2025 FINAL MANAGEMENT REPORT

Brisbane City Council

9 September 2025

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

Final management report for Brisbane City Council

We have completed our 2025 financial audit for Brisbane City Council. The Auditor-General issued an unmodified audit opinion on your financial statements.

The purpose of this report is to update you on any matters that have arisen since we presented our interim report to you on 6 May 2025.

Reporting on issues identified after the closing report

I can confirm that we have not identified significant issues since the presentation of our closing report to the audit committee. 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.

Please note that under section 213 of the Local Government Regulation 2012*,* you must present a copy of this report at your council's next ordinary meeting.

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 your entity in our report to parliament *Local Government 2025*. We will comment on the results of our audit, any significant internal control issues, and the overall results for the sector, including major transactions and events. We will discuss the proposed report content with your entity contact and continue to consult as we draft it. Formally, entities have an opportunity to comment on our report, and for these comments to be included in the final version tabled in parliament.

Audit fee

The final audit fee for this year is $619,000, exclusive of GST. This fee is in line with the fee estimated in our external audit plan.

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

If you have any questions about this report or would like to discuss any matters regarding our services and engagement, please do not hesitate to contact me on 3149 6208 or Jessica Rossouw, Senior Manager, on 3149 6157.

Yours sincerely

Sri Narasimhan
Senior Director

cc Dr K Freeman, Chief Executive Officer
Ms G Jukes, Chair of the Audit Committee

Appendix A1 – Status of issues

Internal control issues

This section provides an update on the control deficiencies and other matters we have identified since our interim report. 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	D	O
Significant deficiency	Deficiency	Other matter

D Deficiency 25-CR1 Active Directory – Password management of privileged user accounts

Background

Due to the level of access that privileged user's accounts are granted, privileged user accounts are secured with stronger or additional security controls. This can include using stricter password management requirements or increased monitoring.

Observation

Per Council's *ICT Security Standard: Access Control & Account Management*, privileged user accounts are required to have stronger password requirements than standard user accounts. This includes passwords to be more than 8 characters in length, password complexity (e.g. use of upper and lower case letters, numbers and special characters) and to be changed every 365 days.

We identified 132 out of 514 enabled privileged user accounts have not passwords changed for over 365 days:

- 121 privileged user accounts.
- 11 external vendor user accounts.

While the *ICT Security Standard: Access Control & Account Management* states a minimum of 8 character passwords, it was observed the implemented minimum password length for all user accounts is 14 characters.

Additionally, all highly privileged user account passwords are stored and managed in Council's privileged access management (PAM) system that requires multi-factor authentication (MFA) to access any of the passwords.

Implication

Due to their elevated access in a computing environment, privileged user accounts are a target of malicious users. Privileged user account passwords that are not sufficiently protected could be at an increased risk of compromise.

QAO recommendation

We recommend that Brisbane City Council:

- changes the passwords for the identified 132 user accounts, and all other privileged user accounts, no less than every 365 days
- updates the *ICT Security Standard: Access Control & Account Management* to reflect the implemented password policy attributes

- develops, documents and implements an effective governance process to ensure the passwords of privileged user accounts are periodically changed per the documented requirements.

Management response

We agree with the observations.

1. The 132 accounts will be reviewed, and passwords changed where appropriate.
2. The *ICT Security Standard: Access Control & Account Management* will be reviewed to confirm the wording states the minimum password length is 8 characters but can be exceeded for stronger password strength.
3. Establish process to notify - a account users before expiry via MIM.

Responsible officer: Manager ICT Service Operations

Status: Work in progress

Action date: 1 June 2026

D Deficiency 25-CR2 Active Directory – User accounts with passwords set to never expire

Background

It is generally accepted practice for user account passwords to be regularly changed. By regularly changing passwords, an organisation may lower its exposure to compromised passwords.

Observation

Per Council's *ICT Security Standard: Access Control & Account Management*, only service account passwords are to be configured to never expire.

We identified 249 non-named user accounts (not assigned or uniquely owned by a named individual) with passwords set to never expire:

- 7 vendor user accounts
- 11 non-named privileged user accounts (e.g. service accounts, shared generic accounts, etc)
- 47 test user accounts
- 184 generic user accounts (e.g. training accounts).

We noted 201 of the 249 non-named user accounts have not had its password changed for over 365 days.

Implication

User accounts that are configured with a password set to never expire are at an increased risk of compromise. Passwords not regularly changed can increase the risk of stolen, cracked, or guessed passwords being identified and used by a malicious user over extended periods of time.

QAO recommendation

We recommend that Brisbane City Council:

- reviews the 249 user accounts for a valid requirement for the password to be configured to never expire, and configures the user account to expire the password, where possible
- restricts the user accounts with a need for their password to never expire to only allow logon to a specified computing device, where possible
- implements a register to track exceptions for user accounts that require passwords to never expire
- identifies, documents and implements effective compensating or mitigating controls for those user accounts configured with passwords to never expire.

Management response

We agree with the observations.

1. Due to potential service availability impacts, service, generic, test and dashboard accounts are provisioned with passwords set to never expire. This position has been assessed and the potential impact on the affected applications that leverage these service accounts could be significant if they were set to expire.
2. Accounts with no set expiry will be tracked for lifecycle management.
3. Process to review accounts with no set password expiry and address accordingly will be implemented.

Responsible officer: Manager ICT Service Operations

Status: Work in progress

Action date: 1 December 2025

D Deficiency 25-CR3 Active Directory – Account expiry dates are not managed effectively

Background

Active Directory user accounts can be configured with an account expiry date to prevent the user account from further use once the date of expiration has been met. Once expired, a user account can no longer be used unless a system administrator or help desk personnel extends or disables the expiry setting on the account.

The use of an account expiry date is often used for non-employee user accounts, e.g. contractor or vendor user accounts. The expiry date is aligned with the end date of their contract or engagement period.

Council uses the user account expiration attribute for user accounts of contractors and external users to reflect each user's agreed end date. Once expired, the account can no longer be used unless a system administrator or help desk personnel extends or disables the expiry setting on the account.

Observation

Council uses the user account expiration attribute for contractors and external users to reflect each user's agreed end date. Once expired, the account can no longer be used unless a system administrator or help desk personnel extends or disables the expiry setting on the account.

Contractor or external user accounts not configured with an expiry date

We identified 131 contractor or external user accounts that do not have an account expiration date configured:

- 120 contractor user accounts
- 11 external vendor user accounts.

Expired user accounts remain enabled

On-premises Active Directory user accounts, including applicable changes to user accounts, are synchronised to Microsoft Entra and vice versa. Microsoft Entra does not recognise the user account expiry attribute.

We identified 6 user accounts in Active Directory that are expired but remain enabled:

- one named privileged user account
- 2 service accounts
- 3 test user accounts.

Additionally, we noted 4 of the 6 expired user accounts also remained enabled in Microsoft Entra.

We noted that Pass-Through Authentication (PTA) is the authentication method used for Microsoft Entra. Authentication requests to Microsoft Entra by synchronised user accounts are transferred to on-premises Active Directory to validate the request prior to the request being granted.

The use of PTA and stringent use of multi-factor authentication (MFA) for any remote access acts as compensating controls in this instance. We noted no unauthorised authentication activity being performed to Microsoft Entra by the six identified user accounts.

Implication

Contractor or external user accounts not configured with an expiry date

External user accounts that are not configured with an expiry date increase the risk of unauthorised access past the contracted end date should the account remain enabled.

Expired user accounts remain enabled

Expired user accounts that remain enabled are potential security vulnerabilities as they could be exploited by unauthorised users.

QAO recommendation

We recommend that Brisbane City Council:

Contractor or external user accounts not configured with an expiry date

- configures the identified 131 user accounts with an expiry date, where appropriate
- devises and implements an effective governance process to identify external user accounts that do not have a configured expiry date

Expired user accounts remain enabled

- reviews and disables the 6 identified expired user accounts, where appropriate
- devises and implements an effective governance process to better address expired accounts and synchronisation to Microsoft Entra, either by:
    - disabling expired accounts in on-premises Active Directory at time of expiration so that the change in account status is synchronised to Microsoft Entra or
    - investigate use of the currently available workarounds[1] to replicate the expired account status to Microsoft Entra to leverage existing processes until Microsoft provides a better solution.

Management response

We agree with the observations.

1. The identified user accounts will be reviewed and disabled or given an expiry date based on outcomes of the review.
2. The user accounts in Active Directory that are expired but remain enabled will be reviewed, and expired accounts will be disabled or moved to a secure OU.
3. Process to review and address expired accounts will be assessed and implemented if appropriate.

Responsible officer: Manager ICT Service Operations

Status: Work in progress

Action date: 1 December 2025

D	Deficiency	25-CR4 Active Directory – Dormant service accounts not identified and actioned

Background

Council creates and utilises service accounts within its Active Directory to support background jobs and processes which do not require human intervention. These accounts need to be configured following the principle of least privilege, i.e. only have the necessary access permission to perform their function.

[1] https://learn.microsoft.com/en-us/archive/blogs/undocumentedfeatures/use-aad-connect-to-disable-accounts-with-expired-on-premises-passwords

https://cloudbymoe.com/f/enable-password-expiration-for-synced-users-with-password-hash

https://www.undocumented-features.com/2023/04/26/working-around-accounts-that-expire-with-aad-connect-redux/

Service accounts, similar to standard user accounts, are also susceptible to becoming stale and unused. User access reviews are performed to identify any unused or stale user accounts that have not been disabled. This is to ensure unused user accounts cannot be unknowingly compromised and used by an unauthorised user

Observation

Management advised there is currently no process in place to identity and disable inactive service accounts.

We identified 1,159 out of 1,824 service accounts have not been used for more than 90 days and 868 service accounts have not been used for over 365 days. This indicates that these accounts may no longer be in use.

Additionally, 250 service accounts have never recorded a logon event since the creation of the service account.

Implication

Service accounts are often the target of malicious users. A malicious user who can compromise a dormant service account that remains enabled could use the service account and 'masquerade' as the service account.

The malicious user would have the rights assigned to the compromised service account. Any actions performed by a malicious user could go unnoticed as it would appear to be performed by an apparently valid and authorised service account.

The Australian Cyber Security Centre (ACSC) has detailed the validity of service accounts being used as an attack vector by malicious users. It released a joint alert[2] detailing cyber espionage activities that successfully used unsecured service accounts to successfully carry out a global supply chain compromise.

QAO recommendation

We recommend Brisbane City Council:

- assesses and deletes the 250 service accounts that have never recorded a logon event, where appropriate
- assesses and disables any of the remaining 909 (of the total 1,159) service accounts that have not recorded a logon event in over 90 days, where appropriate
- devises and implements an effective governance process to regularly identify and remediate service accounts that are no longer being used.

Management response

We agree with the observations.

1. Service accounts that have been dormant for over 90 days will be assessed and disabled where appropriate.
2. Assess and implement process and standards improvements to identify and disable inactive service accounts at the appropriate interval threshold.
3. All accounts identified as never been accessed will be reviewed. Accounts will be disabled dependent on the outcomes of the review.

Responsible officer: Manager ICT Service Operations

Status: Work in progress

Action date: 1 May 2026

[2] https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/svr-cyber-actors-adapt-tactics-initial-cloud-acces

O Other matter — 25-CR5 Microsoft Entra – Security configuration settings have not been set to recommended values

Background

As with the introduction of any new technology platform within an organisation, an organisation should identify and establish a minimum baseline security configuration as part of the platform's deployment.

Microsoft Entra's default configuration settings should be reviewed and configured to provide such a baseline security configuration to minimise potential risk from a malicious user leveraging default settings to gain unauthorised access to information.

Observation

We noted one security setting in the Microsoft Entra environment that has not been configured to align with industry recommended values[3] or Council documented values:

Entra Configuration Setting	Center for Internet Security (CIS) Recommended Value	Brisbane City Council Configured Value
Devices | Device Settings: Require Multifactor Authentication to register or join devices with Microsoft Entra	Yes	No

It is noted that use of multi-factor authentication (MFA) is stringently enforced for all authentication to Microsoft Entra. The use of MFA acts as a compensating control in this situation.

Implication

Not requiring MFA to register or join devices increases the risk of unauthorised device registrations and potential access by malicious users. Additionally, the lack of a configured minimum security baseline for Microsoft Entra could result in unauthorised access occurring should any compensating security controls fail.

QAO recommendation

We recommend that Brisbane City Council reviews the configuration setting and changes the setting to align with the recommended value where appropriate to do so.

Management response

We agree with the observations.

Council has consulted with and confirmed with Microsoft that the configuration is combined with conditional access. The "NO Value" observed in the audit finding serves the purpose of allowing enforcement via conditional access policies. No further action required.

Responsible officer: Manager ICT Service Operations

Status: Resolved

Action date: 21 May 2025

[3] https://www.cisecurity.org/benchmark/azure

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 or may have been reported as resolved in the closing report. The listing includes issues from our report this year and those issues raised in prior years.

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	D	O
Significant deficiency	Deficiency	Other matter

Financial reporting issues		
H	M	L
High	Medium	Low

Internal control issues

Ref.	Rating	Issue	Status
24-CR1	D	**Infrastructure charges register – status not updated** Per the Planning Regulation 2017, council must publish on its website an infrastructure charges register. This register is required to be updated monthly. Our testing identified two ICNs that were either not approved by council or were fully paid, however these were not updated in the register published on council website to reflect the correct status.	**Resolved** Our testing of the infrastructure charges register did not identify any errors in FY25.
24CR2	D	**Key Management Personnel – missing declarations** **and inconsistencies** AASB 124 Related Party Disclosures requires Council to identify related party relationships and transactions with the related parties that require disclosure in the financial statements. Council facilitates this process by requiring its key management personnel (EMT and councillors) to complete declarations on an annual basis. Five declarations were not completed during the 2024 financial year.	**Resolved** Declarations have been completed by all KMP in FY25.
24-IR1	D	**Active Directory – Service accounts lacking appropriate security configuration** 2024 summary: 10 service accounts were identified not to be restricted from interactive logon and 4 service accounts not appearing in the user evidence extract. 2025 update: We identified an increase to 358 service accounts not restricted from interactive logon and a decrease to zero service accounts not appearing in the user evidence extract. We identified 1,732 service accounts have not changed passwords in over 365 days and 55 service accounts not using the service account specific password policy.	**Re-raised** Refer below for details. **Responsible officer:** Manager ICT Service Operations **Action date:** 30 September 2024 **Revised action date:** 1 March 2026

Ref.	Rating	Issue	Status
24-IR2	D	**Active Directory and Microsoft Entra – Dormant user accounts not actioned in a timely manner (originally IS Audit 24-IR2 and 24-IR6)** 2024 summary: 1,642 user accounts in Active Directory and 312 user accounts in Microsoft Entra were identified as being dormant for over 90 days. 2025 update: We identified a decrease to 1,022 dormant user accounts in Active Directory and 270 dormant user accounts in Microsoft Entra. We noted BCC is in the process of automating the user access reviews.	**Resolved** Updated ICT Security Standard: Access Control & Account Management to reference threshold for dormant accounts Access management process implemented to fit policy definition.
24-IR3	D	**Active Directory and Microsoft Entra – User accounts of terminated employees not disabled (originally IS Audit 24-IR3 and 24-IR7)**	**Resolved** All 11 user accounts have been disabled. We noted no exceptions in 2025.
24-IR4	D	**Microsoft Entra – Security configuration settings have not been set to recommended values (originally IS Audit 24-IR9)**	**Resolved** User and external collaboration settings have been configured to recommended values.
24-IR5	D	**Microsoft Entra – Privileged Identity Management (PIM) is not configured to require approval for use of privileged roles (originally IS Audit 24-IR10)** 2024 summary: All user accounts assigned to privileged roles in Microsoft Entra are assigned permanent status as opposed to an eligible status. 2025 update: BCC has implemented a process where privileged roles are requested and assigned as needed for a specific period of time. Inclusion of all privileged users in the process is still progressing.	**Resolved** Permanent assignments have been reviewed and removed where appropriate. Approval process established for highly privileged roles.
24-IR6	D	**Microsoft Entra – On-premises Active Directory accounts are synchronised and granted Microsoft Entra privileged roles (originally IS Audit 24-IR11)** 2024 summary: 512 privileged user accounts in Active Directory were synchronised to Microsoft Entra and granted privileged roles in Microsoft Entra. 2025 update: We identified the number of privileged user accounts synchronised from Active Directory to Microsoft Entra and granted privileged roles in Microsoft Entra increased to 526.	**Resolved** BCC has improved the consistency of account segregation and controls rather than turn off synchronisation broadly to mitigate potential service availability risks.

Ref.	Rating	Issue	Status
24-IR7	D	**SAP ECC – Background system users assigned with standard SAP profiles (originally IS Audit 24-IR13)**	**Resolved** BCC has reduced the number of background system users assigned with standard SAP profiles from 41 in FY24 to 24 in FY25. BCC provided risk acceptance for the remaining 24 accounts assigned with standard SAP profiles.
24-IR8	D	**SAP ECC – Timeliness of SAP FireFighter session reviews (originally IS Audit 24-IR14)**	**Resolved** All FireFighter sessions initiated between 1 July 2024 to 27 March 2025 have been reviewed and approved.
24-IR9	O	**Active Directory – One user account has password set to never expire (originally IS Audit 24-IR4)**	**Resolved** Council has reviewed and set password expiry for the identified account.
24-IR10	O	**Microsoft Entra – User accounts in Microsoft Entra are not disabled when their corresponding on-premises Active Directory user account is disabled or expired (originally IS Audit 24-IR8)**	**Resolved** All 23 user accounts have been disabled in Microsoft Entra. We noted no exceptions in 2025.
24-IR11	O	**Active Directory – Fine-gained password policy is not reflected in the password policy standard and is not updated (originally IS Audit 24-IR5)**	**Resolved** The fine-grained password policy document is referenced in BCC's *ICT Security Standard: Access Control & Account Management.*
24-IR12	O	**Microsoft Entra – Use of privileged role assignments**	**Resolved** With the progress made in 24-IR5, BCC has implemented the just-in-time access to limit the number of privileged role assignments used at any time.
24-IR13	O	**SAP ECC – SAP obsolete clients not deleted (originally IS Audit 24-IR15)**	**Resolved** Obsolete clients have been removed.

4.1 Details of re-raised issues

D **Deficiency** **24-IR1 Active Directory – Service accounts lacking appropriate security configuration (Re-raised)**

Background

Council creates and maintains 'service accounts' within its Active Directory to support background processes and jobs that do not require human intervention. Due to the nature of service accounts and their lack of human intervention, additional security controls are required for service accounts.

These controls include service accounts being configured with strong passwords that are changed regularly and the accounts being configured following the principle of least privilege. Implementing least privilege entails not granting service accounts membership in any built-in administrator security groups and only granting the minimum user rights and permissions required.

Observation

Service accounts not restricted from interactive logon (i.e. can be used by human user to log on)

Service accounts that are unrestricted from interactive logon can be used by a malicious user to gain unauthorised privileged access and move undetected within a computing environment.

Per Council's *ICT Security Standard: Access Control & Account Management*, service accounts are to be configured to restrict interactive logon.

During the prior audit in FY24 and this year's audit, we identified the following number of service accounts that are not restricted from interactive logon nor were appearing in the user account evidence extract:

Service accounts	FY24	FY25
Service accounts not restricted from interactive logon	10	358
Service accounts not appearing in the user evidence extract	4	-

It is noted that 254 of the 358 service accounts did have an exemption to not enforce restrictions on interactive logons, but all of the exemptions have since expired.

Password management of service accounts

In addition to the prior year finding of service accounts not restricted from interactive logon, this year an observation as to password management of service accounts is identified.

Per the *ICT Security Standard: Access Control & Account Management*, service accounts are required to have complex passwords greater than 12 characters and to be changed every 365 days.

We identified:

- 9 of the 1,824 enabled service accounts use a password policy that enforces a minimum password length of 8 characters
- 46 of the 1,824 enabled service accounts are not assigned the service account specific password policy that enforces a minimum password length of 14 characters
- 1,732 of the 1,824 enabled service accounts have not changed password in over 365 days.

It is noted that the passwords of the 46 identified service accounts are still compliant with Council's password policy. The default password policy, which is applied to the service accounts, enforces a minimum password length of 14 characters which is the same as the service account specific policy.

Implication

Malicious users are more likely to target service accounts[4] as the accounts are often less actively managed or insufficiently configured. Depending on the privileges assigned to the service account, the malicious user could perform unauthorised actions against financial or other business systems undetected.

The Australian Cyber Security Centre also released a joint alert[5] with its equivalent partners in the US, Canada and New Zealand governments in February 2024. The alert detailed cyber espionage activity that successfully used insufficiently secured and managed service accounts to successfully carry out a global supply chain compromise.

QAO recommendation

We recommend that Brisbane City Council:

Service accounts not restricted from interactive logon (i.e. can be used by human user to log on)

- assesses and denies all 358 service accounts from interactive logon, where possible, by assigning 'Deny log on locally' and 'Deny log on via Terminal Services' user rights to the service accounts
- devises and implements an effective governance process to approve and track service accounts that require exemptions from being required to be disabled for interactive logon
- identifies and implements effective compensating or mitigating controls for those service accounts exempted from being denied interactive logon

Password management of service accounts

- assesses and assigns the 55 service accounts to the service account specific password policy, where possible
- devises and implements an effective governance process to ensure passwords are rotated in accordance with the *ICT Security Standard: Access Control & Account Management*, were possible.

Management response

We agree with the observations.

1. The 358 identified service accounts will be reviewed to ensure they have a valid exemption for interactive logon. Any accounts identified as requiring Deny log on locally and/or Deny log on via Terminal services will have this configuration applied where appropriate.
2. Review the process to manage account exemptions and update to reflect any identified improvement opportunities.
3. Review all recorded account exemptions to ensure they are compliant with their agreed exemption lifecycle dates.
4. Assessment of an automated process to assign all new accounts in the default FGPP group

   Responsible officer: Manager ICT Service Operations

   Status: Work in progress

   Action date: 1 March 2026

[4] https://www.silverfort.com/blog/3-cyberattacks-in-which-compromised-service-accounts-played-a-key-role/

[5] https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/svr-cyber-actors-adapt-tactics-initial-cloud-access

Appendix A3 – Climate-related financial disclosures

Next year's planning considerations	Potential effect on your reporting obligations	Potential effect on your audit
As a non-mandatory reporting entity, your entity does not need to prepare climate-related financial disclosures in compliance with AASB S2 Climate-related Disclosures and have this audited under the ASSA 5010 timetable. Queensland Treasury has communicated to us that it does not intend to include your entity within its whole-of-government reporting framework. The department of local government is considering a sector-wide response. We encourage local governments to engage with the department prior to devoting time and resources to determining their approach to reporting.	At this point there is no effect on your reporting obligations for 2026 or future years. Your entity may choose to voluntarily report against AASB S2. As part of your decision making, you should also consider who your report users are, and what their information needs are. We strongly encourage you to engage with us prior to making this decision. Planning to develop a valuable report is a significant commitment.	We have commenced our engagements for clients who are preparing mandatory reports now. Our experience is that engagement at least 18 months out from the first reporting date allows us to develop a shared understanding of the roles and responsibilities and assess your readiness for reporting. If you chose to prepare a voluntary S2 compliant report, we would recommend that you allow a similar amount of time.

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