AUDIT AND RISK MANAGEMENT SUBCOMMITTEE
17 JUNE 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 – Jun 2013**	**Audit New Zealand Comments – Mar 2013**
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 were published on the Council Intranet in January 2013. Internal audit also picked up some issues and these were implemented as noted below. 1. Enforce the password reset timeframes as stipulated in the Guidelines. There must be valid business reasons for any exceptions required to this rule. These should be documented and approved by relevant management. This was actioned on Wednesday 13 March and all those people identified as not having a valid reason for no password expiry have now been set to expire like normal users	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.

	and are required to change their password every 90 days. 2. Ensure password lengths are system enforced to comply with the Guidelines. This was approved by the Change Advisory Board and has been enforced effective from 20 March 2013	
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 carried out this year.	**Target date for completion: JULY/SEPTEMBER QUARTER** The intention was to carry out an IT Disaster Recovery (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 Business Continuity Plan (BCP) steering group met early to activate the BCP. There was an independent inquiry into the BCP process as a result of a power 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	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.

	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.	
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: COMPLETED** Generic accounts for unknown business units have been disabled on the network. If we are not contacted with objections to the disabling of the accounts is raised over the next 3 to 6 months the accounts will be deleted. Generic accounts are reviewed as part of the normal deletion process on a continuous basis. 108 generic accounts have been deleted in the last 6 months. A further 100 accounts have been moved into the "Mark for deletion" container. Creation of generic accounts is discouraged but sometimes unavoidable	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.
Responsibility: Stephanie Mardell, Gerard Paver and Miles Dunkin		