INFORMATION SYSTEMS AUDIT – REPORT ADDRESSING SIGNIFICANT MATTER RAISED BY THE OAG

The City of Swan was a participant in the Information Systems Audit 2020 - Local Government Entities completed by the Office of the Auditor General (OAG).

In a report issued to the City March 2021, the OAG identified one significant matter that requires attention by the City.

Under section 7.12A (4)(b) of the Local Government Act 1995, the City is required to prepare a report addressing any matters identified as significant by the auditor in the audit report, and stating what action the local government has taken or intends to take with respect to each of those matters.

Within 14 days after a local government gives a report to the Minister, the CEO must publish a copy of the report on the local government's official website.

The City takes this matter seriously and to ensure a high standard of due diligence in relation to the management of information systems and controls the City will monitor and track progress of implementation of actions through quarterly progress reporting which will be reported to the Audit Committee.

SIGNIFICANT MATTERS – INFORMATION SYSTEMS AUDIT

1. REMOTE ACCESS MANAGEMENT

Recommendation: The City should:

- limit the number of privileged accounts with remote access
- enforce multi-factor authentication for all remote access
- prevent users from copying information from the City's resources to personal devices
- establish a review process for all remote access accounts to confirm that the access is still required and appropriate.

Management Comment: Management accepts the finding and agrees that there are opportunities for improvement as many of the remote access settings are relatively new to the City, having been implemented in 2020 to ensure business continuity during the COVID pandemic. Management notes that there are many compensating controls such as password lockouts and multi-factor authentication on privileged accounts that reduce the risk profile of this finding.

Agreed Action: A risk assessment to determine management approach will be completed, consideration of progressively implementing multi-factor authentication within the organisation and disabling the Citrix functionality to copy files to a user's desktop, as well as regular review of accounts with remote access will all be considered to address this matter.

Responsible Person: Chief Executive Officer