

CITY OF KARRATHA

PERIOD OF AUDIT: YEAR ENDED 2025

FINDINGS IDENTIFIED DURING THE IT GENERAL CONTROLS AUDIT

Index of findings	Potential impact on audit opinion	Rating			Prior year finding
		Significant	Moderate	Minor	
1. Data loss prevention	No		✓		
2. IT governance and strategy	No			✓	
3. Penetration testing	No			✓	
4. Financial application access management	No			✓	✓

Key to ratings

The Ratings in this management letter are based on the audit team's assessment of risks and concerns with respect to the probability and/or consequence of adverse outcomes if action is not taken. We give consideration to these potential adverse outcomes in the context of both quantitative impact (for example financial loss) and qualitative impact (for example inefficiency, non-compliance, poor service to the public or loss of public confidence).

Significant - Those findings where there is potentially a significant risk to the entity should the finding not be addressed by the entity promptly. A significant rating could indicate the need for a modified audit opinion in the current year, or in a subsequent reporting period if not addressed. However, even if the issue is not likely to impact the audit opinion, it should be addressed promptly.

Moderate - Those findings which are of sufficient concern to warrant action being taken by the entity as soon as practicable.

Minor - Those findings that are not of primary concern but still warrant action being taken.

CITY OF KARRATHA

PERIOD OF AUDIT: YEAR ENDED 2025

FINDINGS IDENTIFIED DURING THE IT GENERAL CONTROLS AUDIT

1. Data loss prevention

Finding

We identified that the following controls are not in place to restrict unauthorised data transfers:

- Use of removable storage devices is not blocked.
- Cloud sharing platforms are not universally blocked. However, we acknowledge that web filtering managed through the Palo Alto firewall is in place to manage some of this risk as this is configured to block only high-risk industry known threat actors and does not block common file sharing platforms such as Dropbox.

Management indicated that a project is underway for the implementation of Microsoft Purview and progressed to preliminary design stage pending ELT (Executive Leadership Team) approval of roll out.

Rating: Moderate

Implication

Without data loss prevention controls, City's IT environment faces an increased risk of exposing sensitive information to unauthorised users, either unintentionally or through malicious intent which may potentially lead to financial and reputational damage.

Recommendation

The City should implement and ensure that technical controls in place to:

- Restrict or disable the use of removable storage devices (e.g., USB drives) unless explicitly approved for business needs.
- Review and control access to cloud sharing platforms, allowing only approved and secure platforms based on business justification and risk assessment.

Management comment

The City has engaged the market for support in implementing Microsoft Purview to enhance AI governance, PRIS readiness, and Data Loss Prevention (DLP) monitoring. A project has commenced, including stakeholder workshops and solution design activities, with implementation pending ELT approval. The initiative will also extend to address additional DLP outcomes, including restrictions on removable storage devices.

While it is acknowledged that no single measure will provide complete protection, the City is actively exploring complementary solutions within the Palo Alto Firewall environment. A business case will be developed and presented to support potential investment in these additional controls.

Responsible person: Manager Information Technology
Completion date: June 2026

CITY OF KARRATHA

PERIOD OF AUDIT: YEAR ENDED 2025

FINDINGS IDENTIFIED DURING THE IT GENERAL CONTROLS AUDIT

2. IT governance and strategy**Finding**

We identified that the Information Classification Policy is in draft stage and has not yet been formally approved.

Rating: Minor

Implication

Without an approved Information Classification Policy, there is a risk that sensitive information may not be appropriately identified and protected and could result in unauthorised disclosure, data leakage or non-compliance with regulatory or contractual obligations. Additionally, it may result in misalignment of the implementation and management of controls with management's expectations. In addition to this, the lack of an endorsed Information Classification Policy may result in an ineffective role out of Microsoft Purview which is meant to address the DLP issues identified in the previous finding.

Recommendation

The City should review, finalise, approve and publish the Information Classification Policy and ensure that the document is appropriately governed.

Management comment

An Information Classification policy has been drafted and provided to stakeholders for input in readiness to meet our Privacy and Responsible Information Sharing (PRIS) legislated requirements. This is now currently being progressed through the approval process by the Manager Governance.

Responsible person: Manager Information Technology / Manager Governance
Completion date: March 2026

CITY OF KARRATHA

PERIOD OF AUDIT: YEAR ENDED 2025

FINDINGS IDENTIFIED DURING THE IT GENERAL CONTROLS AUDIT

3. Penetration testing**Finding**

We were informed that no penetration testing was performed during the audit period.

Management advised that they are currently in the process of awarding the penetration testing project.

Rating: Minor

Implication

Not conducting regular penetration tests can leave vulnerabilities undetected, potentially leading to data breaches, financial loss, and reputational damage.

Recommendation

Management should regularly perform security assessments based on the endorsed policy, risk or significant changes to identify and mitigate vulnerabilities that could lead to cyber security exposures.

Management comment

Annual penetration testing has formed part of the Annual IT Operational plan. For the 24/25 audit period this was put on hold due to planned firewall infrastructure changes. These changes will be completed in November 2025.

The City has since gone to market for the provision of penetration testing and an Essential Eight gap analysis. This engagement has been awarded, and the work will commence following the completion of the firewall infrastructure changes to ensure accurate and comprehensive testing outcomes.

Third party testing will be resumed annually.

Responsible person: Manager Information Technology
Completion date: June 2026

CITY OF KARRATHA

PERIOD OF AUDIT: YEAR ENDED 2025

FINDINGS IDENTIFIED DURING THE IT GENERAL CONTROLS AUDIT

4. Financial application access management**Finding****User access reviews**

We identified that the City logs service tickets for user access reviews to be performed. However, the ticket lacks evidence that the review/s were conducted in accordance with established procedures. As a result, we were unable to verify whether user access reviews:

- Were completed as scheduled and covered the entire user population.
- Included review over user roles assigned to Finance personnel.
- Were conducted by appropriate personnel and approved by an appropriate manager.
- Resulted in timely remediation following the review (e.g., users disabled or roles modified).

This finding was raised in 2023. However, we acknowledge that the user access review process has since improved. We further acknowledge that the Chief Financial Officer (CFO) has reviewed the roles assigned to Finance personnel outside of the audit period and no major discrepancies were identified. Upon inspection of the artefacts noted that access roles were also reviewed.

Rating: Minor (2024: Moderate)

Implication

Without adequate recording and documentation of user access reviews, and in the absence of evidence confirming that such reviews were performed, it is not possible to validate the adequacy and effectiveness of the access review process.

Recommendation

The City should ensure that documentation is retained to demonstrate that the user access reviews performed include details on the user population, assigned user roles, approvals and any remediation actions taken.

Management comment

As part of the CiAnywhere ERP implementation, user access privileges were developed based on the principle of least privilege, with approvals obtained from relevant line managers. All access roles were reviewed, tested, and endorsed by the Chief Financial Officer (CFO) and Director Corporate prior to go-live.

Quarterly role-based access reviews have been established, with responsibility assigned to the ERP Systems Analyst to conduct reviews, maintain documentation, and ensure all production changes are supported by approved change requests.

During the 2024/25 audit period, a comprehensive review was undertaken to address prior documentation gaps, including evidence of user population, role assignments, approvals, and remediation actions. This process has now been formalised and will be continuously improved.

Responsible person: Manager Information Technology
Completion date: June 2026