AUDIT AND RISK MANAGEMENT SUBCOMMITTEE
18 June 2012

REPORT 2
(1215/52/01/IM)

PROGRESS AGAINST AUDIT NEW ZEALAND RECOMMENDATIONS

1. Purpose of report

The purpose of this regular report is to update the Subcommittee on Audit New Zealand arrangements and progress in implementing the recommendations contained in the audit management letters presented to the Subcommittee.

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 a summary of the current status of this issue and all outstanding issues from previous years.

Contact Officer: Nicky Blacker, Manager, Financial Accounting

SUPPORTING INFORMATION

1) Strategic fit / Strategic outcome

This project supports Activity 1.1 Information, Consultation and Decision Making, 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.

Appendix 1: Summary of recommendations and their current status

Overarching IT security policy and disaster recovery	Recommendation date: 2007/08	Target date for completion: IT Security Policy – September 2012 End-User Computing – June 2012 Disaster Recovery – September 2012
Recommendations	**Management response – Apr 2012**	**Current update**
During the period Audit assessed the risk around the overarching processes addressing IT Strategy and IT Governance, IT Processes and IT Controls. They identified two areas for improvement: • 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. • 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	**IT Security Policy** IT-IM have developed an overarching IT security policy which was approved by IT-IM Management. This policy provides a framework for IT security governance, risk assurance, policies, standards, and guidelines. 23 policies covering aspects of IT security, as recognised by NZ government organisations, are being progressively implemented over the next six months. A new position (Senior Security and Telecommunications Engineer) has recently been filled in IT Operations with a focus on progressing the implementation of the IT security policies. During recent discussions with Audit NZ, the Senior Auditor reviewed and endorsed the IT Security Policy and Framework and recommended that it be circulated to other local authorities.	**IT Security Policy** IT-IM have developed an overarching IT security policy which was approved by IT-IM Management. This policy provides a framework for IT security governance, risk assurance, policies, standards, and guidelines. The policies cover all aspects of IT security, as recognised by NZ government organisations, are being progressively implemented over the next six months. A Senior Security and Telecommunications Engineer has been appointed (May 2012) and tasked with the development and the rollout of the IS Security Framework and develop a communication plan for the policies. The time frame and priority of policy rollout to be agreed with Manager Risk Assurance. The initial rollout of high priority policies will be complete by end September 2012. During recent discussions with Audit NZ, the

reporting without (at the same time) being subject to the same level of controls as business key systems. Therefore, data in these systems may be incomplete or inaccurate. Audit recommended that Council • Develop and implement an IS/IT Security Policy as an overall statement of the importance of security to the organisation. • 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. • Formally document the results of the IT Disaster recovery tests	**End-User Computing** Although it is difficult to manage the creation of Excel spreadsheets and Access databases, IT-IM are progressing the development of a specific guideline to address end-user computing. This will require involvement of Risk Assurance, including risk assessment and development of internal controls. Currently, Microsoft Access requires a business case to be approved by the Business Unit Manager before installation. This enables IT-IM to provide advice and guidance regarding other ways of achieving the same outcome, e.g. utilisation of Enterprise Reporting. **Disaster Recovery** A disaster recovery test has been scheduled for 15 June 2012. The outcome of the test will be formally documented and reviewed by Risk Assurance by 31 July 2012. This will be a test of the technical recovery of systems defined as critical. Business Units will be invited to undertake user testing of recovered applications. Audit NZ has reviewed the previous DR test outcome documentation. A BCP Programme Manager has been	Senior Auditor reviewed and endorsed the IT Security Policy and Framework and recommended that it be circulated to other local authorities. **End-User Computing** End-user computing policy included in the Policy and Security Framework. An inventory of all desktop applications has been developed as part of the Security Framework and will be updated on an ongoing basis. Although it is difficult to manage the creation of Excel spreadsheets and Access databases, IT-IM are progressing the development of a specific guideline to address end-user computing. This will require involvement of Risk Assurance, including risk assessment and development of internal controls. Currently, Microsoft Access requires a business case to be approved by the Business Unit Manager before installation. This enables IT-IM to provide advice and guidance regarding other ways of achieving the same outcome, e.g. utilisation of Enterprise Reporting. Once the End-user policy is in place, IT-IM

	appointed through the Project Management Office. Risk Assurance is currently working with Business Units to update their business continuity plans. Opportunities to align the BCP and DR testing will be discussed once a programme of work has been defined.	will develop and implemented an engagement procedure to support the policy, using it as an education opportunity across the organisation. **Disaster Recovery** A disaster recovery test was scheduled for 15 June 2012. This has been deferred until the end of August at the request of the Finance team, due to year end demands. The outcome of the test will be formally documented and reviewed by Risk Assurance within 20 working days of the test completion. This will be a test of the technical recovery of systems defined as critical. Business Units will be invited to undertake user testing of recovered applications. Audit NZ has reviewed the previous DR test outcome documentation. A BCP Programme Manager has been appointed through the Project Management Office. Risk Assurance is currently working with Business Units to update their business continuity plans. Opportunities to align the BCP and DR testing will be discussed once a programme of work has been defined.
Responsibility: Stephanie Mardell, Gerard Paver and Miles Dunkin		