ADELAIDE HILLS COUNCIL
AUDIT COMMITTEE MEETING
WEDNESDAY 15 August 2016
AGENDA BUSINESS ITEM

Item:	**7.1**
Originating Officer:	**Andrea Sargent, Manager Governance and Risk**
Responsible Director:	**Terry Crackett, Director Corporate Services**
Subject:	**ICT Security Assessment Action Implementation Update**
For:	**Information**

---

1. ICT Security Risk Assessment Action Implementation Update – Exclusion of the Public

a) Under the provisions of section 90(2) of the *Local Government Act 1999* the Audit Committee (the Committee) orders that all members of the public, except:

- **CEO, Andrew Aitken**
- **A/Director Corporate Services, Lachlan Miller**
- **Manager Governance & Risk, Andrea Sargent**
- **Manager Finance, Paul Francis**

be excluded from attendance at the meeting for Agenda Item 7.1: ICT Security Risk Assessment Action implementation Update to be considered in confidence.

b) The Audit Committee is satisfied that it is necessary that the public, with the exception of Council staff in attendance as specified in (a) above, be excluded to enable the Audit Committee to consider the report at the meeting on the following grounds:

> **Section 90(3)(e) of the Local Government Act, that is, *matters affecting the security of the council, council members or employees of the council, or council property, or the safety of any person;***

The Audit Committee is satisfied that it is reasonably foreseeable that public disclosure of information contained in the report may result in vulnerabilities to council's information and communication technology being breached and the security of council property and the safety of council employees and members of the public may be impacted.

c) Accordingly, on this basis the principle that meetings of the Audit Committee should be conducted in a place open to the public has been outweighed by the need to keep the information and discussion confidential.

2. ICT Security Risk Assessment Action Implementation Update – Confidential Item

SUMMARY

This report provides the Audit Committee with an update on the current status of actions arising from the ICT Security assessment as shown in Appendix 1. A significant amount of work has occurred to progress the identified actions, with 62.9% completed and 22.8% in progress.

Given the nature of the information from the security assessment and actions contained in Appendix 1 it is recommended that this report be considered in confidence.

RECOMMENDATION

The Audit Committee resolves:

1. To receive and note the report and appendix.

ICT Security Risk Assessment Action Implementation Update – Period of Confidentiality

2. That having considered the ICT Security Risk Assessment Action Implementation Update at Agenda Item 7.1 in confidence under sections 90(2) and 90(3)(e) of the Local Government Act 1999, that an order be made under the provisions of sections 91(7) and (9) of the Local Government Act 1999 that the report, related attachments, the minutes of the Committee and the discussion of the subject matter be retained in confidence until ICT Security Risk Assessment actions have been addressed.
3. Pursuant to section 91(9) (a) of the Local Government Act 1999, that the Audit Committee delegates the duty to conduct an annual review of the confidentiality order to the Chief Executive Officer, or his sub-delegate.
4. Pursuant to section 91(9)(c) of the Local Government Act 1999, that the Audit Committee delegates the power to revoke the confidentiality order to the Chief Executive Officer.

2.1 GOVERNANCE

- **Strategic Management Plan/Council Policy**

Goal 4	A Recognised Leading Performer
Key Issue 4.1:	Leadership
Action 4.1.4:	Meet legislative, regulatory and good governance responsibilities and obligations.
Key Issue 4.2	Managing Risk and Responsibility
Key Action 4.2.5	Ensure legislative compliance occurs through the application of core policies and procedures.

- **Legal Implications**

Section 125 of the Local Government Act 1999 requires councils to ensure that appropriate policies, practices and procedures of internal controls are implemented and maintained in order to assist the council to carry out its activities in an efficient and orderly manner to achieve its objectives, to ensure adherence to management policies, to safeguard Council's assets, and to secure (as far as possible) the accuracy and reliability of Council records.

The Internal Audit program is an important tool to provide an objective appraisal of the adequacy on internal controls in managing our risk and supporting the achievement of council objectives.

- **Risk Management Implications**

The implementation of the internal audit program will assist in mitigating the risk of:

Internal control failures occur which lead to greater uncertainty in the achievement of objectives and/or negative outcomes.

Inherent Risk	Residual Risk	Target Risk
High (4C)	Medium (3C)	Medium (3C)

- **Financial and Resource Implications**

The Internal Audit budget for this financial year includes funding to resource the proposed audits and enable them to be outsourced under the oversight of the Manager Governance and Risk. Given the range of demands on this role, and the specialised nature of a number of the audits, it is not possible to undertake audits internally.

- **Customer Service and Community/Cultural Implications**

There is a high expectation that Council has appropriate corporate governance processes in place including an effective internal control environment.

- **Environmental Implications**

Not applicable

- **Engagement/Consultation with Committee, Regional Subsidiary, Advisory Group and Community**

Internal consultation occurs in the preparation of an internal audit scopes, in finalising audit reports and in the development and implementation of actions to address the audit findings. External consultation was not applicable.

2.2 BACKGROUND

2.2.1 Implementation of actions arising from the ICT Security Assessment

A cyber security audit was nominated on the Strategic Internal Audit Plan and subsequently an ICT Security Risk Assessment was conducted in 2015 and finalised early in 2016. The findings of the ICT Security Risk Assessment were considered by the Committee in confidence at the February 2016 meeting and so this will be the first update on the status of actions arising from that audit.

As work is continuing on the actions from this audit and information on these security matters has potential for miss-use the update on the action status is being presented in a separate report for consideration in confidence.

2.3 ANALYSIS

2.3.1 Implementation of actions – ICT Security Assessment

As mentioned above, progress against actions arising from the ICT Security Risk Assessment is being considered in this separate confidential report given the nature of the ICT security information provided.

Significant progress against actions arising from the ICT Security Risk Assessment has been made (as indicated in the action register in Appendix 1). Twenty two actions out of the 35 recommendations have been completed, that is a completion percentage of 62.9%. Four of the recommendations will be dealt with in an alternative manner as the Datacentre is to be relocated. One recommendation is considered not appropriate, but will be considered within the development of training options under recommendation 27. As such five of the 35 recommendations will not be addressed as recommended, ie 14.3%). The remainder of recommendations are being actioned, that is 8 actions being 22.8% percent are in progress. As can be seen significant progress has been made in actioning the recommendations of the Security assessment. The work of the ICT team in addressing the findings of the Security assessment is recognised.

2.4 OPTIONS

The Committee has the following options:

I. To note the status of the Action Progress report as presented; and / or

II. To make formal comment on progress on the audit actions and / or identify additional actions to be undertaken.

2.5 APPENDICES

(1) IA Action Implementation Register – ICT Security Assessment

Appendix 1

IA Action Implementation Register –
ICT Security Assessment

AHC INTERNAL AUDIT - ACTION REPORT

Ref	Issue/*Recommendation*	Response/*Proposed Action*	Priority	Responsible Department	Complexity to action	Estimated Hours to implement recommendation	Estimated Budget to implement recommendation	Due Date	Revised Date	Date of Update	Progress/Comment
ICT Security Risk Assessment - August 2015 - CQR											
REC 1	Policy and Governance - Information Security Policy	IS to create as part of a suite of policies around information and document management. Some core aspects have been captured in the Records Policy adopted by council in August.	Moderate	IS	Moderate	5 to 10 days	Staff Time	30-Jun-16	31/12/16		**Ongoing** - An internal governance group has been formed (IISIP) where a number of representatives across the organisation are involved in creating a suite of policies
REC 2	Policy and Governance - Risk Management	ICT/IS to review the specific risks identified in Councils risk register	Moderate	ICT & IS	Low	1 day	Staff Time	31-Dec-15			**Completed -** Review and updated risks identified in Councils Risk Register
REC 3	Policy and Governance - Business Continuity Planning	ICT to action - (ICT BCP Plan only) included in 2015/16 Capital Works Program	High	ICT	High	8 weeks	$70k	30-Jun-16	31/12/16		**Ongoing** - ICT BCP is currently progressing well with 50% of the works already undertaken. BCP Systems Recover Software has been purchased and undergoing configuration and testing. Building of Datacentre Communication links to CDB commenced in May 2016 and will be completed in August 2016. Tender for Datacentre equipment to commence in August and completion by December 2016
REC 4	Policy and Governance - Incident Management	ICT to action - create a security incident management procedure	Low	ICT	low	1 week	Staff Time	30-Jun-16	31/12/16		**Ongoing** - An internal governance group has been formed (IISIP) where a number of representatives across the organisation are involved in creating a suite of policies
REC 5	Servers - Access Control	ICT to action - Create separate Administration Accounts for ICT and IS Team Members	Moderate	ICT	Low	1 Day	Staff Time	31-Dec-15			**Completed -** ICT/IS all now have separate Administration Accounts for logging onto servers & systems
REC 6	Servers - Monitoring and Logging	ICT to action - Project to identify a technology solution to Logging	Moderate	ICT	Low	1 Week	Unknown at this stage	31-Dec-15			**Completed** - Implemented 4 monitoring systems to cover monitoring (Cacti, neon, rancid and splunk)
REC 7	Servers - Vulnerability Management	ICT to action - A proactive Patch Management Procedure for Microsoft Updates to be created and then implemented	High	ICT	Low	1 Week	Staff Time	31-Dec-15			**Completed** - Proactive patching being undertaken and looking at software solutions to enhance the process from an auditing perspective.
REC 8	Servers - Backup and Recovery	ICT to action - due to the ICT BCP Capital Works Program 2015/16 this task will need to be completed after its implementation as configuration changes will impact on how this is performed	Low	ICT	Low	1 Week	Staff Time	30-Jun-16	31/12/16		**Ongoing** - Linked to Rec 3
REC 9	Servers - Configuration Management	ICT to action - prepare a standard server build guide and template	Low	ICT	Medium	1 week	Staff Time	31-Mar-16			**Completed -** Virtual Template created that is used to build & deploy servers
REC 10	Network - Access Control	ICT to action - implement a procedure for logging of access to systems by external contractors	Moderate	ICT	low	3 Days	Staff Time	31-Dec-15			**Completed** - Software solution in place to and record network access.

Ref	Issue/*Recommendation*	Response/*Proposed Action*	Priority	Responsible Department	Complexity to action	Estimated Hours to implement recommendation	Estimated Budget to implement recommendation	Due Date	Revised Date	Date of Update	Progress/Comment
REC 11	Network - Monitoring and Logging	ICT to action - expand on already implemented monitoring system (Site24x7) to report on all network systems	Moderate	ICT	Low	2 weeks	Staff Time	31-Dec-15			**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 12	Network - Vulnerability Management	ICT to action - Document network devices and patch level and compliance	Moderate	ICT	Low	2 days	Staff Time	31-Dec-15			**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 13	Network - Backup and Recovery	ICT to action - currently AHC has a backup of network device configurations, however they may now be out of date. Implement a procedure for backup configurations to be captured when changed and stored in backup systems	Low	ICT	Low	2 days	Staff Time	31-Dec-15			**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 14	Network - Configuration Management	ICT to action - will need to consult with networking engineers to consider recommendation	Low	ICT	Medium	unknown	unbudgeted cost	30-Jun-16			**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 15	Workstations and Laptops - Configuration Management	ICT to action - Create a build guide for the hardening of the Virtual Desktop	Low	ICT	Medium	1 Week	Staff Time	31-Dec-15			**Completed -** Virtual template created to consistently deploy a standard template with security controls deployed
REC 16	External Access - Monitoring and Logging	ICT to action - implement a syslog server to capture firewall logs	Moderate	ICT	Medium	1 Week	Staff Time	30-Jun-16			**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 17	External Access - Vulnerability Management	ICT to action - Document network devices and patch level and compliance	Low	ICT	Low		Staff Time	31-Dec-15			**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 18	External Access - Backup and Recovery	Incorrect - Backups are taken of our ASA appliance									**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 19	External Access - Configuration Management	ICT to action - Implement a review of firewall configuration	Low	ICT	Low	4 Weeks	Staff Time	31-Dec-15			**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 20	Wireless - Monitoring and Logging	ICT to Action - Capital Works Program for 2015/16 to review the wireless network	Low	ICT	Low	4 Weeks	Staff Time	31-Mar-16			**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 21	Wireless - Vulnerability Management	ICT to Action - Capital Works Program for 2015/16 to review the wireless network	Low	ICT	Low	4 Weeks	Staff Time	31-Mar-16			**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 22	Wireless - Backup and Recovery	ICT to Action - Capital Works Program for 2015/16 to review the wireless network	Low	ICT	Low	4 Weeks	Staff Time	31-Mar-16			**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 23	Wireless - Configuration Management	ICT to Action - Capital Works Program for 2015/16 to review the wireless network	Low	ICT	Low	4 Weeks	Staff Time	31-Mar-16			**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 24	Mobile Devices - Monitoring and Logging	ICT to Action	Low					30-Jun-16			**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 25	Mobile Devices - Vulnerability Management	ICT to implement a proactive patching schedule for Mobility Devices	Low	ICT	Low		Staff Time	30-Jun-16	31/12/16		**Ongoing** - Investigations of systems underway
REC 26	Mobile Devices - Configuration Management	ICT to implement - review the MDM solution in place and implement recommendation	Low	ICT	Medium	4 Weeks	Staff Time	30-Jun-16	31/12/16		**Ongoing** - Investigations of systems underway

Ref	Issue/*Recommendation*	Response/*Proposed Action*	Priority	Responsible Department	Complexity to action	Estimated Hours to implement recommendation	Estimated Budget to implement recommendation	Due Date	Revised Date	Date of Update	Progress/Comment
REC 27	Personnel - Awareness and Education	ICT and Information Systems to implement	Low	ICT/IS	low	Unknown	Staff Time	30-Jun-16			**Ongoing** - training options being considered
REC 28	Document Management - Removable Media	Unable to block the use of USB. Security to be addressed as part of Information Management Security policy suite	Low	IS	High	Unknown	Staff Time	30-Jun-16			**Not Applicable** - Will not be implementing this recommendation. Training referenced in Action 27 will incorporate guidance for use of USBs.
REC 29	Physical Security Stirling - Fire Detection	ICT to investigate - Further information on costing and risk analysis to be performed before acceptance of recommendation. AHC already has invested in multiple redundancy systems and questions the need for such a solution	Low	ICT	High	Unknown	Unknown Budget	30-Jun-16	31/12/16		**Ongoing -** Long term strategy is for Council to relocate systems to Datacentres with appropriate fire detection and suppression. Council will investigate costs for systems at Stirling and will assess the risk vs the remaining time equipment will be located here against cost.
REC 30	Physical Security Stirling - Power Management	ICT to action - Setup UPS alerting system	Moderate	ICT	low	1 Day	Staff Time	31-Dec-15			**Completed** - Implemented 4 monitoring systems to cover network monitoring (Cacti, nfsen, rancid and splunk)
REC 31	Physical Security Stirling - Physical Security	ICT to action - Lock cabinets and record the access to keys	Low	ICT	Low	1 Day	Staff Time	31-Dec-15			**Completed** - Access to Stirling Datacentre is logged by the Security System and cabinets are locked.
REC 32	Physical Security Woodside - Fire Detection	No Action - Capital Works Program in 2015/16 to relocate the Server Room to CBD		ICT				Nil			**Not Required due to relocation of Datacentre to CBD**
REC 33	Physical Security Woodside - Power Management	No Action - Capital Works Program in 2015/16 to relocate the Server Room to CBD		ICT				Nil			**Not Required due to relocation of Datacentre to CBD**
REC 34	Physical Security Woodside - Access Control	No Action - Capital Works Program in 2015/16 to relocate the Server Room to CBD		ICT				Nil			**Not Required due to relocation of Datacentre to CBD**
REC 35	Physical Security Woodside - Physical Security	No Action - Capital Works Program in 2015/16 to relocate the Server Room to CBD		ICT				Nil			**Not Required due to relocation of Datacentre to CBD**