



Sunshine Coast Regional Council

2018 Interim report to the Mayor

15/05/2018

Your ref: 2018-4139

IN-CONFIDENCE

15 May 2018

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

Dear Councillor Jamieson

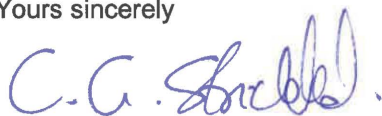
2018 Interim report

We present to the Council our interim report for Sunshine Coast Regional Council for the financial year ending 30 June 2018. In this report we detail the internal control and financial reporting issues we identified during our interim audit visit. It includes an assessment of the internal control environment; status of the audit; and a summary of significant control deficiencies, financial reporting issues 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.

This interim report is based on the audit work performed to our April 2018 interim visit. This includes our assessment of the design and implementation, and operating effectiveness, of controls.

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

Yours sincerely



Charles Strickland
Sector Director

Enc.

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



Audit progress

Internal control assessment and issues

We have tested the operating effectiveness of controls for the period 1 July 2017 to 28 February 2018 for revenue, expenditure and payroll.

We identified two new internal control deficiencies in Council's information systems area. These are detailed on pages 5 and 6 of this report.

Of the six prior year issues, four have not yet been resolved and have been re-raised. These are detailed from page 7 of this report.

We will complete our controls testing for the remainder of the financial year during our later visit and provide you with another update in our final report at the conclusion of the final audit testing.

Financial reporting issues and other matters

No financial reporting issues or other matters were identified during our interim audit testing.

Areas of audit significance

Valuation and depreciation of assets – We have commenced our audit on some early non-current asset valuation reports, however the majority of our review over valuation and depreciation is planned as part of our July 2018 visit.

Investment in associate valuation – We will test this as part of our final visit.

Expenditure on major contracts and projects – We have tested the effectiveness of key expenditure controls for the period 1 July 2017 to 28 February 2018, with no deficiencies noted. Substantive testing to date includes transactional analytical procedures, review of procurement processes for a 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 final visit.

Financial sustainability reporting – We will test this as part of our final visit.

Milestones – financial reporting and audit deliverables

All agreed Council financial reporting and audit deliverable milestones have been met, or are not yet due.

Pro forma financial statements – Due 30 May 2018.

Resolve known accounting issues – None at the date of the external audit plan.











Finalise non-current assets valuations – Due 30 June 2018



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	-	-	-	1	
 Risk assessment Processes for identifying, assessing and managing risk	-	-	-	-	
 Control activities Implementation of policies and procedures to prevent or detect errors and safeguard assets	-	-	2	3	
 Information and communication Systems to capture and communicate information to achieve reliable financial reporting	-	-	-	-	
 Monitoring activities Oversight of internal controls for existence and effectiveness	-	-	-	-	

Our ratings



Effective

Not significant deficiencies identified.



Generally effective

One significant deficiency identified.



Ineffective

More than one significant deficiency identified.





Deficiencies

The following table details control deficiencies identified through our audit as at April 2018. It includes a response from management.

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

 Significant deficiency  Deficiency  Other matter

Deficiency

2.1 Configuration setting to process invoices

Observation

Council has a three-way match function in the FinanceOne system. This enables matching of invoices to goods receipt and purchase orders with a tolerance limit of \$50.

The configuration settings for authorisation code 'Payable' provides Accounts Payable staff with the ability to process an invoice even when the \$50 tolerance limit has been exceeded.

Implication

Accounts Payable staff can process invoices that are more than \$50 greater than approved purchase orders.

QAO recommendation

We recommend that Council updates this configuration setting to prevent the processing of invoices that exceed the \$50 tolerance limit and review whether the \$50 is still appropriate.

Management response

The access to allow invoice matching above the tolerance limit of \$50 was active in the PAYABLES authorisation code within T1Financials. Although this access was active, Management has no knowledge or found any evidence of this access being used. The Accounts Payable internal process is to reject any invoices with a variance over the \$50 tolerance limit, and return them to the responsible officer for order receipt amendment.

The access to allow invoice matching above the \$50 tolerance limit has now been removed from the authorisation code and testing is currently underway to ensure the tolerance is working correctly.

Management expects to have this testing completed and the issue resolved by 30 June 2018.

Responsible officer: Accounts Payable Team Leader

Status: Work in progress – management undertaking corrective action

Action date: 30/06/2018





2.2 Disabling system access for terminated users

Observation

Council does not have a consistent process to ensure removal of system access for personnel who are no longer working for Council and/or have been re-hired.

We compared a list of terminated personnel to the list of users who can access Council's network (Active Directory) and FinanceOne system. We found sixteen instances where access had not been removed as follows:

- Eleven instances where Digital and Information Services (DIS) did not disable user accounts after Human Resources or the business area requested that the access be removed or the Active Directory system did not automatically disable the accounts after the accounts had passed their validity (end-date) period. Due to DIS not completing the termination process appropriately, five of the eleven terminated personnel were able to access Council network without authorised re-activation requests from the business area or Human Resources team when Council re-hired them. Seven of these eleven user accounts had access to the FinanceOne system.
- Three instances where the business area or Human Resources did not provide end date information to DIS when activating access for temporary personnel and contractors ('contingent workers').
- Two instances where Human Resources did not have records of personnel for whom the business areas had engaged directly and had requested system access with DIS.

Implication

There is an increased risk of unauthorised access to the systems or users having access to the system and information that is not compatible with their roles and responsibilities.

QAO recommendation

We recommend that:

- DIS removes access based upon notification from the business areas and Human Resources and ensures that automatic disabling occurs when end-dates for user accounts are reached.
- DIS re-activates access of disabled accounts upon authorised request from Human Resources.
- The business areas and Human Resources establish a consistent process to notify DIS when they terminate or extend the service of temporary personnel and contractors. This includes notification when users change their roles and responsibilities within Council and providing the account end-date information to DIS.

Management response

QAO's review of the employee termination process across Council covered all staff terminations (full time, temporary, part time, casual and contingent) for the period of July 2017 to January 2018. The review has uncovered 16 instances where the termination process had failed either through human, process or system error.

Digital Information Services acknowledges some weaknesses have been found in the off-boarding process.

SCC acknowledged in the QAO 2017 audit that Council's worker on-boarding and off-boarding processes would be revised during the HR system refresh/replacement. The procurement of the new HR system did not progress in 2017. Subsequently the HR and DIS teams have developed and implemented an interim worker on-boarding process that ensures contingent workers and permanent staff will be effectively managed until the new system is implemented.

The project to secure a new HR system has recommenced and is due to go to tender this financial year. It is expected it will provide permanent resolution to the issues identified by QAO.

DIS and HR will start work immediately to develop and implement changes to the staff off-boarding processes that will mitigate the issues raised by QAO until the new system is implemented.

Responsible officer: Chief Information Officer, and Manager People and Culture

Status: Work in progress – management undertaking corrective action

Action date: 31/07/2018



2 Internal control issues



2.3 Managing password for privileged accounts (Re-raised issue)

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 who access these passwords leave Council.

These passwords are stored in a password safe application that does not have controls to prevent copying by system support staff or support staff remembering the password when they leave Council.

Implication

There is an increased risk of unauthorised access to the Active Directory and financial systems which may result in unauthorised transactions or changes to system and data.

QAO recommendation

We recommend that Council implements a process to regularly change passwords on:

- default and generic system accounts
- accounts with privileged access.

We also recommend that Council change passwords on these accounts when personnel with access to these accounts leave the Council.

Management response

DIS note that following the 2017 audit recommendations actions have been taken to secure a number of accounts with privileged access. In this audit process QAO have identified that the Master Database Accounts (a default and generic system account) have not yet been addressed.

We have performed the following activities in relation to the master database account:

- Identified the key computer service accounts for SCC's finance, property and payroll systems.
- Subject to test outcomes, these accounts will be restricted to use by computer services and not available to be logged in to a console. This eliminates the use of these accounts for staff to log on via a console to gain higher privileges.
- Accounts that cannot be restricted to only computer services, application master logins and database master logins will have their passwords changed periodically and also following staff departures within the DIS Solutions Delivery team. The Solutions Delivery team consists of business analysts and database administrators who in order to perform their duties, access these passwords.

Responsible officer: Chief Information Officer

Status: Work in progress – management undertaking corrective action

Action date: 30/09/2018.





2.4 IT security policy and procedures (Re-raised issue)

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 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.

Implication

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

QAO recommendation

We recommend that Council:

- finalise the IT security policy
- develop a suite of directives or procedures to guide and detail the implementation of the policy.

Management response

DIS has undertaken an extensive process of developing a security policy that meets the Queensland Government IS18 standards and documenting the relevant procedures in Council.

The Draft Policy has been reviewed by the Chief Executive Officer and DIS is working to incorporate his feedback along with the outcomes of the recent deep dive review of the branch.

DIS had worked on addressing the recommendation and acknowledge that QAO have found there is further work to be done to fully complete it.

DIS will work to develop this once the policy has been finalised.

Responsible officer: Chief Information Officer

Status: Work in progress – management undertaking corrective action

Action date: 01/12/2018





2.5 Monitoring the activities of users with privileged access (Re-raised issue)

Observation

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

- high risk activities of 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).

Since our recommendation, Digital and Information Services has performed some risk assessments. There is a plan for implementing the relevant processes to review activities requiring logging and regular monitoring.

Implication

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:

- finalise the risk assessments to identify:
 - sensitive, highly privileged and system administration activities requiring regular monitoring
 - direct data changes to critical tables in database and security configuration files in the database
- monitor and review security related transactions on a regular (i.e. monthly) basis and require personnel, independent from the system administration function, to review activities performed by privileged users
- log, monitor and perform independent reviews of critical security and direct data changes to databases in accordance with the results of the risk assessment.

Management response

DIS have performed the following activities in relation to this item:

Based on the findings from the KPMG Audits in 2016 and 2017, which reviewed SCC's finance, property and payroll business processes, sensitive information and key business and system processes were identified and risk assessments performed.

Each medium to high risk process that involved systems was further analysed to determine what business, application and system levels of controls or monitoring are in place to mitigate or manage this risk.

Business, application and system changes have been proposed and implemented for a number of these identified risks and this work will continue until all risks are mitigated or managed. This work includes the monitoring of application databases for direct and application changes as well as monitoring of network folder access where required.

Auditing of the finance systems databases for changes to key application configuration data will be investigated.

An Application Support Group charter which includes roles and responsibilities for business and ICT staff has been drafted. This includes the responsibility to review the privileged (application admin) membership as well as auditing exceptions reported from the finance systems.

A DIS security group has been established which will meet fortnightly to manage significant security issues and to review the privileged systems (domain admin) membership as well as auditing exceptions reported from active directory.

Responsible officer: Chief Financial Officer, Chief Information Officer, and Manager People and Culture

Status: Work in progress – management undertaking corrective action

Action date: 30/09/2018



3 Prior year issues



Status

The following table summarises the status of issues and other matters reported by audit in prior years.

Reference	Rating	Issue	Status
Internal control issues			
Issue 3.1.1 QAO letter 08/05/17		IT security policy and procedures	Re-raised in the current year. Refer to deficiency no 2.4
Issue 3.1.2 QAO letter 08/05/17		Active Directory – Managing access to Councils network	Resolved
Issue 3.1.3 QAO letter 08/05/17		Managing contractor access	Resolved
Issue 3.1.4 QAO letter 08/05/17		Finance One, TechnologyOne Property and Chris 21 – Monitoring activities of users with privileged access	Re-raised in the current year. Refer to deficiency no 2.5
Issue 3.1.5 QAO letter 08/05/17		Logging and monitoring critical database changes	Re-raised in the current year. Refer to deficiency no 2.5
Issue 3.1.6 QAO letter 08/05/17		Managing password for privileged accounts	Re-raised in the current year. Refer to deficiency no 2.3



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.</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>



5 Appendix B—Information on internal controls



What is internal control?

'Internal control' is the processes, systems, records and activities that your entity designs, implements and maintains to provide you with reasonable assurance about the achievement of organisational objectives regarding:

- reliability of financial reporting
- effectiveness and efficiency of operations
- compliance with applicable laws and regulations.

Your governing body and executive management collectively are responsible for preparing reliable financial statements in accordance with generally accepted accounting principles. They are similarly responsible for maintaining effective internal control over financial reporting.

Our assessments of your internal control framework

The auditing standards that we must comply with require us to understand and assess those aspects of your internal control that relate to our financial statement audit objectives. In the planning phase of our audit, we sought to understand and evaluate how controls are designed and implemented. We communicated to you the results of our analysis in our external audit plan.

If we decide that we can rely on your controls, we must then test them to confirm they operated effectively. The results of our testing may highlight deficiencies in your internal controls. We assess whether any identified deficiencies in internal control constitute, individually or in combination, a significant deficiency in internal control.

Limitations of our reporting on internal control deficiencies

No system of internal control can provide absolute assurance about the absence of error or compliance. Even in the absence of identified control weaknesses, inherent limitations in your internal controls over financial reporting may not prevent or detect material misstatements.



qao.qld.gov.au



[Suggest a performance audit topic](#)

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

[Subscribe to news](#)

[Connect with QAO on LinkedIn](#)

Charles Strickland
T: (07) 3149 6032
E: Charles.Strickland@qao.qld.gov.au

T: (07) 3149 6000
E: qao@qao.qld.gov.au
W: qao.qld.gov.au
Lvl 14, 53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002

 **Queensland
Audit Office**
Better public services

