CONFIDENTIAL

Note: Confidential Provisions released on 03/02/2021

REPORT FOR:	**Audit Committee**		
MEETING DATE:	18 August 2020		
REPORT FROM:	Director City Services		
REPORT TITLE:	**Auditor General Cyber Security Audit Draft Report**		
FILE NAME:	F20/204	RECORD NO:	AR20/36002

STRATEGIC DIRECTIONS	
5	**Governance and Financial Sustainability**
5.5	We meet or exceed legislative and accreditation requirements for all relevant programs.

SUMMARY/ABSTRACT

The purpose of this report is to provide the Audit Committee with a copy of the Draft Audit Report, including Council's response, in relation to the Cyber Audit Process that Council has been required to participate in, by the State Government Auditor General.

RECOMMENDATION

Audit Committee recommends Council receives and notes the report (AR20/36002) dated 10/08/2020, submitted by the Director City Services in relation to the Auditor General Cyber Security Audit Draft Report.

BACKGROUND

In December 2019, Council was informed that Port Augusta City Council had been randomly selected to be subject to an Audit for 'Examination of the cyber security within Local Government' by the State Government Auditor General, under the Public Finance and Audit Act 1987. The audit was undertaken both on site and externally between December 2019 and February 2020. The Audit was conducted on two metropolitan and one regional Council.

Reports have been provided to the Audit Committee with progress of this audit process, in February and May 2020.

DISCUSSION

Draft Report

The Audit reviewed Council's security governance arrangements, system security, change management processes and backup operations and disaster recovery. A draft report was first received in early May and Council has been provided with an opportunity to correct any factual inaccuracies as well as proving some additional comments to provide context to some of the findings. The final draft report has now had a formal response from Council included, and is being presented to Council and the Audit Committee for noting. The Draft Report is attached for Members information.

The completed report will be submitted to Parliament later in the year. The Auditor General has requested that all information in relation to the Audit is to be retained in confidence until such time as the final report is tabled in Parliament.

Audit Committee was previously advised of the 16 findings made, as detailed in the attached report. Ten of these will be addressed with the formalisation and adoption of Policies and Procedures or changes to other documentation that evidence the current arrangements. For many of these findings we already have the systems and processes in place however we were able to demonstrate this as they are not formally documented. For the remaining 6 findings, Council will provide further training and review the physical and electronic access to accounts and systems. Reports on the progress against these findings will continue to be provided to the Audit Committee.

CONFIDENTIALITY PROVISIONS

The Council is satisfied that, pursuant to Section 90(3)(j) of the Act, the information to be received, discussed or considered in relation to this Agenda Item is information the disclosure of which would divulge information provided on a confidential basis by a public authority - Auditor General. It is considered that the open discussion in relation to the Audit, the disclosure of which would breach the Council's obligation to maintain confidentiality, should be considered under confidential provisions.

In addition, the disclosure of this information would, on balance, be contrary to the public interest. The public interest in public access to the meeting has been balanced against the public interest in the continued non-disclosure of the information. The benefit to the public at large resulting from withholding the information outweighs the benefit to it of disclosure of the information. The Council is satisfied that the principle that the meeting be conducted in a place open to the public has been outweighed in the circumstances because the disclosure of the Audit information may severely prejudice Council's Cyber Security and breach confidentiality requirements imposed by a public authority.

Having considered this agenda item in confidence under Section 90(2) and (3)(j) of the Local Government Act 1999, the Council, pursuant to Section 91(7) of that Act orders that report (AR20/20999), discussions and minutes be retained in confidence for a period of 12 months or until such time as advice is received from the Auditor General that the information can be released, and that this order be reviewed every 12 months.

RISK MANAGEMENT

1: Financial/Budget/Asset Management
Council's Information Systems budget includes provisions for the ongoing security, maintenance and upgrade of Council's IT systems and applications.

2: Legal/Policy
The Auditor-General conducted this examination under section 32(1)(a) of Public Finance and Audit Act 1987.

3: Environment/Planning
Not applicable.

4: Community
Council is committed to ensuring the security of all electronic systems and applications, to ensure the ongoing provision of services to the community, and to protect the personal information held within those systems.

Melissa Kretschmer
10/08/2020

1. Executive summary

1.1 Introduction

South Australia has 68 councils that govern and manage their local areas in accordance with the *Local Government Act 1999* (LG Act). Each council is primarily accountable to its community for the use of public money and its performance in providing services and carrying out various activities.

Information Communication Technology (ICT) systems play an important role in assisting the day to day operations of each council and providing services to their ratepayers.

Strong cyber security controls are important for Councils to deliver on their commitment to protect their community, employees and operations from cyber threats. Due to the operational and personal nature of the information handled in the council environment, cyber security is an important area of inherent risk that must be managed.

Avoiding disruption to operations from ransomware, maintaining integrity of operational technology systems and protecting personal information and commercial data are vital for the Port Augusta City Council (the Council) to be able to deliver its services securely while also maintaining the public's trust. As the community demands greater connectivity and more personalised interactions, cyber security is no longer 'nice to have', it is simply expected.

In this Report we sought to understand the cyber maturity of the Council's ICT environment and to examine whether the Council effectively managed its ICT resources through appropriate internal controls. These controls are needed to mitigate cyber security and technology risks within the Council.

We examined whether the Council has established and adhered to appropriate processes and structures for managing cyber security, including security governance, system security, change management, backup operations and disaster recovery. Our examination also involved a website vulnerability assessment of the Council's external facing website and associated webserver(s) which is hosted and managed by the Local Government Association (LGA).

Our examination testing was conducted over the December 2019 to March 2020 period.

This Report refers to several technical terms. For additional details refer to Section 9 "Abbreviations and explanation of terms used in this Report".

1.2 Conclusion

<<To be completed once the procedural fairness process has been finalised. Conclusion will take into consideration the council's response to our findings and recommendations>>

1.3 What we found

<<Will be summarised once draft findings and recommendations have been discussed with the Council >>

1.4 What we recommended

<<Will be summarised once draft findings and recommendations have been discussed with the Council >>

1.5 Response to our recommendations

Council welcomes the external review of systems and processes to ensure that our practices meet current industry standards and to mitigate any risk to the organisation.

Council appreciates the open flow of information and communication with the Auditors throughout the process, which has allowed Council the opportunity to mitigate and address any organisational risk in a timely manner.

As this Audit was done as a point in time assessment, Council has since made significant progress and changes to enhance the Cyber Security systems and processes both during and after the formal Audit process.

The Local Government sector does not have mandatory cyber security arrangements, such as ICT control frameworks or standards for providing ICT services. Whilst it is acknowledged that there are minimum security standards that must be maintained, a standard compliance framework should take into account the size of the Council, the available resources and level of risk. It may be appropriate within the Local Government context to implement a tiered approach.

An additional factor for Council is the financial context in which we currently operate. Any increase in resourcing to ICT services comes at a direct cost to other community services, and impacts upon the service expectations of the community.

The Local Government Association and Local Government Risk Services have acknowledged the increased cyber risk in recent years. Council has accessed several funded programs including the 'Cyber Vulnerability Program' fully funded cyber audit, and has provided the Fraud and Cyber Awareness Training to Council staff.

Council has been quick to respond to the findings that have been made, and many of these are being addressed with the formalisation and adoption of Policies and Procedures or changes to documentation to provide formal evidence of the current arrangements that are in place. Council will also provide further training to staff and review the physical and electronic access to accounts and systems.

Council is committed to ensuring the security of all electronic systems and applications, to ensure the ongoing provision of services to the community, and to protect the personal information held within those systems.

2. Background

2.1 Cyber security overview

Cyber security is the practice of protecting networks, computer systems and data from unauthorised access or malicious attack.

Councils provide a valuable service to the public through their multiple ICT systems. The Parliament and the public would expect councils to have clear plans and strategies to maintain a reasonable level of security controls applied to their ICT services proportionate with the Council's risks. Achieving and maintaining appropriate cyber security arrangements of these ICT systems is important to protect sensitive information, including the public's personal data.

A report from the global professional services firm AON titled '2018 Risk Report – A focus on Local Government'[1] indicated that cyber security was a top 4 risk to the Australian Local Government sector.

The South Australian Government maintains its own Cyber Security Framework. It provides Government agencies with direction and guidance through an approach for establishing, implementing, maintaining, and continually improving their cyber security controls. This framework was developed with Government agencies to help them implement cyber security measures that are deemed appropriate for their risk profile.[2]

The Local Government sector does not have any mandatory cyber security arrangements, such as ICT control frameworks or standards, in providing ICT services. Despite the lack of a mandatory framework and standards, individual councils should have developed ICT control policies and procedures outlining expected basic controls. We consider that key reference sources and better practice guides for examining the effectiveness of cyber security are:

- the South Australian Cyber Security Framework
- guides developed by the Federal government's Australian Signals Directorate (ASD).

We acknowledge that some councils relate with each other to get a better understanding of ICT activities, trends and controls. But largely there are opportunities to increase across-sector ICT communications.

South Australian Councils, together with the Local Government Association of South Australia (LGA) and Regional Local Government Association should consider its position moving forward regarding cyber security direction and guidance and sector ICT communications.

---

1 Refer to https://www.aon.com.au/australia/local-government/files/risk-report-for-local-government-2018.pdf, viewed 30 April 2020.

2 Refer to https://www.dpc.sa.gov.au/responsibilities/protective-security-framework/cyber-security, viewed 12 March 2020.

2.2 Cyber security questionnaire

In July 2019, we sent a letter to all South Australian councils[3] requesting a response to a high-level questionnaire regarding each council's ICT environment and security arrangements. The purpose of this questionnaire was to get a better understanding of ICT arrangements and challenges within the local government sector.

We were pleased by the 100% response rate to this questionnaire.

Councils' responses, understandably, varied with respect to the level of detail that was provided for each question. We have accordingly applied a degree of interpretation. We did not assess the accuracy of the responses provided and provided no assurance as to the cyber security arrangements across local government nor individual councils as a result of this questionnaire.

In September 2019, a high-level summary of questionnaire responses and observations was provided to all Councils, the LGA and Local Government Risk Services (LGRS). We encouraged council's management to discuss the high-level observations in the context of its overall ICT cyber security maturity and risk profile.

Questionnaire responses suggested that councils use a broad range of ICT systems. These systems are either managed by each councils' internal ICT support team and infrastructure or through the engagement of external support and hosting arrangements (including hosting in a Cloud environment).

Other observations from the questionnaire included:

- completing ICT projects within time, budget and with the required functionality, limited IT resources and upgrading legacy systems were the top three ICT challenges
- spear phishing, malware, and ransomware were the top three cyber security threats
- 40 councils (60% of the total) reported that they had experienced a cyber security threat in the past 2 years. Of these 40 councils, 7 (10% of the total) reported that they had experienced a cyber security incident over the past 2 years
- 25 councils (37% of the total) were either still developing or did not have a formal ICT risk register
- 13 councils (20% of the total) were either still developing or did not have a formal risk treatment plan
- ICT operational and support resources, improving ICT security controls, documenting policies and procedures and upgrading legacy system/hardware were nominated as the top areas of focus if extra funding was provided to councils' ICT budgets
- 20 councils (30% of the total) had not conducted an independent ICT security assessment in the last 2 years or had plans to do so.

[3] Except for the District Council of Coober Pedy. We have previously examined ICT arrangements for this council.

Responses to our questionnaire did generally indicate that the local government sector was proactively working towards performing independent ICT security assessments. 47 councils (70% of the total) had either planned, were in-progress or have had independent ICT security assessments conducted.

The questionnaire also indicated that many councils had participated in a voluntary risk mitigation program by the LGA. This program involved assessing participating council's ICT vulnerabilities against the Essential Eight[4] and/or to conduct some penetration testing through an independent security vendor.

2.3 Port Augusta City Council

2.3.1 Overview

The Council area covers over 1,150 km^2 with a population of almost 14,000 people. The area surrounds the northern tip of the Spencer Gulf, with the region extending from the foothills of the Flinders Ranges in the east to the Whyalla Council and Lincoln Gap in the west. It is located approximately 320 kilometres north of the state capital, Adelaide.[5]

[4] In August 2017, the Commonwealth Government through the Australian Cyber Security Centre (ACSC), developed a strategy to mitigate potential cyber security incidents. While no single mitigation strategy guarantees the prevention of cyber security incidents, entities were encouraged to implement eight essential mitigation strategies as a baseline. This baseline, known as the "Essential Eight", reduces the opportunity for adversaries to compromise systems and inappropriately gain access to data.

[5] Taken from the Council website, https://www.portaugusta.sa.gov.au/home, viewed 21 April 2020.

The Council provides a diverse range of community services. These include:

- childcare
- tourism facilities,
- parks and gardens, ovals and sporting facilities
- beach, foreshore and levy bank management
- airport and cemeteries management
- environmental health services and horse stables
- events, art galleries and performance centres
- Aboriginal community development
- drug and alcohol management services
- library and information services
- roads, footpaths and street lighting
- waste, recycling and organics collection.

Some of the above Council services are not generally provided by other councils within South Australia, notably the management of the local airport.

The Council is also responsible for a range of administrative type services, such as town and building planning and development, rates administration, human resources, governance, records management and dog and cat management.

2.3.2 Council challenges

The Council advised that they have been through a period of significant economic downturn in recent years, following the closure of the Port Augusta Power Station and the delay in commencement or failure of several renewable energy projects. This has resulted in job losses and has increased financial stress within the community.

2.3.3 Budget

Council has reported an underlying operating deficit in its audited financial statements for some time and has focussed on reducing this through its service level reviews and long-term financial plan break even targets.

The Council reported an operating deficit of $1.27 million in 2018-19. It recorded a surplus of $2.23 million in 2017-18. The Council advised this was mainly attributed to a one-off receipt of $3.1 million received from the sale of assets linked to aged care facilities. During 2017-18 the Council also confirmed that they incurred operational expenditure for the aged care facilities from 1 July to 1 November which influenced other areas of operating income and operating expenditure (additional employee costs, grant and subsidies funding).

Figure 1 and 2 below display the Council's sources of income and expenditure incurred to deliver services to the local community in the past two financial years[6].

[6] Data sourced from the Council's audited financial statements for the year ended 30 June 2018 and 2019.

Figure 1: Sources of income and expenditure incurred in 2018-19

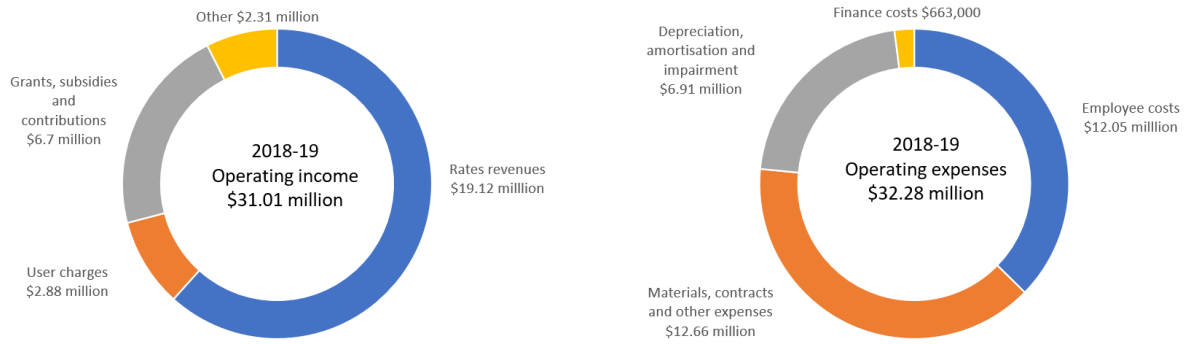
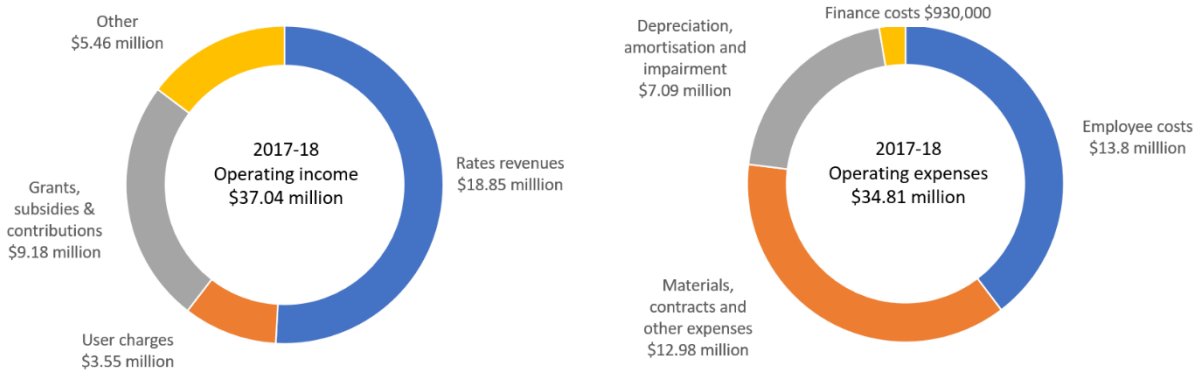


Figure 2: Sources of income and expenditure incurred in 2017-18



The Council's ICT spend for 2018-19 was $1.02 million, which was down slightly from 2017-18.

In 2019-20, the Council has allocated $1.23 million to ICT, split between operating expenditure ($1.12 million) and capital expenditure ($110,000).

The ICT spend amounts above include wages and on-costs, software licenses and upgrades, leases, internet and data costs, purchase of equipment and depreciation.

2.3.4 Information Communication Technology

The Council employs 183 staff (134 full time equivalent) of which the Information Technology (IT) team consists of four members. An Information Systems and Records manager leads this team and has primary responsibility for information security management. This incorporates providing the community with the ability to interact with the Council electronically[7].

The IT team performs a range of critical functions to provide support, management, and control of the Council's multiple computer systems (ICT applications and hardware).

[7] Refer to the Port Augusta Annual Reports for 2018-19 and 2017-18.

Activities undertaken include maintaining and upgrading Council websites, software applications, information databases and hardware.

The Council indicated that most of the its key ICT systems, while hosted internally, are supported by external contractors.

We noted that the Council continues to work through several ICT areas which are posing a challenge operationally. In particular, the Council's current ICT infrastructure, including their network, will need to be upgraded or replaced. Given the tight ICT budget the Council advised that they are developing a plan to replace over several years.

2.3.5 Relevant law and guidance

South Australian councils are established and governed by the LG Act.

A key internal control relates to how Councils secure their ICT infrastructure and associated data. Section 125 of the LG Act states that:

> *A council must ensure that appropriate policies, practices and procedures of internal control 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 the council's assets, and to secure (as far as possible) the accuracy and reliability of council records.*

There are no specific legislative requirements or current sector wide guidance on how ICT controls should be applied. Councils are individually elected bodies, responsible and accountable for their own decisions taken within the LG Act framework. Consequently, it is important that individual councils have their own policies, practices and procedures to enable the implementation of adequate ICT controls that suits their environment and risk profile.

As mentioned in section 2.1, in the absence of specific legislative requirements or current sector wide guidance within local government, we have used the South Australian Cyber Security Framework and ASD guides as a reference for our examination.

3. Audit mandate, objective and scope

3.1 Our mandate

The Auditor-General conducted this examination under section 32(1)(a) of *Public Finance and Audit Act 1987* (the PFAA). This section allows the Auditor-General to examine the accounts of a publicly funded body and the efficiency, economy and effectiveness of its activities.

The PFAA provides for the examination of the degree of efficiency, economy and effectiveness with which public resources are used. Public resources include public money, assets, facilities and staff labour.

The Council is a publicly funded body under section 4 of the PFAA, which defines such a body to include a council constituted under the LG Act.

3.2 Our objective

Our objective was to examine whether the Council effectively managed its ICT resources through appropriate internal controls established to mitigate cyber security and technology risks within the Council. This included the protection of ratepayer data on these systems.

3.3 What we examined and how

We sought to understand the cyber maturity of the Council's ICT environment, with proposed remediation recommendations where opportunities for improvement in controls were identified.

We examined whether the Council established and adhered to what we considered to be appropriate structures (refer to section 2.1) for managing cyber security, including:

- **Security governance -** policies, procedures, and standards; contract management; risk management; ICT steering committee; auditing and compliance
- **System security -** password and account settings; system access; user account management; audit logging and monitoring; patch management; physical security; network segmentation; end-user device security
- **Change management -** secure systems lifecycle; change management repository; environment segregation
- **Backup operations and disaster recovery.**

The examination also involved a website vulnerability assessment of the Council's external facing website and associated webserver(s). Testing included aspects such as detection of

default configurations, general security controls such as patching and user access management and controls against malicious user input.

Our examination testing was conducted over the December 2019 to March 2020 period.

3.4 What we did not examine

As part of our external website vulnerability assessment we did not conduct a denial of service test. This testing aims to test the resilience of the network by attempting to see if a hacker was able to overload the Council's website with superficial requests to prevent legitimate requests from being processed.

4. Security governance

4.1 Detailed findings

4.1.1 Gaps in cyber security related policies and procedures

Recommendation

The Council should address the gaps in cyber security related policies and procedures.

Finding

At the time of the examination, cyber security policies and procedures had not been fully developed and formalised that address the following controls:

- user access management
- vulnerability and patch management
- change management
- contract management
- risk management
- network security and monitoring
- security incident management
- backup operations.

Following this, we note that the Council drafted an Information Technology General Security Policy which still required finalisation and approval. At a high level, the draft policy covered:

- passwords and password construction (password parameters)
- recovery of data
- email filtering and scanning
- internet/intranet access (firewall)
- backups
- mobile phone device security
- reporting of security breaches or incidents
- change management.

The Council also has a Records Management Policy, which includes some ICT control requirements for the appropriate storage of Council information.

Why is this important?

Policies and standards establish clear Council direction and expectations of how information security is to be managed. They should include an appropriate definition of accountability and responsibilities for information security.

Without established policies and standards, experienced and skilled key personnel may not meet Council's requirements when managing cyber security.

Preliminary Council response

The draft Information Technology General Security Policy has defined all the responsibilities and includes the methodologies and standards required for the basis of consistent cyber security controls.

4.1.2 Lack of cyber security user awareness

Recommendation

The Council formalise an introductory and ongoing user awareness program which covers cyber security threats and protective techniques for all employees. This should include a balance of both personal and organisation cyber security considerations.

Training participation by employees should be formally tracked.

Finding

The Council has user awareness materials published on the intranet which includes a range of security related topics in cyber-criminal activities and prevention techniques. The Council advised that this material is updated monthly.

We noted the following cyber awareness training deficiencies:

- informal cyber awareness sessions are held on an infrequent basis and attendance is not tracked
- the new user process does not include cyber awareness training
- some employees are not clear of the security benefits to maintain strong password controls (refer to finding 5.1.1), as a previous attempt to implement more complex passwords was not well received by Council employees.

Following our examination, the Council advised it provided fraud and cyber awareness training to council management and employees in February 2020. This program was developed and funded by Local Government Risk Services and was specifically designed for Councils.

Why is this important?

As society's data dependency continues to rise, so does the frequency of cyber security incidents. Attacks are becoming more sophisticated and actual data breaches across all industries are more frequent. User credentials are often targeted by attackers as a key point of vulnerability.

Education of employees is widely considered to be one of the most important and effective elements of a cyber security control strategy. It is important that cyber security awareness efforts are continued and enhanced within the Council to ensure all employees are aware of their responsibilities and how to protect themselves and the Council from cyber threats.

Preliminary Council response

The Council's current awareness program has proved successful in maintaining cyber security awareness, with two recent major cyber security attacks unsuccessful. This was due to staff notifying IT of suspect emails, whereas other metropolitan and regional councils were disrupted by the same attacks.

4.1.3 Insufficient management of risks and contracts over third-party service providers

Recommendation

The Council should formalise a security risk management approach to identify and manage third party service provider risks. The approach should include how security requirements are to be addressed and communicated in line with contractual terms. In addition, for high risk service providers, the Council should consider an ongoing performance review of their security risk management.

Finding

We identified there are no formal risk assessments conducted or documented prior to the Council procuring third-party services.

The Council advised that some third-party services are engaged by the LGA on behalf of Councils.

There is also no formally documented approach to identify, manage and monitor third-party service providers over their lifecycle, including contract compliance and security performance on an ongoing basis.

Why is this important?

If the Council allows third party service providers and contractors to access Council systems or hold Council data, the exposure to potential cyber threats is often increased. Numerous industry studies and findings from other cyber incidents suggest that third parties are one of the main paths exploited by attackers to compromise business networks.

Controlling third-party security risks is essential to reduce the likelihood of new security threats being introduced to the Council and services are provided in alignment with the Council's risk appetite.

Preliminary Council response

The specifications and tender documents provided to vendors require the provision of relevant information. This allows the Council to make a risk-based assessment of the information provided, prior to making a purchasing decision.

Where third-party services are engaged by the LGA on our behalf, the Council is not involved in the procurement process, including any risk assessments.

Contractors are monitored against the required service provision requirements over the contract period. External providers are recorded as they remote into the Council network to manage their connections to any Council systems.

4.1.4 ICT risk register and reporting does not exist

Recommendation

The Council should establish a dedicated ICT risk register which adequately captures and rates the Council's cyber risks. This should include clearly defined ownership and associated treatment plans for all risks. Risks should be periodically reviewed and reported to a governance committee(s) responsible for ICT.

Finding

There is currently no formal risk management process or dedicated register for ICT or information security. Information security risks are therefore not formally tracked or reported upon.

Why is this important?

ICT risk management is a process of identifying risks, evaluating their severity, applying treatment plans and monitoring for effectiveness. A typical ICT risk register might include a risk assessment of the network, hardware and software failures, viruses and malicious attacks, service providers, procurement, records management, disaster recovery and business continuity, data centre and organisational (people).

Without formal processes to capture and report information security risks, the Council ability to understand, prioritise and allocate responsibilities for risk mitigation is reduced. This can lead to information security risks not being adequately addressed, increasing the likelihood or severity of security incidents.

Preliminary Council response

The Council has advised that is has a corporate risk register which contains some general ICT risks, including failure to follow policies, procedures and legislation, the use of social media, and contractor management. The Corporate Risk Register is currently out of date. Council has commenced a process to update the Corporate Risk Register and will take the opportunity to include the items identified throughout this audit. It is anticipated that this process will be complete by late 2020.

4.1.5 Lack of evidence of ongoing ICT security audits, penetration testing or vulnerability assessments

Recommendation

The Council should conduct and maintain evidence of periodic security testing and audits to evaluate the information security control environment. This should include penetration testing of internet facing services, a vulnerability assessment of assets and security control audits.

The results of these activities should be documented and tracked in the ICT risk register and reported to the Council's Audit Committee.

Finding

The Council advised that it conducted a penetration test in 2016. The Council also advised that it assesses some basic information security aspects and conducts minor testing of new system implementations or any major upgrade or update of an existing systems. This is included in the tender contract for any major ICT system or application.

During our examination, the Council was not able to provide any documented evidence of the above activities.

Why is this important?

Security testing and audits help to identify potential security weaknesses that could be exploited by malware or an attacker. They can also be used to evaluate the effectiveness of cyber security capabilities against different threat scenarios.

Preliminary Council response

The two year penetration testing cycle has been incorporated into the new Information Technology General Security Policy, which is currently in draft form. A penetration test that had been scheduled for 2019-20, has now been conducted by Council since the time of the Audit, to test the actions that have been implemented by Council as a result of this Audit process.

5. System Security

5.1 Detailed findings

5.1.1 Weaknesses in password controls

Recommendation

The Council should review the current password setting and define a password policy which is in line with what we consider to be better practice.

Finding

Active Directory is used to authenticate Council employees to the network. This allows employees to access their email, file storage and print servers and applications.

At the time of the examination, the Council's password parameters configured in Active Directory did not align with what we consider to be better practice:

Password setting	Our recommended settings	Council's Active Directory settings during the examination
Enforce password history	Users are unable to repeat their last 8 passwords	0 passwords remembered
Maximum password age	90 days	365 days
Password complexity	Enabled	Disabled
Minimum password length	10 characters [Where Complexity Enabled]; 13 characters [Where Complexity Not Enabled]	6 characters

We conducted a password cracking exercise and were able to compromise 160 weak passwords across the Council within a short period of time. Several of the weak passwords compromised had domain administrative privileges[8], some with only two character in length.

Following our examination, the Council advised it has since strengthened its password controls for users across the organisation and initiated a further password assessment in June 2020.

Why is this important?

[8] Domain administration users have privileged access permissions. This allow them to make changes to Active Directory, including altering user access profiles and making system changes.

A lack of appropriate password controls weakens the Council's overall IT security. It increases the risk of accounts being compromised and unauthorised access to Councils' IT system, potentially resulting in data loss and access to sensitive information.

Strong password rules should be enforced to improve the uniqueness of passwords which include a mix of character types. Users should create a password that is difficult for an attacker to compromise (i.e. not commonly used or easily identifiable information such as a family member's name, birthday or a pet's name).

Preliminary Council response

Stronger password controls have now been implemented and enforced across the Council, including password history of 3 passwords, password age of 6 months and password complexity enabled. Council initiated a further password cracking attempt in June 2020 to ensure compliance and enhanced security has been achieved, with only 3 passwords compromised.

5.1.2 Weaknesses in privileged access management practices

Recommendation

The Council should consider the following control improvements:

- conduct a review of privileged accounts across Active Directory, databases and applications to identify accounts that should be removed, or accounts that should have privileges reduced. Implement a periodic review process thereafter
- activities that require a heightened level of access should be conducted using individual privileged accounts, which are separate to the user's standard account
- implement stronger password controls for privileged accounts, which includes increasing the password length, adding complexity and ensuring they are changed every 30 to 90 days.

Finding

Our review of privileged access management practices identified the following weaknesses:

- testing of Active Directory privileged users identified more than 30 accounts having inappropriate domain level access

  employees performing privileged activities on Council servers use a shared administrator account rather than use unique individual administrative accounts
- the Council has not implemented any policies or procedures to strengthen the password controls that apply to privileged service and shared accounts, potentially resulting in weak passwords being used
- the ICT Manager's standard user account has domain administrator privileges

- there are no periodic user access reviews to confirm the appropriateness of privileged accounts.

Following our examination, the Council advised it has since reviewed all privileged user accounts and removed accounts that were not required. Vendor privileges have also been reduced to a minimum level. It also advised it strengthened the controls passwords that apply to privileged accounts.

Why is this important?

Privileged user accounts allows the user to make system changes and access sensitive data. Insufficient controls over these accounts potentially increases the severity of any compromise.

The use of generic/shared accounts reduces individual accountability and traceability of actions performed through these accounts.

In addition, insufficient periodic reviews of privileged accounts increases the risk of inappropriate or unauthorised access remaining on Council systems. This may result in loss of confidentiality, integrity or availability of sensitive information.

Preliminary Council response

Password controls have now been implemented and enforced across the Council, and all privileged accounts have had their passwords changed including a minimum of 15 characters. An audit of the elevated privileged user accounts has been performed and all accounts that are not required have been deleted. Privileges have been revised in discussions with vendors and modified to meet only the minimum privileges required.

5.1.3 Insufficient user access management policy, procedures and practices

Recommendation

The Council should establish a user access management policy and procedure which formally outlines the process for adding, modifying and removing user access. Given the termination exceptions identified, greater emphasis should be placed on this process to improve its effectiveness. The policy and procedure should also include the documented process for conducting regular user access reviews across Council systems. User access reviews should be:

- are conducted at least annually across all Council IT systems, to confirm the appropriateness of all current user accounts and associated privileges at the application, operating systems and database level. Refer to finding 5.1.2 for privileged users
- reviews should be performed by business unit managers and formally documented

- system roles and profiles should be documented and mapped to job roles to simplify the verification process.

The Council should also review the terminated user exceptions and investigate activities performed post termination date. Terminated employee accounts should typically be removed no later than 3-5 working days from termination date. To support the process, a monthly review should be performed of terminated employees against systems access listings.

Finding

The Council does not have a user access management policy and procedure for adding, modifying and removing user access. In addition, there is currently no requirement for regular user access reviews to be conducted across ICT systems.

Our testing identified five terminated user Active Directory accounts that were still enabled. Two of these accounts had been logged into post-termination date.

Why is this important?

Not having a formal user access management and review process increases the risk of users being granted and retaining inappropriate or unauthorised access to Council IT systems.

In addition, dormant accounts are also common targets during cyber-attacks. If terminated employee or contractor accounts are not removed in a timely manner, there is an increased risk that an obsolete user account could be used to perform inappropriate or unauthorised activity. This may result in the loss of confidentiality, integrity or availability of sensitive information.

Preliminary Council response

Council's currently undocumented processes for controlling user account access will be formalised as a result of this audit. This will capture the disabling all accounts when users exit the Council, yet maintaining accounts to ensure State Records compliance and continuity of service.

5.1.4 Privileged user security events were not logged or monitored

Recommendation

The Council should establish an audit logging and review procedure that outlines the approach, requirements and the roles and responsibilities to capture and review security events and audit logs. It should apply to all systems containing sensitive information.

Active Directory audit logging should be increased to include logs of 'Privileged Use'. Periodic audit log reviews should be conducted to identify and examine key high-risk activities. This

may include events such as unauthorised access attempts or privileged activities performed out of working hours.

Finding

The Council uses a tool to monitor the server health and antivirus software to monitor security events on core servers.

We observed that audit logging is enabled on Active Directory but the current logging policy does not capture successful logins by privileged users.

We also noted that the activities captured in the audit logs are not proactively reviewed to identify key security events.

Why is this important?

Gaps in collecting audit logs and active monitoring reduces the likelihood of unauthorised or inappropriate access or system changes through privileged user access, being identified in a timely manner. It also compromises the ability to conduct forensic investigations or root cause analysis of security incidents, if required.

Preliminary Council response

Council will actively work with vendors to developed suitable privileged user access controls for the large number of services that need to be monitored. Whilst logs are currently monitored a more formalised system will be implemented in the next upgrade of the monitoring systems.

5.1.5 Security updates not regularly installed, and no recent vulnerability assessment conducted

Recommendation

The Council should apply more rigour to its vulnerability management processes by establishing and applying a formal patch management policy and procedure. It should include:

- regular patching of all Council applications, databases and infrastructure
- a process to ensure that high priority security updates are identified, evaluated and implemented within an appropriate timeframe after release
- the requirement to document the rationale for deciding not to install a patch
- decommission the remaining legacy servers.

The Council should review the results from the vulnerability assessment performed as part of this examination (refer to Section 8) and ensure that missing patches are tested and

remediated. Consideration should also be given to either upgrade or replace unsupported software and underlying components.

Vulnerability assessments should also be undertaken periodically to identify any potential missing patches in systems software and applications.

Finding

We identified the following weaknesses in the Council's vulnerability patching of its systems:

- there is no formal patch management policy and procedure
- no vulnerability testing has been conducted across the internal network, which has resulted in an inconsistent approach to patching Council's IT systems
- patches are not tested in a non-production environment prior to being implemented in production. All but one of the Windows servers were appropriately security patched. The exception was the Active Directory domain controller where no patches or security updates were applied since August 2014
- there are numerous unsupported software and operating systems installed within the environment.

Following the examination, the Council advised that is has since appropriately patched the Active Directory domain controller.

Why is this important?

Software patches released by vendors often remediate known security vulnerabilities. These vulnerabilities are common targets for attackers seeking to compromise the Council's systems and data. Not keeping up to date with system patching also increases the risk of ransomware attacks.

Further, a lack of vendor support implies that no new security patches will be released for those products, and vendors are unlikely to investigate, acknowledge, or address new vulnerabilities that may be reported. This provides attackers widely known and tested system points of entry.

Without a well-documented patching and vulnerability management process that is consistently applied to Council IT systems, there is a risk that vulnerabilities are not identified and remediated in a timely and efficient manner.

5.1.6 Physical access to the server room is not appropriately restricted

Recommendation

The Council should implement adequate physical security controls to restrict access to the primary site server room.

Authorised access should be subject to periodic review and monitoring should be performed to ensure only authorised personnel are accessing the server room when required.

Finding

The Council does not have a dedicated and lockable server room, due to the lack of space within the Council's principal office.

access to the primary site server room is not restricted to authorised personnel. The room also contains a vaccine fridge and a printer which is regularly accessed by Council employees.

We did note that the Council's disaster recovery site is physically locked and controlled.

The Council advised it intends to review the current server room arrangement when it conducts its disaster recovery update during 2020-21.

Why is this important?

The server room contains the infrastructure required to support the Council's IT systems. Securing and monitoring access to the server room is essential to maintain data security.

Unauthorised access increases the risk of the Council's IT systems being tampered with, inappropriately accessed or data lost. Limiting access to authorised personnel reduces the risk of improper use.

5.1.7 Insufficient network segmentation

Recommendation

The Council should review the existing network segmentation to identify any devices which are located on incorrect network segments. It should also enforce network security zones based on system risk and exposure, to reduce the impacts of potential cyber security incidents.

A network security policy should be established which includes a requirement to perform periodic network security reviews. This is to ensure any risks or instance of non-compliance with policy are identified and resolved in a timely manner.

Finding

The Council network is segmented both internally and from external traffic. The Civic Centre, which incorporates the Council's library and other community and administrative services is also segregated from the rest of the internal network.

Despite this, we identified a commonly used computer located in a meeting room that can remotely connect to the Council's primary domain controller located in a different network

segment. The Council advised that the IT team use this computer for testing purposes, however, we noted it is also used by Council employees during meetings.

Why is this important?

Network segmentation is one of most effective controls the Council can implement to mitigate the risk of intrusion spreading throughout the network. If implemented correctly, it can make it significantly more difficult for an attacker to locate and gain access to the Council's sensitive information, as sensitive services and data are isolated. This acts as both a preventative technical control and a deterrent for attackers.

Preliminary Council response

These findings will be reviewed and discussed with the network 'vendor' during the upgrade of Council's network. The current network segmentation has proven reliable and functional and no intrusions have been detected.

5.1.8 Insufficient end-user device security

Recommendation

The Council should define and implement policies and an approach to secure workstations, servers, databases and network devices, in accordance with industry standards (such as the Centre for Internet Security standards[9]).

Attack surface reduction should be activated within the existing antivirus solution to combat the threat of malware in Microsoft Office applications. Application whitelisting should also be implemented on all endpoints across its IT environment.

Finding

Council user workstations and laptops (end user devices) are protected by several fundamental security controls, such as restricting administration privileges and the use of antivirus software.

Despite this, we identified that more advanced end-point protection techniques have not been implemented to reduce the ability for malicious software to execute. Techniques include enabling:

- attack surface reduction within the Windows antivirus solution (Windows Defender)
- application whitelisting.

It was also noted that the Council does not have any formal policies or standards established for end-user device security.

Why is this important?

[9] Refer to https://www.cisecurity.org/, last viewed 27 April 2020

User workstations and laptops are often involved in the first stage of a cyber-attack. While restricting administrative privileges stops some software from executing, some applications and malware do not require administrative privileges, so increased protection is required.

Attack surface reduction is a security feature within the Windows 10 antivirus solution designed to combat the threat of malware exploiting legitimate functionality in Microsoft Office applications.

Application whitelisting is a technique that prevents unauthorised or malicious software (including many forms of ransomware) from executing on workstations and servers.

Without an established and robust approach to security hardening, there is a risk that devices or systems (such as workstations, servers and network devices) are implemented in the environment in an insecure manner. They may be exploited by attackers to gain unauthorised access to Council information and systems, or to cause disruption, such as ransomware.

Preliminary Council response

Council has adopted the ASD's Windows hardening high priority recommendations as its basis for desktop and laptop device security. This has been included in the Information Technology General Security Policy (pending endorsement).

6. Change Management

6.1 Detailed findings

6.1.1 Insufficient change management controls

Recommendation

The Council should develop a change management policy and procedure that is applicable to its ICT environment. The procedure should be endorsed by management and agreed by both the business (including vendors) and the IT team. It should also include how security risks are to be addressed as part of a system acquisition and implementation.

In addition, all system changes and patches released by vendors should be evaluated in a separate test environment prior to being promoted into production. Evidence of this assessment and formal system owner's approval should be documented and tracked in a central change management repository. Segregation of duties should be applied between the developer, approver and promoter of system changes.

Finding

We sought information relating to the Council's change management environment and identified the following shortfalls:

- the Council does not have formalised change management policies and procedures to control changes applied to its ICT environment
- no records are retained of system testing and approval of major changes before they are implemented
- there is no central repository to record all approved Council system changes
- there is no separate environment available to test system changes and patches before they are promoted to the production environment.

It was also noted that security requirements to be addressed as part of system acquisition and implementation (secure system lifecycle) are not established.

Why is this important?

Governance and control over system changes are important to ensure consistency in change management across all ICT systems and that changes are effective and in line with Council's expectations.

The lack of a robust change management process, including documentation of testing and approval, increases the risk of unauthorised or potentially defective changes being made to

the production environment. This can introduce security vulnerabilities into the environment.

Preliminary Council response

Council will continue to manage all major systems updates jointly with vendors, and ensure that these processes are formally documented in the future. Minor changes to systems that are managed internally by ICT staff will also be subject to greater documentation requirements that have been outlined with the draft Information Technology General Security Policy.

7. Backup operations, disaster recovery and incident response

7.1 Detailed findings

7.1.1 No backup policy and procedure and disaster recovery plan and associated testing

Recommendation

The Council should implement a backup policy and procedure and a disaster recovery plan which applies to all ICT systems and clearly defines roles and responsibilities.

It should include the scope and coverage of all backups/replications and the formal backup and disaster recovery testing process to be conducted regularly.

Finding

We identified that the Council has not documented its current practices for backing up and restoring its ICT systems. This includes a backup policy and procedure and a disaster recovery plan to help recover ICT systems in the event of a disaster or system failure.

The Council's current backup processes involve replicating its production environment to its secondary disaster recovery site. The Council advised that it is planning a disaster recovery update during 2020-21. As part of this process offsite backup media storage will be introduced as a secondary form of recovery.

We also noted that the Council has not recently tested its backup/replication restoration capabilities and there is no periodic backup or disaster recovery testing scheduled.

Why is this important?

Without an established and robust approach to backup and recovery management, backup and recovery practices are dependent on individual professional skills and judgement.

An established ICT disaster recovery plan is important to ensure that systems can be recovered from a major systems disruption.

Without conducting regular backup testing, the Council has no assurance of its ability to restore systems and data in the event of a disaster, system failure or data loss (e.g. as a result of a ransomware security incident).

Preliminary Council response

Council acknowledges the need to document the back up operations and disaster recovery processes formally, and these items have been included in the draft Information Technology General Security Policy. Further detail will also be incorporated into the existing business continuity plans, which include ICT system recovery for business units.

7.1.2 Information security incident response plans have not been established

Recommendation

The Council should define an information security incident response plan. This plan should include the technical procedures and activities needed to respond to common cyber incident scenarios and security threats.

Finding

We noted that information security incident response plans to key scenarios and security threats have not been established.

Why is this important?

Without an established, understood and tested cyber security incident response plan, there is a risk that the Council may not be able to activate a quick and appropriate response to a cyber event or information security incident.

Employee confusion or a lack of clarity of actions required during a security incident can result in a delayed or ineffective response. This may cause an incident to have a prolonged negative impact on business operations, including the costs and resources needed to respond.

Clearly established roles and responsibilities, and robust processes for when to engage third parties during an incident and how to deal with an incident after hours, are essential to responding to, and recovering from cyber security incidents as swiftly as possible. It is also important to define a robust operating model to support detection of, response to, and recovery from cyber security incidents without single points of failure introduced through key person risk.

Testing of incident response plans should be conducted to assess the Council's preparedness and responsive capabilities.

8. Vulnerability assessment results

We conducted some vulnerability testing of the Council's external website environment.

We identified and raised several concerns with the Council for remediation. This included some unsupported software versions running on different types of platforms and some software and operating system security patch levels which required updating.

The web application was using vulnerable software libraries and we identified exposures related to the administrative portal. Certain documents within the application required increased protection against external attack and some underlying software disclosures needed to be reduced.

We also identified a communication protocol that needed updating and documents created and hosted by the Council required greater security to be applied. These documents may contain additional information that could be used by an attacker. Further, some fundamental security aspects also required strengthening so that other potentially vulnerabilities are not exploited.

The Council and supporting vendors responded positively to our findings and recommendations and at the time of writing this Report they had commenced remediation activities.

9. Abbreviations and explanation of terms used in this report

Term	Description
Application whitelisting	specifies a list of approved software applications or executable files that are permitted to be present and active on a computer system.
Audit log management	audit logging and monitoring of the ICT environment involves the recording and analysing of system and user activities to detect and respond to unusual events within the IT system.
Backup management	refers to the process of managing the copying of computer data to an archive file. This copy can then be used to restore the original data in the event of data corruption or data loss event.
Change management	is a systematic and standardised approach to ensuring all changes to the IT environment are appropriate, authorised and preserve the integrity of the underlying programs and data.
Cyber security	is the practice of protecting networks, computer systems and data from unauthorised access or malicious attack.
Cyber security incident	a malicious and/or unauthorised system security breach that may impact the confidentiality, integrity or availability of data. This may have a financial and reputational impact to the council.
Disaster recovery	is a documented process, or set of procedures, to assist in the recovery of an organisation's ICT infrastructure in the event of a disaster.
Legacy system	relates to outdated application and or operating systems that can no longer receive support and maintenance rather than utilising available upgrades system versions.
Malware	malicious software like computer viruses, worms, trojan horses, spyware, and scareware.
Password management	are a common means of verifying a user's identity before access is given to an information system or service according to the user's authorisation.
Patch management	is the process of updating (acquiring, testing and installing) a set of changes or upgrades to support software, application and technology enhancements and to fix defects and vulnerabilities to an information system.
Ransomware	a type of malicious software, designed to deny access to a computer system/data or threatens to publish the victim's data until a ransom is paid.
Risk Register	is a tool for documenting risks, and actions to manage each risk. The Risk Register is essential to the successful management of risk. As risks are identified they are logged on the register and actions are taken to respond to the risk.

Spear phishing	the fraudulent practice of sending emails from a known or trusted sender to obtain sensitive information like usernames, passwords, or credit card details.
Treatment plan	outlines how an entity plans to respond to potential risks. Risks are categorised as low, high, or acceptable risks. This assists in identifying level of risk and the degree of attention required when assigning resources to rectify / respond to identified risk.
User access management	relates to the process of managing access to applications and data, including how access is approved, revoked and periodically reviewed. This helps to ensure that access is aligned with employee roles and responsibilities and prevents unauthorised access to information systems. It includes appropriately restricting and monitoring privileged access permissions, which have a heightened level of access to alter user access profiles and make system changes.