# AUDIT AND RISK MANAGEMENT SUBCOMMITTEE
**12 DECEMBER 2012**

**REPORT 2**
*(1215/52/01/1M)*

## 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 outstanding issues raised in the Management Report to Council issued by Audit New Zealand for the current and previous years.

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 – Oct 2012** | **Current update** |
| **IT Security Policy**<br><br>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.<br><br>Audit recommended that Council develop and implement an IS/IT Security Policy as an overall statement of the importance of security to the organisation. | 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.<br><br>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.<br><br>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. | **Target date for completion: September 2012**<br>**Completed December 2012**<br>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.<br><br>The proposed IT Policy and guides have been reviewed and approved by Manager Risk and Assurance, and Director approval was given by Greg Orchard on 28 August 2012. They are now ready for general release. |

| | | |
|---|---|---|
| **End-User Computing**<br>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 time) being subject to the same level of controls as business key systems. Therefore, data in these systems may be incomplete or inaccurate.<br><br>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. | 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.<br><br>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. | End-user computing policy is included in the Policy and Security Framework.<br><br>An inventory of all desktop applications has been developed as part of the Security Framework and will be updated on an ongoing basis.<br><br>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 databases is being undertaken by Information Management and will be a incorporated as an amendment to the end user policies.<br><br>The policy incorporates<br>1. Evaluating the current situation (spreadsheet and database risk questionnaire).<br>2. Control activities (preventative and detective/audit)<br>3. Develop roadmap to leverage advances in Office 2007 and new Enterprise Content Management system once deployed. |

| | | |
|---|---|---|
| | | 4. Audit cycle to refresh position<br><br>Once the End-user policy is in place, IT-IM will develop and implement an engagement procedure to support the policy, using it as an education opportunity across the organisation. |
| **Management of generic and powerful user accounts**<br><br>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.<br><br>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. | Agreed. A Review of generic and powerful accounts will be undertaken as part of the Security Framework and policy implementation rollout.<br>The review will document the current generic and powerful accounts and the extent of their access. A periodic review will be formalised with the business owners to confirm whether powerful accounts are still required.<br><br>Recommendations will be supplied to GM IT operations and Manager Risk Assurance for further action. | **Target date for completion: March 2013**<br><br>Agreed. Included as part of 2012/13 work programme, target March 2013. Coordinated by the Senior Security and Telecommunications Engineer. |

| | | |
|---|---|---|
| **IT-IM Risk Framework**<br><br>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 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).<br><br>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. | Agreed. As part of 2012/13 work programme, a risk assessment framework based on NZ standards will be developed. | **Target date for completion: December 2012**<br>A Risk Assessment Framework and Risk Register focused on IT and Information Management risk is due for completion in December 2012.<br><br>After discussions with Risk Assurance it has been decided that ITIM will utilise Council's existing Risk Management Framework rather than create a specific framework for ICT. |
| **Unnecessary access to the computer room**<br><br>We recommend that management limit the access to the main computer room and consider reviewing the appropriateness of the cardholders.<br><br>We noted that there are 81 cardholders that were authorised to gain access to the computer room. | Agreed. A Review of existing Access to limit the access to the main computer room is being undertaken as part of the Security Framework and policy implementation rollout. A report and recommendations will be supplied to GM IT operations and Manager Risk Assurance. The initial rollout of high priority policies will be complete by end September 2012<br><br>The access list will be reviewed on an | **Target date for completion: September 2012 - Completed**<br>The list of secure access has been compiled and an initial review undertaken. All users had valid requirements at the time of issue. The Senior Security and Telecommunications Engineer will follow up with individual cardholders to ensure access is still valid.<br><br>Note: A decision to outsource using |

| | | |
|---|---|---|
| | annual basis. | external hosting of the computer room within the next 8 months has superseded this requirement. |
| **Responsibility: Stephanie Mardell, Gerard Paver and Miles Dunkin** | | |