Queensland Audit Office
Better public services

Your ref:
Our ref: 2019-4139
Carolyn Dougherty 3149 6129

23 October 2019

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

Dear Councillor Jamieson

Final Management Report for Sunshine Coast Regional Council

We have completed our 2019 financial audit for Sunshine Coast Regional Council. I 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.

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

Reporting on issues

Issues and other matters formally reported to management and an update on actions taken by management to resolve these issues are included in Appendix A to this letter. Our rating definitions for internal control deficiencies is shown in Appendix B.

Report to parliament

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

Consistent with previous years, we intend to include the results of our audit of Sunshine Coast Regional Council in our report to Parliament on the results of the Local Government sector. We will discuss the proposed content of our report with your Chief Financial Officer and will continue to consult as we draft our report.

Formally, you and the Chief Executive Officer will have an opportunity to comment on our report and for these comments to be included in the final report.

Audit fee

The final audit fee for this year is $265,000 exclusive of GST (2018: $260,000) which is $19,000 higher than our original estimated audit fee of $246,000. This increase represents the cost of additional time spent analysing and testing data in response to prior period errors identified by management relating to property, plant and equipment. We also assessed and responded to additional complexities associated with major projects during this audit.

Queensland Audit Office
Level 13, 53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002

Phone 07 3149 6000
Email qao@qao.qld.gov.au
Web www.qao.qld.gov.au
Queensland Audit Office (QAO)

We would like to thank you and your staff for their engagement in the audit this year.

If you have any questions about this letter or would like to discuss any matters regarding our audit service, please contact me on 3149 6129.

Yours sincerely

Carolyn Dougherty
Director

Enc.

cc: Mr M Whittaker, Chief Executive Officer
Mr P Dowling, Audit Committee Chair

Appendix A

Issues formally reported to management

This table provides you with a summary of issues that we have formally reported to management.

Financial reporting issue

No.	Issue	Our recommendation	Status update from management
18FR-1	**Delays in recording contributed assets** **(Re-raised from 2017-18)** **Risk rating: High** **Observation** As a result of delays in processing contributed asset information, there are 2706 assets (2018: 4,333) with a net value of $29.258m (2018: $38.404m) that were under control of council in previous financial years that have been brought to account during the 2018–19 financial year. Financial Year / Net Value of Assets / Number of Assets 2017-18 / 9,354,257 / 1274 2016-17 / 16,119,122 / 1214 Pre 2016-17 / 3,784,569 / 218 This represents a material misstatement to revenue disclosed in Council's 2017–18 financial report. **Implications** Delays in processing contributed asset information into Council's systems increases the risk that revenue, non-current assets and depreciation expense will be materially understated in the financial report. Where material prior period errors occur in the financial report, the users of the report may be misled which can impact the decisions they make regarding this information.	The Council adopt measures to ensure the timely recording of contributed asset information into council's systems to ensure revenue, non-current assets and depreciation expense are not materially misstated in the financial report.	Council acknowledges this misstatement and will work with appropriate internal and external stakeholders to improve the timeliness of receipt of information necessary to enable recognition of contributed assets in the appropriate financial year. Further detail will be added to this response after consultation with the relevant areas within Council. *Responsible officer:* Chief Financial Officer *Status:* Work in progress *Action date:* 30 June 2020

Appendix A

Previously raised control deficiencies as reported in our second interim management letter dated 28 June 2019

No.	Issue	Our recommendation	Status update from management
19IML-New	**Payroll process deficiency for changes to employee bank account details** **Rating: Significant deficiency** **Observation** Recently, the Queensland public sector entities were targeted by scammers through the use of fraudulent emails. These emails had the appearance of being from the employee and requesting their payroll bank account be changed for the next pay run. These emails were also addressed directly to a payroll officer. Sunshine Coast Regional Council processed one of these changes which resulted in the fraud being successful. The council's procedures in place at the time of this incident allowed for bank accounts to be changed by the following three methods: • by email • through the Employee Self Service system, or • a physically signed form. Changes made through an email request required no further enquiry or information before actioning. We note that since this incident, payroll changes requested by email now require a follow up phone call from the payroll team to confirm any bank account changes.	As these fraud attempts are becoming more common and sophisticated: (a) Council should review practices relating to any bank account changes to ensure controls are in place to prevent future incidents occurring. (b) Furthermore, fraud awareness training should be extended to all staff.	(a) Management agrees with the recommendation and completed a review of the current procedure which resulted in the implementation of additional control measures to prevent future security incidents. The review process was completed in consultation with the Payroll Team. These control measures include additional identity checks, system generated emails to the employee confirming when a primary bank account changes, and updated forms and factsheets. *Responsible officer:* Head of People & Culture *Status:* Resolved (b) The Corporate Governance Branch has recently reviewed the Fraud and Control documentation and will be rolling out specific Fraud Awareness Training as part of the Governance Awareness Program, commencing in July 2019. The branch currently provides Risk Management Training to employees and this training does include a short element on Fraud Risk. The specific Fraud Awareness Training will consist of both face-to-face sessions as well as an online module that will be rolled out later in the year (pending external development timelines). The training will initially be tailored to high risk areas. *Responsible officer:* Manager Corporate Governance *Status:* Resolved, subject to QAO verification

Appendix A

Previously raised control deficiencies as reported in our first interim management letter dated 15 April 2019

No.	Issue	Our recommendation	Status update from management
19IML-1.1	**Monitoring the activities of users with privileged access (Re-raised from previous audits)** **Rating: Significant deficiency** **Observation** 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 TechonologyOne, 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. **Implications** There is an increased risk that Council will fail to detect unauthorised activities and transactions in a timely manner.	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 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:* 29 November 2019

Appendix A

Previously raised control deficiencies as reported in our first interim management letter dated 15 April 2019

No.	Issue	Our recommendation	Status update from management
19IML-1.2	**Deficiency in monthly financial reporting** **Rating: Deficiency** **Observation** 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. **Implications** 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.	That 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.	Council will prepare a formalised framework for monthly financial reporting. *Responsible officer:* Chief Financial Officer *Status:* Work in progress *Action date:* 29 February 2020

Appendix A

Previously raised control deficiencies as reported in our first interim management letter dated 15 April 2019

No.	Issue	Our recommendation	Status update from management
19IML-1.3	**Disabling system access for terminated users** **(Re-raised issue)** **Rating: Deficiency** **Observation** 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. 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. **Implications** 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.	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 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:* Resolved, subject to QAO verification

Appendix A

Previously raised control deficiencies as reported in our first interim management letter dated 15 April 2019

No.	Issue	Our recommendation	Status update from management
19IML-1.4	**Managing password for privileged accounts** **(Re-raised issue)** **Rating: Deficiency** **Observation** 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. 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. **Implications** There is an increase risk of unauthorised access and changes to systems and information which may result in security breaches or unauthorised transactions in the systems.	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 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:* 29 November 2019

Appendix A

Previously raised control deficiencies as reported in our first interim management letter dated 15 April 2019

No.	Issue	Our recommendation	Status update from management
19IML-1.5	**IT security policy and procedures** **(Re-raised issue)** **Rating: Deficiency** **Observation** 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. 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. **Implications** 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.	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 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:* Resolved

Appendix B—Our rating definitions

Internal control rating definitions

	Definition	Prioritisation of remedial action
Significant deficiency	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: • 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.	This requires immediate management action to resolve.
Deficiency	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.	We expect management action will be taken in a timely manner to resolve deficiencies.
Other matter	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.	Our recommendation may be implemented at management's discretion.

Financial reporting issues definitions

	Potential effect on the financial statements	Prioritisation of remedial action
High	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.	This requires immediate management action to resolve.
Medium	We assess that there is a medium likelihood of this causing a material misstatement in one or more components of the financial statements.	We expect management action will be taken in a timely manner.
Low	We assess that there is a low likelihood of this causing a material misstatement in one or more components of the financial statements.	We recommend management action to resolve; however, a decision on whether any action is taken is at management's discretion.