2023 FINAL MANAGEMENT LETTER

Brisbane City Council

5 September 2023

Queensland
Audit Office
Better public services

Your ref:
Our ref: 2023-3961
              Sri Narasimhan 07 3149 6208

5 September 2023

The Right Honourable the Lord Mayor of Brisbane
Councillor A Schrinner
Brisbane City Council
GPO Box 2287
BRISBANE QLD 4001

Dear Lord Mayor

Final management report for Brisbane City Council

We have completed our 2023 financial audit for Brisbane City Council. The Auditor-General issued an unmodified audit opinion on your financial statements.

The purpose of this letter is to provide the council with details on audit matters and other important information related to the audited financial statements.

Reporting on issues identified after the closing report

I can confirm that we have not identified any significant issues since the presentation of our closing report. The issues and other matters we have formally reported to management and an update on management's actions taken to resolve these issues is included as Appendix A.

Report to parliament

Each year we report the results of all financial audits and significant issues to parliament.

We intend to include the results of our audit of Brisbane City Council in our report to parliament *Local Government 2023*. We will comment on the results of our audit of your financial report, any significant internal control issues we identified, and the overall results of the sector, including major transactions and events. We will discuss the proposed content of our report with your Chief Financial Officer and continue to consult as we draft our report. Formally, you will have an opportunity to comment on our report, and for these comments to be included in the final version tabled in parliament.

Queensland Audit Office   Phone   07 3149 6000
Level 13, 53 Albert Street, Brisbane Qld 4000   Email   qao@qao.qld.gov.au
PO Box 15396, City East Qld 4002   Web   www.qao.qld.gov.au
                                                                     Queensland Audit Office (QAO)

Audit fee

The final audit fee for this year is $538,500 exclusive of GST (2022: $535,000). This fee is in line our estimate in our external audit plan.

We would like to thank you and your staff for their engagement in the audit this year and look forward to working with your team again next year.

If you have any questions about this letter or would like to discuss any matters regarding our services and engagement, please do not hesitate to contact me on 07 3149 6208.

Yours sincerely

Sri Narasimhan
Senior Director

Enc.

cc.   Mr C Jensen, Chief Executive Officer
        Ms G Jukes, Chair of the Audit Committee

Appendix A1 – Status of issues

This section provides an update on the control deficiencies we have identified. It includes a response from management.

Our risk 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 Significant deficiency   **D** Deficiency   **O** Other matter

Financial reporting issues

H High   **M** Medium   **L** Low

D **Deficiency**

23-CR-1 Exceptions identified with employee on-boarding process

Observation

As a part of our review over employee on-boarding process, we identified the following exceptions:

- One employee was appointed at the incorrect band i.e pay rate in the system. This has now been corrected and back payment has been made to the employee.

- One employee's appointment date in the system did not match letter of offer. Council has confirmed the correct process was not followed and a new letter of offer should have been issued to reflect the change in start date.

- One employee's end date in the letter of offer was before their start date.

- One employee's position type (temporary fulltime) was incorrect in letter of offer. This has now been corrected with the system reflecting the correct pay as per the letter of offer and payscale group.

Implication

While the impact is not material, council has an obligation to ensure employees are paid appropriately and in accordance with their agreements.

QAO recommendation

We recommend employment details entered in the system be independently reviewed for accuracy. Council should also ensure that the document signed in relation to the appointment are accurate.

Management response

Employee Services and Payroll Services (Pay Audit) teams have added additional controls to ensure the data on the SuccessFactors offer letter is consistent in the payroll system. Additional fields in the SARD document have been added to which include Pay scale, Pay point and a manual confirmation check from each recruiter to ensure these details are accurate and consistent. Pay Audit will also add an additional step to ensure start and end dates, pay scale and pay points are reviewed from the SARD and cross referenced in the payroll system. Pay Audit currently review 100% new hires and re-hires that are added to the payroll system from the recruitment team.

SENSITIVE

Council currently has strong controls in place where the hiring manager and delegate (level 1,2 or 3 delegate) must approve the offer to the candidate in SuccessFactors prior to the recruitment team being able to generate the Letter of Offer. The approval in SuccessFactors contains all information related to the recruitment process, start date, end date (if applicable) as well as the pay scale and pay point. By implementing the additional control on the SARD, this will ensure consistency in the documents being generated. Employee Services has also put additional processes in place on a monthly basis to audit a sample set of data to confirm accuracy in the pay scale, pay point, start and end sates as well as Letter of Offer quality.

These additional controls were implemented on 5 June 2023.

> Status: Resolved pending audit clearance

23-CR-2 Financial System – Access to administer batch jobs not restricted

Observation

We identified 15 user accounts (internal and managed service provider) who can create or modify a scheduled program that the system will run automatically without human interaction (also known as batch jobs).

Council does not specifically assign this level of access to these users. The users, however, inadvertently obtained the access because of the combination of their existing access privileges in the system.

We have confirmed that the identified users have not processed any transactions in the general ledger system in the current year. While there is no current financial risk there may be in the future, if these access levels are not restricted.

Better practice suggests that access to create or modify batch jobs should be secured to a process that ensures accountability of use. Council has implemented corrective actions on 29 March 2023.

Implication

There is a risk that unauthorised system changes remain undetected in the system when the system executes unauthorised batch jobs. This may result to undesirable outcomes, such as:

- unauthorised changes to user access
- unauthorised changes to system configuration
- unauthorised batch transactional processing.

QAO recommendation

We recommend that Council restricts the access to maintain and administer batch jobs to a process that ensure accountability of use.

Management response

Council have restricted the access to maintain and administer batch jobs on 23 March 2023 as verified by the QAO. QAO have verified that the identified users have not processed any transactions in the general ledger in the current financial year. Future batch job processes will be executed only via Firefighter or approved role access permissions.

> Status: Resolved

SENSITIVE

23-CR-3 Financial and Operating Systems – System administrator's accounts not used effectively

Observation

Council creates system administrator accounts for staff members who need to maintain, manage, and support the systems. This includes access to servers hosting critical business applications. Council has engaged a managed service provider (MSP), Tata Consultancy Services, as system administrators and to manage these servers.

We identified 20 system administrator accounts assigned to the MSP. Council, however, did not create 2 separate accounts for them, i.e., for day-to-day activities and system administrator activities. Instead, the system administrator accounts are used for both everyday business functions (for example, browsing internet and accessing emails) and for system administration activities.

The Australian Cyber Security Centre recommends that the assignment of administrative and other high privileged access should be assigned by creating a separate user account that a user can use when they are performing high privileged tasks in the system. The purpose of a separate account is to ensure sensitive and/or critical system administrative tasks are performed using special elevated permissions only when absolutely required.

Implication

Better practice is for system administrators to have a standard/regular account to perform their day-to-day activities and a separate administrative account used only when really required, and for the shortest time required.

When system administrator uses their administrator account for day-to-day functions, this can increase the risk of cyber security incidents. For example, the account will be vulnerable to phishing and malware attacks.

QAO recommendation

We recommend that Council to create a separate general user account for the system administrators for their everyday business functions.

Management response

Council agrees with the issue and QAO recommendation. Separate general user accounts (without administrative privileges) have been created for the system administrators for their everyday business functions. The existing privileged accounts have been preserved exclusively for critical and sensitive system administrative responsibilities.

Status: Resolved

SENSITIVE

O **Other Matter**

23-CR-4 Financial and Operating Systems – System settings not appropriately secured or configured

Observation

We reviewed the financial system and the underlying Windows operating systems and noted that some server settings were not appropriately secured or configured per better practices recommended by the vendor.

Implication

Strengthening of servers with higher levels of security protects sensitive data stored on the server and prevents unauthorized users from using and accessing the data for malicious purposes.

QAO recommendation

We recommend Council performs a risk assessment and configures the financial system and operating systems based on the vendor's recommended settings.

Management response

Council has modified the system configuration to align with the vendor's recommended settings. This reconfiguration was completed 14 July 2023, and will be activated by system restart – planned to occur between 17 July 2023 and 29 July 2023.

Status: Resolved

SENSITIVE

Appendix A2 – Matters previously reported

The following table summarises all control deficiencies, financial reporting issues and other matters that have previously been raised but are not yet resolved. The listing includes issues from our reports this year and those issues raised in prior years.

Internal control issues			Financial reporting issues		
S Significant deficiency	**D** Deficiency	**O** Other matter	**H** High	**M** Medium	**L** Low

Ref.	Rating	Issue	Status and comment
23-IR-3	**D**	**Service accounts need to be secured** Council should secure the service accounts and investigate the 38 service accounts to disable interactive login to improve security, where applicable.	**Resolved** All 38 have been investigated and action taken.
22-IR-3	**O**	**Define critical functions for monitoring privileged user activities in 3 systems** To define what the critical functions are in all systems and monitor privileged user activities.	**Resolved** Identification and assessment of critical activities that require monitoring is now completed.

SENSITIVE

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: 07 3149 6208
E: Sri.Narasimhan@qao.qld.gov.au

**Queensland
Audit Office**
Better public services