AUDIT AND RISK MANAGEMENT SUBCOMMITTEE
18 MARCH 2013

REPORT 1
(1215/52/01/1M)

PROGRESS AGAINST AUDIT NEW ZEALAND RECOMMENDATIONS

1. Purpose of report

The purpose of this report is to present the Audit New Zealand's Report to Council to the Subcommittee. This report contains audit recommendations from Audit New Zealand related to the 2011/12 audit as well as progress against recommendations made in prior years.

2. Recommendations

Officers recommend that the Audit and Risk Management Subcommittee:

1. *Receive the information.*

2. *Note the progress made in implementing the Audit New Zealand recommendations attached in Appendix 1.*

3. Summary of improvements in recommendations since the last report

Refer to Appendix 1 for the current status of all outstanding audit recommendations.

Contact Officer: Nicky Blacker, Manager, Financial Accounting

SUPPORTING INFORMATION

1) Strategic fit / Strategic outcome

This project supports Activity 1.1 Governance, Information and Engagement, specifically 1.1.1 City Governance and Engagement. As per the Annual Plan, City Governance and Engagement includes all those activities that make the Council accountable to the people of Wellington and ensure the smooth running of the city. That includes all meetings of the Council and its committees and subcommittees.

2) LTP/Annual Plan reference and long term financial impact

The report has no specific Annual Plan reference. There is no long term financial impact arising from the report.

3) Treaty of Waitangi considerations

There are no specific Treaty of Waitangi considerations.

4) Decision-making

There are no significant decisions required by the paper.

5) Consultation
a) General consultation

There are no parties significantly affected by this paper.

b) Consultation with Maori

Maori are not significantly affected by this paper.

6) Legal implications

This report has no specific legal implications.

7) Consistency with existing policy

This report is consistent with existing policy.

Summary of recommendations and their current status

Overarching IT security policy and disaster recovery	**Recommendation date: 2007/08**	
Recommendations	**Management response – Mar 2012**	**Audit New Zealand Comments – Mar 2012**
IT Security Policy Council does not have one overarching IS/IT Security Policy. This potentially allows unauthorised access to systems and/or fraudulent, malicious or unintended transactions to be posted. Audit recommended that Council develop and implement an IS/IT Security Policy as an overall statement of the importance of security to the organisation.	**Target date for completion: COMPLETED** The proposed IT Policy and guides have been reviewed and approved by Manager Risk and Assurance December 2012, and Director approval was given by Greg Orchard on 28 August 2012. They are now ready for general release and have been published on the Council Intranet	In progress Audit New Zealand has sighted approved IS Security Framework and Security Policies. As at February 2013, the implementation of the password policies to all server and desktop equipment is still in progress.
Business Continuity and Disaster Recovery We recommend that Business Continuity Plans be finalised and tested as planned. The results should be documented and communicated to all affected staff so that improvements to procedures can be made. Business Continuity and IT Disaster Recovery plans are now well developed, and tests of these plans are to be	**Target date for completion: COMPLETED** The intention was to carry out an IT DR test in August 2012. On the morning of 27 June a power surge took down all the council's computer systems. The directors on the BCP steering group met early to activate the BCP. There was an independent inquiry into the BCP process as a result of a power	In progress The project to move the datacentre is underway and DR Planning will be incorporated into that. A project Manager has been appointed to look at Business Continuity Planning.

carried out this year.	failure which caused an IT Outage which focused on the response to the incident. This report was presented to the BCP steering group and the recommendations acted upon. Given that this incident necessitated the initiation of the BCP, and lessons learned will be incorporated into DR and BCP planning, it was decided not to run another DR test. We have selected a partner for the hosting of the Council's computer centre and the project will be completed July 2013. The DR computer centre needs to be relocated prior to November 2013 and a prerequisite is a review of the BCP.	
End-User Computing Council's Knowledge Solutions (KS) organisation is not aware of the extent of end-user applications and does not have controls in place to manage end-user computing. The risk around end- user computing applications (such as Excel spreadsheets and Access databases) is that they might be used for key business processes, and/or business decisions and/or reporting without (at the same	**Target date for completion: COMPLETED** End-user computing policy is included in the Policy and Security Framework. The proposed IT Policy and guides have been reviewed and approved by Manager Risk and Assurance in December 2012. An inventory of all desktop applications has been developed as part of the	Completed We have sighted an approved End-user computing policy included in the IT Policy and Security Framework. This policy is now being enforced by Information Management.

time) being subject to the same level of controls as business key systems. Therefore, data in these systems may be incomplete or inaccurate. Develop and implement a policy for end-user computing as a basis for controlling the employment of end-user application. This also helps that adequate processes and controls for end-user application development, security, change management and operations are in place to ensure the reliability of these systems.	Security Framework and will be updated on an ongoing basis. The end user policy is part of the proposed IT Policy and guides that have been reviewed and approved by Manager Risk and Assurance. A refinement of these policies specifically to cover the use of Microsoft excel and access has been incorporated in to the end user policies. The policy incorporates 1. Evaluating the current situation (spreadsheet and database risk questionnaire). 2. Control activities (preventative and detective/audit) 3. Develop roadmap to leverage advances in Office 2007 and new Enterprise Content Management system once deployed. 4. Audit cycle to refresh position Training and Guidelines have been included in the Desktop Transition project as part of the Office 2010 rollout.	

Management of generic and powerful user accounts When generic accounts are used they should be restricted to specific use situations and reduced to read only access wherever possible to prevent changes being made without accountability. For powerful users there is a higher risk of malicious or accidental changes having significant impacts on systems. These users should be known and adequately monitored. IT and business application owners should develop a process to document the current generic and powerful accounts within their network domain and various applications. This should include an assessment to determine the extent of their access and whether they are still required.	**Target date for completion: March 2013** **February 2013** An initial review of Generic and Powerful Accounts has been completed and monitored for usage. **Initial Recommendations Implemented 2013** A Reduction in Generic accounts: Where an account has not been utilised for a period of 3 months it is disabled for a period of 1 month then deleted. The Senior Security and Telecommunications Engineer will provide further recommendations with a target date of 30 March 2013.	In progress We understand that 3 monthly reviews of generic and powerful accounts have been performed but are not a complete review of all generic accounts. IT Management is currently investigating their findings on some generic accounts with unknown business units. Decisions will still need to be made as to whether these accounts will be kept or deleted.
IT-IM Risk Framework IT-IM should establish a risk assessment framework that is used periodically to assess information risk to achieving business objectives. Where risks are considered acceptable, there should be formal documentation and acceptance of	**Target date for completion: COMPLETED** After consultation with Risk Assurance the decision was made to utilise the Council's standard Risk Management Framework. A Risk Register was developed and was reviewed and accepted by Risk Assurance in	Completed An IS risk assessment framework was completed in 2012 based on NZ standards. Continuous improvements to the risk assessment framework and reporting are being worked on.

residual risk with related offsets. Where risks have not been accepted, management should have an action plan to implement risk response (including system and data availability). Whilst the council has an organisational risk framework in which major IT - IM risks are recorded, there is no risk framework or register within IT - IM itself to record and assess risk.	December 2012.	
Unnecessary access to the computer room We recommend that management limit the access to the main computer room and consider reviewing the appropriateness of the cardholders. We noted that there are 81 cardholders that were authorised to gain access to the computer room.	**Target date for completion: COMPLETED** There have been two audits of secured access. The list of secure access has been compiled and an initial review undertaken. All users had valid requirements at the time of issue and review. The latest review February 2013 has resulted in all users being ratified as valid and four names to be removed. Access will be reviewed on an Annual basis	Completed We noted that a review of existing access to limit the access to the main computer room has been undertaken. IT Management confirmed that all users have valid requirements at the time of issue. Due to external hosting arrangement of the Council data centre, we will review the appropriateness of access to the main computer room as part of next year audit.

	Note: A decision to outsource using external hosting of the computer room in a hosted secure environment under DIA access guidelines has superseded this requirement.	
Responsibility: Stephanie Mardell, Gerard Paver and Miles Dunkin		