



Sunshine Coast Regional Council

2019 Interim report
15 April 2019

Your ref:
Our ref: 2019-4139

IN-CONFIDENCE

15 April 2019

Councillor M Jamieson
Mayor
Sunshine Coast Regional Council
Locked Bag 72
SUNSHINE COAST MAIL CENTRE QLD 4560

Dear Councillor Jamieson

2019 Interim report

We present to Council our interim report for Sunshine Coast Regional Council for the financial year ending 30 June 2019. This report details the results of our interim work performed to 28 February 2019. In this phase we assessed the design and implementation of your internal controls, and whether they are operating effectively.

This report also includes our assessment your internal control framework; and a summary of control deficiencies, financial reporting and other matters identified to date.

The *Auditor-General Act 2009* requires the auditor-general to report to parliament on an issue raised during an audit if he considers it to be significant. To date our work has identified one significant deficiency in your information system internal controls.

If you have any questions or would like to discuss the audit report, please contact me on 3149 6129 or Michael Keane on 3149 6077.

Yours sincerely



Carolyn Dougherty
Director

Enc.

cc. Mr Michael Whittaker, Chief Executive Officer
Mr Peter Dowling, Chair of the Audit Committee, Sunshine Coast Regional Council

1. Summary



Audit progress

Internal control assessment and issues	On track
<ul style="list-style-type: none">• Testing of internal controls for operating effectiveness is completed for revenue, payroll and expenditure systems for the period 1 July 2018 to 28 February 2019.• We have identified five deficiencies in internal controls of which 4 relate to prior years. We have reassessed the prior year issues based on their potential risk to Council and as a result, one of these matters has been elevated to a significant deficiency. Details on these deficiencies are in section 2 of this report.• We have also assessed the elements of your internal control environment, as well as the progress made towards resolving prior year issues. <p>Based on the results of our testing completed to date, we have assessed your internal control environment as generally effective, meaning the environment supports an audit strategy that can rely upon these controls.</p>	

Financial reporting issues and other matters	On track
<p>We note progress has been made on the prior year financial reporting issue regarding delays in recording contributed assets. However, this issue is not yet due and will be assessed during our final visit.</p> <p>No new financial reporting issues have been raised.</p>	

Areas of audit significance	On track
<p><u>Valuation/depreciation of infrastructure assets</u> – We will test this area of audit significance as part of our September 2019 visit.</p> <p><u>Revenue recognition of infrastructure charges and contributed assets</u> – We have completed substantive testing through verification to supporting documentation for the period 1 July 2018 to 28 February 2019 with no deficiencies noted. We have planned further testing in this area for the period 1 March 2019 to 30 June 2019 as part of our September 2019 visit.</p> <p><u>Appropriateness of procurement policies and practices</u> – We have tested the effectiveness of key controls for the period 1 July 2018 to 28 February 2019 for expenditure with no deficiencies noted. Substantive testing to date included transactional analytical procedures, review of procurement processes for selection of awarded contracts and verification to supporting documentation. We have planned further testing in this area for the intervening period as part of our June 2019 visit.</p> <p><u>Financial sustainability</u> – We will test this area of audit significance as part of our September 2019 visit.</p> <p><u>Valuation of investment in associate</u> – We will test this area of audit significance as part of our September 2019 visit.</p> <p><u>Major projects and application of accounting standards</u> – We have commenced our audit of the accounting papers covering your entities major projects. We are due to provide feedback on these later in April and May 2019.</p>	











Milestones—financial reporting and audit deliverables	On track
<p>All agreed financial reporting and audit deliverable milestones have been met.</p>	



2. Internal control issues






The following table summarises our reporting on deficiencies in internal controls.

	Number of significant deficiencies		Number of deficiencies		Rating
	Current year issues	Prior year unresolved issues	Current year issues	Prior year unresolved issues	
 Control environment Structures, policies, attitudes and values that influence daily operations	-	-	-	2	
 Risk assessment Processes for identifying, assessing and managing risk	-	-	-	-	
 Control activities Implementation of policies and procedures to prevent or detect errors and safeguard assets	-	1*	-	1	
 Information and communication Systems to capture and communicate information to achieve reliable financial reporting	-	-	1	-	
 Monitoring activities Oversight of internal controls for existence and effectiveness	-	-	-	-	

*Issue elevated from deficiency to significant deficiency

Our ratings

-  **Effective**
 No significant deficiencies identified.
-  **Generally effective**
 One significant deficiency identified.
-  **Ineffective**
 More than one significant deficiency identified.



2. Internal control issues



Significant deficiencies and deficiencies

The following table details deficiencies identified from testing of controls as at 28 February 2019. It includes responses from management.

Our risk ratings are as follows—refer to [Our rating definitions](#) for more detail.



Significant deficiency

1. Monitoring the activities of users with privileged access (Re-raised issue) COSO Component – Control Environment

In our 2016–17 audit, we recommended that Council perform a risk assessment to identify sensitive, highly privileged or system administration activities that require logging and regular monitoring for TechnologyOne, TechnologyOne Property, Chris21 systems and databases. This would enable Council to determine the following areas to monitor:

- activities of high risk performed by users assigned with privileged/system administrator access
- security related transactions and critical changes to the database of financial systems (e.g. direct data changes, changes to database configuration, changes to executable code).

Digital Information Services (DIS) has now set up a charter for application support group to define roles and responsibilities to review who have privileged accesses in the systems. However, DIS has not implemented a process to review the activities of the users with these privileged accesses.

Establishing this process is also important as Council is now commencing an arrangement with an external organisation to provide virtual database administration services to Council. Users from this organisation will have high privileged, system administration access to Council's databases.

There is an increased risk that Council will fail to detect unauthorised activities and transactions in a timely manner.

QAO recommendation

We recommend that Council identifies, logs, monitors and reviews:

- sensitive, highly privileged and system administration activities
- direct data changes to critical tables and security configuration files in the databases.

Management response

Management accepts the recommendations and have implemented an immediate review of users with privileged access. This will include a monthly report being provided to the Head of Information Technology listing all approved users and the basis of their membership.

Ongoing work will be performed to monitor the activities of users with privileged access. This will include identifying the user accounts that require monitoring, implementing the necessary logging of activities and establishing the process to ensure logs are reviewed and appropriate actions taken.

Responsible officer: Head of Information Technology

Status: Work in progress

Action date: 30 April 2019





2. Deficiency in monthly financial reporting (New issue) COSO Component – Information and Communication

As part of our 2018–19 audit, one of our focus areas is management reporting and the delivery of the right information to the right people at the right time. Through this review we observed the following:

- During the period 1 July 2018 to January 2019, there was an average delay of 45 days in the provision of the monthly financial performance report to Council. This delay means the information provided to decision-makers is not considered timely. Since January 2019, we acknowledge the Council made a change to the timeframe for management reporting and has reduced this average delay to 28 days.
- There is no formalised framework for monthly financial reporting. Whilst the applicable staff are aware of the roles and responsibilities relating to monthly financial reporting, it is not centrally documented.
- Additional processes occur in the production of Council's financial statements beyond normal month-end reporting. These include true-ups for actual depreciation and full year adjustments for provisions causing fluctuations from the June management reports to the financial statements.

Untimely monthly financial reporting and true-ups/adjustments performed exclusively at year end may impact on the timing and quality of the annual financial statements. A lack of a formalised framework may also have a negative effect on this process.

QAO recommendation

We recommend Council

- formalise a framework for monthly financial reporting
- improve month-end reporting to allow for review and challenge of the information presented in the management reports and to reduce the likelihood of errors and adjustments in the annual financial statements.

Management response

Council will prepare a formalised framework for monthly financial reporting.

Responsible officer: Chief Financial Officer

Status: Not started

Action date: 29 February 2020

3. Disabling of inactive accounts in Active Directory (network) (Re-raised issue) COSO Component – Control Activities

In 2017–18 we identified instances when Council did not remove system access of terminated personnel. Council has now implemented a process so that terminated personnel will not be able to log on to Council's network (Active Directory) by setting their password to expire on termination date.

While this is an improvement to the existing process, Council does not have a process to review and disable user accounts:

- that have password expired
- that have not been used for an extended period.



2. Internal control issues (continued)



During our analysis of access to TechnologyOne application and Council's network (Active Directory), we identified that:

- There are 40 terminated contingent workers with access to Council's network remain enabled even though their passwords have expired. These accounts also have not been used for more than 120 days. Three of them has access to TechnologyOne system.
- There are 21 user accounts that have not been used to access Council's network for more than 120 days, but their accounts remain enabled and their password are not set to expire. Council does not have a process to review these accounts to determine its legitimacy and currency.

Council is exposed to the risk of:

- unauthorised access or transactions to system as user accounts with expired password can be accidentally or intentionally activated
- inability to detect and remove access to council's network when it is no longer required.

QAO recommendation

We recommend that Council defines a process to:

- review user accounts whose password have expired and have not been used for an extended period
- review user accounts that have not been used for an extended period for eligibility.

Management response

Management accept the recommendations.

There are existing processes that ensure user accounts are set to expired when people leave the organisation which prevents these accounts from being used.

A process will be defined to review user accounts that have been set to expired and user accounts that have not been used for an extended period to identify accounts that will be disabled. A maximum timeframe will be identified for expired accounts before they are disabled.

Responsible officer: Head of Information Technology

Status: Work in progress

Action date: 30 June 2019

4. Managing passwords for privileged accounts (Re-raised issue) COSO Component – Control Activities

In 2016–17 we identified that Council does not have a process to:

- regularly change passwords for default and/or generic system accounts with privileged access
- change the passwords when system administrators or support staff who access to these passwords leave Council.

Digital Information Services (DIS) advises that it has now implemented a process to change default and/or generic system accounts with privileged access during annual system upgrades.



2. Internal control issues (continued)



DIS, however, does not have a process in place to change the passwords of default and/or generic system accounts when system administrators or support staff leave Council. These staff have access to password safe application that stores passwords of default and/or generic system accounts. The password safe application does not have controls to prevent system administrator or support staff to download / copy the password. In addition, system administrators or support staff may remember the passwords if DIS does not regularly change them.

Council is commencing an arrangement for an external organisation to provide for virtual database administration services to Council. It is now an opportune time for Council to revisit the overall processes and controls for managing passwords of privileged accounts to ensure the security of systems and information.

There is an increase risk of unauthorised access and changes to systems and information which may result in security breach or unauthorised transactions in the systems.

QAO recommendation

We recommend that Council:

- assesses and implements a process to manage the use and changes of passwords for default and/or generic system accounts with privileged access
- changes these passwords when system administrator or support staff with access to these passwords leave Council or leave the external organisation who provides services to Council.

Management response

Management accept the recommendations.

Passwords for default and/or generic system accounts with privileged access are currently changed during annual system upgrades and this process will continue. Work is also currently being performed to identify a replacement password vault tool to manage the security of default and/or generic system accounts with privileged access.

Work will be performed to increase the frequency that passwords for default and/or generic system accounts with privileged access are changed. A process will be established to change passwords for default and/or generic system accounts with privileged access when system administrator or support staff with access to these passwords leave Council or leave an external support provider.

Responsible officer: Head of Information Technology

Status: Work in progress

Action date: 30 September 2019

5. IT security policy and procedures (Re-raised issue)

COSO Component – Control Environment

In our 2016–17 audit, we recommended that Council update its IT security policy and procedures as they were incomplete, and Council had not updated them since 2014.

As at May 2018, Council advised that Digital and Information Services (DIS) is in the process of revising and updating the IT security policy. In addition, the detailed components supporting the policy are either in draft, or part of fact sheets and other IT operational documents. Council has not yet formalised these documents as part of the procedures or directives supporting the IT security policy and they are not yet in effect.



2. Internal control issues (continued)



As at March 2019, DIS has updated draft Information Security policy and is currently consulting the business on this draft policy. The draft policy requires DIS to establish several information security guidelines to implement the policy. While some of these guidelines exist as part of fact sheets or other IT operational documents, DIS has not reviewed the currency of these documents and determines which documents will form the IT security guidelines to support the implementation of IT security policy.

Failure to develop, implement and enforce an effective security policy can result in ad-hoc business practices that leave the financial systems exposed to confidentiality, integrity and availability risks.

QAO recommendation

We recommend that Council:

- finalises the IT security policy.
- formalises and/or develops a suite of guidelines to support the implementation of the policy to cover areas, including but not limited to, the following:
 - access management including:
 - security requirements and baseline password settings
 - management of accounts with privileged access, including securing default and/or generic accounts
 - monitoring the use and activities of accounts with privileged / system administrator access
 - system acquisition, development and maintenance
 - incident management
 - business continuity management.

Management response

Management accept the recommendations.

Stakeholder consultation on the draft Information Security Policy and Information Security Guidelines will be completed and final versions of the policy and guidelines will be endorsed and implemented.

Responsible officer: Head of Information Technology

Status: Work in progress

Action date: 31 May 2019



3. Prior year issues



Status

The following table summarises the status of issues and other matters reported by audit in the final management letter dated 8 November 2018.

Reference	Rating	Issue	Status
Internal control issues			
1.1		Treasurer approval not obtained for loans under <i>Statutory Bodies Financial Arrangements Act</i>	Resolved
1.2		Configuration setting to process invoices	Resolved
1.3		Disabling system access for terminated users	Partially resolved – see details at Section 2 – Issue #3
1.4		Managing password for privileged accounts	Matter re-raised – see details at Section 2 – Issue #4
1.5		IT security policy and procedures	Matter re-raised as a deficiency – see details at Section 2 – Issue #5
1.6		Monitoring the activities of users with privileged access	Matter re-raised as a significant deficiency – see details at Section 2 – Issue #1
Financial reporting issues			
2.1		Delays in recording contributed assets	Work in progress
2.2		EDQ interest free loan not accounted for at fair value	Work in progress



4. Appendix A—Our rating definitions



Internal rating definitions

	Definition	Prioritisation of remedial action
Significant deficiency 	<p>A significant deficiency is a deficiency, or combination of deficiencies, in internal control that requires immediate remedial action. Also, we increase the rating from a deficiency to a significant deficiency based on:</p> <ul style="list-style-type: none"> the risk of material misstatement in the financial statements the risk to reputation the significance of non-compliance with policies and applicable laws and regulations the potential to cause financial loss including fraud, or where management has not taken appropriate timely action to resolve the deficiency. 	<p>This requires immediate management action to resolve.</p>
Deficiency 	<p>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.</p>	<p>We expect management action will be taken in a timely manner to resolve deficiencies.</p>
Other matter 	<p>An other matter is expected to improve the efficiency and/or effectiveness of internal controls, but does not constitute a deficiency in internal controls. If an other matter is not resolved, we do not consider that it will result in a misstatement in the financial statements or non-compliance with legislative requirements.</p>	<p>Our recommendation may be implemented at management's discretion.</p>

Financial reporting issues

	Potential effect on the financial statements	Prioritisation of remedial action
High 	<p>We assess that there is a high likelihood of this causing a material misstatement in one or more components (transactions, balances and disclosures) of the financial statements, or there is the potential for financial loss including fraud.</p>	<p>This requires immediate management action to resolve.</p>
Medium 	<p>We assess that there is a medium likelihood of this causing a material misstatement in one or more components of the financial statements.</p>	<p>We expect management action will be taken in a timely manner.</p>
Low 	<p>We assess that there is a low likelihood of this causing a material misstatement in one or more components of the financial statements.</p>	<p>We recommend management action to resolve; however, a decision on whether any action is taken is at management's discretion.</p>



qao.qld.gov.au



[Suggest a performance audit topic](#)

[Contribute to a performance audit in progress](#)

[Subscribe to news](#)

[Connect with QAO on LinkedIn](#)

Carolyn Dougherty
T: 07 3149 6129
E: Carolyn.Dougherty@qao.qld.gov.au

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

 **Queensland
Audit Office**
Better public services

