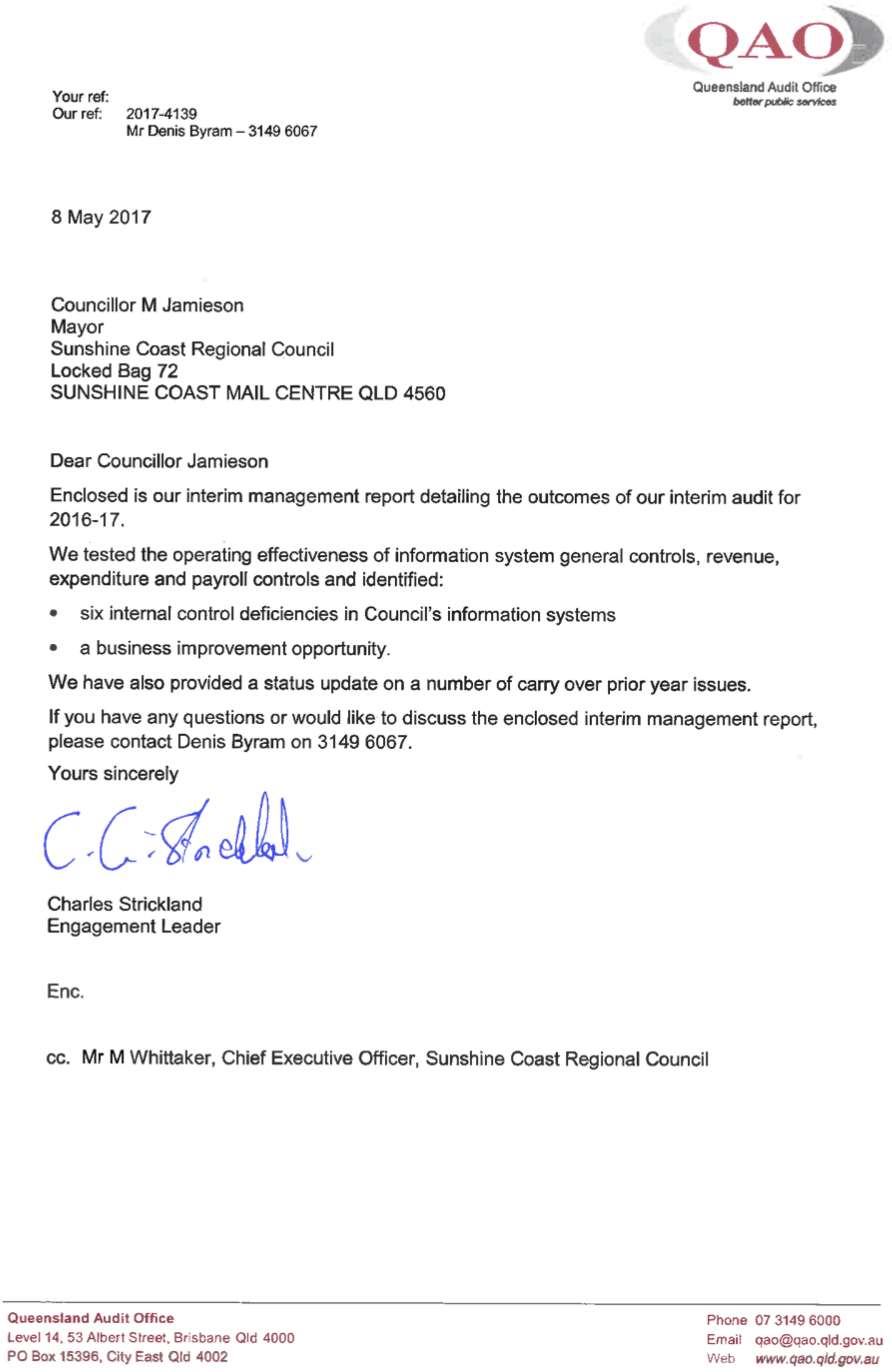


QAO
Queensland Audit Office
better public services

Your ref:
Our ref: 2017-4139
Mr Denis Byram – 3149 6067

8 May 2017

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

Dear Councillor Jamieson

Enclosed is our interim management report detailing the outcomes of our interim audit for 2016-17.

We tested the operating effectiveness of information system general controls, revenue, expenditure and payroll controls and identified:

- six internal control deficiencies in Council's information systems
- a business improvement opportunity.

We have also provided a status update on a number of carry over prior year issues.

If you have any questions or would like to discuss the enclosed interim management report, please contact Denis Byram on 3149 6067.

Yours sincerely

Charles Strickland
Engagement Leader

Enc.

cc. Mr M Whittaker, Chief Executive Officer, Sunshine Coast Regional Council

Queensland Audit Office
better public services

Sunshine Coast Regional Council

Interim management report to the Mayor

For the financial year ended 30 June 2017

As at: 8 May 2017

Contents

Summary.......................................3
Understanding this report.......................................6
Control and risk issues.......................................8
Status update of prior year reported issues.......................................16
Risk ratings used in this report.......................................19

About the Queensland Audit Office (QAO)

QAO is the external auditor of the Queensland public sector. We provide audit opinions on the reliability of financial statements produced by state and local government entities. We give independent assurance directly to the Queensland Parliament about public sector finances and performance.

We help the public sector meet its accountability obligations by providing advice, assistance and unique insights to help improve performance. Our vision is better public services and world-class audits.

1. Summary

In this report, we detail the internal control and financial reporting issues we identified during our interim audit visit of Sunshine Coast Regional Council in respect to the 30 June 2017 financial statement audit. For each issue, where we have received management responses, we have included them. We have also provided a status update on prior year reported issues.

Internal control issues

Before testing

In our *External audit plan,* we set out our audit approach based on your overall internal control framework being assessed as effective. We based our assessment on our understanding of your entity, including relevant controls in the areas of information systems, revenue, expenditure and payroll. We planned to test the operating effectiveness of controls in these areas reducing the expected level of other audit procedures to be performed in combination with a detailed substantive testing approach for all material financial statement components

Results of testing

We have tested the operating effectiveness of information system general controls, as well as key controls over revenue, expenditure and payroll. In summary, we:

- did not identify any significant internal control deficiencies
- identified internal control deficiencies in Council's information system general controls. Refer to 3.1 for details.

The following table outlines the number and classification of deficiencies by COSO element and indicative traffic lights for your information. This is a progress update only and final traffic lights for the year will be advised in our *Closing report.*

COSO element	Number of significant deficiencies		Number of deficiencies		Indicative traffic light to date per COSO element
	Current year issues	Prior year unresolved issues	Current year issues	Prior year unresolved issues	
Control environment ▪ Culture and values ▪ Governance, plans and policies ▪ Organisational structure ▪ Management's integrity and operating style	0	0	1 Refer to 3.1	0	🟢
Risk assessment ▪ Strategic risk assessment ▪ Financial risk assessment ▪ Operational risk assessment	0	0	0	0	🟢
Control activities ▪ Manual controls ▪ Automated controls	0	0	5 Refer to 3.1	0	🟡
Information and communication ▪ Non-financial systems ▪ Financial systems ▪ Reporting systems	0	0	0	0	🟢
Monitoring activities ▪ Management supervision ▪ Self-assessment ▪ Internal audit	0	0	0	0	🟢

Legend – Traffic Light

🟢 Effective	No significant deficiencies identified and less than 3 deficiencies in one element
🟡 Generally effective	1 significant deficiency or 3 or more deficiencies in one element
🔴 Ineffective	More than 1 significant deficiency in one element

Approach after testing

Based on results of our testing of internal controls, we have confirmed our assessment of your overall control framework as effective. Accordingly, we will rely on the operating effectiveness of your internal control environment to reduce the level of substantive procedures we will perform on the following financial statement areas of revenue, expenditure and payroll, with remaining financial statement areas of cash, property, plant and equipment, equity and financial statement related disclosures to have a detailed substantive testing approach.

Financial reporting issues

We did not identify any financial reporting issues during our interim audit that we assessed as high risk.

If we identify any further issues as the audit progresses, we will include them in our *Closing report* issued at the conclusion of our audit.

Based on the issues raised in this report, we will not make major changes to the audit approach as presented in our *External audit plan*.

Other matters

We identified other matters that we consider represent business process improvement opportunities. Refer to 3.2 and 4.2 for details.

If we identify any further issues as the audit progresses, we will include them in our *Closing report* issued at the conclusion of our audit.

Based on the issues raised in this report, we will not make major changes to the audit approach as presented in our *External audit plan*.

2. Understanding this report

2.1 Internal control issues

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.

The Council and executive management collectively are responsible for preparing reliable financial statements in accordance with generally accepted accounting principles, and 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. This is based on their potential to cause a material misstatement (an error that could affect the judgement or opinion of readers) in the financial statements. Refer 5.1 for a further explanation of how we rate identified internal control deficiencies.

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.

2.2 Financial reporting issues

Financial reporting issues relate to the reliability, accuracy and timeliness of your financial reporting and are not control deficiencies. We have rated them based on their potential to impact on our auditor's report and/or for giving rise to material misstatement in the financial statements. Refer 5.2 for a further explanation of how we rate identified financial reporting issues.

Where we have identified financial reporting issues not already included in our *External audit plan*, or where issues related to previously reported risks have significantly changed, we have included them in this report.

2.3 Auditor-General reporting to parliament

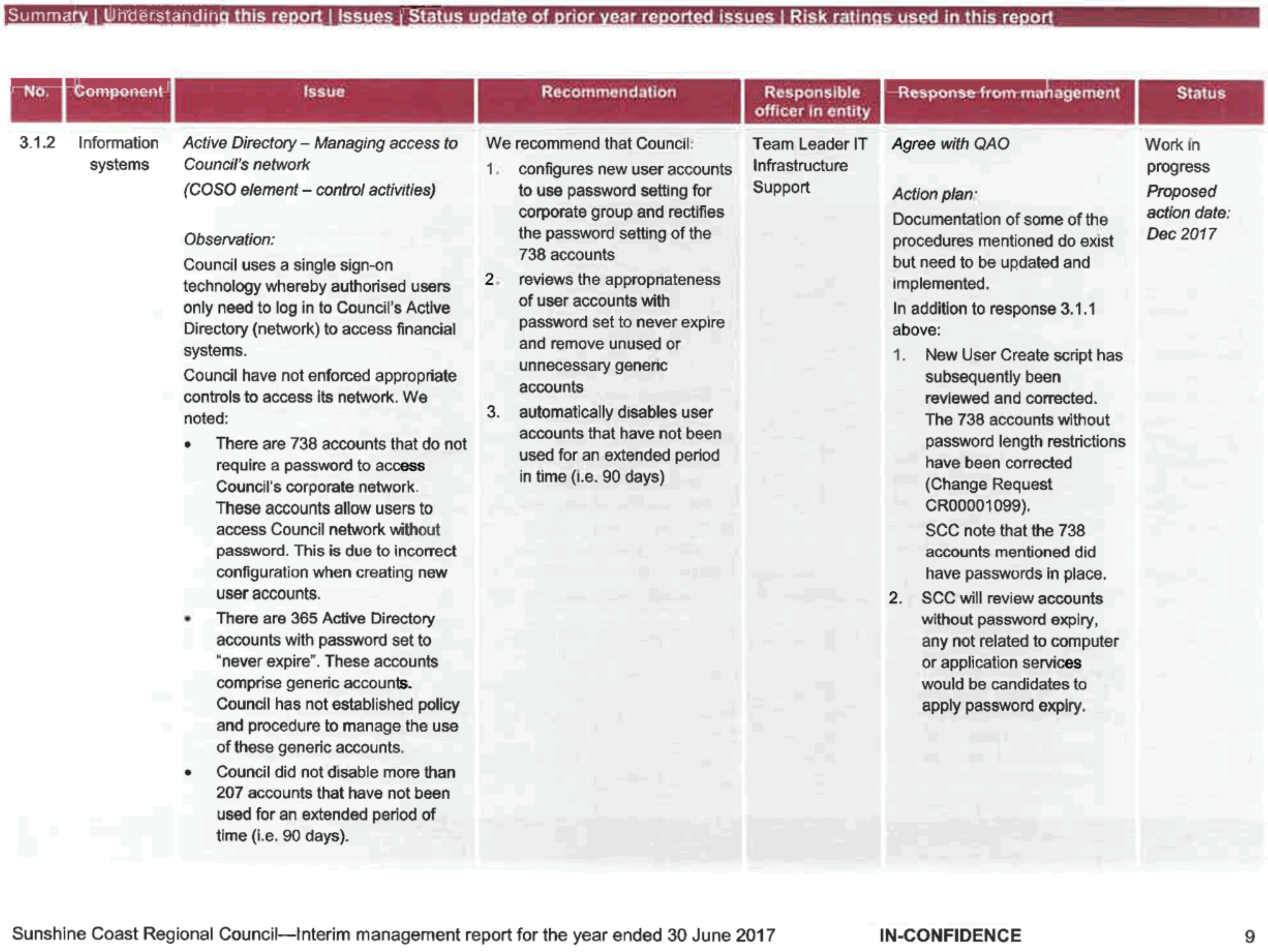
The *Auditor-General Act 2009* requires the Auditor-General to report to parliament on an issue raised during an audit if he considers it to be significant. This includes consideration of identified significant deficiencies in internal control and financial reporting issues. However, whether these issues are reported depends on a number of factors, including action taken to resolve the issues prior to the completion of the audit. If the Auditor-General intends to include an issue from this audit in a future report to parliament, you will be given an opportunity to comment on the issue raised and your comments, or a summary of them, will be reflected in the report.

3. Control and risk issues

3.1 Internal control deficiencies

The following table summarises internal control deficiencies which are not significant deficiencies identified through our audit testing as at 8 May 2017, and includes a response from management. Refer 5.1 for a further explanation of how we rate identified internal control deficiencies.

No.	Component	Issue	Recommendation	Responsible officer in entity	Response from management	Status
3.1.1	Information systems	*IT security policy and procedures* *(COSO element – control environment)* Council does not have a current and complete security policy. The policy document provided by Council is incomplete and has not been updated since 2014. We noted, for example: • Standards and documentation for password controls, management of privileged passwords and user access do not exist. • Management of contractor accounts is ad-hoc with no identified process for the timely removal of contractor access. *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 unauthorised access.	We recommend that Council updates the IT security policies and procedures to include, at the minimum: • security requirements and system settings • management of password and use of accounts with privileged access • management of default and/or generic accounts • user access management process, both for employees and contractors • monitoring the use of privileged accounts and high risk access • change management process.	Team Leader IT Infrastructure Support	*Agree with QAO* *Action plan:* ICTS will work to have these policies and processes appropriately documented through a process of reviewing what procedures and documentation is already in place to build a complete framework. Processes and some documentation was developed for minimum standard for passwords, and advice provided to users. Further work is needed, as recommended, to document the implemented policy, and other associated procedures.	Not yet commenced *Proposed action date: Dec 2017*



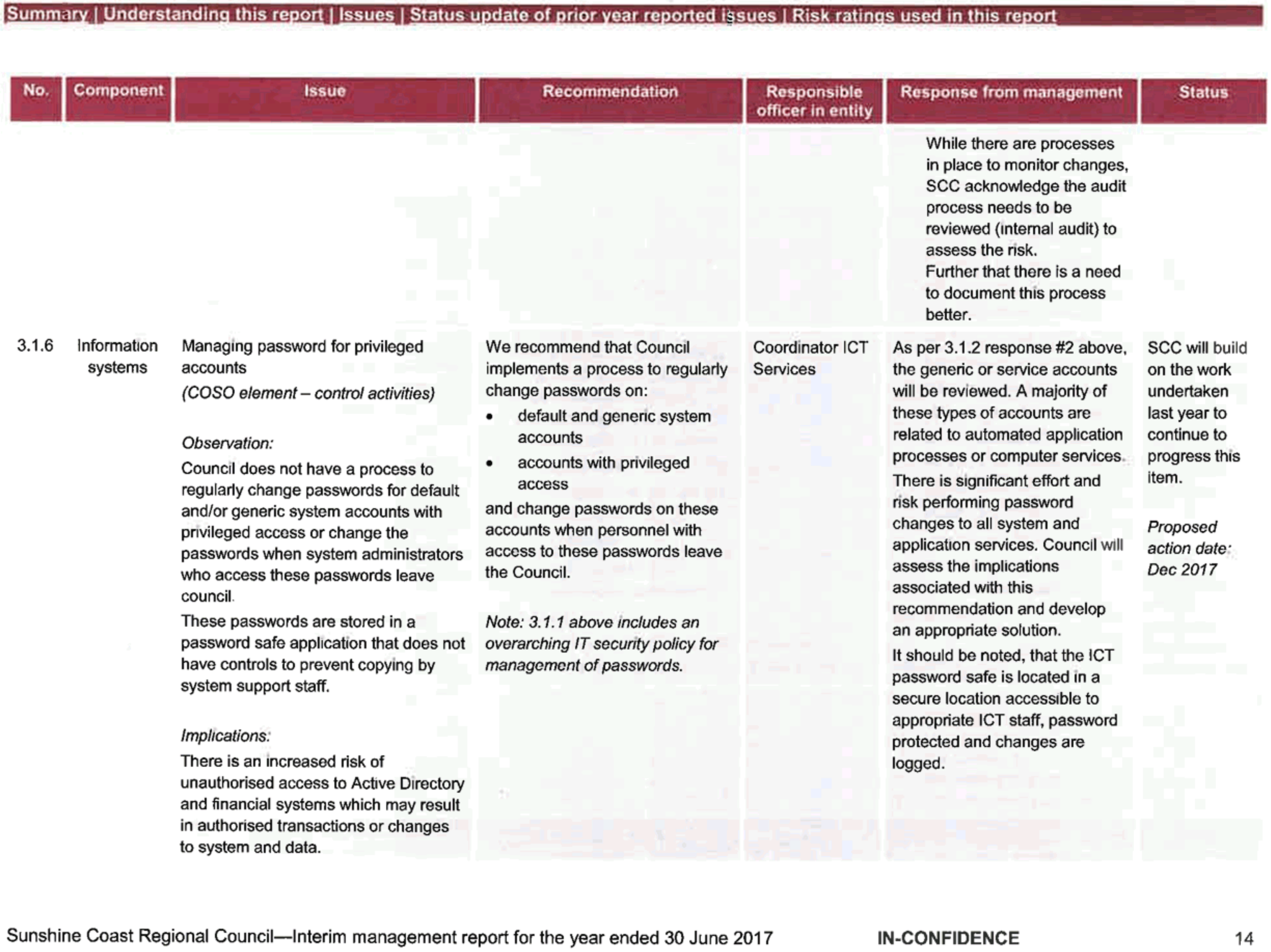
No.	Component	Issue	Recommendation	Responsible officer in entity	Response from management	Status
3.1.2	Information systems	*Active Directory – Managing access to Council's network* *(COSO element – control activities)* *Observation:* Council uses a single sign-on technology whereby authorised users only need to log in to Council's Active Directory (network) to access financial systems. Council have not enforced appropriate controls to access its network. We noted: • There are 738 accounts that do not require a password to access Council's corporate network. These accounts allow users to access Council network without password. This is due to incorrect configuration when creating new user accounts. • There are 365 Active Directory accounts with password set to "never expire". These accounts comprise generic accounts. Council has not established policy and procedure to manage the use of these generic accounts. • Council did not disable more than 207 accounts that have not been used for an extended period of time (i.e. 90 days).	We recommend that Council: 1. configures new user accounts to use password setting for corporate group and rectifies the password setting of the 738 accounts 2. reviews the appropriateness of user accounts with password set to never expire and remove unused or unnecessary generic accounts 3. automatically disables user accounts that have not been used for an extended period in time (i.e. 90 days)	Team Leader IT Infrastructure Support	*Agree with QAO* *Action plan:* Documentation of some of the procedures mentioned do exist but need to be updated and implemented. In addition to response 3.1.1 above: 1. New User Create script has subsequently been reviewed and corrected. The 738 accounts without password length restrictions have been corrected (Change Request CR00001099). SCC note that the 738 accounts mentioned did have passwords in place. 2. SCC will review accounts without password expiry, any not related to computer or application services would be candidates to apply password expiry.	Work in progress *Proposed action date: Dec 2017*

No.	Component	Issue	Recommendation	Responsible officer in entity	Response from management	Status
		Implication: There is an increased risk of unauthorised access to the Active Directory and financial systems which may result in authorised transactions or changes to system and data.			3. SCC will implement a process to highlight these accounts for review and potential disabling. Automatically disabling staff accounts could have undesired consequences for staff who have significant leave times.	
3.1.3	Information systems	*Managing contractor access* *(COSO element – control activities)* *Observation:* Council does not have a formalised process and centralised register to manage system access for contractors. In addition, IT relies on the diligence of business units to notify help desk to remove system access for terminated contractors. We also noted that: • Council has not disabled access to the Active Directory and Finance One system for at least five contractors who have not accessed these systems for more than 90 days.	We recommend that Council: 1. establishes a central register and processes to manage system access for contractors 2. automatically disables user accounts that have not been used for more than 90 days 3. establishes processes to verify the identity of contractors requesting their password be reset.	Coordinator ICT Services	*Agree with QAO* *Action plan:* Documentation of some of the procedures mentioned do exist but need to be updated and implemented.	Work in progress *Proposed action date*: Completion of this item is dependent on the implementation of a new HR Management System which is due June 2018

No.	Component	Issue	Recommendation	Responsible officer in entity	Response from management	Status
		▪ The process to reset passwords over the phone does not cater for contractors. Council encourages contractors to use a self-service facility, however it has not established a process for validating contractors over the phone. *Implications:* There is an increased risk that contractors are able to access Council's system after termination. This may result in authorised transactions or changes to system and data			1. Management of contractual staff is in scope for the current project to replace the current HR Management System therefore the finalisation of this issue will be part of the procurement and implementation of the new system. SCC will automate the comparison of the intranet contractor list (manually maintained) and the Active Directory contractor list, the differences to be referred to the contractors' supervisor for clarification. Additional validation will be added to the current Intranet contractors list. 2. Refer to 3.1.2, response # 3 above. 3. Council does not rely on phone communication for contractors to reset their passwords, SCC instead require the use of OKTA our identity management solution. SCC will ensure this is reflected in official documentation of our procedures.	

No.	Component	Issue	Recommendation	Responsible officer in entity	Response from management	Status
3.1.4	Information systems	*Finance One, TechnologyOne Property and Chris 21 – Monitoring the activities of users with privileged access* *(COSO element – control activities)* *Observation:* Council has not undertaken a risk assessment to identify sensitive, highly privileged or system administration activities that require logging and regular monitoring. Council also does not monitor the activities of users assigned with privileged access. We noted that Council regularly review user access rights as part of the Application Support Group (ASG) group meetings, however no monitoring of activities perform by privileged users is being performed. *Implications:* There is an increased risk that council will fail to detect unauthorised activities and transactions in a timely manner.	We recommend that Council: 1. performs risk assessments to identify sensitive, highly privileged and system administration activities requiring regular monitoring within one year 2. monitors and reviews security related transactions on a regular (i.e. monthly) basis 3. requires personnel, independent from the system administration function, to review activities performed by privileged users.	Coordinator ICT Services	*Agree with QAO* In 2016 SCC adapted their process to include a standing agenda item at each Application Support Group (ASG) Meeting to review the users that have application admins or "elevated privileges. Each ASG has performed the initial review and this process is now in practice. 1. SCC will undertake a risk assessment of this item which will consider the multiple processes which exist across the business and ICTS. Gaps identified through the risk assessment will be addressed. 2. Inbuilt application monitoring of all financial transactions was implemented and subsequently reverted due to significant performance degradation. Whilst SCC currently monitor security changes within the application and at the database level, monitoring of all transactions made by privileged users could also have significant performance impacts and needs careful consideration.	SCC will build on the work undertaken last year to continue to progress this item. *Proposed action date: Feb 2018*

No.	Component	Issue	Recommendation	Responsible officer in entity	Response from management	Status
					3. SCC will review the current business and ICTS processes for independence and document.	
3.1.5	Information systems	*Logging and monitoring critical database changes* *(COSO element – control activities)* *Observation:* The Council does not log and independently monitor security related transactions and critical changes to the databases of financial systems (e.g. direct data changes, changes to database configuration, changes to executable code). We noted that the system sends automatic email notifications to the database administrators when changes are made. However, there is no monitoring, independent from database administrators, for these notifications. *Implications:* Unauthorised changes in the financial systems production databases may not be detected.	We recommend that Council: 1. assesses the risk, impact and criticality of: • direct data changes to critical tables in the database • changes to security configuration files for the database 2. logs, monitors and performs independent reviews of critical security and direct data changes to databases in accordance with the result of the risk assessment.	Coordinator ICT Services	*Agree with QAO* *Action plan:* 1. As provided during this audit, SCC currently monitor database security changes and database object changes. As per 3.1.4 response #2 above, monitoring every database transaction will need careful consideration. 2. Further to ICTS monitoring, the SCC Finance team perform various audits of user transactions and Council's Internal Audit carries out reviews on financial processes. A risk versus benefits analysis will be considered in the design of any ongoing process.	SCC will build on the work undertaken last year to continue to progress this item. *Proposed action date: Dec 2017*



No.	Component	Issue	Recommendation	Responsible officer in entity	Response from management	Status
					While there are processes in place to monitor changes, SCC acknowledge the audit process needs to be reviewed (internal audit) to assess the risk. Further that there is a need to document this process better.	
3.1.6	Information systems	Managing password for privileged accounts *(COSO element – control activities)* *Observation:* Council does not have a process to regularly change passwords for default and/or generic system accounts with privileged access or 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. *Implications:* There is an increased risk of unauthorised access to Active Directory and financial systems which may result in authorised transactions or changes to system and data.	We recommend that Council implements a process to regularly change passwords on: • default and generic system accounts • accounts with privileged access and change passwords on these accounts when personnel with access to these passwords leave the Council. *Note: 3.1.1 above includes an overarching IT security policy for management of passwords.*	Coordinator ICT Services	As per 3.1.2 response #2 above, the generic or service accounts will be reviewed. A majority of these types of accounts are related to automated application processes or computer services. There is significant effort and risk performing password changes to all system and application services. Council will assess the implications associated with this recommendation and develop an appropriate solution. It should be noted, that the ICT password safe is located in a secure location accessible to appropriate ICT staff, password protected and changes are logged.	SCC will build on the work undertaken last year to continue to progress this item. *Proposed action date: Dec 2017*

3.2 Other matters

The following table summarises other matters related to business improvement opportunities we identified through our audit testing as at 8 May 2017, and includes a response from management.

No.	Opportunity	Recommendation	Management response	Status
3.2.1	*Controlled entity financial statements not published on councils website* *Observation:* We noted Sunshine Coast Regional Council's wholly owned subsidiary, SunCentral Maroochydore Pty Ltd does not currently make its audited financial statements publicly available, either by posting their financial statements on the company's website or alternatively placing them on the parent entity's (SCRC) website.	In the interest of enhancing accountability and providing greater transparency around the company's activities it is recommended that Sunshine Coast Regional Council make the company's audited financial statements publicly available through posting on applicable websites. We perceive this measure will enable the community to assess the performance of the entity, and more generally reflect the fostering of good governance practices in the Council. This recommendation remains consistent with the observations recently detailed in the recent Queensland Auditor-General's Report to Parliament, *Local government entities: 2015-16 results of financial audits Report 13: 2016-17 (refer Recommendation 1 page 7).*	*Responsible officer in entity:* *Director Corporate Services* *Action plan:* As SunCentral Maroochydore Pty Ltd is a Corporations Law company with an independent Board of directors, Sunshine Coast Regional Council will discuss this recommendation with the Board. *Implementation date:* 30 November 2017	Management undertaking for corrective action

4. Status update of prior year reported issues

4.1 Internal control deficiencies

The following table provides a summary update on the status of identified prior year reported internal control deficiencies that were not resolved before the issuance of our Closing report, and includes a response from those charged with management.

No.	Prior year issue	Recommendation	Rating	Status update
4.1.1	*Raised at interim – 27 June 2013* ***User Profile Maintenance and Financial Delegations*** *Observation* Finance One user profile management processes identified control weaknesses over user profile matrix, system logging, and review and monitoring of financial delegations.	We recommended that Council initiate action to address the control weaknesses identified.	Deficiency	**QAO Update:** Based on action taken and our testing, issue considered **Resolved.**
4.1.2	*Raised at interim – 9 June 2016* ***Logging & Monitoring Changes in the Database Environment*** *Observation* It was found that there is no logging and independent monitoring of security related transactions and changes in the database environment (e.g. direct data changes; changes to database configuration parameter settings; changes to executable code). *Implication:* Unauthorised changes in the production database instances may not be identified in a timely fashion.	We recommended that: • Logging is switched on for changes to: - data made at the database level, and - configuration files for the database instance. • The changes are monitored to ensure they are authorised.	Deficiency	**QAO Update:** Issue still exists and **re-raised within current year issue 3.1.5 as a deficiency**.

No.	Prior year issue	Recommendation	Rating	Status update
4.1.3	*Raised at interim – 9 June 2016* ***Privileged user activities*** *Observation* The council does not independently monitor and review key financial systems on security related transactions such as assignment of elevated privileges, changes to profile / role configurations, enabling and disabling user accounts with elevated privileges. *Implication:* There is an increased risk that unauthorised activities and transactions may not be timely detected.	We recommended that personnel, independent from system administration activities, monitor and review security related transactions for: • assigning of elevated privileges to users. • changes to privileges allocated to a profile / role • enabling and disabling user accounts with elevated privileges.	Deficiency	**QAO update:** Issue still exists and **re-raised within current year Issue 3.1.4 as a deficiency.**
4.1.4	*Raised at interim – 9 June 2016* ***Resetting passwords over the phone*** *Observation* There are no processes in place to verify the users' identity when they request password reset over the phone. *Implication:* There is a risk that password reset is requested by unauthorised user who intends to breach system security.	We recommended that council implement processes and/or technology to verify users who request password reset over the phone.	Deficiency	**QAO update:** Issue still exists for resetting of password for contractors and **re-raised within current year issue 3.1.3 as a deficiency.**
4.1.5	*Raised at interim – 9 June 2016* ***User access for TechnologyOne Property system*** *Observation* There is no periodic review of user access to the system to ensure that access privileges are commensurate with users' roles and responsibilities and segregated from incompatible functions. *Implication:* The council may not detect and correct unauthorised or incompatible access privileges and this may result in unauthorised or incorrect transactions being processed fraudulently or in error.	We recommended that Council review user access on a regular basis (biannual or annually).	Deficiency	**QAO Update:** Based on action taken and our testing, issue considered **Resolved.**

4.2 Other matters

The following table provides a summary update on the status of prior year business improvement opportunity.

No.	Opportunity	QAO recommendation	Status update
4.2.1	*Raised at interim – 9 June 2016* *Asset Management Plans awaiting adoption by Council.* *Observation:* Management has completed seven Asset Management Plans (AMPs) during the 2015-16 financial year that are awaiting formally adoption by Council. The AMPs awaiting adoption are • Buildings and Facilities; • Coastal & Environment; • Holiday Parks; • Parks & Gardens; • Stormwater; • Transportation; and • Waste and Resources Management.	We recommend council's website reflect current Asset Management Plans.	*Prior year Management comment:* Council accepts the above recommendation and will commence tabling Annual Asset Management Plans at Council for endorsement. Proposed action date is 16 December 2016. **QAO update** While we understand that Council is utilising the completed 2015-16 AMPs, a review of Council's intranet revealed that only the 2014 Asset Management Plans were available. As at date of issue of this interim management letter, Council has planned to adopt their AMP's at their June 2017 meeting. *NOTE – We will follow-up as part of the 2016-17 PPE interim visit in June.*

5. Risk ratings used in this report

5.1 Our rating of internal control deficiencies

We have assessed all internal control deficiencies in this report based on their potential to cause a material misstatement in the financial statements. The risk assessment categories are as follows:

Assessed category	Potential effect on the financial statements	Prioritisation of remedial action
Significant deficiency	This is a deficiency in internal control or combination of deficiencies in internal control that, in our professional judgement, is of sufficient importance to merit the attention of those charged with governance, and includes deficiencies that may lead to a material misstatement of the financial statements.	This requires immediate management action to resolve. Ie an implementation plan should be developed as **a** priority to ensure action is taken to resolve.
Deficiency	We have assessed that the control: (i) is designed, implemented or operated in such a way that it is unable to prevent, or detect and correct, misstatements in the financial statements component on a timely basis, or (ii) is necessary to prevent, or detect and correct, misstatements in the financial statements component on a timely basis, but is missing.	This requires management action to resolve within eight months of this report date.

5.2 Our rating of financial reporting issues

We have assessed all financial reporting issues in this report based on their potential to cause a material misstatement in the financial statements. The assessed risk ratings are as follows:

Risk rating	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, whether due to fraud or error, in one or more components (transactions, balances and disclosures) of the financial statements.	This requires immediate management action to resolve.
Medium	We assess that there is a medium likelihood of this causing a material misstatement, whether due to fraud or error, in one or more components of the financial statements.	This requires management action to resolve within four months of this report date.
Low	We assess that there is a low likelihood of this causing a material misstatement, whether due to fraud or error, 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.

5.3 Other matters

Other matters relate to business improvement opportunities we identified through our testing.

Queensland Audit Office
better public services

Charles Strickland
Queensland Audit Office
Level 14, 53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002

Phone	07 3149 6032
Email	charles.strickland@qao qld.gov.au
Web	*www.qao.qld.gov.au*

'Queensland Audit Office (QAO)'

Join us on LinkedIn®