

CITY OF WEST TORRENS



Notice of Committee Meeting

NOTICE IS HEREBY GIVEN in accordance with Sections 87 and 88 of the Local Government Act 1999, that a meeting of the

AUDIT AND RISK PRESCRIBED COMMITTEE

Members: Councillor S Rypp (Presiding Member),
Councillor G Vlahos
Independent Members: R Haslam, E Moran, S Spadavecchia

of the

CITY OF WEST TORRENS

will be held in the Mayor's Reception Room, Civic Centre
165 Sir Donald Bradman Drive, Hilton

on

**TUESDAY, 10 APRIL 2018
at 6.00pm**

**Terry Buss PSM
Chief Executive Officer**

City of West Torrens Disclaimer

Please note that the contents of this Committee Agenda have yet to be considered by Council and Committee recommendations may be altered or changed by the Council in the process of making the formal Council decision.

INDEX

1	Meeting Opened.....	1
1.1	Evacuation Procedures	
2	Present	1
3	Apologies	1
4	Disclosure Statements	1
5	Confirmation of Minutes.....	1
6	Communication by the Chairperson.....	1
7	Presentations	1
	Nil	
8	Outstanding Reports/Actions	2
8.1	Open Actions Update	2
9	Reports of the Chief Executive Officer.....	4
9.1	Financial Reporting and Sustainability.....	4
9.1.1	Financial Reporting	4
9.2	Internal Controls and Risk Management Systems.....	5
	Nil	
9.3	Internal Audit	5
9.3.1	Information Fraud Audit Report	5
9.3.2	Procurement Roadmap Continuous Internal Audit Report - Stages 2 and 3.....	27
9.3.3	2017-2018 Internal Audit Program Update	49
9.4	External Audit.....	66
	Nil	
9.5	Committee Performance and Reporting	66
	Nil	
10	Other Business	66
11	Confidential	66
	Nil	
12	Next Meeting	66
13	Meeting Close	66

1 MEETING OPENED**1.1 Evacuation Procedures****2 PRESENT****3 APOLOGIES****4 DISCLOSURE STATEMENTS**

Committee Members are required to:

1. Consider Section 73 and 75 of the *Local Government Act 1999* and determine whether they have a conflict of interest in any matter to be considered in this Agenda; and
2. Disclose these interests in accordance with the requirements of Sections 74 and 75A of the *Local Government Act 1999*.

5 CONFIRMATION OF MINUTES**RECOMMENDATION**

That the Minutes of the meeting of the Audit and Risk Committee held on 13 February 2018 be confirmed as a true and correct record.

6 COMMUNICATION BY THE CHAIRPERSON**7 PRESENTATIONS**

Nil

8 OUTSTANDING REPORTS/ACTIONS

8.1 Open Actions Update

Brief

This report presents an update on the current status of open actions from previous meetings of the Audit and Risk Prescribed General Committee.

RECOMMENDATION

It is recommended to the Audit and Risk Committee that it notes there are no current open actions.

Introduction

A report is presented to each ordinary meeting of the Audit and Risk Prescribed General Committee (Committee) detailing the status of open actions from previous Committee meetings.

Discussion

As detailed in **(Attachment 1)**, there are no open actions as at 31 March 2018.

Conclusion

This report advises that all open actions from previous meetings have been completed.

Attachments

1. Open Actions Report

April 2018

EMT = Executive Management Team
CEO = Chief Executive Officer
GMB&CS = General Manager Business & Community Services
GMCR = General Manager Corporate & Regulatory
GMUS = General Manager Urban Services
PLIA&R = Program Leader Internal Audit and Risk

[illegible]

9 REPORTS OF THE CHIEF EXECUTIVE OFFICER

9.1 FINANCIAL REPORTING AND SUSTAINABILITY

9.1.1 Financial Reporting

Brief

This report lists those finance related reports which were considered by Council between 7 February 2018 and 3 April 2018.

RECOMMENDATION

It is recommended to the Audit and Risk Committee that the Financial Reporting report be received.

Introduction

The Audit and Risk Prescribed General Committee (Committee) is presented with a list, at each of its ordinary meetings, of those finance related reports considered by Council since the Committee's last ordinary meeting. These reports and associated minutes, which are detailed below, are available on Council's website at www.westtorrens.sa.gov.au.

Discussion

The following reports were considered by Council/Council Committee between 7 February 2018 and 3 April 2018.

20 February 2018

- Creditor Payments
- Taxi Voucher Usage
- Elected Members' Telephones
- Register of Allowances and Benefits - 6 Months to 31 December 2017
- Council Budget report - SEVEN Months to 31 January 2018
- Budget Review - December 2017

6 March 2018

- Nil

20 March 2018

- Creditor Payments
- Council Budget Report - EIGHT Months to 28 February 2018

03 April 2018

- Budget and Annual Business Plan 2018/19

Conclusion

This report lists finance related reports which were considered by Council between 7 February 2018 and 3 April 2018.

Attachments

Nil

9.2 INTERNAL CONTROLS AND RISK MANAGEMENT SYSTEMS

Nil

9.3 INTERNAL AUDIT

9.3.1 Information Fraud Audit Report

Brief

This report presents the results of the Information Fraud Internal Audit.

RECOMMENDATION

The Committee recommends to Council that this report be received.

Introduction

In accordance with the approved *Internal Audit Program 2015-2018*, the *Information Fraud Audit* (Audit) was approved and commenced in December 2017 in accordance with the approved scope to report on:

- the adequacy and effectiveness of Council's approach to managing the risk of information fraud;
- management of privileged access to information and core business systems (including whether higher-risk information/systems are identified and managed appropriately);
- controls related to cumulative access to information;
- oversight and review of temporary access to information;
- access controls related to personally identifiable information; and
- handling of incoming documentation including, but not limited to, mail and tender responses.

Following completion of the Audit, a draft internal audit report (Report) was issued to the General Manager Corporate and Regulatory, Manager Information Services and the Senior Administrator for comment and individual risk assessment with a closing meeting held to provide an opportunity to clarify audit findings with the Auditor. The final Report was provided to the Executive in March 2018 (**Attachment 1**).

Internal Audit Findings

The Auditor's found that the City of West Torrens' (CWT) approach to managing the risk of information fraud is robust and substantially compliant with legislation, policy and procedure. Strong controls are in place to manage access to privileged information and core business systems. Policies and procedures are robust and well written. The Auditor also found that Information Security (IS) staff are conscientious and follow expected process.

Eleven (11) Audit findings were made by the auditor of which six (6) attracted a moderate level of risk, four (4) attracted a low level of risk and one (1) was a better practice initiative.

All Audit findings are within CWT's risk tolerance levels. The recommendations are minor in nature and the cost of implementing the recommendations exceeds the benefits, therefore progress updates will not be reported to the Committee.

Conclusion

The *Information Fraud Internal Audit*, undertaken by Council's contract auditor has been completed. Eleven (11) audit findings were made all of which are within CWT's risk tolerance levels. As such, the Administration will implement the recommendations only if the benefit of doing so exceeds the costs of resource allocation.

Attachments

1. Audit Report CWT Information Fraud March 2018



City of West Torrens Information Fraud

Internal Audit Report

Audited By: Tim Muhlhausler, Partner Galpins
Janna Burnham, Internal Audit Director Galpins
Jo Stewart-Rattray, Director of Information Security & IT Assurance BRM
Holdich
Elliot Raboy, Auditor Galpins

Draft Report Issued: February 2018

Final Report Presented: March 2018

Final Report Executive Management Approval: March 2018

Liability limited by a scheme approved under Professional Standards Legislation

Table of Contents

1. EXECUTIVE SUMMARY	3
1.1 Background	3
1.2 Objectives and Scope.....	3
1.3 Associated Risks	4
1.4 Examples of Good Practice	5
1.5 Key Findings and Recommendations	6
2. INTERNAL AUDIT FINDINGS AND RECOMMENDATIONS	8
2.1 Potential for error in Provisioning/De-provisioning process	8
2.2 Granting of System Access across Council.....	9
2.3 Use of separate accounts for every day vs privileged administrator activities for IS' team members	10
2.4 Communication of updates to the Elected Members Electronic Communications Facilities Policy	11
2.5 Review and approval of the use of Cloud Services	12
2.6 Definition of 'confidentiality' in the Policy	13
2.7 2013 Audit Findings: Implement an annual review of user application access.....	14
2.8 Risk from external media connecting to the CWT network	15
2.9 Staff training around information fraud	16
2.10 Introducing data leakage prevention tools	17
2.11 A need to use encrypted media.....	18
Appendix 1: Implementation 2013 Audit 'Logical Security: Technology One Financials and BIS' Recommendations	19
Appendix 2: Documents reviewed and interviews conducted	21

1. EXECUTIVE SUMMARY

1.1 Background

The approved 2017-18 Internal Audit Program provides for an internal audit to review the City of West Torrens' risk of information fraud. The *Council Policy Fraud and Corruption Prevention, Control, Reporting and Investigation* describes fraud as meaning "the use of misrepresentation, deception or dishonest conduct in order to obtain benefit from or cause financial detriment to the CWT". Information fraud is one subset of fraud involving the inappropriate access or use of an organisation's information.

Information fraud can arise from weaknesses in an organisation's information security. Fraud can occur when individuals have greater access to information than is required to perform their job roles or functions or when controls relating to the protection of information can be bypassed or are less robust than they should be. The Australian Government Information Security Manual (AGISM), while not mandated for Local Government, has been used by audit as guiding principles which promote strong information security (and therefore reduced risk of information fraud) within organisations.

It is well documented that a significant amount of fraud is uncovered via employee tipoffs. Consequently, it is important to understand Council's broader approach to minimising the risk of information fraud.

1.2 Objectives and Scope

The objectives of the audit were to evaluate and report on the adequacy and effectiveness of Council's approach to managing the risk of information fraud. This was achieved through a review of whether select information security controls are applied, as outlined in the AGISM, including;

- management of privileged access to information and core business systems (including whether higher-risk information/systems are identified and managed appropriately);
- controls related to cumulative access to information;
- oversight and review of temporary access to information;
- access controls related to personally identifiable information; and
- handling of incoming documentation including, but not limited to, mail and tender responses.

In addition, the audit reviewed:

- Progress against prior audit findings in relation to logical security of Technology One Financials and BIS
- Council's broader approach to preventing the risk of fraud at a high level.

This review included, but was not limited to, the following:

- Consideration of framework, policies and procedures in relation to information access, including:
 - Council Policy: Fraud and Corruption Prevention, Control, Reporting and Investigation
 - Administration Policy: Information Technology and its Use
- Assessment of the adequacy of the process for allocating and revoking information privileges. This included:
 - the approach to the allocation of basic privileges (for example, on a role basis, by name)
 - information access where staff members' information needs change – for example due to position changes, acting responsibilities, contract positions
 - the approach to the use of mobile and portable storage devices
 - authorisations required to grant information access (delegations and sign offs required)
- Assessment of closure of findings from 2013 internal audit into Logical Security (Technology One Financials and BIS)

The appropriateness of specific IT access was also tested in detail, based on risk. Risk was assessed based on discussion with the Program Leader Audit and Risk, relevant General Managers, auditor understanding of key risk areas (based on experience) and review of available information. These areas included:

- Information privileges as granted to Freedom of Information (FOI) Officers
 - this included a review around the auditability of what information FOI Officers and Software Administrators access
- A review of access to:
 - tender information technology
 - records information technology
- Physical access to information, particularly confidential mail

A list of documents reviewed and staff interviewed is included at Appendix 2.

1.3 Associated Risks

Potential risks associated with Information Fraud identified through Internal Audit include, but are not limited to:

- Non-compliance with legislation such as, but not limited to, the ICAC Act, Local Government Act and Mandatory Code of Conduct resulting in:
 - investigation by an external agency
 - fraud, corruption, misconduct and/or maladministration
 - breach of employment and associated performance management
 - conflicts of interest(s) not being declared
 - reputational damage
- Inadequate monitoring, follow up and reporting

1.4 Examples of Good Practice

Internal controls / processes assessed as demonstrating good practice in mitigating risk included the following:

- ✓ The Information Management team use the Local Government General Disclosure Schedule to classify information that is stored and held by CWT. These classifications are then used to determine the access rights and the retention period for this information.
- ✓ FOI requests are initiated via an online service request available to the Governance team via "GovHub". The requests generate a helpdesk ticket which is then used to provide appropriate access to the FOI officer. Access is automatically withdrawn after a specific time period linked to the request.
- ✓ Major CWT applications such as Objective, FinanceOne, Pathway and CHRIS21 have auditable tracking, providing an electronic history of data being accessed or downloaded.
- ✓ Automatic computer screen saver locks activate after ten minutes of idle time for general staff and after four minutes for the Information Services (IS) team.
- ✓ Network passwords are set in accordance with the Microsoft Password Policy and complexity is enforced.
- ✓ After audit fieldwork, the IS team introduced the use of Secure File Transfer Protocol (SFTP) instead of the insecure File Transfer Protocol for transferring files with external parties. This helps to avoid breaches of security when transferring data.
- ✓ System backup and recovery is set up and utilised with off-site replication.
- ✓ Disaster Recovery facilities are offsite and a formal agreement is in place with the City of Adelaide.
- ✓ Users downloads are restricted and no local administration rights are assigned to users. This means that applications cannot be downloaded to PCs. Unauthorised downloads represent a large security risk if not managed appropriately.
- ✓ The onsite server room requires a swipe card and key access, which is only provided to the IS team and management. This reduces the risk of unauthorised access to information.
- ✓ Access to high risk information sharing sites such as Dropbox has been denied, ensuring greater control over data imports and exports.
- ✓ All IT equipment is barcoded and registered.
- ✓ Regular auditing of the inventory of authorised network devices occurs.
- ✓ All IT purchases are approved by the IS team before devices can be connected to the network.
- ✓ IT hardware is either disposed of if not in use and destroyed at the CWT depot, or records are removed by Information Services prior to recycling or sale.
- ✓ A process is in place for administrative staff to not open any physical mail marked 'confidential', 'sensitive' or similar.

1.5 Key Findings and Recommendations

Overall, we found that the City of West Torrens' (CWT's) approach to managing the risk of information fraud is robust and substantially compliant with legislation, policy and procedure. Strong controls are in place to manage access to privileged information and core business systems. Policies and procedures are robust and well written, and Audit found that Information Security (IS) staff are conscientious and follow expected process.

Audit identified a need to formally document some processes, to reduce the risk of information fraud occurring into the future. Currently, there is a reliance on the Information Services and Information Management teams' significant intellectual property and tacit corporate knowledge that would be lost should these individuals leave CWT for any reason. Such intellectual property and corporate knowledge should be harnessed and documented to ensure that this knowledge is not lost and that the processes can be repeated when necessary. For example, the processes related to opening tender boxes (both logical and physical) and registering each response are strong, however these current processes require documenting and dissemination to relevant staff.

During the course of our interviews with staff from both the Information Management and Information Services teams, it seemed that there had been no formal training given in relation to information fraud. It is understood that there is little available training specific to this space however there may be some availability through professional bodies such as AIIM or RIMPA.

Findings were rated in accordance with the CWT's Risk Management Framework, as follows:

- *Extreme risk* recommendations
- *High risk* recommendations
- *Moderate risk* recommendations
- *Low risk* recommendations
- *Better practice* or improvement recommendations

Findings Summary Table

A summary of the internal audit findings is provided in the table below.

Finding and Recommendation/s - Risk Table	Extreme Risk	High Risk	Mod Risk	Low Risk	Better Practice
2.1 Potential for error in the access provisioning/de-provisioning process.			✓		
2.2 System Access across Council is devolved and 'department based' access granted rather than role based access			✓		
2.3 There is a need for IS' team members to have separate accounts for every day vs privileged administrator activities			✓		
2.4 Updates to the Elected Members Electronic Communications Facilities Policy should be communicated			✓		

6

Liability limited by a scheme approved under Professional Standards Legislation

Finding and Recommendation/s - Risk Table	Extreme Risk	High Risk	Mod Risk	Low Risk	Better Practice
2.5 There is a need for the IS team to review and approve the use of Cloud Services			✓		
2.6 There is a need to confirm the definition of 'confidentiality' in the Policy					✓
2.7 2013 Audit Findings: Implement an annual review of user application access				✓	
2.8 Risk from external media connecting to the CWT network				✓	
2.9 There is a need to introduce staff training around information fraud				✓	
2.10 Introducing data leakage prevention tools				✓	
2.11 There is a need to use encrypted media			✓		

Section 2 of the report details the key findings and recommended actions proposed to be undertaken by management.

2. INTERNAL AUDIT FINDINGS AND RECOMMENDATIONS

Risk Rating - Moderate			
Auditor	Descriptor	Consequence	Likelihood
Galpins	Reputation	Moderate	Unlikely
Manager Chris James, Manager Information Services			
Treatment: Treat the risk			
Issues and Impact	Recommendation/s	Management Response	Target Date
<p>2.1 Potential for error in Provisioning/De-provisioning process</p> <p>Provisioning and de-provisioning of users refers to the way in which users gain access to systems and data and how their access is removed when they no longer require it. As outlined in control #0405 in the AGISMM, 'personnel seeking access to a system need to have a genuine business requirement to access the system, as verified by their manager'. It is important this is undertaken in a timely manner at both ends of the process.</p> <p>Intranet based forms are completed to identify an individual's system access requirements. This form must have the Manager's approval via a checked box. The Information Services (IS) team then manually review the form and grant access.</p> <p>This process relies on the IS staff member knowing who the appropriate manager is for each staff member across more than 200 staff. Audit found it is also possible for general staff members to check the box and send the form without gaining management approval.</p> <p>HR sends changes to roles or positions to the IS team and in turn these changes are scanned to ensure that users have been provisioned or de-provisioned appropriately.</p> <p>There is potential for human error and time delays using the current process.</p>	<p><i>Recommendation 1</i></p> <ul style="list-style-type: none"> Consider establishing a workflow (perhaps in SharePoint) that will forward on-line system access (and removal of access) forms to the relevant manager for approval, then to IS staff for review. This will reduce the potential for error and improve efficiency of the process for the IS team. 	<p>The existing workflow includes the opportunity to notify the person lodging the request that their request is complete.</p> <p>The existing workflow will be modified to advise the manager that the access request has been processed.</p>	<p>30th April 2018</p>

Liability limited by a scheme approved under Professional Standards Legislation

Risk Rating - Moderate				
2.2 Granting of System Access across Council	Auditor <i>Galpins</i>	Descriptor <i>Reputation/Financial</i>	Consequence	Likelihood
	Manager Chris James, Manager Information Services	Treatment: Tolerate the risk	Moderate	Unlikely
Issues and Impact	Recommendation/s		Management Response	Target Date
<p>Audit understand that the Finance Department manage access to restricted functionality in the finance and payroll systems. The IT department provides base level access to new users and it is then the responsibility of the Finance Manager to provide provision additional access rights. Better practice would entail centralizing role based access with the IT Department who would be guided by formalized role based access rights from the managers of each department.</p> <p>The Principle of Least Privilege (POLP) should be applied wherever possible. The POLP is the practice of limiting access rights for users to the minimum permissions they require to perform their work.</p>	<p><i>Recommendation 2</i></p> <ul style="list-style-type: none"> Consider centralising roles-based access with the IT Department, rather than the business unit. <p><i>Recommendation 3</i></p> <ul style="list-style-type: none"> Establish the Principle of Least Privilege as standard practice to ensure that users have only the system access level they require to perform their job role or function. 		<p>The current practice is consistent with providing minimum permissions.</p> <p>Accountability and responsibility for access to restricted functionality in the finance and payroll systems is best owned by the Finance Manager who has the knowledge and expertise to ensure that access is consistent with the council's sub-delegation framework.</p>	No further action required.

Risk Rating -				
Auditor <i>Galpins</i>	Descriptor <i>Organisational</i>	Consequence <i>Moderate</i>	Likelihood <i>Unlikely</i>	
Manager Chris James, Manager Information Services		Treatment: Monitor the risk		
Recommendation/s		Management Response	Target Date	
Issues and Impact IS team members each have a single account for all activities they undertake, including both privileged administrator activities and everyday activities. Day to day activities could include access to email, accessing the ERP system, and using the internet. This does not follow the Principle of Least Privilege, which is considered better practice. Under this principle, separate accounts should be used for administrator activities and every day activities. This allows an easy audit trail of privileged activities, should it become necessary to review them. It also reduces the risk of full access to the CWT's systems if a data or system breach occurs, for example while the IS team members are using the internet. Recent Forrester Research found that 80% of today's security breaches involve the use of privileged user credentials. Therefore, Information Services administrators should only log in using their privileged account when they really need to in order to perform a particular task.		Recommendation 4 <ul style="list-style-type: none"> Ensure that relevant Information Services staff have two separate user accounts. One account is for performing day to day activities such as internet searches. The day to day account would have POLP applied. The second account would be used specifically for administration activities, and used on an as-needed basis. 	Whilst acknowledging the POLP, the overhead of the three key people constantly changing between profiles would negatively impact response times. The risk will be added to the Information Services risk profile for annual review in June each year.	30 th June

Liability limited by a scheme approved under Professional Standards Legislation

Risk Rating - Moderate		Likelihood Unlikely	
Auditor <i>Galpins</i>	Descriptor <i>Reputation</i>	Consequence <i>Moderate</i>	Likelihood <i>Unlikely</i>
Manager Chris James, Manager Information Services		Treatment: Treat the risk	
Recommendation/s		Management Response	Target Date
Issues and Impact The audit scope called for a review of policies and procedures in relation to information access. Audit reviewed the <i>Elected Members Electronic Communications Facilities Policy</i> . Elected Members are taken through this policy as part of Council's induction process. The policy states in section 5.1 Personal Use that 'Subject to this policy, reasonable personal use, including by family members, of CWT electronic communication facilities is permissible.' Audit consider that this presents a risk to the CWT's information security. If, for instance, the elected member's email account was left open and used by another person to send inappropriate emails, this could potentially result in reputational damage to Council as well as to the elected member. Another statement on page seven under section 5.7 Security and Confidentiality , states that "Elected Members should be alert to the fact that sensitive or personal information conveyed through electronic communication facilities cannot be guaranteed as completely private." Audit considers that, to ensure there is no misunderstanding, the policy needs to clearly state that email or any other electronic means of communication cannot be considered private.		The policy will be reviewed in conjunction with the new Council after the November elections. That e-mail is not private will be highlighted in induction processes for Elected Members after the November elections.	December 2018

Liability limited by a scheme approved under Professional Standards Legislation

Risk Rating -		Likelihood	
Auditor	Descriptor	Consequence	Unlikely
Galpins	Reputation/ Organisational	Moderate	
Manager Chris James, Manager Information Services		Treatment: Treat the risk	
Recommendation/s		Management Response	Target Date
Issues and Impact The audit scope called for a review of policies and procedures in relation to information access. Audit reviewed the <i>Information Technology and Its Use</i> Administration Policy and identified some potential for improvement. Section 5.9.3 covers the approval process for moving services or applications to the Cloud. Approval is given by the GM Corporate and Regulatory. The Manager of Information Services then meets with the GM on a fortnightly basis to discuss any approvals that have been given to move services or applications to the Cloud from across Council. There is a potential for sensitive data or services to be shipped to the Cloud before the Information Services team are aware of this. It is often very difficult to retrieve data from the Cloud after it has been moved. Audit consider that an Information Technology risk assessment should be undertaken in advance of any such move. This would help to treat the risk of data being moved to less than reputable organisations. It would also help to address the risk that Cloud services are used without appropriate Service Level Agreements (SLAs). Once sensitive data has 'been sent to the Cloud' without appropriate SLAs it may be very difficult to ensure that the data is returned to Council and all other copies destroyed. Audit also consider that a register of all Cloud Services being used should be developed. This will assist CWT to maintain appropriate oversight of the range of these services.		Recommendation 7 <ul style="list-style-type: none"> Consider changing the approval process for moving services or applications to the Cloud to require review and approval from the Manager of Information Services before moves occur. This would help to ensure that the risks and impacts of using the Cloud is understood from a technical perspective prior to a final decision being made. Recommendation 8 <ul style="list-style-type: none"> Ensure appropriate Service Level Agreements are in place with all Cloud Services providers. Recommendation 9 <ul style="list-style-type: none"> Develop a register of all Cloud Services being used. 	1 st July 2018

Liability limited by a scheme approved under Professional Standards Legislation

Risk Rating – Better Practice				
2.6 Definition of 'confidentiality' in the Policy	Auditor	Descriptor	Consequence	Likelihood
	Galpins Manager Chris James, Manager Information Services	N/A Treatment: Treat the risk	N/A	N/A
Issues and Impact	Recommendation/s		Management Response	Target Date
<p>One element of information security relies upon staff understanding and following the principles of confidentiality.</p> <p>The <i>Information Technology and Its Use</i> Administration Policy (section 5.4.3) states that 'confidentiality requirements must be observed.'</p> <p>Audit considers that, in order for there to be as little ambiguity as possible, the term 'confidentiality' needs to be defined in the document. This explanation could also point to guidance on how confidentiality should be applied.</p>	<p><i>Recommendation 10</i></p> <ul style="list-style-type: none"> To ensure that the <i>IT and Its Use</i> Administration Policy is clear, include a definition of 'confidentiality', including what confidentiality requirements are and how they should be applied. 		<p>The policy will be modified to include a definition of 'confidentiality'.</p>	1 st July 2018

2.7 2013 Audit Findings: Implement an annual review of user application access	Risk Rating - Low			
	Auditor Galpins	Descriptor Organisational / Customer	Consequence Minor	Likelihood Unlikely
	Manager Chris James, Manager Information Services	Treatment: Treat the risk		
Issues and Impact	Recommendation/s		Management Response	Target Date
<p>The scope of this audit called for a review of the 2013 Audit 'Logical Security: Technology One Financials and BIS' recommendations. Overall, we found that four of the six 2013 recommendations have been implemented (see Appendix 1 for further information).</p> <p>Recommendation 3 of the 2013 report related to periodic review of user access rights. It recommended the introduction of controls to review users' system access right listings. It specifically recommended:</p> <p><i>'Regular generation and review of reports detailing user access rights. Where reports are not currently available, they may be able to be written by the IT department or software provider. Evidence of this review should be maintained as an audit trail.'</i></p> <p>Recommendation 2 of the report related to procedures and controls for privileged accounts. A finding related to this is at Recommendation 2.3.</p>	<p><i>Recommendation 11</i></p> <ul style="list-style-type: none"> Conduct a regular (at least annual) review of access for all users across applications. 		<p>An annual review of user access will be conducted.</p> <p>The review will include listing the existing user rights and manager consideration of the identified access.</p>	<p>June each year commencing in 2018.</p>

Liability limited by a scheme approved under Professional Standards Legislation

Risk Rating - Low				
2.8 Risk from external media connecting to the CWT network	Auditor <i>Galpins</i>	Descriptor <i>Organisational / Customer</i>	Consequence <i>Minor</i>	Likelihood <i>Unlikely</i>
	Manager Chris James, Manager Information Services	Treatment: Monitor the risk		
Issues and Impact	Recommendation/s		Management Response	Target Date
<p>The audit scope called for a review of controls in relation to information fraud.</p> <p>Audit reviewed the process for connecting to the CWT network. We found that external media, laptops or other devices such as USBs that are connected to the network are not scanned for viruses or malware. This would include, for example, external media connected by suppliers and/or vendors.</p> <p>Malware or viruses may be inadvertently transferred to the network.</p>	<p><i>Recommendation 12</i></p> <ul style="list-style-type: none"> Create a policy or procedure that mandates that all external USBs, laptops or other devices are scanned for viruses before they are connected to the network. 		<p>Currently USBs are not scanned when they are plugged into a device on our network. When a file on a USB is accessed it is scanned by our antivirus. Additionally we use whitelisting to prevent unidentified executables from executing.</p> <p>Given the low risk rating, the risk will be added to the annual Information Services risk review.</p>	30 th June

Risk Rating – Low				
Auditor Galpins		Descriptor Organisational / Customer	Consequence Minor	Likelihood Unlikely
Manager Chris James, Manager Information Services		Treatment: Treat the risk		
2.9 Staff training around information fraud		Recommendation/s		
Issues and Impact		Management Response		
<p>One key control for managing the risk of information fraud is training and education of staff about expectations.</p> <p>The Information Management and Information Services teams at CWT were unaware of any recent training provided to employees in relation to information fraud.</p> <p>Information fraud techniques are continually evolving and employees will naturally lose awareness or forget training over time. Information fraud is more likely to occur when staff are less vigilant. Audit considers that there is a need to regularly remind staff of information fraud risks.</p>		<p>Recommendation 14</p> <ul style="list-style-type: none"> Ensure that appropriate information fraud and information security awareness training programs are provided to personnel. Training programs can also be supplemented by methods that can be used to continually promote awareness including logon banners, system access forms and departmental bulletins or memoranda. <p><i>Note – the intention of this recommendation is to promote awareness and the training is not intended to be an onerous / burdensome process.</i></p>		
		<p>Our intranet site provides access to 17 information security videos.</p> <p>The intranet banner advertising will be used twice per annum to promote information security awareness.</p> <p>Additionally, the IT team will provide a lunch'n'learn on information security at the Civic Centre and at the new Depot.</p>		
		30 th June		

Liability limited by a scheme approved under Professional Standards Legislation

Risk Rating – Low				
2.10 Introducing data leakage prevention tools	Auditor <i>Galpins</i>	Descriptor <i>Organisational / Customer</i>	Consequence <i>Minor</i>	Likelihood <i>Unlikely</i>
	Manager Chris James, Manager Information Services	Treatment: Tolerate the risk		
Issues and Impact	Recommendation/s		Management Response	Target Date
<p>One way to manage the risk of information fraud is to prevent data 'leakage'. Data leakage occurs when information is shared without appropriate authorisation.</p> <p>Data leakage can occur in numerous ways, for example by physically removing material, by sending information out by email attachments or on USB sticks. In addition, embedded viruses/malware can export information without an organisation's knowledge.</p> <p>One way to track the usage and copying/sharing of information is through data leakage prevention tools. Audit found that data leakage prevention tools are not used in the CWT network. There is a potential for large amounts of data to be exported from the network without detection.</p>	<p><i>Recommendation 15</i></p> <ul style="list-style-type: none"> Consider deploying a Data Leakage Prevention tool across the CWT network. 		<p>A suitable product to cater for monitoring and encryption of information has recently been costed at \$25,000 per annum for the product alone.</p> <p>The other significant cost is the time commitment to monitor and analyse what people are up to.</p> <p>The cost well exceeds the value of these measures being introduced at this time.</p>	No action

Liability limited by a scheme approved under Professional Standards Legislation

Risk Rating – Low				
2.11 A need to use encrypted media	Auditor <i>Galpins</i>	Descriptor <i>Reputation / Relationships</i>	Consequence <i>Moderate</i>	Likelihood <i>Rare</i>
	Manager Chris James, Manager Information Services	Treatment: Tolerate the risk		
	Recommendation/s		Management Response	Target Date
Issues and Impact While CWT personal computers are password protected, USBs supplied by CWT to employees are not password protected nor are they encrypted. USBs may be lost or misplaced and have potentially sensitive information on them. One control recommended by the SA Information Security Management Framework is to ensure that USBs are encrypted. Encrypted USBs are readily available and the cost of these devices has decreased over time.	Recommendation 16 • Consider mandating the use of encrypted USBs throughout the CWT.		Mandating encrypted USBs will put an impost on anybody needing to use a USB. With the increase in file-shares and mobile devices the volume of USBs is reducing.	No action

Liability limited by a scheme approved under Professional Standards Legislation

Appendix 1: Implementation 2013 Audit 'Logical Security: Technology One Financials and BIS' Recommendations

Recommendation	Implemented?	Comment
<p>1. An effective process and controls for authorising access rights at application system level is established. Examples of suitable controls include:</p> <ul style="list-style-type: none"> Formal documentation of the responsibilities of application system owners in relation to providing access rights to new and existing users. Implementation of an audit trail for the authorisation of user access rights providing details of the access rights granted to the user at application system level. This could for example be a form, or a screen shot of the original access rights set up that is printed and signed by the application system administrator ("champion"). 	Implemented	Processes are in place using on line forms for provisioning/de-provisioning of users. Audit identified some opportunity for improving the controls in the use of these forms (see Recommendation 2.1).
<p>2. An effective process and controls for ensuring that access rights have been removed for all employment terminations is established. Examples of suitable controls include:</p> <ul style="list-style-type: none"> Provision of a periodic report of terminated/transferred employees by the HR department to the IT department and application system owners ("champions") to review and ensure no terminated employees have access rights. Review of inactive account listings (e.g. no activity for greater than 90 days). <p>In addition, similar controls should be in place for employees on extended leave and employees changing roles within Council.</p>	Partially implemented.	<p>Access rights are not formally reviewed however the de-provisioning process is traceable and can be cross referenced to HR reports provided to the IS team.</p> <p>Audit identified some opportunity for improving the controls in the use of these forms (see Recommendation 2.1).</p>

Liability limited by a scheme approved under Professional Standards Legislation

19

<p>3. Effective processes and controls for reviewing user's access right listings are introduced. Examples of suitable controls include:</p> <ul style="list-style-type: none"> Formal documentation of the responsibilities of application system owners in relation to the review of user's access rights. Regular generation and review of reports detailing user access rights. Where reports are not currently available, they may be able to be written by the IT department or software provider. Evidence of this review should be maintained as an audit trail. 	Not yet implemented.	Each major application is administered by the department responsible, and a high-level overview of access rights is not yet in place. See Recommendation 2.7
<p>4. Effective procedures and controls for assigning and using privileged accounts are established. Examples of suitable controls include:</p> <ul style="list-style-type: none"> Assigning responsibility for management and creation of privileged accounts. Defining the objectives and responsibilities of system administrators. Review of privileged user's access rights currently in place. Formal delegation of privileged account access rights. 	Mostly implemented.	We found that the intent of this recommendation has been mostly implemented. We also identified, however, a related finding. IS Administrators (the ultimate privileged users) only use single accounts for all of their activities including day to day and privileged activities. This finding is addressed in Recommendation 2.3.
<p>5. The current setup of password syntax is reviewed and strengthened. A policy for the setup and use of passwords is developed specifying minimum password syntax rules and requirements for the use of passwords by system users.</p>	Implemented	Better practice is being followed in relation to password management, complexity and recycling and reuse.
<p>6. New users are not linked to existing user access right templates that are in the name of staff members. Rather, templates for access rights are set up in the name of position titles or other meaningful grouping, and all users are linked to their appropriate template.</p>	Implemented	The online form currently being used for provisioning/de-provisioning and access amendment is equivalent to an Access Right Template.

Liability limited by a scheme approved under Professional Standards Legislation

Appendix 2: Documents reviewed and interviews conducted

The list below identifies key documentation reviewed as a part of this internal audit:

- CWT Information Services Risk Summary (December 2017)
- CWT Administration Policy: Information Technology and Its Use (November 2016)
- CWT Mobile Device Policy (November 2016)
- CWT Remote Access and Network Security Administration Policy (November 2016)
- CWT Council Policy: Elected Members' Electronic Communication Facilities (November 2012)
- SME Security Services – Vulnerability Assessment for City of West Torrens (July 2016)
- Service Level Agreement for Rack Space Hire and Optic Fibre Connectivity Agreement between the City of West Torrens and the Corporation of the City of Adelaide (May 2015)
- CWT Logical Security Technology One Financials and BIS Internal Audit Report (July 2013)
- The Australian Government Information Security Manual 2017
- The Australian Government Information Security Manual Controls 2017
- Information Security Management Framework, Government of South Australia (September 2017)

As a part of this engagement, the following staff were interviewed:

- Manager Information Services: Chris James
- Network Administrator : Jason Bury
- IT Customer Support Officer: Gary Dodd
- Senior Network Administrator: Jesse Iannone
- Senior Information Management Officer: Andrea Ristevski
- Information Management Officer: Kerstin Hedstrom

Liability limited by a scheme approved under Professional Standards Legislation

9.3.2 Procurement Roadmap Continuous Internal Audit Report - Stages 2 and 3

Brief

This report presents the results of Stages 2 and 3 of the Procurement Roadmap Continuous Internal Audit.

RECOMMENDATION

The Committee recommends to Council that this report be received.

Introduction

In accordance with the approved *Internal Audit Program 2015-2018*, the *Continuous Audit - Procurement Roadmap* (Audit) was approved and commenced in January 2015 to report on:

- the adequacy of documents, templates, policies etc. in providing legal protection and probity of process;
- assurance at key milestones that procurement activity complies with procurement and contractor management policies;
- the adequacy of internal controls to address the risk associated with procurement activity;
- opportunities for the introduction of better practices and process improvement throughout the life of the City of West Torrens Procurement Roadmap Program (the Program); and
- the management and resolution of the PMMS findings that form the basis of the Program.

This continuous/rolling audit was planned to be undertaken at each of the four key stages of the Program to add value to each of its upcoming stages. The first of these audits was completed during the first half of 2015 while this report presents the report from stages 2 and 3 of the Audit.

Discussion

As there was a delay in progressing the Procurement Roadmap (Roadmap), there was a delay in the completion of stage 2. However, now that the Roadmap is underway again, there was value in merging both stages 2 & 3 to confirm that the:

- Recommendations from stage 1 of the Audit were being implemented;
- Procurement had a strong intranet presence leading to an ease of obtaining relevant procurement information;
- Document management is effective and compliant;
- Contractors are well managed in accordance with policy; and
- Stakeholders understood their procurement responsibilities through clearly defined procurement roles.

The Audit was undertaken during December 2017 and January 2018 by Council's contract internal auditor (Auditor).

Following completion of the Audit, a draft internal audit report (Report) was issued to the Senior Strategic Procurement Officer and Manager Strategy and Business Services for comment and individual risk assessment with a closing meeting held to provide an opportunity to clarify audit findings with the Auditor. The final report was provided to the Executive in February 2018 (**Attachment 1**).

Stage 4, the final stage of this continuous audit, is expected to commence in August 2018.

Internal Audit Findings

The auditor found that the organisation is making strong progress towards implementing the Roadmap, in particular through the development of a rigorous procurement framework that meets stakeholder needs and also conforms to ICAC (*Independent Commissioner Against Corruption Act 2012*) principles. While several opportunities for improvement were identified, all of which are low or moderate risk, the Audit emphasises the strength of the overall procurement framework and Roadmap.

Six (6) internal audit findings were identified with all findings attracting a moderate level of risk.

While the organisation tolerates moderate and low risk, the proposed recommendations add value to the Program. Consequently, all recommendations will be actioned. However, given the level of residual risk is within risk tolerance levels and the recommendations are of a minor nature, they are not subject to priority actioning at this point but those that already form part of the Roadmap will be actioned over the next six to twelve months.

Conclusion

Stages 2 and 3 of the *Continuous Audit - Procurement Roadmap Program* has been undertaken by Council's contract internal auditor. The Audit found that the organisation has made good progress towards implementing its Procurement Roadmap regardless of the unexpected delays. In particular, it found that the procurement framework meets stakeholder needs, ICAC principles and is likely to be robust enough to withstand an ICAC investigation.

As the findings are within risk tolerance levels and the recommendations are minor in nature, progress updates will not be reported to each meeting of the Audit and Risk Committee.

Attachments

1. Continuous Audit - Procurement Roadmap Program Report - Stages 2 and 3



City of West Torrens

Continuous Internal Audit

Procurement Roadmap - Stages 2 and 3

January 2018

Prepared by: Galpins Accountants Auditors and Business Consultants

Liability limited by a scheme approved under Professional Standards Legislation



City of West Torrens

Table of Contents

1. Executive Summary.....	3
2. Findings	6
2.1. Implementation of Stage 1 Audit Recommendations	6
2.2. Intranet / Information Availability	8
2.3. Roles and Responsibilities.....	9
2.4. Document Management.....	10
2.5. Progress in implementing Procurement Roadmap Recommendations	14
3. Added Value: Additional Insights.....	16
3.1. Risk to implementation of the Procurement Roadmap.....	16
Appendix 1: Documentation Reviewed / Interviews Conducted.....	17
Appendix 2: Implementation of Stage 1 Audit Recommendations	18



1. Executive Summary

1.1 Background

The City of West Torrens (CWT) is currently implementing a Procurement Roadmap Program, aimed at improving the Council's procurement framework and rigour. Initially sponsored by the Local Government Association (LGA), the Roadmap Program aims to help councils identify opportunities to save money and to also improve procurement efficiency. CWT has a list of actions to implement as part of its roadmap.

In 2016-17, Council spent over \$46 million on procurement activities. This represents a significant proportion of Council's income. Spend occurred across all areas of the business and with over 1100 different vendors. The Procurement Officer plays an important role in ensuring a consistent approach to procurement across Council, in helping to work across departments to obtain buying power / discounts for bulk purchases, ensuring probity by helping staff to follow appropriate processes, and ensuring that appropriate contracts are used.

1.2 Audit Objectives

This continuous audit is being conducted in four stages to evaluate and report on:

- the adequacy of documents, templates, policies etc. in providing legal protection and probity of process
- assurance at key milestones that procurement activity undertaken complies with procurement and contractor management policies
- the adequacy of internal controls to address the risks associated with procurement activity
- opportunities for the introduction of better practices and process improvement throughout the life of the Program, and
- management and resolution of the findings of the PMMS¹ Procurement Roadmap Program.

1.3 Audit Approach

The audit is being undertaken at four key stages of the Program. The scope of the audit is to review each stage of the Program as it is completed, and this report is for Stages 2 and 3 of the continuous audit. Stage 1 of the audit was finalised in April 2015, and due to a lack of resources in the Procurement Team, there has subsequently been a three year gap. Therefore, the first step of this audit was to re-familiarise with the CWT procurement environment.

Stage 2 then involved assessment of:

- the implementation of Stage 1 recommendations

¹ PMMS is a private consulting organisation with a procurement specialisation.



- intranet / information availability, including:
 - the level of consultation
 - the ease of obtaining procurement / contract management information
 - sufficiency of evidence of probity of process (documentation and reporting)
 - availability of templates including contracts and other documents
- roles and responsibilities, including:
 - whether roles and responsibilities for procurement are documented clearly, available and understood
 - sufficiency of training available and provided to staff to undertake procurement activity in accordance with internal expectations (policy, processes etc).

Stage 3 involved assessment of:

- document management, including:
 - use and understanding of ECM naming conventions
 - the ease of obtaining relevant procurement / contractor management information
 - evidence of probity of process (documentation)
 - if contract documents are readily available and appropriately authorised within delegated financial limits
 - the compliance with contractor induction and monitoring
 - the effectiveness of ECM/Pathway/Procurement Register to facilitate reminders for contract and performance monitoring activities.

A new step in the scope, assessment of progress against the original Procurement Roadmap recommendations, was included in this review. It replaces a review of contractor management elements. Contractor management was removed from the scope of this audit as it is being addressed in a separate 2018 review.

A summary of documentation reviewed and interviews conducted is at Appendix 1.



1.4 Summary of Results

Stage 1 of this audit identified that the CWT initially made strong progress in implementing the procurement roadmap. Subsequently, due to staffing and responsibility changes, action to strengthen the organisation's procurement processes stalled.

The engagement of a new Senior Strategic Procurement Officer in 2017 has meant that work is now underway to ensure the CWT obtains value for money and efficiency in the procurement space. Audit's review found that this officer has built on previous work and made significant progress in implementing the Procurement Roadmap. In particular, improvement has occurred in relation to:

- proactively using spend data to target those CWT staff that require procurement training
- working through a bulk of raw data to meaningfully understand procurement trends across the CWT and to identify areas where savings and efficiencies can be made
- updating the 'Compass' procurement intranet site to make it more user friendly, and
- promoting awareness of record keeping requirements on the Objective system.

Audit considers that a **key risk** to progress in implementing the Procurement Roadmap is that the Procurement Officer's role could be diverted/broadened to include other responsibilities. When this previously happened, implementation of the Procurement Roadmap stalled.

A summary of the audit findings is below.

Audit scope element	Audit's assessment
Implementation of Stage 1 audit recommendations	● 5 of 7 audit recommendations have been implemented.
Intranet / Information Availability	● The Compass intranet site is easy to use and includes templates/ guidance.
Roles and Responsibilities	● Roles and responsibilities are defined in policy. A procurement training program is being progressively delivered.
Document Management	● Document management practices have improved. There is a need for a reminder system for contract management.
Progress against the original Procurement Roadmap actions	● Most elements of 'Phase 1' of the roadmap have been implemented. Work is underway to implement 'Phase 2' actions, for example preparing a priority contract establishment program and developing annual procurement plans with departments.

KEY: ● Strong progress ● Progress underway, opportunities for improvement exist
 ● Significant work required



2. Findings

2.1. Implementation of Stage 1 Audit Recommendations

This section summarises the results of testing whether the recommendations from Stage 1 of this continuous audit have been completed. Overall, 5 of 7 recommendations have either been completed or partially completed. Full details are included in *Appendix 2* of this report.

Stage 1 Recommendation	Response and due date	Completed?
1. Consider including a requirement in the draft procurement policy for acquisition plans to be developed prior to conducting a procurement exercise, for example for high risk and/or high value procurement. This may assist in ensuring that procurement is transparent, rigorously planned, scoped and approved prior to market approach. Inclusion of this requirement must be balanced against efficiency considerations and CWT's other existing methods for approving procurement.	Agree with the recommendation. February 2016	Not yet completed. There is not yet a policy requirement for pre-approval of a strategy to approach market (ie for Council to approve the overall way that the procurement is planned / why procurement is necessary).
2. Clarify or strengthen requirements in the draft procurement policy around documentation and approval requirements when exemptions from the policy are required in approaching the market. <further detail in Appendix 2>	Agree with the recommendation. September 2015	Completed.
3. To strengthen the CWT's draft procurement policy, consider: <ul style="list-style-type: none"> including guidance on contract variations, and including guidance on use of contingency funding. 	... Agree with including guidance on variations/contingencies in policy. 'As a low risk, this will be considered within the next 12 months.' (from April 2015)	Not yet completed.
4. Develop procedural guidelines for staff on how to conduct the tendering process. This will ensure strong probity in tendering activities and help to avoid a situation where the organisation is unable to support a tender decision.	Agree with the recommendation.	Completed.

Stage 1 Recommendation	Response and due date	Completed?
5. To ensure the ongoing engagement of stakeholders with the Procurement Roadmap, provide regular (for example, bi-monthly or quarterly) updates to Steering Group and Reference Group members about progress towards achieving the roadmap.	To ensure efficient allocation of staff resources across the organisation, meetings are held as required when there are issues to discuss.	Ongoing. Audit notes that only two steering committees were held between 2015 and the audit commencement – one in June 2017 and one in Sept 2017.
6. Publish the CWT's terms and conditions for low value purchases on an internet site. Include a link to this site on all Purchase Orders. Remind staff of the importance of providing suppliers with a complete listing of terms and conditions.	Agree with the recommendation... March 2016	Completed. <i>Further detail in Appendix 2.</i>
7. Consider revising the current draft Purchasing, Tendering and the Sale and Disposal of Assets ... If a new policy is created to cover the sale and disposal of assets, this should cover key elements/principles in line with the LGA Guide Policy for Disposal of Land and Assets.	Agree with the recommendation to remove the sale and disposal and create a separate policy. October 2015.	Completed

The table above shows that only two recommendations have not been implemented to date. Audit consider that there is still potential benefit in implementing these recommendations.

Recommendation 1	Review the outstanding recommendations from the Stage 1 Procurement Roadmap continuous audit, and work to implement these.				
Rating (Auditor)	Moderate	Likelihood	Moderate	Consequence/Descriptor	Moderate Reputation/Financial
Rating (CWT)		Likelihood		Consequence/Descriptor	
Response					
Target Date					



2.2. Intranet / Information Availability

The audit scope called for a review of the adequacy of procurement information available on the intranet.

- ✓ Overall, a review of the *Compass* intranet site found that procurement information is available and easy to locate. The website steps users through steps of the procurement process and includes clear links to guidance and templates.
- ✓ 2 of 3 stakeholders consulted as a part of the audit also commented that the intranet site is user friendly. The third commented that she preferred to approach the Procurement Officer directly, and did not try to use the website.

Audit tested a sample of contracts to understand whether appropriate documentation/templates were used. This helped to demonstrate whether the procurement information on the intranet is sufficient. Testing results are discussed in Section 2.4 – *Document Management*.

There are no recommendations for this section.



2.3. Roles and Responsibilities

The audit scope called for an assessment of whether the roles and responsibilities in relation to procurement are readily available **and** understood across the:

- Centre-led Procurement Team
- Procurers
- Council representatives (contract managers).

This was to include an assessment of the sufficiency of training provided to staff in relation to procurement.

Findings

Results of testing the clarity of roles and responsibilities are summarised in the table below.

Area for testing roles and responsibilities	Result
Are procurement roles and responsibilities defined?	✓ Roles and responsibilities are clearly defined. For example, they are clearly set out in the Procurement Policy and the Procurement Administration Policy.
Is a sufficient training program in place in relation to procurement?	✓ The new Procurement Officer has developed a training strategy, and has also used internal spend data to identify which CWT staff require this training. This is a proactive way to target training where it is needed most. <ul style="list-style-type: none"> ○ Audit viewed evidence that the training program has begun. ○ There was no procurement training between 2015 and late 2017, however it is positive that the new Procurement Officer is now actively working to address this need.
Does audit testing support whether roles and responsibilities are clearly understood?	✓ Audit tested a range of procurement activities to assess compliance with responsibilities – for example whether the appropriate approach to market was used, appropriate evaluations occurred, procurement recommendations were in place. Further detail is included in Section 2.4 over page. We found that, overall, there has been an improvement in the awareness of roles and responsibilities between 2016/17 and 2018. We found it difficult to obtain complete information when testing procurement from 2016/17, and found it easier to obtain information from more recent procurement activities.

There are no recommendations for this section.



2.4. Document Management

The audit scope called for a review of the adequacy of document management, including the use of file naming conventions, the ease of obtaining procurement information and evidence of probity of process. It also asked for a review of the effectiveness of the Objective system in facilitating reminders for contract and performance monitoring activities.

Findings

Audit conducted testing on a sample of 31 procurement activities from 2016/17, and a further seven (7) procurement activities from the Contracts Register from late 2017. The sample choice from 2016-17 was chosen randomly, based on spend information from the CWT's financial system. The difficulty in this method was that contracts/procurement may have occurred long before the 2016/17 spend. As the Contracts Register for that time period had very little detail, this was our only way of trying to identify and test 2016/17 procurement.

The sample choice from late 2017 was chosen more deliberately, from contracts identified in the Contracts Register. Results are summarised below.

	2016/17 Procurement testing results	Late 2017 Procurement testing results
Objective file naming conventions and file paths used	Difficult to track. Intermittent use of conventions.	Improved file naming. A staff member is also allocated to ensuring filing of documentation.
Ease of obtaining relevant procurement information	Difficult. Contracts / relevant documentation obtained in 5 (of 31) instances from Objective system.	Easier to obtain information. Contracts / key information obtained for 7 of 7 sample items from Objective system.
Evidence of probity of process (documentation) available	Needed to approach staff directly for information.	Mixed results. Further detail in the following table. For example, require improvements in relation to risk assessment and maintaining documentation on file.

The table over page includes further detail of testing procurement from late 2017. The details of the procurement testing from 2016/17 are not included as this procurement happened prior to the new Procurement Officer beginning work with the CWT.



Key documentation tested for (on Objective)	Result
Risk assessment on file?	7 of 7 – no
Appropriate approach to market as per estimated value?	7 of 7 – yes
RFQ form on file?	5 of 7 – yes 2 of 7 – no
Evaluation / assessment (record of) on file?	4 of 7 – yes 3 of 7 – no
Responses kept on file?	5 of 7 – yes 2 of 7 – no
Contract on file?	3 of 5 relevant – yes 2 of 5 relevant – no

The table above indicates that recordkeeping in Objective is not complete. For example, although risk assessment is a mandatory step in the procurement process, this step is routinely not undertaken for procurement.

We note that our testing was of procurement activities that have been declared and formally entered into Objective, and that other procurement may have occurred with documentation kept wholly outside of the system. This presents a risk of Council not being able to demonstrate probity and appropriate processes in procurement activities.

It is also important to note that the Objective system has been set up to make record keeping as easy as possible. The procurement support officer creates four e-folders in Objective when a contract number is requested, and it is clear what documentation is required. In addition, this officer follows up with officers to request that they put all documentation on the system. Deficiencies in record keeping, therefore, are not system related.

There is opportunity, as a part of the ongoing training program, to educate CWT staff about what procurement documentation is required to be used and stored in the Objective system.

Recommendation 2	Continue providing regular training and reminders to CWT staff about the importance of filing all key procurement documentation in the Objective system. This will facilitate Council's ability to demonstrate probity and appropriate process in procurement activities.				
Rating (Auditor)	Moderate	Likelihood	Moderate	Consequence/Descriptor	Moderate Reputation
Rating (CWT)		Likelihood		Consequence/Descriptor	
Response					
Target Date					

Recommendation 3	Educate CWT staff responsible for procuring goods and services about the mandatory risk assessment process required to be undertaken before conducting procurement exercises. This education could be included as a part of the formal procurement training program, and as part other ongoing one on one interactions with staff.				
Rating (Auditor)	Moderate	Likelihood	Moderate	Consequence/Descriptor	Moderate Reputation
Rating (CWT)		Likelihood		Consequence/Descriptor	
Response					
Target Date					

Recommendation 4	Implement a process to check the adequacy of record keeping for a sample of procurement activities each quarter. Report on results to the Executive team. This process is aimed to help promote a 'tone from the top' that encourages organisation-wide compliance.				
Rating (Auditor)	Moderate	Likelihood	Moderate	Consequence/Descriptor	Moderate Reputation
Rating (CWT)		Likelihood		Consequence/Descriptor	
Response					
Target Date					

Using the Objective System for Contract Monitoring

The audit also assessed whether the Objective system facilitates reminders for contract and performance monitoring activities. This functionality can be very important in helping internal staff to drive value from contracts, for example in regularly checking that deliverables are obtained and milestones achieved.

The Objective system does not currently facilitate reminders for contracts and performance monitoring activities. The Procurement Officer explained that there may be other internally owned software capable of this functionality. There is opportunity for the Procurement Officer to further explore how reminders can be set up to assist in contract management.



City of West Torrens

Recommendation 5	Research and implement a process that regularly reminds contract managers of deliverables / key monitoring actions as a part of managing their contracts.				
Rating (Auditor)	Moderate	Likelihood	Moderate	Consequence/ Descriptor	Moderate Financial
Rating (CWT)		Likelihood		Consequence/ Descriptor	
Response					
Target Date					



City of West Torrens

2.5. Progress in implementing Procurement Roadmap Recommendations

This section includes a summary of progress in implementing phases of the Procurement Roadmap.

Phase 1 0-6 months Structure, Team Establishment, Documentation and Training	Assessment of progress	Phase 2 6-12 months Contract Establishment, Planning & Processes	Assessment of progress	Phase 3 12-24 months Supplier Engagement, Strategic and Contract Management	Assessment of progress
Build Procurement Roadmap into Council Strategy	Procurement is mentioned at a high level in the Strategy	Prepare new priority contract establishment program	Discussing this and working towards this	Explore opportunities for multi-year budgeted contracts	Underway. Have developed approximately 10 multi-year projects as need arises.
Confirm Centre-led procurement model and new roles and responsibilities	✓	Undertake review of procurement planning processes	Planned meeting with all departments on 23 March to develop plans	Develop corporate procurement KPIs and targets	Developed and to be presented at Steering Group 6.2.18.
Develop business case for Procurement Resources	✓ procurement officer in place	Develop annual procurement plan	Underway	Develop a compliance and audit plan	Not yet occurred
Establish Procurement Steering Group	✓	Implement targeted program to reduce invoice numbers and transaction costs	Not yet occurred	Develop and implement standard contract management processes	Underway
Introduce standard documentation / templates	✓	Develop and implement standard project procurement plans	Have trialled this with two internal stakeholders. Underway.	Develop supplier education program to assist local businesses	Not yet occurred

Procurement Roadmap - Stages 2 and 3
Internal Audit – January 2018

Page 14



City of West Torrens

Phase 1 0-6 months Structure, Team Establishment, Documentation and Training	Assessment of progress	Phase 2 6-12 months Contract Establishment, Planning & Processes	Assessment of progress	Phase 3 12-24 months Supplier Engagement, Strategic and Contract Management	Assessment of progress
Develop central document management responsibilities and intranet procurement portal	✓			Develop on-going procurement training program	✓ in progress
Develop and hold awareness training	Underway			Develop and implement cost savings tracking register	✓ in progress
Prepare detailed spend data report	✓ manually intensive process				

The Procurement Officer showed clear focus on implementing actions from the Procurement Roadmap. She has an action plan in place, and her record of achievements show progress. Audit consider it unnecessary to make any further recommendations in this area.



3. Added Value: Additional Insights

This section includes discussion of items noted for improvement during this audit. These findings were outside of the direct scope of the audit, and therefore are included separately in this section. In accordance with Internal Audit standards, we are obliged to report items that we consider may potentially impact on the achievement of the organisation's objectives.

3.1. Risk to implementation of the Procurement Roadmap

Audit considers that a key risk to progress in implementing the Procurement Roadmap is that the Procurement Officer's role could be diverted/broadened to include other responsibilities. When this happened to the previous procurement officers, implementation of the Procurement Roadmap stalled. For example, further work in developing procurement panels, delivering procurement training and achieving procurement targets did not occur.

To help the CWT achieve savings and efficiency benefits from the Procurement Roadmap and from a strong procurement function, it may be useful to confirm a commitment to ensuring that there is a resource allocated to this role, and that the role is not diluted with other responsibilities.

It is noteworthy that, during audit fieldwork, we received positive feedback from staff about the Procurement Officer, including the benefit of having someone to approach with procurement queries. They felt it was helpful to be able to ask questions about a range of things, including process, risk, request specifications.

One way of ensuring that management is aware of the value of the Senior Strategic Procurement Officer's work is to ensure that the Procurement Savings and Benefits Register is regularly updated. This register does not only need to include examples of tangible savings, but can include examples of successes in ensuring appropriate procurement across the CWT. For example, include:

- instances (anonymous if required) where officers have approached the Procurement Officer to request a contract be put in place for activities that were previously informal, and
- examples of departments / officers that approached for help in relation to areas of risk.

Recommendation 6	Ensure that the role of the Senior Strategic Procurement Officer remains dedicated to strengthening the procurement function across CWT.				
Rating (Auditor)	Moderate	Likelihood	Moderate	Consequence/ Descriptor	Moderate Reputation
Rating (CWT)		Likelihood		Consequence/ Descriptor	
Response					
Target Date					



Appendix 1: Documentation Reviewed / Interviews Conducted

Key documentation reviewed as a part of this engagement is listed below. Further documentation was also reviewed, this list is high-level for ease of reading and understanding the scope of assessment conducted:

- The Procurement Roadmap
- Procurement Policy
- Procurement Roadmap Action Plan 2017
- Spend information / reports, for example:
 - Spend category matrix
 - CWT savings and benefits register
 - 2016-17 CWT Panel Contract Spend
 - Data of full 2016-17
- Contract information relating to the audit sample (as available, including requests for quotation/tender, purchase recommendations, contracts, quotations etc).
- Training Strategy 2018
- Procurement Steering Committee documentation
- Procurement templates.

In addition, interviews were held with:

- Robyn Cusick, Senior Strategic Procurement Officer

Further interviews were held with staff involved in procurement activities identified through random sampling:

- Margaret Steuart
- Baskar Kanappan
- Celine Luya.



Appendix 2: Implementation of Stage 1 Audit Recommendations

Detail of implementation of audit recommendations.

Stage 1 Recommendation	Response and due date	Implemented?
1. Consider including a requirement in the draft procurement policy for acquisition plans to be developed prior to conducting a procurement exercise, for example for high risk and/or high value procurement. This may assist in ensuring that procurement is transparent, rigorously planned, scoped and approved prior to market approach. Inclusion of this requirement must be balanced against efficiency considerations and CWT's other existing methods for approving procurement	Agree with the recommendation, Acquisition strategies to be developed for high value procurements. It is anticipated a position will be implemented within 12 months February 2016	Not implemented. There is not yet a policy requirement for pre-approval of a strategy to approach market (ie for Council to approve the overall way that the procurement is planned / why procurement is necessary).
2. Clarify or strengthen requirements in the draft procurement policy around documentation and approval requirements when exemptions from the policy are required in approaching the market. For example, what approval (if any) is required when officers wish to: <ul style="list-style-type: none"> enter into direct negotiation with a supplier instead of releasing a Request for Tender obtain a reduced number of quotes than the standard use an alternative procurement method than that identified in the policy. This will assist in demonstrating probity in line with ICAC requirements.	Agree with the recommendation. Need to determine appropriate mechanism for implementing so as to minimise the administrative effort. September 2015	Complete.

Stage 1 Recommendation	Response and due date	Implemented?
3. To strengthen the CWT's draft procurement policy, consider: <ul style="list-style-type: none"> including guidance on contract variations, and including guidance on use of contingency funding. 	<p>Risk ratings do not determine the procurement method to be used. They inform the document type ie. conditions of contract. Agree with including guidance on variations/contingencies in policy. Not inclined to include a requirement for lessons learned in a policy document but may include on the intranet as a good practice guideline.</p> <p>'As a low risk, this will be considered within the next 12 months.' (from April 2015)</p>	Not yet complete.
4. Develop procedural guidelines for staff on how to conduct the tendering process. This will ensure strong probity in tendering activities and help to avoid a situation where the organisation is unable to support a tender decision.	<p>Agree with the recommendation. Process is the subject of a continuous improvement project including electronic tendering options.</p> <p>30 September 2015 to determine desired solution</p>	Complete. Procedural guidance on the Compass procurement website.
5. To ensure the ongoing engagement of stakeholders with the Procurement Roadmap, provide regular (for example, bi-monthly or quarterly) updates to Steering Group and Reference Group members about progress towards achieving the roadmap.	To ensure efficient allocation of staff resources across the organisation, meetings are held as required when there are issues to discuss.	Partially complete. Audit notes that only two steering committees were held between 2015 and the audit commencement – one in June 2017 and one in Sept 2017.

Stage 1 Recommendation	Response and due date	Implemented?
<p>6. Publish the CWT's terms and conditions for low value purchases on an internet site. Include a link to this site on all Purchase Orders. Remind staff of the importance of providing suppliers with a complete listing of terms and conditions.</p>	<p>Agree with the recommendation, this is low risk when assessed against the CWT Risk Matrix (likelihood & consequence) and will be actioned within twelve months.</p> <p>March 2016</p>	<p>Complete. This step was achieved, but Audit found that the link on the web site has been removed.</p> <p>We note that our current testing identified that terms and conditions are automatically attached to Purchase Orders. Therefore, the intent of this recommendation has been achieved.</p>
<p>7. Consider revising the current draft Purchasing, Tendering and the Sale and Disposal of Assets policy to either:</p> <ul style="list-style-type: none"> include more detailed guidelines sale or disposal of assets, in line with the LGA Guide Policy for Disposal of Land and Assets, or remove the section on the sale or disposal to a separate new policy. <p>If a new policy is created to cover the sale and disposal of assets, this should cover key elements/principles in line with the LGA Guide Policy for Disposal of Land and Assets.</p>	<p>Agree with the recommendation to remove the sale and disposal and create a separate policy.</p> <p>October 2015.</p>	<p>Complete</p>

9.3.3 2017-2018 Internal Audit Program Update

Brief

This report presents the 2017-2018 Internal Audit Program Update.

RECOMMENDATION

It is recommended to the Audit and Risk Committee that the 2017-2018 Internal Audit Program update report be received.

Introduction

An update report is provided to each ordinary meeting of the Audit and Risk Prescribed General Committee (Committee) on the status of current and, if appropriate, the previous Internal Audit Program.

Discussion

This report summarises the status of all planned audits contained in the 2017-18 *Internal Audit Program* (Program) as at 31 March 2018. The full internal audit program update is attached (**Attachment 1**).

Summary

Audit Status	Number
Audits Not Started	3
Complete	7
In Progress	4
Total Audits Programmed (excluding staged audits)	14
Audit Status (Staged Audits)	Number
Staged Audits Not Started	2
Staged Audits Complete	1
Staged Audits in Progress	0
Total Staged Audits	3
Cancelled/Deferred	1
Total Audits	18

Audits Completed

Two (2) of the programmed audits have been completed since 13 February 2018 bringing the total to eight (8) for the year:

No.	Audit Description	Meeting Presented
1.	Information Fraud	April 2018
2.	Continuous Audit Procurement Roadmap Stages 2 & 3	April 2018

Compliance Audits in Progress

The following audits are in progress as at 31 March 2018:

1. The *Community Consultation* audit is currently underway, an opening meeting occurred during March 2018. The scope for this audit is attached (**Attachment 2**).
2. The *Governance Framework* audit is currently underway, with an opening meeting scheduled for April 2018. The scope for this audit is attached (**Attachment 3**).

Audits Cancelled

The following audit has been cancelled:

1. Cash Handling Spot Audit was cancelled at the suggestion of the Audit Committee.

Facilitative/Staged Audits Underway

The following three (3) facilitative and staged audits will continue to be progressed with activity spanning over multiple internal audit programs:

1. *Debtor Management* - currently underway.
2. *Maintenance of Plant and Equipment*.
3. *Continuous Audit - Procurement Roadmap (CAPR)* - Currently underway. Stages 2 and 3 completed at 31 March 2018 - Stage 4 to be progressed.

Conclusion

Following the deletion of the Cash Handling Spot Audit from the 2017-18 Internal Audit Program, eight (8) of the remaining planned seventeen (17) audits (approx. 50%) are complete as at the end of the third quarter. Of the remaining nine (9) audits, four (4) are in progress and five (5) have not started. Overall twelve (12) of the planned seventeen (17) audits (70%) are either complete or in progress. As such, the completion of the 2017-18 Internal Audit Program is essentially on track.

Attachments

1. **2017-2018 Internal Audit Program Update**
2. **Community Consultation Internal Audit Scope**
3. **Governance Framework Internal Audit Scope**

Report as at 31 March 2018

2017/18 Internal Audit Program

Audit No.	Internal Audit	Audit Objectives	Quarter	Status	Comments
Status of 2016/17 Internal Audits Carried Forward					
1	Accounts Payable	<ul style="list-style-type: none"> An appropriate approval process is in place and in line with the CEO sub-delegations and Administration Policy: Financial Authorities Internal controls are assessed and operating effectively, including separation of duties Expenditure registers are maintained where applicable, including the Local Government Act 1999 (s79 Register of allowances and benefits and s105 Register of remuneration, salaries and benefits) Alignment with the Enterprise Risk Management Framework/operational risk register <p>Audit will also undertake data analysis of accounts payable data using data analytics software in order to analyse accounts payable data over an extended period.</p>	1	Complete	Final report is presented to the 10 October 2017 meeting of the Committee.
2	Hazard Register - Controls	<p>The objectives of this audit are to evaluate and report on:</p> <ul style="list-style-type: none"> Audit will sample departmental hazards from the each departments hazard register and review the: <ul style="list-style-type: none"> completeness and existence of hazard registers and associated risk assessments processes and controls in place to ensure legitimacy linkage with the Enterprise Risk Management Framework through the use of the risk matrix 	1	Complete	Final report is presented to the 10 October 2017 meeting of the Committee

	Not Started	In Progress	Complete	Deferred	Cancelled
Not Started					

2017/18 Internal Audit Program

Report as at 31 March 2018

Audit No.	Internal Audit	Audit Objectives	Quarter	Status	Comments
3	Land and Building (Sale and Conveyancing) Act 2010 Section 12 Statements	The objectives of the review are to evaluate and report on the level of compliance with the: <ul style="list-style-type: none"> • <i>Land and Building (Sale and Conveyancing) Act 1994</i> • <i>(Sale and Conveyancing) Regulations 2010</i> (the Regulations) • Opportunities for the introduction of better practices and process improvement 	1	Complete	Final report is presented to the 10 October 2017 meeting of the Committee
4	Food Act 2001.	The objectives of the review are to evaluate and report on the level of compliance with the: <ul style="list-style-type: none"> • <i>South Australian Food Act 2001</i> • <i>South Australian Food Regulations 2002</i> • Australian Food Safety Standards • Opportunities for the introduction of better practices and process improvement 	1	Complete	Final report is presented to the 10 October 2017 meeting of the Committee
Status of 2017/18 Internal Audits					
Assurance Audits					
5	Business Continuity and Emergency Management Plan - Review and Exercise Event.	A surprise mock event or scenario designed to test the effectiveness and/or raise awareness of the Business Continuity Emergency Management Plan (BCP).	4	Not Started	
6	Budget Planning and Strategic Planning Alignment	An audit to provide assurance whether the budgeting process is aligned with the organisations strategic objectives (Community Plan) and obligations under the Local Government Act, 1999 & CWT Policies.	3	Not Started	
7	Community Consultation	An audit designed to determine the effectiveness of community consultation when aligning and forming key business strategies such as the Community Plan and associated corporate and departmental service plans.	2	In progress	The audit, undertaken by the Contract Internal Auditor, commenced in March 2018. The approved audit scope is attached (Attachment 2).

	Not Started	In Progress	Complete	Deferred	Cancelled
--	-------------	-------------	----------	----------	-----------

Page 2 of 7

2017/18 Internal Audit Program

Report as at 31 March 2018

Audit No.	Internal Audit	Audit Objectives	Quarter	Status	Comments
8	Information Fraud	This organisation manages information of a confidential and commercially sensitive nature. This audit will test the robustness of the process of allocating and revoking information privileges.	2	Completed	
Legislative Audits					
9	Governance Framework - Compliance with the Local Government Act.	An audit to determine whether the organisation is meeting its governance obligations under the Local Government Act, 1999.	4	In progress	This audit will be undertaken by Norman Waterhouse with an opening meeting scheduled for April 2018. The approved audit scope is attached (Attachment 3).
Third Party Audits					
10	Vic Roads Annual Audit	Self-assessment mandated as part of the agreement with Vic Roads	1	Complete	The Enterprise Risk Officer completed this audit during July 2017.
Spot Audits					
11	Service Centre Procedures and Systems	This audit will test the provision of information from the Contact Centre aligns with the CWT telephone protocols, scripting, team agreements and stakeholder expectations.	3	Not Started	A scope has been drafted.
12	Internal Audit Recommendations	An annual audit designed to provide assurance that the agreed audit findings actions are being completed consistent with the original action.	3	Completed	<p>The purpose of this audit is to verify that internal audit recommendations which are agreed for actioning (agreed actions) are completed in line with the auditor's recommendation.</p> <p>Rather than undertake a specific audit, the internal auditor will align a verification process against the existing six-monthly agreed action report.</p> <p>At the time of the report, each completed agreed action will be verified against the intent of the original audit recommendation and/or against</p>

	Not Started	In Progress	Complete	Deferred	Cancelled
--	-------------	-------------	----------	----------	-----------

Page 3 of 7

2017/18 Internal Audit Program

Report as at 31 March 2018

Audit No.	Internal Audit	Audit Objectives	Quarter	Status	Comments
WHS Audits					
13	Traffic Management	A WHS/Legislative Compliance audit to determine whether CWT (or contractor) traffic management activities occur in line with legislation to ensure the safe movement of people throughout the city.	2		alternative measures which appropriately mitigate risk. An internal auditors statement of verification will be included as part of the Agreed Action Report.
14	Contractor Management Audit	The purpose of this audit is to: 1. document progress against the 2012 audit findings and re-evaluate the overall compliance rating 2. establish policy compliance against the WHS Act and Regulations 3. report on departmental compliance against the current version of CWT Contractor Management Policy with emphasis on contractor induction, monitoring and evaluation. 4. report on compliance with the WHS aspects of contractor engagement as part of the procurement process, specifically the WHS information being provided and evaluated as part of the tender/quotation.	2	In Progress	The audit, undertaken by the Contract Internal Auditor is in progress. An opening meeting was held during January 2018, data collection and interviews are underway. The audit, undertaken by the Contract Internal Auditor is in progress. An opening meeting was held during January 2018, data collection and interviews are underway.

	Not Started	In Progress	Complete	Deferred	Cancelled
--	-------------	-------------	----------	----------	-----------

Page 4 of 7

2017/18 Internal Audit Program

Report as at 31 March 2018

Audit No.	Internal Audit	Audit Objectives	Quarter	Status	Comments
Facilitative Audits (Long term duration).					
15	Maintenance Plant and Equipment - Operational Sites	<p>Stage 1 - Develop Solution Action Plan An objectives and agreed outcomes report will replace the traditional audit findings report. This report will use internal resources to investigate those gaps previously identified and use a 'cause and effect' approach to identify and document:</p> <p>Gap Analysis (Internal Work Group)</p> <ul style="list-style-type: none"> • What should be done; • What is currently being done; • Significant differences between 'what should' and 'what is' being done; • Assess the current residual risk in respect of continuing to operate in the current state. <p>Outcomes (Internal Work Group) The Audit objectives will be the benchmark from which to develop outcomes (solutions). The work group will design a project plan for management approval which identifies:</p> <ul style="list-style-type: none"> • Proposed solutions against the relevant audit objective(s); • An implementation plan which assigns roles, responsibilities, deliverables and timeframes; • A future risk assessment reflective of the proposed solution. 		<p>Stage 1 complete</p> <p>Stage 2 Not Started</p>	Phase 1 complete. The gap-analysis was presented to the July 2016 meeting of the Committee.

	Not Started	In Progress	Complete	Deferred	Cancelled
--	-------------	-------------	----------	----------	-----------

Page 5 of 7

2017/18 Internal Audit Program

Report as at 31 March 2018

Audit No.	Internal Audit	Audit Objectives	Quarter	Status	Comments
16	Debtor Management	<p>Stage 1: The objectives of the audit are to work with stakeholders to:</p> <ul style="list-style-type: none"> Undertake a risk assessment against the process of debt management in its current state. Undertake high level benchmarking of debt management policies and debt ratios within the local government sector to propose methodologies which are effective and efficient in managing debt. To assess the current state of debt management and document a risk-based gap analysis which proposes findings for implementation. <p>Stage 2: The objectives of the audit are to work with stakeholders to:</p> <ul style="list-style-type: none"> Develop debt management policy/methodology content including documenting the processes for debt escalation, recovery, waiver or write off. Develop a technical specification to quote for services with reference to correcting those gaps and/or control weaknesses identified and/or review options available through pre-existing purchasing panels. 	2	In Progress	<p>Phase 1 is in progress. The gap-analysis was presented to the July 2016 meeting of the Committee.</p> <p>A meeting is scheduled with the Manager Financial Services during quarter 2 to progress this audit.</p>
17	Continuous Procurement Roadmap (Stage 2).	<p>Stage 2 objectives seek to assess the completeness of delivering procurement information, defining roles and responsibilities and the provision of procurement training. In addition, progress against the agreed actions identified in Stage 1 and the overall progress against the Roadmap will be assessed.</p> <p>Intranet/Information availability - the audit will determine the:</p>	2	<p>Stage 1 Complete</p> <p>Stage 2 & 3 Complete</p> <p>Stage 4 Not Started</p>	<p>The audit, undertaken by the Contract Internal Auditor is in progress. An opening meeting was held during November 2017, data collection and interviews are underway.</p>

Not Started	In Progress	Complete	Deferred	Cancelled

2017/18 Internal Audit Program

Report as at 31 March 2018

Audit No.	Internal Audit	Audit Objectives	Quarter	Status	Comments
		<ul style="list-style-type: none"> level of consultation ease of obtaining relevant procurement / contractor management information sufficient evidence of probity of process (documentation and reporting) availability of contracts documents and templates <p>Roles and responsibilities - the audit will assess the:</p> <ul style="list-style-type: none"> Roles and responsibilities are available and understood Sufficiency of training to undertake procurement activity in accordance with the procurement policy and using the procurement processes, contracts and templates. 			

	Not Started	In Progress	Complete	Deferred	Cancelled
--	-------------	-------------	----------	----------	-----------

Page 7 of 7



Internal Audit Scope

Community Consultation Audit

Introduction

The approved 2017-18 Internal Audit Program provides for an internal audit to review the effectiveness of the City of West Torrens' community consultation when aligning and forming key business strategies. Public consultation constitutes one aspect of Council's decision-making process. In consulting with the public, Council seeks to ascertain the views, ideas and concerns of the community and stakeholders, therefore allowing for informed decisions to be made. The *Local Government Act 1999* (SA) (the Act) provides basic requirements for local government in consulting and engagement with their communities.

It is acknowledged that there are a wide breadth of consultation methods and there is no 'one size fits all' strategy to suit each consultation activity. Consequently, it is important to understand Council's broader approach to minimising the risk of poor decision making based on inappropriate community consultation.

Audit Objectives

The objectives of the audit are to evaluate and report on the adequacy and effectiveness of Council's approach to community consultation when aligning and forming key business strategies such as the Community Plan and associated corporate and departmental service plans.

This will be achieved through a review of whether appropriate community consultation tools, methods and strategies are used including:

- Whether community consultation strategies reflect the scale, purpose and level of public interest in the Council's decision or project.
- What principles have been considered in the design and implementation of community consultation activities.
- Management and documentation of community consultation activities.
- Handling and management of responses to community consultation activities and strategies

Audit Scope

This audit will include, but not be limited to, the following:

- Consideration of framework, policies and procedures in relation to community consultation, not limited to:

Community Consultation Audit Scope

- *Council Policy: Public Consultation*
 - *Administration Policy: Public Consultation*
 - *Draft Community Engagement Strategy*
- Consideration of community consultation activities and strategies against the International Association for Public Participation (IAP2) model.
- Consideration of community consultation activities and strategies for plans, budgets and other documents legislatively requiring community consultation.

In addition, the audit will review:

- Past community consultation strategies against the draft *Community Engagement Strategy* and *Council Policy: Public Consultation*
- Council's broader approach to preventing the risk of poor decision making based on inadequate community consultation
- The implications of recent common law decisions to current community consultation strategies with specific reference to *Coastal Ecology Protection Group Inc & Ors v City of Charles Sturt* [2017] SASC 136

Approach

The Program Leader Internal Audit and Risk will distribute the scope and overview of work to be performed with the relevant stakeholders prior to the commencement of testing. An opening meeting will be held with relevant managers where the Auditor will discuss the scope and overview of work to be performed prior to the commencement of testing.

A key component of the audit is to conduct interviews with managers and staff with the responsibility of community consultation, to establish any issues, concerns or opportunities for improvements. Field-testing will be undertaken to establish if controls are implemented that are effective in addressing high to extreme risks.

An audit will be undertaken of available documents including CWT policies, documentation, procedure manuals, performance reports, correspondence etc. This is critical in supporting audit recommendations and providing evidence to support audit conclusions.

The audit is to be assessed using CWT approved Enterprise Risk Management Framework and tools.

Risks

Potential risks associated with *community consultation* identified through Internal Audit include, but are not limited to:

- Non-compliance with the *Local Government Act 1999*, policies and strategies resulting in:
 - investigation by an external agency
 - fraud, corruption, misconduct and/or maladministration
 - litigation
 - reputation damage
- Inadequate monitoring, follow up and reporting.

Community Consultation Audit Scope

General Administration

This audit will be performed by Galpins.

Initial planning, interview and scoping commenced March 2018 with fieldwork and reporting to commence by negotiation during April 2018. A draft report will be completed for Management comment by 31 May 2018 to allow for corrections of fact and management comments to be incorporated. The final report will be issued to the Executive Management Team for review.

Audit Findings and Recommendation Ratings*Compliance Rating*

Audit must provide a compliance rating. Compliance ratings are classified as having a good level of compliance, a substantial level of compliance, a partial level of compliance or as being not compliant.

Recommended actions are classified as corrective where they relate directly to legislative, policy or procedural requirements and/or present an unacceptable level of risk to Council and improvement where they are in response to generally accepted industry standards or better practice.

Definitions are as classified in the table below.

<i>Non compliant</i>	<i>There is no evidence of compliance with legislation, policy, procedure and/or internal controls.</i>
<i>Partial level of compliance</i>	<i>There is partial evidence of compliance with legislation, policy, procedure and/or internal controls.</i>
<i>Substantial level of compliance</i>	<i>There is a substantial level of compliance with legislation, policy, procedure and/or internal controls.</i>
<i>Good level of compliance</i>	<i>There is a good level of compliance with legislation, policy, procedure and/or internal controls.</i>

Control Risk Rating

Findings/issues are classified in accordance with a risk rating consistent with Council's Risk Management Framework so that recommendations are reported as:

- *Extreme risk recommendations*
- *High risk recommendations*
- *Moderate risk recommendations*
- *Low risk recommendations*
- *Better practice or improvement recommendations*

Community Consultation Audit Scope

Sign Off

I have read the above Internal Audit Assignment Plan and I am satisfied the objectives and scope meet the expectations for this audit.

Signed



General Manager Business and Community Services

Date

21/2/18



Internal Audit Scope

Legislative Audit: Governance Compliance

Introduction

Elected Members, from time to time, experience conflicts of interests between their personal affairs and matters requiring the consideration of Council. Part 4 Division 3 of the *Local Government Act 1999* (SA) (the Act) provides the statutory procedures that must be undertaken by Elected Members in relation to conflicts of interest, their disclosure and management. The Mandatory Code of Conduct for Council Members also states that the Act must be complied with in regards to conflicts of interest so that decisions are made without bias and in the best interests of the whole community.

The approved 2017-18 Internal Audit Program provides for an internal audit to review the CWT's Governance Framework compliance with the Act. However, rather than audit a large process and as a result of the recent media focus on Elected Member's compliance with the conflict of interests provisions contained in the Act, the audit has been refocussed to the management of conflict of interest provisions.

Audit Objectives

The objectives of the review are to evaluate and report on the level of compliance with the:

- *Local Government Act 1999* (SA) - Part 4 Division 3
- *Local Government (General) Regulations 2013* (SA)
- Mandatory Code of Conduct for Council Members
- City of West Torrens Statutory Code - *Code of Practice - Procedures at Meetings*
- Any identified opportunities for the introduction of better practices and process improvement.

Scope Exclusions

The Audit will specifically exclude the following:

- Processes to manage Council employee conflicts of interest disclosures.
- Compliance of the City of West Torrens Statutory Code - *Code of Practice - Procedures at Meetings* against the Act or associated Regulations.

Legislative Audit - Governance Compliance

- Procedures and processes dealt with under the Act or the *Local Government (Procedures at Meetings) Regulations 2013* except insofar as the management of Elected Member conflicts of interest.

Approach

The Program Leader Audit and Risk will discuss the scope and overview of work, to be performed, with the contract internal auditor prior to the commencement of testing.

The Program Leader Internal Audit and Risk will distribute the scope and overview of work to be performed with the Executive Coordinator - Office of the Mayor and CEO and the Executive Assistant within this department prior to the Audit engagement.

The key components of this audit are to:

1. Review available documentation e.g. legislation, policies, conflict of interest disclosure forms, procedures, manuals, working documents and files etc. used in fulfilling CWT's responsibilities under the Act to determine compliance with the Act.
2. Conduct interviews with key managers, staff and stakeholders to establish any issues, concerns and potential improvements.

Risks

Potential risks associated with administering the Act as identified by Internal Audit include, but are not limited to:

- Non-compliance with legislation
- Inadequate records management and review processes
- Failure to act on a conflict of interest matter that compromises the reputation of the CWT such as:
 - a customer complaint
 - investigation by an external agency
 - litigation or prosecution

General Administration

This audit will be performed by Council's contract legal auditors, Wallmans Lawyers.

Initial planning, interview and scoping commenced during January with fieldwork and reporting to be conducted between March and April 2018.

A draft report is required to:

- Include an excel spreadsheet or word table that contains recommendations/assessments
- Be issued to the Internal Auditor for comment, and
- Allow for corrections of fact and incorporation of managers comment and risk assessment using CWT approved Enterprise Risk Management Framework and tools.

Legislative Audit - Governance Compliance

The final report will be issued to the Executive Management Team and the Executive Coordinator. This report will also be tabled at the Audit and Risk Committee meeting for review.

A draft report for management consideration should be completed by the end of June 2018.

Audit Findings and Recommendation Ratings

Compliance Rating

Findings are classified as having a good level of compliance, a partial level of compliance, a substantial level of compliance or as being not compliant.

Recommended actions are classified as corrective where they relate directly to legislative, policy or procedural requirements and/or present an unacceptable level of risk to Council and improvement where they are in response to generally accepted industry standards or better practice.

Definitions are as classified in the table below.

<i>Non-compliant</i>	<i>There is no evidence of compliance with legislation, policy, procedure and/or internal controls.</i>
<i>Partial level of compliance</i>	<i>There is partial evidence of compliance with legislation, policy, procedure and/or internal controls.</i>
<i>Substantial level of compliance</i>	<i>There is a substantial level of compliance with legislation, policy, procedure and/or internal controls.</i>
<i>Good level of compliance</i>	<i>There is a good level of compliance with legislation, policy, procedure and internal controls.</i>

Control Risk Rating

Findings/issues are classified in accordance with a risk rating consistent with Council's Risk Management Framework so that recommendations are reported as:

- *Extreme risk recommendations*
- *High risk recommendations*
- *Moderate risk recommendations*
- *Low risk recommendations*
- *Better practice or improvement recommendations*

Legislative Audit - Governance Compliance

Sign Off

I have read the above Internal Audit Scope and I am satisfied the objectives and approach meet the expectations for this audit.

Signed

A handwritten signature in black ink, appearing to be 'P. K. Q.', written over a horizontal line.

General Manager Business and Community Services

Date 21/2/18

9.4 EXTERNAL AUDIT

Nil

9.5 COMMITTEE PERFORMANCE AND REPORTING

Nil

10 OTHER BUSINESS

11 CONFIDENTIAL

Nil

12 NEXT MEETING

12 June 2018, 6.00pm in the Mayor's Reception Room.

13 MEETING CLOSE