ADELAIDE HILLS COUNCIL
AUDIT COMMITTEE MEETING
Monday 13 February 2017
AGENDA BUSINESS ITEM

Item:	**7.1**
Originating Officer:	**Lachlan Miller, Executive Manager Governance & Risk**
Responsible Director:	**Terry Crackett, Director Corporate Services**
Subject:	**ICT Security Assessment Action Implementation Update**
For:	**Decision**

---

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**
- **Director Corporate Services, Terry Crackett**
- **Executive Manager Governance & Risk, Lachlan Miller**
- **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.

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	Organisational Sustainability
Strategy	Governance

Monitoring the implementation of the actions arising from audits assists in meeting legislative and good governance responsibilities and obligations.

- **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 the first update on the status of actions arising from that audit was provided in August 2016.

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***).

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	Moderate	IS	Moderate	5 to 10 days	Staff Time	30-Jun-16	30-Mar-17	07-Feb-17	**Ongoing -** The first two policies have been completed and are with the Executive Leadership Team for comment prior to implementation.
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	28-Feb-17	07-Feb-17	**Ongoing** - ICT BCP is currently progressing well with 95% of the works completed. BCP Systems Recover Software has been purchased and is undergoing configuration and testing. Project to be
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	30-Jun-17	07-Feb-17	**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. This policy is still to commence
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	07-Feb-17	**Ongoing** - Linked to Rec 3 scheduled to be completed mid Feb 17
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-Dec-17	07-Feb-17	**Ongoing** - Investigations of software completed and to be included into budget process for 2017/18.
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-Dec-17	07-Feb-17	**Ongoing** - Investigations of systems completed and will be apart of new Microsoft License renewal process in October 2017.
REC 27	Personnel - Awareness and Education	ICT and Information Systems to implement	Low	ICT/IS	low	Unknown	Staff Time	30-Jun-16	30-Jun-17	07-Feb-17	**Ongoing** - training options being considered. Project to yet to commence
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	30-Jun-17	07-Feb-17	**Ongoing -** Long term strategy is for Council to relocate systems to Datacenters 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. Quoting process underway to receive indicative costs.