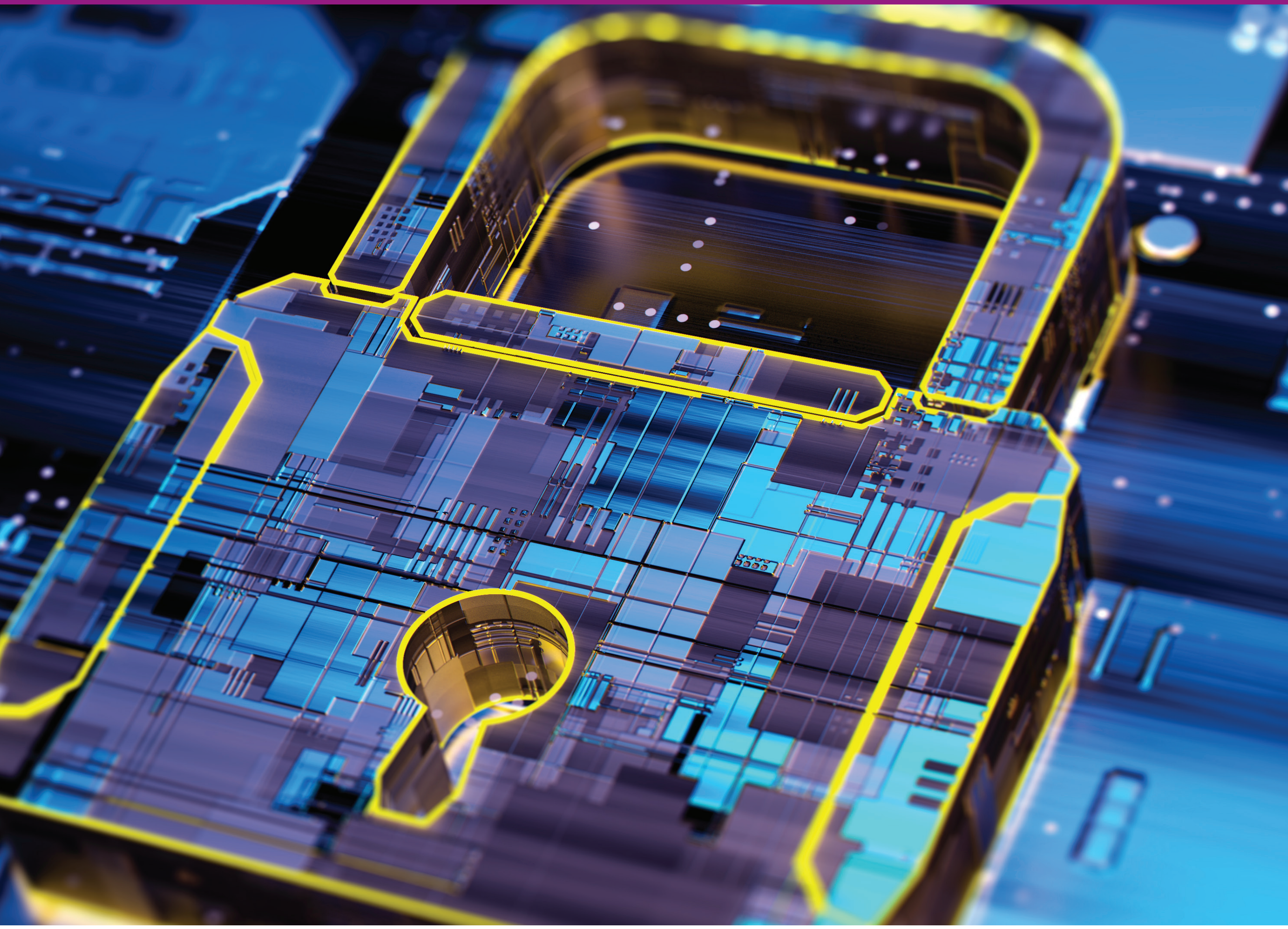
# Report of the Auditor-General

Auditor-General's Department

**Report 3 of 2021**

Examination of cyber security:
Port Augusta City Council



Government of South Australia

[P.P.4R

# Report of the Auditor-General

## Report 3 of 2021

## Examination of cyber security: Port Augusta City Council

*Tabled in the House of Assembly and ordered to be published, 2 February 2021*

Second Session, Fifty-Fourth Parliament

By authority: S. Smith, Government Printer, South Australia

2021

*The Auditor-General's Department acknowledges and respects Aboriginal people as the State's first people and nations, and recognises Aboriginal people as traditional owners and occupants of South Australian land and waters.*

**Auditor-General's**
Department

www.audit.sa.gov.au

Enquiries about this report should be directed to:

Auditor-General
Auditor-General's Department
Level 9, 200 Victoria Square
Adelaide SA 5000

ISSN 0815-9157

Government of South Australia
Auditor-General's Department

Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000
Tel +618 8226 9640
Fax +618 8226 9688
ABN 53 327 061 410
audgensa@audit.sa.gov.au
www.audit.sa.gov.au

1 February 2021

President
Legislative Council
Parliament House
ADELAIDE SA 5000

Speaker
House of Assembly
Parliament House
ADELAIDE SA 5000

Dear President and Speaker

## Report of the Auditor-General: Report 3 of 2021 *Examination of cyber security: Port Augusta City Council*

Under section 32(1) of the *Public Finance and Audit Act 1987* (PFAA), I have conducted an examination of the way cyber security is managed by the Port Augusta City Council.

The objective of the examination was to assess the effectiveness of the Council's cyber security management.

I present to each of you my independent assurance report on the findings of the examination.

A copy of this report has also been provided to the Port Augusta City Council.

### Content of the Report

We examined the arrangements established by the Port Augusta City Council to manage cyber security.

We concluded that for the period December 2019 to March 2020, important internal control elements to mitigate cyber security and technology risks within the Council were not operating effectively.

### My responsibilities

Examinations conducted under section 32(1)(a) of the PFAA are assurance engagements that assess whether a publicly funded body is achieving economy, efficiency and effectiveness in its activities. These engagements conclude on the performance of the activities evaluated against identified criteria.

The Auditor-General's roles and responsibilities in undertaking examinations are set out in the PFAA. Section 32(1)(a) of the PFAA empowers me to conduct this examination while section 32(3) deals with the reporting arrangements.

The examination was conducted in line with the Standard on Assurance Engagements ASAE 3500 *Performance Engagements*. We complied with the independence and other relevant ethical requirements for assurance engagements.

## Acknowledgements

The audit team for this report was Andrew Corrigan, Tyson Hancock, Brenton Borgman and the Local Government team. They were assisted in the review by Deloitte Risk Advisory Pty Ltd.

We appreciate the cooperation and assistance given by the staff of the Port Augusta City Council.

Yours sincerely

Richardson

Andrew Richardson
**Auditor-General**

# Contents

# 1 Executive summary

## 1.1 Introduction

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

Information and communications technology (ICT) systems play an important role in the day-to-day operations of a council and in servicing ratepayers.

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

Avoiding disruption to operations from security threats such as ransomware, maintaining the integrity of operational ICT 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 just nice to have – it is simply expected.

In this examination 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 had 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 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 uses a number of technical terms. Section 9 explains them in more detail.

## 1.2 Conclusion

We acknowledge that the Council has a small IT team and budgetary constraints. However, for the period that we examined we concluded that important internal control elements to mitigate cyber security and technology risks within the Council were not operating effectively.

In my opinion, the Council has some way to go to achieve ICT security standards that appropriately mitigate the risk of cyber security threats.

The Council did respond positively to our examination recommendations and commenced improvement activities during our examination by drafting an Information Technology General Security Policy. We also noted that the Council does maintain:

- user awareness materials on its intranet
- a tool to monitor the health of all servers and antivirus software to monitor security events on core servers
- a documented network diagram, with some network segmentation implemented
- some fundamental security protection on its end user devices, including restricting administration privileges and using antivirus software.

## 1.3 What we found

Our key findings are summarised in figure 1.1 and more details are provided in sections 4 to 8.

**Figure 1.1: Key findings**

| Area | Findings |
|---|---|
| Security governance (section 4) | • Gaps in cyber security related policies, procedures and standards.<br>• Lack of cyber security user awareness.<br>• Insufficient management of risks and contracts over third party service providers.<br>• No ICT risk register and reporting.<br>• Lack of evidence of ongoing ICT security audits, penetration testing or vulnerability assessments. |
| System security (section 5) | • Weaknesses in password controls and privileged access management practices.<br>• Insufficient user access management policy, procedures and practices.<br>• Privileged user security events not logged or monitored.<br>• Security updates not regularly installed, and no recent vulnerability assessment conducted.<br>• Physical access to the server room not appropriately restricted.<br>• Insufficient network segmentation and end user device security. |
| Change management (section 6) | • Inadequate change management controls. |

| Area | Findings |
|---|---|
| Backup operations, disaster recovery and incident response (section 7) | • No backup policy and procedure and disaster recovery plan and associated testing.<br>• Information security incident response plans not established. |
| Vulnerability assessment (section 8) | • Some unsupported software and some software and operating system security patch levels required updating.<br>• 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.<br>• A communication protocol needed updating and documents created and hosted by the Council required greater security to be applied. |

## 1.4 What we recommended

Our key recommendations are summarised in figure 1.2.

**Figure 1.2: Key recommendations**

| Area | Recommendations |
|---|---|
| Security governance (section 4) | • Address gaps in cyber security related policies and procedures.<br>• Formalise an introductory and ongoing user awareness program, with employee participation tracked.<br>• Formalise a security risk management approach to identifying and managing third party service provider risks.<br>• Establish a dedicated ICT risk register, with risks periodically reviewed and reported.<br>• Conduct and maintain evidence of periodic security testing and audits to evaluate the information security control environment, with the results documented and tracked in the ICT risk register. |
| System security (section 5) | • Review current password settings and define a password policy that is in line with what we consider to be better practice.<br>• Periodically review privileged accounts, with activities that require a heightened level of access conducted using individual privileged accounts.<br>• Establish a user access management policy and procedure, with user access reviewed at least annually.<br>• Review terminated user exceptions and investigate activities performed after the termination date. |

| | |
|---|---|
| | • Establish an audit logging and review procedure, with Active Directory audit logging increased to include logs of privileged use.<br>• Apply more rigour to the vulnerability management processes by establishing and applying a formal patch management policy and procedure.<br>• Decommission remaining legacy servers, and consider either upgrading or replacing unsupported software and underlying components.<br>• Conduct vulnerability assessments periodically and implement adequate physical security controls to the primary site server room.<br>• Review the existing network segmentation and establish a network security policy. Define and implement policies and an approach to secure workstations, servers, databases and network devices.<br>• Activate attack surface reduction and implement application whitelisting. |
| Change management (section 6) | • Develop a change management policy and procedure that suits the Council's ICT environment.<br>• Evaluate all system changes and patches released by vendors in a separate test environment before they are promoted into production. Apply segregation of duties between the developer, approver and promoter of system changes. |
| Backup operations, disaster recovery and incident response (section 7) | • Implement a backup policy and procedure and a disaster recovery plan that applies to all ICT systems and clearly defines roles and responsibilities.<br>• Define an information security incident response plan. |
| Vulnerability assessment (section 8) | • Remediate issues highlighted in our vulnerability testing of the Council's external website environment. |

## 1.5 Response to our recommendations

The Council stated the following:

> *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 strategies to maintain a reasonable level of security controls for their ICT services, commensurate with a council's assessed risks. Achieving and maintaining appropriate cyber security arrangements is critical to protecting sensitive information, including the public's personal data.

A 2018 report from a global professional services firm[1] indicated that cyber security was a top four risk to the Australian local government sector.

The SA Government maintains its own cyber security framework. It provides SA Government agencies with direction and guidance through an approach for establishing, implementing, maintain and continually improving their cyber security controls. The framework was developed with SA 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. Despite this, individual councils should develop ICT control policies and procedures outlining expected basic controls. We consider that key references and better practice guides for examining the effectiveness of cyber security are:

- the South Australian Cyber Security Framework
- guides developed by the Commonwealth 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 ICT communications across the sector.

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

[1] AON 2018, *2018 Risk Report – A focus on Local Government,* <https://www.aon.com.au/australia/local-government/files/risk-report-for-local-government-2018.pdf>, viewed 30 April 2020.

[2] Department of the Premier and Cabinet, *Cyber security*, <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 wrote to all South Australian councils[3] requesting a response to a high-level questionnaire about each council's ICT environment and security arrangements. The purpose of this questionnaire was to get a better understanding of ICT arrangements and challenges in the local government sector.

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

Council responses, understandably, varied with respect to the level of detail given for each question. We have, accordingly, applied a degree of interpretation. We did not assess the accuracy of their responses and provided no assurance as to the cyber security arrangements across local government or in individual councils as a result of this questionnaire.

In September 2019, we provided a high-level summary of questionnaire responses and our observations to all councils, the LGA and Local Government Risk Services. We encouraged each council's management to discuss the observations in the context of its own ICT cyber security maturity and risk profile.

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

Other observations we made from the questionnaire responses included:

- completing ICT projects on time, within budget and with the required functionality, limited ICT 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 two years. Of these 40 councils, seven (10% of the total) reported that they had experienced a cyber security incident in the past two years
- 25 councils (37% of the total) were still developing or did not have a formal ICT risk register
- 13 councils (20% of the total) were 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 systems/hardware were nominated as the top areas of focus if extra funding was provided to council ICT budgets
- 20 councils (30% of the total) had not either conducted an independent ICT security assessment in the last two years or made any plans to do so.

[3] Except the District Council of Coober Pedy, as 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, started or had an independent ICT security assessment.

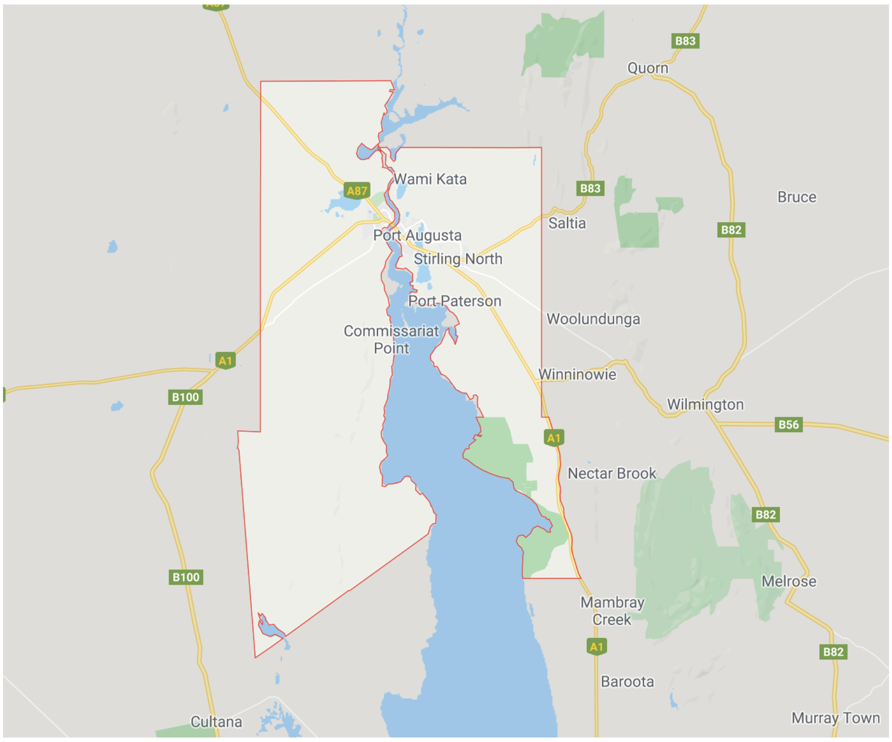
The questionnaire responses also indicated that many councils had participated in a voluntary risk mitigation program run by the LGA. This involved assessing a council's ICT vulnerabilities against the Essential Eight[4] and/or conducting penetration testing through an independent security vendor.

## 2.3 Port Augusta City Council

### 2.3.1 Overview

The Council area covers over 1150 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 Adelaide.[5]

**Figure 2.1: Council area map**



[4] In August 2017 the Commonwealth Government, through the Australian Cyber Security Centre, 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's website, <https://www.portaugusta.sa.gov.au/home>, viewed 21 April 2020.

The Council provides a diverse range of community services, including:

- childcare
- tourism facilities
- parks and gardens, ovals and sporting facilities
- beach, foreshore and levy bank management
- airport and cemeteries management
- environmental health services
- 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 these services are not generally provided by other councils in South Australia, notably the management of the local airport.

The Council is also responsible for a range of administrative 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 it has been through a period of significant economic downturn in recent years, following the closure of the Port Augusta Power Station and the delayed start or failure of several renewable energy projects. This has resulted in job losses and increased financial stress within the community.

### 2.3.3 Budget

The Council has reported operating deficits 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, advising that this was mainly due to the one-off receipt of $3.1 million from the sale of assets linked to aged care facilities. In 2017-18 the Council also confirmed that it 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).

Figures 2.2 and 2.3 show the Council's sources of income and expenditure incurred to deliver services to the local community in the past two years.[6]

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

**Figure 2.2: Sources of income and expenditure incurred in 2018-19**

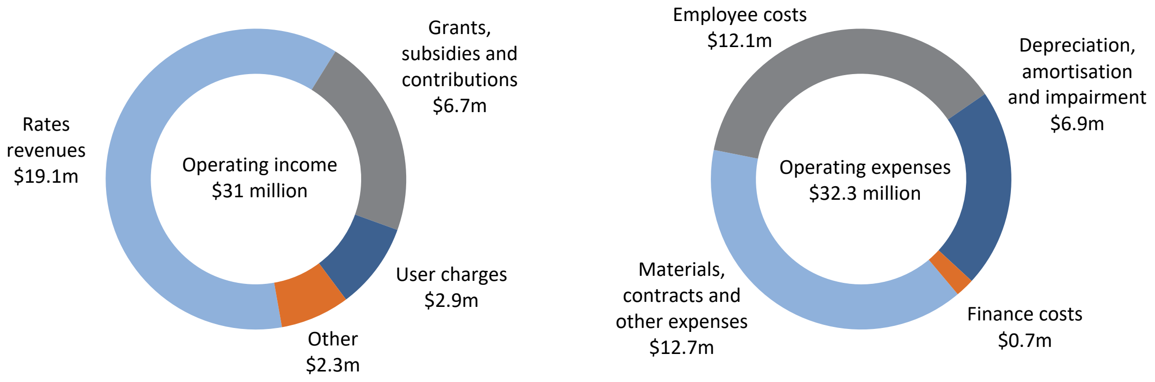
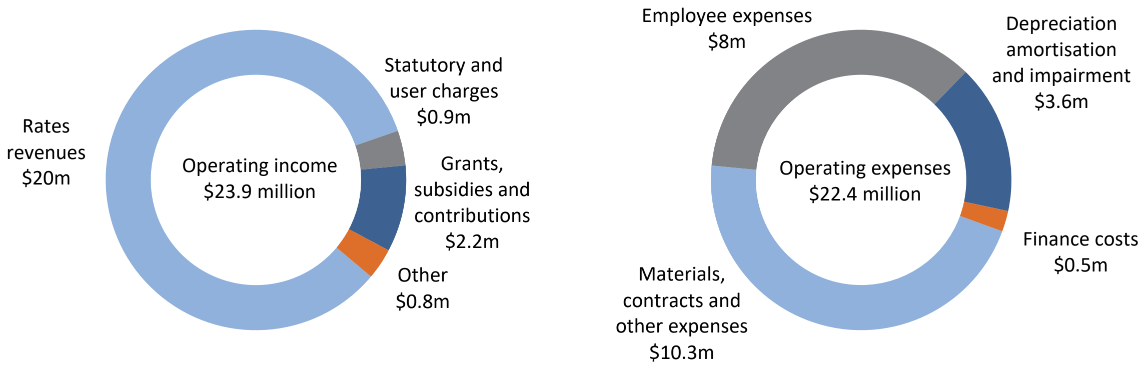


**Figure 2.3: Sources of income and expenditure incurred in 2017-18**



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

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

These ICT expenses include wages and on-costs, software licences and upgrades, leases, internet and data costs, equipment purchases and depreciation.

### 2.3.4 Information and communications technology

The Council employs 183 staff (134 full-time equivalents), four of whom are allocated to the Information Technology (IT) team. An Information Systems and Records Manager leads this team and has primary responsibility for information security management. This includes providing the community with the ability to interact with the Council electronically.[7]

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

[7] Refer to the Council's annual reports for 2018-19 and 2017-18.

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

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

We noted that the Council continues to work through several ICT areas that are posing a challenge operationally. In particular, the Council's current ICT infrastructure, including its network, will need to be upgraded or replaced. Given its tight ICT budget the Council advised that it is developing a plan to do this 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 making their own decisions within the LG Act framework. Consequently, it is important that individual councils have their own policies, practices and procedures to implement adequate ICT controls to suit 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 references 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, and proposed remediation recommendations where we identified opportunities for improvement in controls.

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 life cycle; change management repository; environment segregation
- **Backup operations and disaster recovery.**

Our examination also involved a vulnerability assessment of the Council's external facing website and associated webserver(s). This testing included areas such as detecting default configurations, general security controls such as patching and user access management, and controls to protect against malicious user input.

Our testing covered the period from December 2019 to March 2020.

## 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 tests the resilience of the network by attempting to see if a hacker could 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 we identified in its cyber security related policies and procedures.

#### Finding

At the time of our examination, the Council's cyber security policies and procedures to address the following controls were not fully developed and formalised:

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

We note that the Council subsequently drafted an Information Technology General Security Policy, which still needed to be finalised and approved. 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 this is important

Policies and standards establish clear Council direction and expectations about 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 the Council's requirements when managing cyber security.

### Council response

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

Training participation by employees should be formally tracked.

### Finding

The Council has published user awareness materials on its intranet that include a range of security related topics in cyber-criminal activities and prevention techniques. The Council advised that it updates this material monthly.

We noted the following cyber awareness training deficiencies:

- informal cyber awareness sessions are held infrequently and attendance is not tracked
- the new user process does not include cyber awareness training
- some employees are not clear about the security benefits of maintaining 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 that 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 this is important

As society's data dependency increases, 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.

Educating 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.

### Council response

The Council stated that its current awareness program has proved successful in maintaining cyber security awareness, with two recent major cyber security attacks being 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 found that the Council did not conduct or document formal risk assessments before it procured third party services.

The Council advised that some third party services were engaged by the LGA on behalf of councils.

There was also no formally documented approach to identify, manage and monitor third party service providers over the term of their engagement, including contract compliance and security performance on an ongoing basis.

### Why this is important

If the Council allows third party service providers and contractors to access its systems or hold its data, the exposure to potential cyber threats is often increased. Many industry studies and findings from other cyber security 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 reducing the likelihood of new security threats being introduced to the Council and ensuring that services are provided in line with the Council’s risk appetite.

### Council response

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

The Council also advised that where third party services are engaged by the LGA on its behalf, the Council is not involved in the procurement process, including any risk assessments.

The Council advised that its contractors are monitored against the required service provision requirements over the contract period. External providers are recorded when they connect remotely to the Council's network to manage their connections to any Council systems.

### 4.1.4 No ICT risk register or reporting

#### Recommendation

The Council should establish a dedicated ICT risk register that adequately captures and rates its cyber risks. This should include clearly defined owners and treatment plans for all risks. Risks should be periodically reviewed and reported to a governance committee responsible for ICT.

#### Finding

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

#### Why this is important

ICT risk management is the 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 organisation (people).

Without formal processes to capture and report information security risks, the Council's 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.

#### Council response

The Council advised that it 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 Council advised that it has commenced a process to update the corporate risk register and will take the opportunity to include the items identified in our examination. It is expected that this process will be complete by late 2020.

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

#### Recommendation

The Council should conduct and maintain evidence of periodic security testing and audits to evaluate its information security control environment. This should include penetration testing of internet facing services, a vulnerability assessment of its 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. It also advised that it assesses some basic information security aspects and conducts minor testing of new system implementations and any major upgrade or update of an existing system. This activity 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 these activities.

#### Why this is 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.

#### Council response

The Council advised that its two-year penetration testing cycle has been incorporated into its new Information Technology General Security Policy, which is currently in draft form.

The Council advised that a penetration test that was scheduled for 2019-20 has now been conducted.  The aim was to test the actions that the Council implemented as a result of our examination.

# 5 System security

## 5.1 Detailed findings

### 5.1.1 Weaknesses in password controls

#### Recommendation

The Council should review its current password setting practices and establish a password policy that is in line with what we consider to be better practice.

#### Finding

The Council uses Active Directory to authenticate its employees to its network. This allows employees to access their email, file storage, print servers and applications.

At the time of our examination, the Council's password parameters configured in Active Directory did not align with what we consider to be better practice. This is shown in figure 5.1.

**Figure 5.1: Recommended password settings**

| Password setting | Our recommended settings | Council's Active Directory settings during the examination |
|---|---|---|
| Enforce password history | Users are unable to repeat their last eight passwords | 0 passwords remembered |
| Maximum password age | 90 days | 365 days |
| Password complexity | Enabled | Disabled |
| Minimum password length | 10 characters where complexity is enabled<br>13 characters (where complexity is not enabled) | Six characters |

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

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

#### Why this is important

A lack of appropriate password controls weakens the Council's overall ICT security. It

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

increases the risk of accounts being compromised and unauthorised access to its systems, potentially resulting in data loss and access to sensitive information.

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

### Council response

The Council advised that stronger password controls have now been implemented and enforced across the Council, including a password history of three passwords, password age of six months and password complexity enabled.

The Council also advised that it had initiated a further password cracking attempt in June 2020 to ensure that compliance and improved security had been achieved, with only three passwords compromised.

## 5.1.2 Weaknesses in privileged access management practices

### Recommendation

The Council should consider the following control improvements:

- review privileged accounts across Active Directory, databases and applications to identify accounts that should be removed or that should have privileges reduced. Implement a periodic review process thereafter
- conduct activities that require a heightened level of access 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 using 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 that it had reviewed all privileged user accounts and removed any that were not required. Vendor privileges were also reduced to a minimum level. It also advised that it had strengthened the controls over passwords that apply to privileged accounts.

### Why this is important

Privileged user accounts allows the user to make system changes and access sensitive data. Inadequate control of 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 increase the risk of inappropriate or unauthorised access remaining on Council systems. This may result in loss of confidentiality, integrity or availability of sensitive information.

### Council response

The Council advised that password controls have now been implemented and enforced across the Council, and all privileged accounts have had their passwords changed and must contain at least 15 characters.

A Council audit of the elevated privileged user accounts was performed, with the Council advising that all accounts that were not required were deleted.

The Council also advised that privileges have been revised in discussions with vendors and modified to be 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 that formally outline 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:

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

In addition, 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 any activities performed after the termination date. Terminated employee accounts should typically be removed no more than 3-5 working days from termination date. To support the process, a monthly review should be performed of terminated employees against system 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 Active Directory accounts for terminated employees that were still enabled. Two of these accounts had been logged into after the termination date.

### Why this is 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 ICT systems.

In addition, dormant accounts are common targets during cyber attacks. If terminated employee or contractor accounts are not promptly removed, 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.

### Council response

The Council advised that its currently undocumented processes for controlling user account access will be formalised as a result of this examination. This will capture the disabling of all accounts when users leave the Council, while maintaining accounts where needed 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 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 its 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 this is important

Gaps in collecting audit logs and in actively monitoring reduce the likelihood of unauthorised or inappropriate access or system changes through privileged user access being promptly identified. They also compromise the ability to conduct forensic investigations or root cause analysis of security incidents, if required.

### Council response

The Council advised that it will actively work with vendors to developed suitable privileged user access controls for the large number of services that need to be monitored.

While logs are currently monitored the Council indicated that a more formalised system will be implemented in the next upgrade of its 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 ICT infrastructure
- a process to ensure that high priority security updates are identified, evaluated and implemented within an appropriate time frame after release
- the requirement to document the rationale for deciding not to install a patch
- decommissioning 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 upgrading or replacing unsupported software and underlying components.

Vulnerability assessments should also be conducted periodically to identify any 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 ICT systems
- patches are not tested in a non-production environment prior to being implemented in production. All but one of the Council's 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.

#### Why this is important

Software patches released by vendors often remediate known security vulnerabilities. These vulnerabilities are common targets for attackers seeking to compromise an entity'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 with widely known and tested system points of entry.

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

#### Council response

The Council advised that following our examination, it had patched the Active Directory domain controller.

### 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 its 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 its 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 that is regularly accessed by Council employees.

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

### Why this is important

The server room contains the infrastructure required to support the Council’s ICT systems. Securing and monitoring access to the server room is essential to maintaining data security.

Unauthorised access increases the risk of data loss and the Council’s ICT systems being tampered with or inappropriately accessed. Limiting access to authorised personnel reduces the risk of improper use.

### Council response

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

## 5.1.7 Insufficient network segmentation

### Recommendation

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

The Council should establish a network security policy that includes a requirement to perform periodic network security reviews. This will ensure that any risks or instances of non-compliance with policy are identified and resolved in a timely manner.

### Finding

The Council’s 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 could remotely connect to the Council’s primary domain controller located in a different network segment. The Council advised that the IT team used this computer for testing purposes, however we noted it was also used by Council employees during meetings.

### Why this is 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.

### Council response

The Council advised that these findings will be reviewed and discussed with the network vendor during the upgrade of the Council's network. The Council also stated that its 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 securing workstations, servers, databases and network devices in line 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 the Council's ICT environment.

### Finding

Council user workstations and laptops (end user devices) are protected by several fundamental security controls, such as restricting administrative privileges and using 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 this is important

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.

[9] <https://www.cisecurity.org/>, viewed 27 April 2020.

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 in the case of ransomware.

## Council response

The Council advised that it has adopted the ASD's Windows hardening high priority recommendations as the basis for its desktop and laptop device security. This has been included in its draft Information Technology General Security Policy.

# 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 the 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 about to the Council's change management environment and identified the following shortfalls:

- the Council does not have a formal change management policy or procedures to control any 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 system changes
- there is no separate environment available to test system changes and patches before they are promoted to the production environment.

We also noted that security requirements to be addressed as part of system acquisition and implementation (secure system life cycle) were not established.

#### Why this is important

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

The absence of a robust change management process, including documentation of any 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.

## Council response

The Council advised that it will continue to manage all major systems updates jointly with its vendors, and will 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 in the Council's 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 that 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 found that the Council had not documented its current practices for backing up and restoring its ICT systems. This includes having 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 in 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 had not recently tested its backup/replication restoration capabilities and there was no periodic backup or disaster recovery testing scheduled.

Why this is important

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

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

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

Council response

The Council advised that it acknowledges the need to formally document its backup operations and disaster recovery processes, and this has been included in its draft Information Technology General Security Policy. Further detail will also be incorporated into its existing business continuity plans, which include ICT system recovery for business units.

### 7.1.2 Information security incident response plans not 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 were not established.

#### Why this is 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 the detection of, response to and recovery from cyber security incidents without single points of failure being introduced through key person risk.

Incident response plans should be tested to assess the Council's preparedness and response capabilities.

#### Council response

The Council advised that security incident response plans will be developed when it reviews its emergency response policies and procedures.

# 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 that needed 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 potential vulnerabilities are not exploited.

The Council and its vendors responded positively to our findings and recommendations with details of their remediation approach.

# 9 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 recording and analysing system and user activities to detect and respond to unusual events within the ICT 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 a data loss event. |
| Change management | is a systematic and standardised approach to ensuring all changes to the ICT 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 | a documented process, or set of procedures, to assist in recovering an organisation's ICT infrastructure in the event of a disaster. |
| Legacy system | an outdated application and\or operating system 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 | 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 | 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 that threatens to publish the victim's data until a ransom is paid. |
| Risk register | a tool for documenting risks and actions to manage each risk. A 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. |

| Term | Description |
|---|---|
| Treatment plan | outlines how an entity plans to respond to potential risks. Risks are categorised as low, high or acceptable. This helps to identify levels 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. |