

2024 Interim report

We present our interim report for Brisbane City Council for the financial year ending 30 June 2024. Our interim audit was undertaken in February-March 2024 and covers our audit of controls over key process for the period 1 July to 31 December 2023. As such, this report details the results of our interim work performed to 31 December 2023.

In May 2024, we will performing additional testing over the key controls for the period 1 January to 31 March 2024 and any matters arising will be reported separately.

Results of our interim audit

We have assessed the design and implementation of your internal controls relevant to the financial report (financial controls), and whether they are operating effectively. Our audit does not assess all controls that management has implemented across the organisation.

Our audit did not identify any significant deficiencies over the key controls. We have however identified **8** deficiencies relating to your IT environment.

A deficiency arises when internal controls are ineffective or missing, and are unable to prevent, or detect and correct, misstatements in the financial statements. A deficiency may also result in non-compliance with policies and applicable laws and regulations and/or inappropriate use of public resources.

In addition to the above, we have also identified 5 other matters – these are business improvement opportunities that may improve the efficiency and/or effectiveness of internal controls, but does not constitute a deficiency in internal controls.

These have been further explained in section 1 to this report.

Conclusion on our interim audit

The deficiencies identified above do not directly affect the council's financial reporting process. As such, they will not impact our planned audit strategy as communicated in our external audit plan.

Based on the results of our testing completed to date, we have determined your internal control environment supports an audit strategy where we can rely upon your entity's controls.

Other audit related matters

We have issued a separate briefing note to the audit committee and management on the status of the audit. In short, the audit of council's financial statements has progressed in line with the audit plan that was agreed with council in November 2023.

If you have any questions or would like to discuss the audit report, please contact me on 3149 6208 or Megan Manuel on 3149 6122.

Yours sincerely

Sri Narasimhan
Senior Director

Enc.
cc. Mr T Wright, Acting Chief Executive Officer
Ms G Juke, Chair of the Audit Committee

1. Status of issues

Internal control issues

The following table identifies the number of deficiencies in internal controls and other matters we have identified. Details of the deficiencies we identified during our interim audit are outlined further in this section. Refer to section 2 *Matters previously reported* for the status of previously raised issues.

Year and status	Significant deficiencies	Deficiencies	Other matters*
Current year issues	-	8	5
Prior year issues – unresolved	-	-	-
Total issues	**-**	**8**	**5**

Note: *Queensland Audit Office only tracks resolution of other matters where management has committed to implementing action.

The following section details control deficiencies and other matters identified as at the date of this report. It includes a response from management.

Our ratings are as follows. For more information and detail on our rating definitions, please see the webpage here: www.qao.qld.gov.au/information-internal-controls or scan the QR code.

Internal control issues

S	D	O
Significant deficiency	Deficiency	Other matter

D Deficiency

24-IR1 Active Directory–service accounts lacking appropriate security configuration

Observation

Council creates and manages ‘service accounts’ within its Active Directory to support background processes and jobs. These accounts are assigned to a security group to so these processes can occur without someone manually logging in (interactive login) to undertake these processes. Due to the nature of these accounts, they need to be configured with certain access levels.

We noted the following:

- 10 service accounts are not assigned to a security group nor are they listed in the exemption register. An exemption register is a register that contains a list of user accounts that are exempt from council’s normal access level protocols. These are maintained for various purposes, including overriding access levels, but with appropriate authority and approval.
- 4 service accounts were not listed in the Active Directory user extract provided to us nor were they included in the exemption register. We have reviewed the activities of these 4 services accounts and did not identify any transaction that have impacted the financial statements.

Implication

Service accounts are generally a target for external attacks as they are often not monitored, due to the nature and the purpose for which they are set up.

If a service account is compromised, this can give the attacker access to sensitive information maintained in the Council’s computing environment.

QAO recommendation

We recommend council reviews and updates the 10 service accounts for inclusion in the security group or updates the exemption records where appropriate.

We also recommend that council investigates the purpose for the 4 service accounts not identified in Active Directory user extract and monitors how these accounts are managed and secured.

Management response

Council agrees with the QAO recommendations. ISB will investigate and implement corrective actions to reduce the risk to an acceptable level.

Status: Work in Progress

Responsible Officer: Manager ICT Service Operations

Due Date: 30 September 2024

D Deficiency

24-IR2 Dormant user accounts not actioned in a timely manner

Observation

There is currently no process at council to review and monitor user accounts that are dormant/inactive but have access to council's IT environment (active directory and applications). Additionally, there is also no policy on how to manage these dormant accounts, including for how long council keeps these dormant accounts open prior to deactivating them.

We identified the following dormant user accounts in the council's IT environment:

IT environment	Total of users inactive for more than 90 days	Inactive users that never used their credentials
Active directory	1,642 users	146 users
Microsoft Entra	312 users	274 users

Implication

Lack of review of dormant user accounts increases the risk of these user accounts being compromised, resulting in unauthorised access to council's data.

This risk is heightened if the dormant user account that is compromised is a privileged account. This could provide the attacker with access to council's sensitive information.

QAO recommendation

We recommend council:

- establish a process to review dormant user accounts and disable unused user accounts on a regular basis
- determine an appropriate threshold on how long a dormant user account remains in the IT environment.

Management response

Council agrees with the QAO implications. ISB will investigate and implement corrective actions to reduce the risk to an acceptable level.

Status: Work in Progress

Responsible Officer: Manager ICT Service Operations

Due Date: 31 May 2025

D Deficiency

24-IR3 User accounts of terminated employees not disabled

Observation

We identified 11 users whose access was not disabled in council's active directory and Microsoft Entra at the time their employment was terminated with council.

The time lag for disabling these credentials is provided in the table below.

IT environment	Active beyond termination date for		
	Up to 90 days	90-180 days	Greater than 180 days
Active directory and Microsoft Entra[1]	9 users	1 user	1 user

[1] *Microsoft Entra is a cloud-based version of Active Directory. It can integrate with Active Directory and provides authentication and authorisation services for various Microsoft and other Software as a Service (SaaS) applications.*

Out of these 11 user accounts:

- 1 user recorded a log on event to Active Directory after the date of termination and
- 7 users recorded a log on event to Microsoft Entra after the date of termination.

Whilst we have not investigated what these 11 user accounts have accessed post their termination date, we can confirm these accounts have not posted any transactions in the financial ledger.

Implication

When access of terminated staff members is not disabled in a timely manner, it provides the terminated staff an opportunity to access council's system that they are not entitled to.

This may result in them accessing sensitive information and the potential for fraudulent transactions being processed in financial systems.

QAO recommendation

We recommend council:

- implements an automated process whereby user accounts are disabled for terminated staff on their last day of employment
- investigates whether there were any activities undertaken by these terminated employees in council's IT environment post their termination date.

Management response

Council agrees with the QAO recommendation and has acted. On investigation, ISB has identified that the samples QAO identified were back-dated terminations raised by the terminating manager and are therefore a process issue rather than a technology synchronisation issue.

Status: Work in Progress

Responsible Officer: Manager ICT Service Operations

Due Date: 31 August 2024

D Deficiency

24-IR4 Microsoft Entra–security configuration settings have not been set to recommended values

Observation

We noted security settings in the Microsoft Entra environment have not been configured to align with industry values as recommended by Centre for Internet Security (https://www.cisecurity.org/benchmark/azure). Where these industry standards are not followed, council should document how they have configured Microsoft Entra to fit the needs of their IT environment.

We note that council has not implemented the following recommendations from the Centre for Internet Security that would strengthen its Microsoft Entra's environment:

- restricting the ability of all users to create security groups in Microsoft 365
- restricting the ability of all users to invite any internal or external person to collaborate on council domain, such as SharePoint Online.

Implication

Administrators may inadvertently use incorrect or unauthorised security groups and accidentally give unauthorised access to resources.

Ability to collaborate on council domain should be restricted to only staff and external contacts that have a business relationship with council. In the absence of such restrictions, council could be at a risk of exposing its sensitive information and IT system to unauthorised access, especially where such invites are either inadvertently or on purpose sent to an external user.

QAO recommendation

We recommend council review the configuration settings and align them with the recommendations made by the Centre for Internet Security.

Management response

Council agrees with the QAO implication and notes the recommendations. ISB will review the configuration settings to determine appropriateness with consideration to operational requirements. Alternative compensating controls will be added where required.

Council provided information to QAO regarding various operational requirements (as specified in design and architecture documents) to confirm that the configuration of Entra is deliberate and considered to ensure operational efficacy (e.g. integration to MS Teams).

Status: Work in Progress

Responsible Officer: Manager ICT Service Operations

Due Date: 30 June 2025

D Deficiency

24-IR5 Microsoft Entra–Privileged Identity Management (PIM) is not configured to require approval for use of privileged roles

Observation

Privileged Identity Management (PIM) is a service in Microsoft Entra that enables greater control and management of privileged user accounts. PIM improves security by providing configurable access controls for use of privileged user accounts. Examples include requiring formal approval to use a privileged role to perform administration tasks, and enforcement of multi-factor authentication (MFA).

User accounts are configured to either be:

a. *active accounts* – these accounts do not need approval to be a privileged account.

b. *eligible accounts* – meaning these accounts need approval to be used as a privileged account.

Additionally, privileged role assignments are either *permanent* (having no end date) or *time-bound* (only allowed for use during a specified time period).

We noted, however, that all user accounts in Microsoft Entra – privileged and non-privileged accounts – were assigned a permanent role with no expiration date, meaning PIM was not achieving its purpose.

Implication

Assigning permanent roles to all users in PIM does not achieve the purpose of PIM which provides better control and monitoring over users performing privileged tasks.

This may increase the risk of a user having unauthorised access to sensitive resources.

QAO recommendation

We recommend council effectively uses the PIM function where it:

- reviews and, where possible, removes the permanent roles of privileged users
- implements a process where privileged roles are requested and assigned as needed and that such requests are assigned for a specific time period.

Management response

Council agrees with the QAO implication. ISB will investigate and implement corrective actions to reduce the risk to an acceptable level.

Status: Work in Progress

Responsible Officer: Manager ICT Service Operations

Due Date: 30 April 2025

D Deficiency

24-IR6 Microsoft Entra–on-premises Active Directory accounts are synchronised and granted Microsoft Entra privileged roles

Observation

Council uses Active Directory to access on-premises systems and uses Microsoft Entra to access cloud-based systems. Council synchronises these two environments to allow existing information in Active Directory to be replicated to Microsoft Entra.

This includes synchronisation of all user accounts and their passwords – such that a staff that has privileged access to the on-premises Active Directory can also have privileged access to Microsoft Entra.

Although this seems operationally convenient, Microsoft does not recommend synchronising user accounts with privileged access in both environments This is to prevent a malicious user from obtaining access to both environments should a user account in one environment be compromised. This is especially important where the user has privileged access levels.

We found a total of 13 privileged user accounts where their access between the two environments was synchronised.

Implication

Synchronising users between the two environments, especially for users with privileged access levels, can put council’s on-premises and cloud-based environment at risk if the user credentials are compromised. This can potentially give the attackers access to council’s financial and non-financial data and other sensitive information.

QAO recommendation

We recommend council review their current synchronisation of user accounts to ensure no privileged on-premises Active Directory user accounts are synchronised with Microsoft Entra.

Management response

Council agrees with the QAO implication. ISB will investigate and implement corrective actions to reduce the risk to an acceptable level.

Status: Work in Progress

Responsible Officer: Manager ICT Service Operations

Due Date: 30 June 2025

D Deficiency

24-IR7 SAP ECC–background system users assigned with standard SAP profiles

Observation

In SAP, the background system accounts serve specific technical functions such as some automated tasks, system maintenance and data processing. Unlike regular user accounts, the background system accounts do not have interactive logins or direct human interactions.

The background system accounts are set up by the vendor to undertake specific tasks in the SAP system such as installation of a specific function/module. These accounts, due to the nature of the tasks they perform, are also assigned higher levels of access than a normal user access levels.

Due to this, there needs to be a specified time that these background system accounts should be set up for. Once their purpose is achieved, they need to be deactivated. We however found that there are 41 background system accounts were set up in SAP on a permanent basis.

Implication

Given that background system accounts are set up for a specific purpose, these accounts are not generally monitored for their usage.

When such accounts are left open (i.e. not deactivated after achieving their purpose), there is a risk that these login credentials may be used for unauthorised access to council's systems.

QAO recommendation

We recommend that council implements a mechanism whereby background system accounts are deactivated/suspended once the necessary tasks are undertaken.

Management response

Council agrees with the QAO recommendation. Council will take action to review the 41 accounts and reduce where possible based on the functional and operational impacts of any reduction in access permissions.

Council will also investigate what monitoring and reporting can be applied to allow greater visibility of changes to these types of accounts.

Status: Work in Progress

Responsible Officer: Manager ICT Commercial Services

Due Date: 30 May 2025

D Deficiency

24-IR8 SAP ECC–timeliness of SAP FireFighter session reviews

Observation

Users are assigned FireFighter access (a superior level of privileged access) in SAP for undertaking emergency or critical tasks. These access levels are assigned by a FireFighter Controller, who is also responsible for undertaking the review of each FireFighter session (each time a FireFighter logs into SAP).

The review process involves verifying the appropriateness of actions taken during these sessions, ensuring compliance with policies, and promptly addressing any anomalies.

Council has implemented a formalised process (as per Council's *Emergency Access Management (FireFighter)* guideline) to review SAP FireFighter sessions within 3 days.

Automated emails from SAP are sent out to the FireFighter Controller for any sessions that have not been reviewed in 3 days. If no action is taken within 3 days of the automated email being sent, an escalation email is sent to the Line Manager of the FireFighter Controller to perform the review.

Despite this process being in place, we noted that 12 of the 94 FireFighter sessions were not reviewed within the stipulated 3-day timeframe.

These reviews were escalated to the Line Manager; however, they were returned to the original FireFighter Controllers who we understand are not employed with the Council anymore or are on leave. As at the date of our review, we note that:

- 4 reviews remained unreviewed for 8 to 15 days
- 8 reviews remain unreviewed for after 21 days or greater.

Implication

The delayed review of FireFighter activities poses security and compliance risks. Lack of timely review may result in unauthorised tasks or potential misuse of privileges not being detected timely.

QAO recommendation

We recommend that council identifies an alternate reviewer to complete the review in the absence of the original reviewer.

Management response

Council agrees with the QAO recommendation. Council will engage with SAP to determine an effective way to ensure the escalation process continues in the absence of default responders. Council will provide refresher training on the FireFighter process including features of escalations to reviewers and line managers.

Status: Work in Progress

Responsible Officer: Manager ICT Commercial Services

Due Date: 31 October 2024

O Other matter

24-IR9 Active Directory–one user account has password set to never expire

Observation

We identified the Active Directory account for one external consultant does not require the user to change the password regularly (i.e. the account's password is set to never to expire).

When passwords are set to not expire, this can increase the risk of passwords being compromised more easily. Other than not meeting internal compliance requirements, this also exposes council to the risk of unauthorised access to their IT environment.

QAO recommendation

We recommend council reviews and sets the password expiry for the user account identified.

Management response

Council agrees with the QAO recommendation. Fully resolved. Council has reviewed and set password expiry for the identified account.

Status: Resolved pending audit clearance

Responsible Officer: Manager ICT Service Operations

Due Date: 18 April 2024

O Other matter

24-IR10 Microsoft Entra–user accounts in Microsoft Entra are not disabled when their corresponding on-premises Active Directory user account is disabled or expired

Observation

Council has a mechanism whereby when a user is provided access to the Active Directory (on-premises), they are also automatically assigned corresponding access to Microsoft Entra (a cloud-based version of Active Directory).

We noted whilst assigning the access levels in the two environments are synchronised, the disabling of access is not. As a result, we identified 23 user accounts where access to the Active Directory was disabled yet their corresponding access to Microsoft Entra was not.

We also note that when a user accesses Microsoft Entra, there is a Pass-Through Authentication (PTA) method. The PTA method ensures that any access to the Active Directory through Microsoft Entra is validated prior to accessing the Active Directory, hence limiting the risk for unauthorised access.

QAO recommendation

We recommend council:

- manually disables or removes the 23 user accounts in Microsoft Entra to ensure consistency between on-premises Active Directory and Microsoft Entra
- investigates whether any of the identified user accounts have been used past their disablement or expiration date for authentication to Microsoft Entra
- investigates why the 23 user accounts that were disabled on-premises did not have their paired user account in Microsoft Entra disabled via synchronisation.

Management response

Council agrees with the QAO implication. ISB will investigate and take action to resolve any unexpected synchronisation issues noted between AD and Entra and implement a process to check / resolve synchronisation issues between AD and Entra.

Status: Work in Progress

Responsible Officer: Manager ICT Service Operations

Due Date: 29 October 2024

O Other matter

24-IR11 Active Directory–fine-gained password policy is not reflected in the password policy standard and is not updated

Observation

Fine Grained Password Policies (FGPP) in Active Directory allows for the creation and use of different password policies to the default password policy where required on an exception basis.

A document titled, *QAO Default policy remediation approach,* lists the use and configurations of each current FGPP within Council. This document was created by council to address a previous audit issue identified by QAO. However, we found that the remediation approach document is not referred to in Council's *ICT Security Standard: Access Control & Account Management*.

QAO recommendation

We recommend that Council ensures the details of the FGPPs are recorded within the Council's *ICT Security Standard: Access Control & Account Management* for easy reference.

Management response

Council agrees with the QAO recommendation. ISB will investigate and implement corrective actions to reduce the risk to an acceptable level.

Status: Work in Progress

Responsible Officer: Manager ICT Service Operations

Due Date: 30 November 2024

O Other matter

24-IR12 Microsoft Entra–use of privileged role assignments

Observation

Microsoft Entra provides pre-configured roles to provide a robust role-based access control (RBAC) framework. This assists in delegating administration responsibilities while abiding by the principle of least privilege. Of the over 100 built-in Microsoft Entra roles, just over 20 of the roles are considered 'privileged'.

It is recommended by Microsoft that no more than 10 privileged roles are used at any time. However, we note that Council currently has 14 active privileged roles assigned in the Microsoft Entra environment.

The use of numerous privileged roles could inadvertently lead to unknown or unauthorised elevation of privilege.

QAO Recommendation

We recommend council:

- reviews the use of privileged role assignments within Microsoft Entra to ensure that each role assignment is understood as to what permissions and functionality it provides
- uses the minimum number of role assignments to fulfill its operational requirements
- implements regular access reviews to remove unneeded membership in privileged roles.

Management response

Council agrees with the QAO implication. ISB will investigate and implement corrective actions to reduce the risk to an acceptable level. Where unnecessary Entra privileged roles are assigned, these will be removed where the baseline security foundations are not compromised.

Status: Work in Progress

Responsible Officer: Manager ICT Service Operations

Due Date: 15 March 2025

O Other matter

24-IR13 SAP ECC–SAP obsolete clients not deleted

Observation

During the initial installation and setup of SAP systems, the system automatically generates SAP standard users. These user accounts, by default, have privileged access and play critical roles in system operations.

The vendor assigns well-known default passwords to these SAP standard user accounts. SAP recommends organisations to change these default passwords after installation to prevent unauthorised access to the system.

We identified that Council has not changed the default password for one of its accounts.

QAO recommendation

We recommend that Council changes the default password for this account.

Management response

Council agrees with the QAO recommendation and has removed these accounts as a result.

Status: Resolved pending audit clearance

Responsible Officer: Manager ICT Commercial Services

Due Date: 29 April 2024

2. Matters previously reported

Our ratings are as follows. For more information and detail on our rating definitions, please see the webpage here: www.qao.qld.gov.au/information-internal-controls or scan the QR code.

Internal control issues

S	D	O
Significant deficiency	Deficiency	Other matter

The following table summarises the status of deficiencies, financial reporting issues, and other matters previously reported to you.

Ref.	Rating	Issue	Status
23-CR1	D	**Exceptions identified with employee on-boarding process** Employment details entered into the system were not in accordance with their signed agreements.	**Resolved** Controls over the on-boarding checking process have been strengthen.

qao.qld.gov.au/reports-resources/reports-parliament

Suggest an audit topic

Contribute to an audit in progress

Subscribe to news and our blog

Connect with QAO on LinkedIn

Sri Narasimhan
Queensland Audit Office
T: 3149 6208
E: Sri.Narasimhan@qao.qld.gov.au

T: (07) 3149 6000
E: qao@qao.qld.gov.au
W: www.qao.qld.gov.au
53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002

Queensland Audit Office
Better public services