



Our ref: 2020-4139
Charles Strickland, 3149 6032

14 October 2020

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 2020 financial audit for Sunshine Coast Regional Council. I issued an unmodified audit opinion on your financial statements.

The purpose of this letter is to update you on any matters that have arisen since we presented our closing report to the audit committee on 6 October 2020.

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. However, we have raised an additional deficiency in relation to the related party declaration process in the lead up to the 2020 local government election. Issues and other matters formally reported to management and an update on actions taken by management to resolve these issues is included as Appendix A to this letter.

Report to parliament

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

Consistent to prior 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. In this report we will comment on the results of our audit of your financial report, any significant internal control issues we identified, and the overall results of the sector, including, major transactions and events. 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 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 \$239,000 exclusive of GST (2019: \$265,000). This fee is less than the \$250,000 estimated fee in our external audit plan due to savings in travel costs during the COVID-19 period.

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)

Financial reporting maturity level

QAO are in the process of finalising a new financial statement preparation reporting tool, called the financial reporting maturity model. This model allows for scalable assessment of financial reporting preparation processes which aims to better reflect the differences in size and maturity of public sector entities. For future years, we are planning to move to assessing the process according to the new maturity model. In the interim we will commence working with management to understand their expected / desired positioning of maturity.

We would like to thank you and your staff for their engagement in the audit this year and look forward to working with your team again next 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 6032.

Yours sincerely



Charles Strickland
Sector Director

Enc.

Appendix A1—Internal control issues



Significant deficiencies, deficiencies and other matters

The following table details control deficiencies and other matters reported to management during the course of our 30 June 2020 financial audit, with management responses and current status.

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



Significant deficiency



Deficiency



Other matter



Significant deficiency

[20-IR-2] Critical security settings are not enabled in the SAP Payroll system

[Control activities]

Council has not enabled the critical security settings in SAP Payroll system to:

- prevent accidental loss of data or SAP deletion programs from automatically resetting data in error
- protect the system against intentional or unintentional overwriting.

There are no compensating controls to prevent this loss of data.

Implication

Council is exposed to the risk of accidental loss of data, data integrity issues or intentional/or unintentional overwriting of system information.

QAO recommendation

That Council enables security settings to prevent accidental loss of data and protect system information from being overwritten.

Management response

The critical security settings in SAP Payroll system have now been locked in addition to being migrated to the test environment to complete final validation.

It is important to note that payroll end users do not have access to this functionality.

I agree with the issue and associated recommendations.

Responsible Officer

Head of People & Culture

Implementation Date

22 May 2020

Status

Resolved.

Appendix A1—Internal control issues



Significant deficiency

[20-IR-3] Insufficient segregation of duties in maintaining the SAP Payroll system

[Control activities]

Council has engaged a third-party service provider to assist with managing and maintaining its SAP payroll system. However, council cannot outsource their responsibility for designing and maintaining an appropriate and effective system of internal control with respect to financial reporting.

Twenty-two user accounts have a high level of privileged access within the SAP system to provide technical support and system maintenance. These users have access to all functions, including maintaining the system, managing user access, changing system security and changing data. This has resulted in a lack of segregation of duties between privileged users.

Implication

Inadequate segregation of duties exposes Council to the risks of unauthorised:

- changes to the system.
- access to sensitive information.
- transactions being processed.

These unauthorised activities may not be detected.

QAO recommendation

That Council:

- develops a plan to implement segregation of duties between staff members that perform system maintenance and those that manage user access and security
- defines and implements detective and monitoring controls while the segregation of duties issue is being addressed.

Management response

Council agrees in part with the issue and associated recommendations. The twenty-two user accounts with privileged access are all with the external vendor. The generic accounts are being revised to ensure segregation of duties between system maintenance and those that manage user access and security.

Responsible Officer

Head of People & Culture

Implementation Date

29 May 2020

Status

Resolved.

Appendix A1—Internal control issues



Significant deficiency

[20-IR-4] Processes and oversight in managing the SAP payroll system

[Control environment]

Council has not defined or formalised with their third party-service provider the following processes for managing the SAP system:

- User access management to ensure access to SAP is valid and appropriate
- Change management to ensure all changes are approved and tested
- Security oversight process to monitor and review critical and high-risk system and user administration activities.

Implication

There is an increased risk of inconsistent practices that could lead to unauthorised access and changes to systems and information. This could result in security breach, unauthorised transactions in the systems or fraud.

QAO recommendation

That Council defines and implements processes for managing user access, system changes and oversight functions for system security.

Management response

Council to implement a process to more effectively manage and monitor SAP user accounts to ensure access is valid and appropriate. Security audit reports will be created to support this process.

Council follows an agreed change management approach to ensure all changes are approved and tested.

Responsible Officer

Head of People & Culture

Implementation Date

29 May 2020

Status

Resolved – Operating effectiveness will be tested in 2020–21.

Appendix A1—Internal control issues



Deficiency

[20-IR-6] Access to SAP background administrator in the SAP Payroll system

[Control activities]

Background processing allows SAP users to execute and schedule tasks “in the background” which means handing the execution of the task over to a system process rather than being directly performed by the user themselves. This function is useful for any long running or regular tasks or processes that can be scheduled.

This access allows the user to use the privileges of another user (i.e. the ‘step user’) when running background jobs.

We noted that there are six SCRC employees and 22 support accounts that have access to SAP background administrator to schedule background jobs or review jobs.

Implication

This access could be used as means to elevate a user’s privileges. Users can potentially misuse the elevated privilege to make changes to existing scheduled background jobs. This may result in intentional or unintentional changes to data and the system.

QAO recommendation

That Council:

- review the appropriateness of the existing background administration access
- review the requirements of the background administrator access and whether background jobs can be performed without providing users with access to background administration
- remove inappropriate access.

Management response

The existing background administration access will be reviewed to ensure it is appropriate. In addition, an assessment will be completed as to whether background jobs can be performed without providing users with access to background administration.

As an alternate solution, Council will investigate if end users can be restricted to their own jobs and spool requests and whether or not this is too restrictive for payroll processing.

Responsible Officer

Head of People & Culture

Implementation Date

29 May 2020

Status

Resolved.

Appendix A1—Internal control issues



Deficiency

[20-IR-7] Unintended user maintenance access within the SAP Payroll system.

[Control activities]

SAP user maintenance can be controlled with various SAP authorisation objects to suit the business requirements. One of the authorisation objects allows the administrator to provide access to users to perform user maintenance on specific "groups" of SAP accounts and any other SAP accounts that do not have a specified user group.

We noted that:

- The People and Culture team have access to perform user maintenance for 'customer' user groups.
- There are 24 privileged SAP accounts that are currently not assigned to any user groups.

This means that the HR team can perform user maintenance activities over the 24 privileged SAP accounts that are not assigned to any user groups.

Implication

There is an increased risk that privileged accounts can be maintained by non-authorised users.

QAO recommendation

That Council assigns an appropriate user group to all SAP accounts and determines an appropriate person/position to manage user maintenance for this group.

Management response

Council will work with the consultant to assign the appropriate user group to all SAP accounts to ensure the functionality of authorisation object S_USER_GRP and S_USER_SAS restricts as intended.

In addition, a new role is to be created for user administration and access to these functions which will be removed from the role Z_CUST_HR_SYSTEM_ADMIN.

I agree with the issue and associated recommendations.

Responsible Officer

Head of People & Culture

Implementation Date

29 May 2020

Status

Resolved.

Appendix A1—Internal control issues



Deficiency

[20-FML-1] Incomplete Key Management Personnel Declarations of Related Party Information.

[Control activities]

Councils related party disclosure policy requires KMP declarations to be obtained from Councillors and executive managers at the end of each financial year.

During the 2019-20 financial year, Council did not obtain KMP declarations for all Councillors in the lead up to the local government election in March 2020 meaning that the five Councillors who were not re-elected did not provide these declarations for the period 1 July 2019 to 28 March 2020. There was also the former Chief Executive Officer and a group executive that were part of the KMP group who left the organisation during the 2019–20 financial year but did not provide KMP declarations upon leaving.

Implication

We acknowledge that Council has processes and procedures in place to identify related party transactions, however failure to obtain these declarations may lead to new related party relationships and transactions going undetected and therefore not being assessed for disclosure in the financial report.

QAO recommendation

That Council amend the related party disclosure processes and procedures to ensure:

1. KMP declarations for all Councillors are obtained in the lead up to future local government elections; and
2. KMP declarations are obtained from any Councillors or staff members who cease to become part of the KMP group during future reporting periods.

Management response

Management acknowledges the recommendation and will implement Item 1. Regarding Item 2, management will implement where possible.

Responsible Officer

Chief Financial Officer

Implementation Date

13 October 2020

Status

Resolved - Pending QAO verification.

Appendix A1—Internal control issues



Other matter

[20-IR-8] Setting the time zone to AUSQLD within the SAP Payroll system.

The time zone for the SAP Payroll system has not been set to Australian (Queensland) time. The system currently uses the installation default of Central European time.

While an incorrect time zone does not necessarily have a negative impact on the system or its operation, it provides the opportunity for misinterpretation of any system logs or document time stamps.

QAO recommendation

That Council sets the system time zone to Australian (Queensland) time.

Management response

Council will further investigate the implications of setting the system time zone to AUSQLD including the downstream impacts to any scheduled processes and procedures.

Responsible Officer

Head of People & Culture

Implementation Date

29 May 2020

Status

Resolved.



Other matter

[20-IR-9] Establishing user licensing processes within the SAP Payroll system.

Council does not have a SAP account offboarding process for terminated accounts to ensure that they are:

1. Clearly identified
2. Not included in a SAP user licensing review.

QAO recommendation

That Council establishes a SAP account offboarding process to ensure terminated accounts are clearly identifiable and will not be included in any user licensing review.

Management response

Council is seeking guidance on the process in SAP Payroll to fully terminate an employee and then release a SAP licence. It was assumed that once an employee terminates from the system that their associated user licence is also terminated.

I agree with the issue and associated recommendations.

Responsible Officer

Head of People & Culture

Implementation Date

29 May 2020

Status

Resolved – Operating effectiveness will be tested in 2020–21.

Appendix A1—Internal control issues



Other matter

[20-IR-10] Clear identification of all support accounts within the SAP Payroll system.

Not all support accounts within the SAP system are clearly identifiable by the name of the account. This is important as it assists SCRC to confirm support account usage and activity. It also helps to identify which support personnel are using the accounts.

QAO recommendation

That Council implements a standard naming convention for all support accounts. This includes maintaining full user account details such as user group(s) and complete names.

Management response

It is important to note that this only relates to the external consultant accounts created by SAP. A standard naming convention will be implemented for all support accounts. This includes maintaining full user account details such as user group(s) and complete names.

All existing accounts will be reviewed and updated including deactivating stale accounts (Dev/Tst/Prd).

I agree with the issue and associated recommendations.

Responsible Officer

Head of People & Culture

Implementation Date

29 May 2020

Status

Resolved.



Other matter

[20-IR-11] Cleaning up of support accounts no longer in use within the SAP Payroll system.

There are privileged support accounts which have been locked and are no longer required for use but have not yet been terminated.

QAO recommendation

That Council properly terminates all support accounts that are no longer required by removing all access and adding the accounts to a user group to clearly identify the accounts that have been terminated.

Management response

This relates to **20-IR-10**. Council will work to fully terminate support accounts that are no longer required by removing all access and adding the accounts to a user group to clearly identify that the accounts have been terminated and not required.

I agree with the issue and associated recommendations.

Responsible Officer

Head of People & Culture

Implementation Date

28 May 2020

Status

Resolved.

Appendix A1—Internal control issues



Other matter

[20-IR-12] Standard housekeeping background jobs that fail within the SAP payroll system

Standard SAP housekeeping background jobs are currently failing due to the 'step user' account being locked for use. These jobs require a 'step user' to action the scheduled task. When the step user account is locked, the background job is unable to execute and cancels with an error.

QAO recommendation

That Council unlocks the appropriate step user accounts to ensure that all required background jobs can successfully run. A generic system account (not a dialog or a service account) for background jobs would ensure that a similar issue does not occur again in the future.

Management response

Council will update the step user for jobs that are currently failing due to locked accounts to ensure all required background jobs can successfully run. Creating a generic existing system account SAP_SYSTEM (not a dialog or a service account) specifically for background jobs would ensure that a similar issue does not occur again in the future.

Council has raised a Service Request with SAP directly to investigate the nature of these two jobs and confirm if required prior to initiating any activity.

I agree with the issue and associated recommendations.

Responsible Officer

Head of People & Culture

Implementation Date

29 May 2020

Status

Resolved.

Appendix A1—Internal control issues



Other matter

[20-IR-13] Contracts over \$200,000 not published on Council's website

Six current contractual arrangements worth more than \$200,000 were not published on Council's website as per the requirements of the *Local Government Regulation 2012*.

Implications

Council is in breach of the *Local Government Regulation 2012*. Apart from non-compliance with legislation, there exists a potential for diminished confidence in Council's commitment to open and transparent governance.

QAO recommendation

That Council publish these contracts on their website to ensure that the regulation is complied with.

Management response

The following response was provided by the Business and Innovation Branch on 28 April 2020.

I agree with the issue and associated recommendations.

The Business and Innovation Branch lead and administer Council's Procurement and Contracting Framework. This sees the vast majority of significant procurement activities (those worth \$200,000 or more) being undertaken by that branch. However, a business unit may, under certain circumstances, undertake procurement activities over the value of \$200,000.

Processes are in place to capture information relating to all procurement activities, including contract values. These processes are presently proving to be effective for the majority of procurement activities but has failed to capture some activities undertaken by individual business units.

The Business and Innovation Branch is undertaking a review of current processes for capturing and reporting procurement activities to ensure details of all contracts above the \$200,000 threshold are identified and published.

The Procurement and Contracting Framework documentation, including the Contract Manual, will be updated to ensure the obligations and responsibilities of those undertaking procurement activities are clear.

It is believed these actions will be sufficient to close to small window that has resulted in the identified failings.

Responsible Officer

Manager Business and Innovation Branch

Implementation Date

31 December 2020

Status

Resolved.

Appendix A2—Matters previously reported



Status

The following table summarises the status of all control deficiencies, financial reporting issues and other matters that have previously been raised but are not yet resolved. The listing may include issues from our reports earlier this year and issues raised in prior years.

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

Internal control issues

Financial reporting issues




Significant deficiency	Deficiency	Other matters	High	Medium	Low

Component	Issue	Status
Deficiency		
Control activity	<p>20-IR-1: Delays in recording contributed assets (updated)</p> <p>As a result of delays in processing contributed asset information, there are 8,111 assets (2019: 2,706) with a net value of \$3.424m (2019: \$29.258m) that were under control of Council in previous financial years that have been brought to account during the 2019–20 financial year. This is a significant improvement on prior financial years as a result of various process improvements driven by a working group formed to address this issue. The working group also identified inconsistencies in "on-maintenance" dates used to capitalise contributed assets, resulting in a restatement of prior year balances of \$16.625m. Refer to Note 35e of the financial statements for more details.</p> <p>Based on this progress, we have downgraded the rating of this matter from a significant deficiency to a deficiency.</p>	<p>Work in progress</p> <p>Council are working 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. This control deficiency has been downgraded from a significant deficiency due to the improvements in Council's processes which has resulted in fewer contributed assets from prior years being recognised in the 2020 financial statements. We will continue to monitor the financial impacts of this situation over the coming years.</p> <p>Due date: 30 June 2021</p>




Appendix B—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.</p> <p>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>