ADELAIDE HILLS COUNCIL
AUDIT COMMITTEE MEETING
Monday 22 February 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 Risk Assessment**
For:	**Information**

---

1. ICT Security Risk Assessment – 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**
- **Manager Governance & Risk, Andrea Sargent**
- **Manager ICT, James Sinden**
- **Manager Information Systems, Matt Strapps**
- **Manager Finance, Paul Francis**

be excluded from attendance at the meeting for Agenda Item 7.1: ICT Security Risk Assessment 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 – Confidential Item

SUMMARY

A high level review was undertaken to provide a level of assurance that the controls deployed relating to the confidentiality, integrity and availability of information within the organisation's ICT environment are appropriate. The review provided findings and recommended actions to address any observed gaps in Information Security management.

The purpose of this report is to present the results of the Adelaide Hills Council (AHC) ICT Security Risk Assessment, conducted by consulting firm CQR in August 2015 together with the AHC Management Response and Action Plan.

The report has 37 recommendations and suggested actions from CQR. Council's Manager ICT, James Sinden and Manager Information Systems, Matt Strapps have used council's risk management matrix to assess each of the issues addressed by the recommendations, with the resultant ratings ranging through High, Moderate and Low. A number of the nominated actions have been completed already and the majority of the remaining actions can be addressed within existing resources.

RECOMMENDATION

That the Audit Committee resolves:

1. **That the report and its attachments be received and noted**
2. **To monitor the implementation of nominated actions in response to the ICT Security Risk Assessment recommendations.**

3. **ICT Security Risk Assessment – Period of Confidentiality**
4. **That having considered the ICT Security Risk Assessment at Agenda Item 12.1 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 Committee and the discussion of the subject matter be retained in confidence until ICT Security Risk Assessment recommendations have been addressed and no longer than 12 months from the establishment of this order.**
5. **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.**
6. **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, or his sub-delegate.**

---

1. GOVERNANCE

- **Strategic Management Plan/Council Policy**

Goal 4	A Recognised Leading Performer
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 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)

The implementation of actions arising from the ICT Security Risk Assessment will assist in mitigating the risk of:

External parties (i.e. hackers) gain access to AHC servers leading to disruptions to AHC operations and/or loss of community confidence

Inherent Risk	Residual Risk	Target Risk
Extreme (5B)	Medium (3D)	Medium (3C)

➢ **Financial and Resource Implications**

The implementation of the Action Plan will have financial implications against certain items. A number of actions have and will be undertaken with current resourcing however, some actions require further resourcing as specified in the Management Response and Action Plan in Appendix 2.

➢ **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; and specifically that risks, including cyber security, are managed appropriately.

➢ **Environmental Implications**

Not applicable

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

External consultation was not applicable. Internal consultation has occurred with James Sinden, Manager ICT and Matt Strapps, Manager Information Systems.

2. BACKGROUND

The four year Strategic Internal Audit Program identified that an ICT Security Risk Assessment on Cyber Security be undertaken in 2015. The ICT Security Risk Assessment was conducted in August 2015.

Since the last internal audit quarterly update to the Audit Committee in November 2015 the report on the ICT Security Risk Assessment by CQR has been finalised and an Action Plan in response to the assessment findings has been developed.

3. ANALYSIS

The overall objective of the project was to undertake a high level risk assessment of AHC's ICT security posture across its key information systems. The risk assessment focussed on the external and internal risks and threats that could adversely impact the security of AHC's IT environment.

The scope included the following aspects of the AHC's IT environment:

- Policy and procedure
- Servers
- Applications
- Databases
- Network
- Workstations
- External access
- Wireless
- Mobile devices
- Personnel
- Document management
- Physical security

An external information security agency, CQR Consulting, undertook the ICT Security Risk Assessment. It should be noted that the assessment that they undertook was an abridged version of a standard Security Audit that they regularly undertake. Some areas were only given cursory consideration. Accordingly, the report is an abridged version of their standard CQR Security Audit offering and is not a complete comprehensive technical review of AHC's ICT environment.

The data in the CQR report was collected over a series of verbal interviews with James Sinden, Manager ICT and Nigel Scholz, ICT Coordinator and the examination of relevant documentation.

The report found that AHC has strong controls and security measures in place in many areas. Thirty seven (37) recommendations and suggested actions were identified by CQR. Council's Manager ICT, James Sinden and Manager Information Systems, Matt Strapps have used council's risk management matrix to assess each of the issues addressed by the recommendations, and assigned a priority based on its risk rating with the resultant priority ratings ranging through High, Moderate and Low. Realistic actions have been developed by management and an implementation complexity rating has also been assigned. The CQR report is presented in appendix 1 and the Management response and proposed actions to address system weaknesses is in appendix 2.

Of the 37 recommendations[1], 2 are disputed as information documented in the report is incorrect and 5 are (or will shortly be) considered redundant given recent activities. Examining the issues addressed by the 37 recommendations; three (8.1%) have been identified as high priority, eight (21.6%) as a moderate priority and the remainder are considered low priority.

Actions responding to 11 of the recommendations have been completed. The majority of the remaining actions can be addressed within existing resources, however, a small number are complex to implement and have potential for significant budget impact. Specifically, recommendations 30 and 34 would be quite complex to implement and offer little on-going benefit to the organisation. Recommendation 30 addresses logging and monitoring devices connected to our wireless network. The assessment identified that the wireless network has appropriate security and users are required to authenticate using their valid AHC username and password combination. This recommendation is an additional layer of monitoring that provides the same information that can currently be obtained from our systems while being extremely complex to implement technically. As such, it is believed that action is not required at this time apart from some low level monitoring with potential to review if required.

Recommendation 34 suggests blocking the usage of USB storage devices for all users. Management believes that this process is not as relevant now as it was in the past. It is technically very challenging to implement, as multiple devices use USB to connect; and this would not prohibit documents, data or information leaving the organisation. With the advent of large online file transfer services, such as DropBox there are many ways that data can be transferred that do not involve physical hardware. As such management recommends this be controlled by the Information Management Security Policy and ongoing user education.

Some of the recommendations have been made redundant; one due to the addition of the ICT Technical Services Coordinator role within the ICT Team. This role has seen AHC resource many aspects of the technical management of the network from external contractors to in-house. Regarding recommendations 39, 40, 41 and 42, council is currently undertaking an approved capital works program that will see the removal of the Server room at the Woodside office. As such there is no action required on these recommendations and they will shortly be redundant.

[1] (NB the report numbers recommendations up to 42, however, 5 recommendations were deleted prior to finalisation of the document, ie there are no recommendations numbered 15, 18, 19, 24 or 29.)

4. OPTIONS

The Committee has the following options:

I. To note the ICT Security Risk Assessment by CQR Consulting and the Management Response and Action Plan; and / or

II. To make comment or identify concerns and or potential amendments or additional actions.

5. APPENDICES

(1) ICT Security Risk Assessment – Report by CQR Consulting
(2) ICT Security Risk Assessment – Management Response and Action Plan

Appendix 1

Security Risk Assessment
Report by CQR Consulting

Security Risk Assessment

Adelaide Hills Council

PREPARED BY CHRIS MONTAUTI 10 FEBRUARY 2016 VERSION 1.2 FINAL RELEASE

CONFIDENTIAL

Document Control

Author	Chris Montauti
Issue Date	10-Feb-2016
Review Date	17-Aug-2015
Version	1.2 Final Release
Location	Adelaide
Description	Security Risk Assessment
Security Classification	Confidential

Date	Version	Description of Modification	Modified By
14/08/2015	1.0	Initial release to client	CM
18/01/2016	1.1	Client requirements	CM
10/2/2016	1.2	Client feedback	CM

Contents

1 Executive Summary

1.1 Introduction

CQR was engaged by Adelaide Hills Council to perform a broad, high level review of Adelaide Hills Council's security posture across its key information systems.

The high level review was designed to provide Adelaide Hills Council with a level of assurance that the controls deployed relating to the confidentiality, integrity and availability of information within the organisation's ICT environment are appropriate.

This review was conducted during August 2015 and this report presents the findings of the review and recommended actions to address any observed gaps in Information Security management.

1.2 Objectives and Scope

The objective of this review was to consider the security controls applied to the ICT environment and provide a gap analysis across the following IT domains:

- Policy and procedure;
- Servers;
- Network;
- Workstations;
- External Access;
- Wireless;
- Mobile devices;
- Personnel;
- Document management; and
- Physical security.

Detailed review of the council's information systems and running applications was out of scope for the review. This report summarises the identified gaps and potential areas of risk that have not been appropriately addressed and delivers recommendations to remediate those gaps.

1.3 Methodology

The methodology of the gap analysis was to review existing Adelaide Hills Council security controls relating to the objectives of maintaining confidentiality, integrity and availability of information systems. An interview with the key Council representative was undertaken to obtain an overall snapshot of the health of IT security management across the domains. Observations from the interview were analysed and overall gaps identified. Recommendations have been formed to remediate identified gaps and residual risk.

1.4 Findings

During this review a total of **35** gaps were identified, in a number of areas that relate to third parties, people, processes and technology across the organisation. In addition to the risk described above, the following gaps are the most critical to address:

- Lack of a formal Information Security Policy;
- Inadequate governance on third party contracts and Service Level Agreements (SLA) to ensure third parties use appropriate contractual and technical security controls to protect confidentiality, integrity and availability of Council data;
- Lack of a formal process for the logging and monitoring of user activity;
- No formal patching procedures;
- No policy to govern the use of mobile devices;
- Inadequate security awareness training for staff;

In order to address these gaps, the following recommendations should be implemented by Adelaide Hills Council:

- Develop an Information Security policy and additional security policies in order to provide overall governance of the environment;
- Ensure that data in transit via portable media is protected by a form of encryption to ensure the security of the data is protected. The council should also assess the storage of material within on-line services to ensure the protection offered meets the requirements of the council. Develop a Business Continuity Plan to ensure Council services can be recovered from disruption in a timely manner;
- Review third party contracts and SLAs to ensure they use appropriate contractual and technical security controls to protect confidentiality, integrity and availability of Council data.
- Develop a policy or procedure to regularly monitor user access and activities on the systems to reduce the risk of unauthorized access or change attempts;
- Define procedures to ensure systems are patched regularly and protected from malicious software;
- Develop a mobile device policy to govern the use of devices connected to the IT environment and ensure users understand the rules for using such devices;
- Conduct internal security awareness training to ensure security roles and responsibilities are known, and users are aware of current security threats.

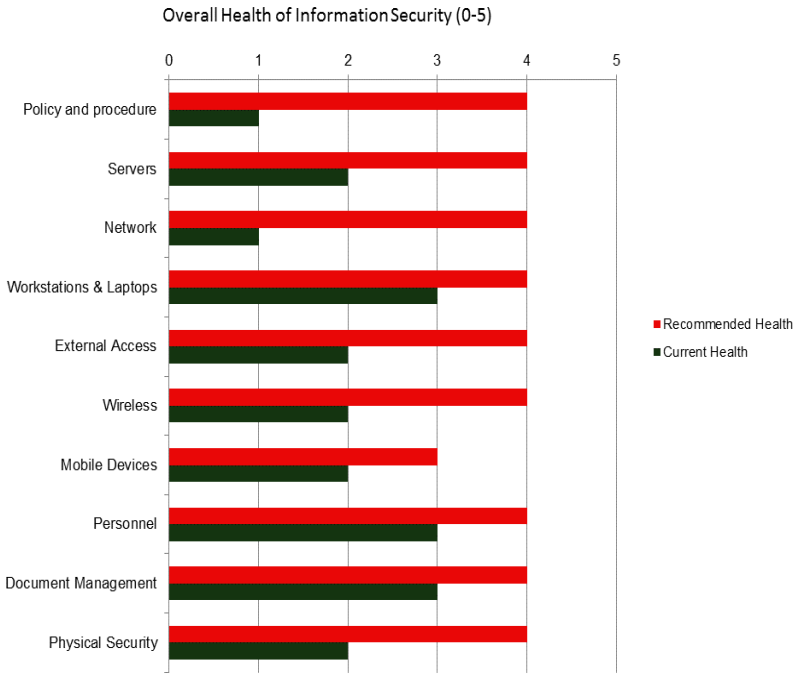
A vulnerability assessment scan was undertaken of the Adelaide Hills Council perimeter network and the report and findings were emailed to the IT Manager. The scan results were reviewed to determine if any systems presented a threat to the security of the internet perimeter. The results indicated that the vulnerability scans were being actively filtered by the firewall or other device resulting in false positive indications of exposed services and incomplete assessment of vulnerabilities due to connection resets. Adelaide Hills Council support staff were unable to resolve the issues to allow a scan to run to completion.

A penetration test of the internet perimeter was not undertaken at the request of Adelaide Hills Council. We recommend that the vulnerability scans be repeated as part of a penetration test and that penetration testing be conducted on a yearly basis and after any significant changes are made to the infrastructure supporting the internet perimeter.

1.5 Maturity Levels

The following graph highlights the current health of Information Security at the Adelaide Hills Council across the 10 domains, as compared to the recommended health of an organisation of similar maturity. In this graph, each area has been rated to the closest level that best describes the observations and findings gathered during the review. Process maturity levels are represented by a score between 0 and 5 which show the status of the internal controls established for each control objective.

0 Non-existent
1 Initial / Ad hoc
2 Repeatable but Intuitive
3 Defined Processes
4 Managed and Measurable
5 Optimised



2 Recommendations

To address the findings of this review we recommend that the identified gaps be addressed. The following recommendations are formed based on the identified gaps in Section 3.

Ref	Finding/Action
	POLICY AND GOVERNANCE
REC-1	Create an information security policy that supports the Councils business and security requirements.
REC-2	Create a procedure to ensure the risk register is reviewed regularly and newly identified risks are added when identified.
REC-3	Define a business continuity plan which includes a business impact assessment to identify the Councils' critical systems and applications to aid disaster recovery planning.
REC-4	The Council should create an incident management procedure.
	SERVERS
REC-5	The ICT team should have separate accounts to manage the servers and perform network administration.
REC-6	Configure the servers to send all logs to a central log management system to monitor alarms. The configured system should have the ability to alert the ICT team if any system hardware or security alerts occur.
REC-7	The Council should create a patch management policy along with a procedure for patch testing and deployment.
REC-8	The testing of the backups should be written into the backup policy and clearly defined when and how the backups should be tested. Once this is done a procedure should be created on how to accomplish the testing of the backups.
REC-9	Create a standard build guide which should be followed for all servers. Procedures for specific supporting roles should also be created to ensure servers in different security domains are hardened appropriately.
	NETWORK
REC-10	An access request form should be created to record and monitor who is using which accounts and when they are accessed.
REC-11	The Council should implement a monitoring tool which allows for real time statistics and monitoring. The tool should also allow for log collection to assist in trouble shooting and any forensic investigation if required.
REC-12 REC-21	A patch management policy for network devices should be created and adhered to by third parties. ICT should actively monitor the status of the network devices to ensure security patches are applied when needed.
REC-13	The network devices should be added to the Council backup policy. Backups should be taken of each device and tested on a regular basis.
REC-14	Create a configuration standard which must be applied to all Council network equipment.
	WORKSTATIONS AND LAPTOPS

Ref	Finding/Action
REC-15	Review the gold build image documentation to ensure that any changes and modifications to the guide are documented and traceable.
	EXTERNAL ACCESS
REC-16	ICT should be actively monitoring the firewall logs to ensure suspicious or malicious activity is being recorded. Logs for the firewall device and all devices within the DMZ should be stored on a syslog server for evidence and technical assistance when required.
REC-18	The Council should ensure regular backup of device configurations for devices providing external access. Backups should be tested as per the backup policy.
REC-17 REC-19	Periodic reviews of the firewalls should be conducted to ensure the management of the firewalls is being performed to a high standard and that configurations are consistent with Council's business requirements
	WIRELESS
REC-20	Conduct a review of the wireless installation to ensure the ICT have a good understanding of how the wireless integrates into the Council network. Implement a wireless monitoring procedure and actively monitor the network.
REC-21	The third party managing the network should adhere to the council backup policy for the network.
REC-22	A procedure should be created which highlights the requirements for patching and monitoring of the network. This should then be adhered to by the third party.
REC-23	Review the security settings on the network devices and ensure they meet the Council standards for security.
	MOBILE DEVICES
REC-24 REC-26	No active monitoring is conducted on the mobile device access. The council should look to deploy a mobile device management policy and procedure which will allow for active monitoring and allow for policy deployments.
REC-25	A patch management policy for mobile devices should be created.
	PERSONNEL
REC-27	Conduct internal security awareness training to ensure security roles and responsibilities are known, and users are aware of current security threats. Training can be delivered in the form of a presentation, walkthrough of policies and procedures, or online training with a quiz to ensure participants have understood the training content.
	DOCUMENT MANAGEMENT
REC-28	Consider restricting the usage of offline and Internet based storage of council documents, by: • enforcing encryption on all removable media devices; • restricting access to the on-line drive storage web sites and; • educating users of the concerns of documents being stored on non council approved device.
	PHYSICAL SECURITY
REC-29 REC-32	Perform a risk assessment of not implementing a fire suppression system for both server rooms.

Ref	Finding/Action
REC-30 REC-33	Install the UPS management software to allow monitoring and alerting of the UPS status. Clearly label the mains isolator in the computer room at the Sterling site.
REC-31 REC-35	All panels on cabinets should be attached with the unit locked. The keys for the cabinets should be stored in secure location with access to the keys recorded.
REC-34	Woodside server room should have the access pin changed periodically and knowledge of the pin should be limited to management. The server room door should be replaced with an approved door with a fire rating. The cabinets in the room should have the panels fitted. The keys for the cabinets should be stored in secure location with access to the keys recorded.
REC-35	The windows in the room should be fitted with security bars to protect entry from the window. The access door should be replaced with an approved fire and security door.

3 Identified Gaps

Each of the review sections will be addressed in detail with reference to overall recommendations for improvement.

3.1 Policy and Governance

Security management controls including, overall governance and risk management and business continuity planning and security incident response.

Control Area	Result	Observations
Information Security Policy	REC-1	There is no formal Information Security Policy which acts as the driver for Information Security and defines management's objectives and requirements for Information Security.
Risk Management	REC-2	There is a risk register to capture Council risks however this is not actively maintained and updated.
Business Continuity Planning	REC-3	There is no formal Business Continuity Plan (BCP) to allow timely recovery and restoration of business functions in the event of a disruption or disaster. Disaster recovery testing is performed in an ad-hoc manner.
Incident Management	REC-4	There is no formal incident management procedure to properly detect, investigate, and report all security incidents and weaknesses.

3.2 Servers

Servers provide a platform for the operation of applications and databases. This section covers security controls supporting servers including, access controls, commissioning of hardware, backup, support, configuration, antivirus, patching, and physical security.

Control Area	Result	Observations
Access Control	REC-5	Access to the servers is controlled by the ICT team, all members of the team have domain administrator permissions. This places the systems at risk if an ICT account was compromised. ICT users should have standard domain account for everyday use and a privileged account for administration work. External access is governed by the use of Active Directory, access is enabled when required to internal systems. However the use of shared accounts is being utilised by vendors. An access request form should be created to monitor who is using the account and when.
Monitoring and Logging	REC-6	The server logs are monitored on an ad-hoc basis for security or system errors. The reviewing of the logs is in a reactive manner. No active monitoring of internal servers is being undertaken. A logging and management system should be implemented to assure the integrity of the systems along with the availability.
Vulnerability Management	REC-7	Anti-virus is installed on all servers and is updated regularly. Patching of the servers is done on an ad-hoc basis and is run manually on the servers. No specific schedule is defined or process in place to maintain the level of patches for server operating systems.
Backup & Recovery	REC-8	The backup procedure is technically adhering to best practice. Backups are written to disk and then backed up to tape at the end of the month. The backup testing is performed on an ad-hoc basis and is not documented and no procedure exists to follow or stipulate the requirements for the testing.
Configuration Management	REC-9	The Council has accumulated various build notes but no official build standard exists along with a server hardening guide based on the server requirement. Create a standard build guide which should be followed for all servers. Procedures for specific supporting roles should also be created to ensure servers in different security domains are hardened appropriately.

3.3 Network

Networks provide interconnections between computer systems and phones throughout the organisation. From a security perspective, network security controls provide perimeter protection from the internet and protect assets from unauthorised access. Network security controls include device configuration, network architecture, physical location of equipment, patching and maintenance, change management, and third party supplier management.

Control Area	Result	Observations
Access Control	REC-10	Third party access to network equipment is controlled via enabling access via Active Directory. The ICT department have access to the devices however this is seldom used as all work on network equipment is carried out by third parties.
Monitoring and Logging	REC-11	No active monitoring or logging of network devices is performed for Council devices.
Vulnerability Management	REC-12	The Council does not apply vendor patches to network devices, although the external network is managed by a third party no knowledge is known if the devices are patched or running the latest versions of software.
Backup & Recovery	REC-13	During the interview it was stated that the Council have no backup of network devices. The network devices should be added to the Council backup policy. Backups should be taken of each device and tested on a regular basis.
Configuration Management	REC-14	No device standards or hardening guides are available for network devices.

3.4 Workstations and Laptops

Workstations and laptops are a primary method for users to connect to IT applications and the internet. Workstation and laptop security controls include access controls, configuration management, backup, support, antivirus, patching, and physical security.

Control Area	Result	Observations
Access Control	N/A	No Council user has local administrator access on any devices.
Monitoring and Logging	N/A	Access to council desktops is via VMware Horizon client which is then governed by Active Directory.
Vulnerability Management	OK	Anti-virus is installed on all devices and is updated regularly.
Backup & Recovery	N/A	The VDI desktop image is cloned from the Gold image and deployed to the relevant pools.
Configuration Management	REC-15	The Council operates a Gold disk image model which in-turn allows for cloning of the image and deployment specific changes per department if required. The build documentation is not consistently updated to reflect all changes to the Gold disk image as part of change and configuration management.

3.5 External Access

External access provides convenient access to IT resources from anywhere. External access also provides a potential attack vector for unauthorised users to access internal network and information. This section covers controls relating to access, patching, monitoring and logging.

Control Area	Result	Observations
Access Control	OK	Access to internal resources is via VMware Horizon client, and is controlled by Active Directory. All third party access is disabled until required. ICT have the ability to VPN into the Council network.
Monitoring and Logging	REC-16	No monitoring of the external access or services is done by ICT, firewall logs are not checked for any suspicious traffic or system alerts. ICT should be actively monitoring the firewall logs to ensure no suspicious or malicious activity is be recorded. Logs for the firewall device and all devices within the DMZ should be stored on a syslog server for evidence and technical assistance when required.
Vulnerability Management	REC-17	The Council has no knowledge of the patching level of the appliances providing external access.
Backup & Recovery	REC-18	No known backups have been taken of the appliances providing external access.
Configuration Management	REC-19	The firewalls governing the external access are supported by a third party which the Council rely on for configuration management.

3.6 Wireless

Wireless networking controls including configuration, usage policy, and maintenance.

Control Area	Result	Observations
Access Control	OK	Access to the Council wireless is protected by the use of Certificates, Radius and Active Directory. A public network is available for library users and is segregated from the Council network.
Monitoring and Logging	REC-20	No active monitoring or logging is being conducted by the ICT team. ICT do not monitor for rogue devices and are unsure if the network has this ability enabled.
Vulnerability Management	REC-21	No patch management is done on the network and ICT are unsure of the level of patching. A third party is responsible for maintaining the network. The council should request information from the third party on the patching standards and policies they apply to the network.
Backup & Recovery	REC-22	ICT are unaware if the network devices are backed up. The third party managing the network should adhere to the council backup policy for the network.
Configuration Management	REC-23	The network was installed by a third party and handed over to the council.

3.7 Mobile Devices

Adelaide Hills Council provide staff with Windows and Apple devices for remote communications.

Control Area	Result	Observations
Access Control	OK	Access to Council email is provided by OWA, this is governed by Active Directory.
Monitoring and Logging	REC-24	No monitoring of the devices is taking place.
Vulnerability Management	REC-25	No active patching of mobiles devices is currently in place.
Backup & Recovery	OK	Mobile devices pull information from Council servers, all data is therefore stored on Council servers.
Configuration Management	REC-26	The Council has no ability to control the devices which connect to the internal network.
Device Security	OK	The Council has the ability to remote wipe devices and block sims if the devices are lost or stolen.

3.8 Personnel

Given personnel have access to all manner of sensitive information to perform their roles, security controls must be appropriately deployed. Personnel security includes employee screening, employee contractual obligations, induction processes and security education and awareness.

Control Area	Result	Observations
Terms of Employment	OK	There are reference checks for employees, along with police checks for all staff working with children.
Induction	OK	There is a formal process for the induction of employees and it is slightly different for volunteers and temp staff.
Termination	OK	A disciplinary procedure is in place for the Council. When the Council is made aware a member of staff is leaving an exit checklist is emailed to the line manager and the member of staff. This list stipulates the exit process for equipment and staff network access.
Monitoring	OK	Internet activity is logged via the TMG server and if logs are required reports can be ran for user activity
Awareness and Education	REC-27	ICT have a one on one with new staff members where they are required to sign a computer usage agreement. No active awareness and education program is being performed by the ICT team.

3.9 Document Management

Document management security controls include documentation management systems, physical security, and policy frameworks supporting the protection of organisational information assets.

Control Area	Result	Observations
Access Control	OK	Access to documents is controlled by job role and Active Directory.
Removable Media and Cloud Based Storage	REC-28	The use of removable media is allowed within the council. The council has reviewed the risk and accepted this as a low risk. The use of cloud based storage solutions such as Dropbox and OneDrive is available to council staff via the Internet; however, no controls were enforced to identify or control acceptable usage of these services. The use of cloud based services for the storage and transmission of Council documents should be reviewed to ensure it is compliant with Council policy and that appropriate controls are implemented.
Physical Security	OK	There is a fire proof records and document room at the Woodside site. Many documents (including originals and only copies) are stored across the organisation, in offices and general shared areas. Backup media are stored in the fireproof safe and offsite; however, it was not clear if supporting documents required as part of the business continuity plan were also stored securely in this location. Adelaide Hills Council is aware of the risk posed to documents outside of these areas and have identified the risk in the Risk Register. We recommend that ICT related documents and media required as part of the business continuity plan are stored in the fire proof records and document room at Woodside and copies kept offsite.

3.10 Physical Security Sterling

The methodology used for examining the physical security is to inspect the site and review each of the controls that are used to lower risk. The controls examined are based on industry best practice and COBIT.

Control Area	Result	Observations
Fire Detection	REC-29	The server room is protected by a smoke detector and thermal detection equipment. This is centrally monitored by the Council fire security system. A CO2 fire extinguisher is located in the server room and is clearly marked if required. The access door to the server room is rated for 2hrs of fire prevention. The server room is not protected with a fire suppression system and places the equipment within the room at risk.
Power Management	REC-30	The equipment within the room is monitored by a Libert UPS device. This has the ability to power all devices within the room and is backed up via a site generator. If power was to fail the UPS would allow for sufficient power to the equipment until the backup generator took over power. The UPS has the ability to send alerts and status emails to a monitoring address and if required shutdown systems in a graceful manner. These options are currently not configured and the reliance of the building power alarms is a risk to the Council. Along with this the main power isolator for the room is not clearly labelled and is not locked.
Air-conditioning	OK	The room has adequate environmental controls. The room is running on the building air conditioning which is regularly maintained. A second unit is mounted on the wall for backup and is set to take over if the temperature rises to 25 degrees. Both systems have redundant power supplied by the building generator if mains power was lost to the room.
Access-Control	OK	Access to the room is provided by a key fob system and is only granted to ICT and building management. All access to the room is logged by the building security system and can be referenced to for logs. If a third party requires access to the room they are escorted by a member of the ICT staff at all times.
Physical Security	REC-31	The server room is not identified by any signage, and no security cameras are in use to monitor the door or the room itself. All racks within the room where found to be open and the keys located in the lock, a number of cabinets have the sides missing which allow direct entry to the devices held within. The Council backups are stored off site and are collected by a third party.

3.11 Physical Security Woodside

The methodology used for examining the physical security is to inspect the site and review each of the controls that are used to lower risk. The controls examined are based on industry best practice and COBIT.

Control Area	Result	Observations
Fire Detection	REC-32	The server room is protected by a smoke detector and is centrally monitored by the Council fire security system. A CO2 fire extinguisher is located outside the server room and is clearly marked if required. The server room is not protected with a fire suppression system and places the equipment within the room at risk.
Power Management	REC-33	The equipment within the room is monitored by a Libert UPS device. This has the ability to power all devices within the room and is backed up via a site generator. If power was to fail the UPS would allow for sufficient power to the equipment until the backup generator took over power. The UPS has the ability to send alerts and status emails to a monitoring address and if required shutdown systems in a graceful manner. These options are currently not configured and the reliance of the building power alarms is a risk to the council.
Air-conditioning	OK	The room is cooled by one standard office split unit which is connected to building power and is able to run on the backup generator if mains power fails. The unit is serviced every six months along with the building system.
Access Control	REC-34	Access to the room is provided by a simplex door lock which requires a code to enter. This code is commonly known within the building and has not been changed for a number of years. The door to the room is a standard office, containing a sheet of glass. Any third party requiring access is escorted by a member of the ICT team.
Physical Security	REC-35	The server room is not identified by any signage, and no security cameras are in use to monitor the door or the room itself. The racks within the room where found to be open and the keys located in the lock. The glass in the door is not re-enforced and could be easily smashed. The room itself has windows which are not re-enforced and would not require force to break. The room is monitored by the building alarm.

Appendix 2

ICT Security Risk Assessment
Management Response and Action Plan

AHC INTERNAL AUDIT - ACTION REPORT

Ref	Issue/*Recommendation*	Response/*Proposed Action*	Priority	Responsible Department	Status	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. 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			
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	31/6/2016			
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 within current budget	30-Jun-16			
REC 4	Policy and Governance - Incident Management	ICT to action - create a security incident management procedure	Moderate	ICT		low	1 week	Staff Time	30-Jun-16			
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-Mar-16			
REC 6	Servers - Monitoring and Logging	ICT to action - Project to identify a technology solution to Logging	Moderate	ICT	Completed	Low	1 Week	Unknown	31-Dec-15			
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	31/6/2016			
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			
REC 9	Servers - Configuration Management	ICT to action - prepare a standard server build guide and template	Low	ICT		Medium	1 week	Staff Time	30-Jun-16			
REC 10	Network - Access Control	ICT to action - implement a procedure for logging of access to systems by external contractors	Low	ICT		low	3 Days	Staff Time	31-Mar-16			
REC 11	Network - Monitoring and Logging	ICT to action - expand on already implemented monitoring system (Site24x7) to report on all network systems	Moderate	ICT	Completed	Low	2 weeks	Staff Time	31-Dec-15			
REC 12	Network - Vulnerability Management	ICT to action - Document network devices and patch level and compliance	Low	ICT	Completed	Low	2 days	Staff Time	31-Dec-15			
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	Completed	Low	2 days	Staff Time	31-Dec-15			
REC 14	Network - Configuration Management	ICT to action -	Low	ICT	Completed	High	unknown		30-Jun-16			
REC15	No recommendation	Nil										
REC 16	Workstations and Laptops - Vulnerability Management	ICT to action - Patching on devices needs to be scheduled as apart of a wider proactive maintenance schedule	Low	ICT		Low	3 Days	Staff Time	31-Mar-16			
REC 17	Workstations and Laptops - Configuration Management	ICT to action - Create a build guide for the hardening of the Virtual Desktop	Low	ICT		Low	1 Week	Staff Time	31/6/2016			
REC 18	No recommendation	Nil										
REC 19	No recommendation	Nil										
REC 20	External Access - Monitoring and Logging	ICT to action - implement a syslog server to capture firewall logs	Moderate	ICT	Completed	High	1 Week	Staff Time	30-Jun-16			
REC 21	External Access - Vulnerability Management	ICT to action - Document network devices and patch level and compliance	Low	ICT	Completed	Low		Staff Time	31-Dec-15			
REC 22	External Access - Backup and Recovery	Incorrect - Backups are taken of our ASA appliance										
REC 23	External Access - Configuration Management	ICT to action - Implement a review of firewall configuration	Low	ICT	Completed	Low	4 Weeks	Staff Time	31-Dec-15			

Ref	Issue/*Recommendation*	Response/*Proposed Action*	Priority	Responsible Department	Status	Complexity to action	Estimated Hours to implement recommendation	Estimated Budget to implement recommendation	Due Date	Revised Date	Date of Update	Progress/Comment
REC 24	No recommendation	Nil										
REC 25	Wireless - Monitoring and Logging	ICT to review - highly complex to resolve with little benefit.	Low	ICT		High	4 Weeks	Staff Time	31-Mar-16			
REC 26	Wireless - Vulnerability Management	NA no longer relevent as its being managed inhouse										Now being supported in house with the addition of the new position.
REC 27	Wireless - Backup and Recovery		Low	ICT	Completed	Low	4 Weeks	Staff Time	31-Mar-16			
REC 28	Wireless - Configuration Management	ICT to Action - Capital Works Program for 2015/16 to review the wireless network	Low	ICT	Competed	Low	4 Weeks	Staff Time	31-Mar-16			
REC 29	No recommendation	Nil										
REC 30	Mobile Devices - Monitoring and Logging	ICT to monitor and review if necessary	Low	ICT		High		Staff Time	30-Jun-16			
REC 31	Mobile Devices - Vulnerability Management	ICT to implement a proactive patching schedule for Mobility Devices	Low	ICT		Low		Staff Time	30-Jun-16			
REC 32	Mobile Devices - Configuration Management	ICT to implement - review the MDM solution in place and implement recommendation	Low	ICT		High	4 Weeks	Staff Time	30-Jun-16			
REC 33	Personnel - Awareness and Education	ICT and Information Systems to review recommendation with Oganisational Development	Low	ICT/IS		low	Unknown	Staff Time	30-Jun-16			
REC 34	Document Management - Removable Media	Unable to block the use of USB. Security to be addressed and managed as part of Information Management Security policy	Low	IS		High	Unknown	Staff and Contractor Time & within current Budget	30-Jun-16			
REC 35	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	High	ICT		High	Unknown	Further investigation - cost benefit anakysis - Staff time Unknown Budget to address recommendation	30-Jun-16			
REC 36	Physical Security Stirling - Power Management	ICT to action - Setup UPS alerting system	Moderate	ICT	Completed	low	1 Day	Staff Time	31-Dec-15			
REC 37	Physical Security Stirling - Physical Security	ICT to action - Lock cabinets and record the access to keys	Low	ICT		Low	1 Day	Staff Time	30-Jun-16			
REC 38	Physical Security Woodside - Fire Detection	No Action - Capital Works Program in 2015/16 to relocate the Server Room to CBD		ICT					Nil			
REC 39	Physical Security Woodside - Power Management	No Action - Capital Works Program in 2015/16 to relocate the Server Room to CBD		ICT					Nil			
REC 40	Physical Security Woodside - Air-conditioning	To be removed as this is incorrect		ICT					Nil			
REC 41	Physical Security Woodside - Access Control	No Action - Capital Works Program in 2015/16 to relocate the Server Room to CBD		ICT					Nil			
REC 42	Physical Security Woodside - Physical Security	No Action - Capital Works Program in 2015/16 to relocate the Server Room to CBD		ICT					Nil			