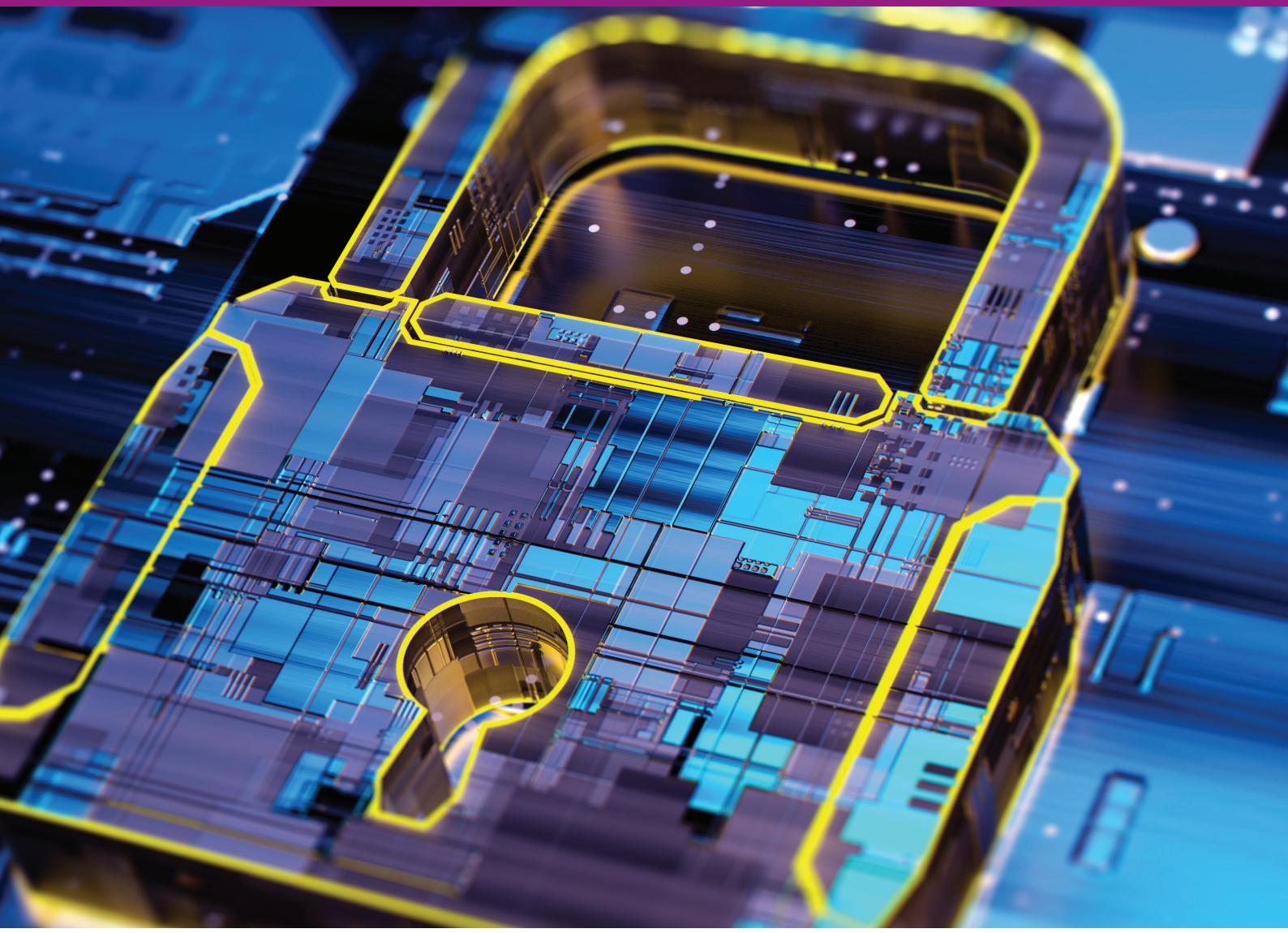
Report of the Auditor-General

Auditor-General's Department

Report 2 of 2021

Examination of cyber security:
City of Prospect



Government of South Australia

[P.P.4Q

Report of the Auditor-General

Report 2 of 2021

Examination of cyber security: City of Prospect

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 2 of 2021 *Examination of cyber security: City of Prospect*

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 City of Prospect.

The objective of the examination was to assess the effectiveness of 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 City of Prospect.

Content of the Report

We examined the arrangements established by the City of Prospect to manage cyber security.

For the period that we examined we concluded that important internal control elements to mitigate cyber security and technology risks within the City of Prospect were not operating effectively. We do acknowledge that the City of Prospect has a small IT team and budgetary constraints and that it implemented some controls over its core Enterprise Resource Planning and records management systems.

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

The City of Prospect responded positively to our recommendations and had already commenced some improvement activities prior to our examination. It continued those improvement activities during and after our examination.

We also noted that the City of Prospect maintains:

- an ongoing user awareness program
- frequent security patching of its core Enterprise Resource Planning system
- detailed documentation of its disaster recovery and backup arrangements and evidence of testing them
- fundamental security controls to end user devices, including restricting local administration privileges, and using antivirus software and a mobile device management solution.

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.

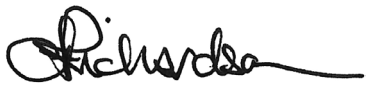
The examination was conducted in line with the Standard on Assurance Engagements ASAE 3500 *Performance Engagements*. We complied with the independence and other relevant ethical requirements for assurance engagements.

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 City of Prospect.

Yours sincerely



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 to the City of Prospect (the Council) being 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 of South Australia (LGA).

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

This Report uses a number of technical terms. Section 8 explains them in more detail.

1.2 Conclusion

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.

We do acknowledge that the Council has a small IT team and budgetary constraints and has implemented some controls over its core enterprise resource planning (ERP)[1] and electronic document and records management (EDRMS)[2] systems.

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

The Council responded positively to our recommendations and had already commenced some improvement activities prior to our examination. The Council continued those improvement activities during and after our investigation. We also noted that the Council maintains:

- an ongoing user awareness program
- frequent security patching of its core ERP system
- detailed documentation of its disaster recovery and backup arrangements and evidence of testing them
- fundamental security controls to end user devices, including restricting local administration privileges, and using antivirus software and a mobile device management solution.

1.3 What we found

Our key findings are summarised in figure 1.1 and more details are provided in sections 4 to 7.

Figure 1.1: Key findings

Area	Findings
Security governance (section 4)	• Gaps in cyber security policies, procedures and standards. • Insufficient cyber awareness training during induction. • Insufficient management of risks over third party service providers. • ICT risk register and reporting does not exist. • No ongoing review or assurance over ICT controls.
System security (section 5)	• Weaknesses in password controls. • Weaknesses in privileged access management practices. • Insufficient user access management. • Weaknesses in patch management. • Insufficient end user device security.
Change management (section 6)	• Gaps in change management controls.

[1] The ERP system is used by the Council in the management and integration its finance, operations (including citizen requests), reporting and human resource activities.

[2] The EDRMS is used by the Council to manage the creation, accessibility, storage and disposal of physical and electronic records and information to help it to comply with the *State Records Act 1997*.

Area	Findings
Vulnerability assessment (section 7)	• Some unsupported software and some software and operating system security patch levels required updating. • The web application was using vulnerable software libraries and we identified exposures related to the administrative portal. Certain forms within the application required greater security to be applied and some underlying software disclosures needed to be reduced. • Some fundamental security aspects required strengthening so that other potential vulnerabilities are not exploited.

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)	• Enhance the existing information security policies and develop a cyber security strategy. • Formalise introductory information security user awareness training for all new employees and a security risk management approach to identify and manage third party service provider risks. • Implement an ICT risk register, with risks periodically reviewed and reported to a governance committee responsible for ICT. • Conduct periodic security testing and audits to evaluate the Council's information security control environment, with the results documented and tracked.
System security (section 5)	• Ensure that password controls are applied to all accounts in line with the Council's password policy with strong password practices encouraged, especially for privileged accounts. • Review privileged accounts to identify any that should either be removed or have privileges reduced. Implement an ongoing periodic review process. • Establish a user access management policy and procedure that formally outlines the process for adding, modifying and removing user access and for conducting regular user access reviews. • Review the terminated user exceptions and investigate any activities performed after the termination dates. • Apply more rigour to vulnerability management processes by establishing a formal patch management policy and procedure.

Area	Recommendations
System security (section 5)	• Review the results of the vulnerability assessment we performed and ensure that missing patches are tested and remediated. Consider either upgrading or replacing legacy unsupported software and underlying components. • Develop and implement a policy that establishes an approach to securing workstations and laptops (end user devices).
Change management (section 6)	• Formally establish a change management policy and procedure that is applicable to the Council's ICT environment. • Evaluate, document and track all system changes and patches released by vendors using a separate test environment and strengthen the segregation of duties.
Vulnerability assessment (section 7)	• Remediate issues highlighted in our vulnerability testing of the Council's external website environment.

1.5 Response to our recommendations

The Council provided a detailed response to each of our recommendations, which included remediation actions, planned time frames and approximate remediation costs.

In its response the Council wanted to highlight various points. In particular, it drew attention to the fact that the local government sector does not have any mandatory cyber security arrangements, such as ICT control frameworks or standards, in the provision of ICT services.

The Council stated:

> *This Audit report referred Council to the following 'best practice' guides for examining the effectiveness of cyber security: South Australian Cyber Security Framework and guides developed by the Federal Government Australian Signals Directorate. However, we also note that your Department's view of 'best practice' was only brought to our attention while undergoing this audit process. Nevertheless, our Administration has embraced the need for remediation to address the matters raised during the audit process.*

The Council also stated:

> *Your report also indicated that there are opportunities to increase cross-sector ICT communications across councils, together with the Local Government Association (LGA) of SA, and that those organisations should consider their position moving forward regarding cyber security and ICT generally. We support your observations in this regard, particularly considering the ongoing resources and expertise that will be required of a small council in an increasingly complex and high risk cyber security environment.*

The examination also acknowledges that Council has a small IT team as well as budgetary constraints and notes that Council maintains:

- *an ongoing user awareness program*
- *frequent security patching of its core Enterprise Resource Planning (ERP) system*
- *detailed documentation of disaster recovery and backup arrangements and evidence of testing*
- *fundamental security controls to end user devices, including restricting local administration privileges, the use of antivirus software and a mobile device management system.*

Finally, the Council stated:

In tabling your report in Parliament, I trust that you will take into account:

- *the absence of an agreed ICT control framework in Local Government;*
- *the absence of our awareness of, or an agreement about, the application of (your Department's view of) 'best practice';*
- *the large amount of remediation Council has already undertaken;*
- *the future remediation Council has already committed to undertake;*
- *the fact that Council has approved initial funding of $60,000 to commence the remediation of the ICT controls identified in the report;*
- *the size and challenges of our internal IT team; and*
- *Council's heavy reliance* on third party providers, including the LGA.

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[3] 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.[4]

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 LGA and Regional Local Government Association, should consider their position moving forward regarding cyber security direction and guidance and sector ICT communications.

2.2 Cyber security questionnaire

In July 2019, we wrote to all South Australian councils[5] requesting a response to a high-level

[3] 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.

[4] Department of the Premier and Cabinet, *Cyber security*, <https://www.dpc.sa.gov.au/responsibilities/protective-security-framework/cyber-security>, viewed 12 March 2020.

[5] Except the District Council of Coober Pedy, as we have previously examined ICT arrangements for this council.

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.

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[6] and/or conducting penetration testing through an independent security vendor.

2.3 City of Prospect

2.3.1 Overview

The Council is responsible for managing its local area of approximately 7.81 km² with a population of over 21 000 people,[7] located about 5 km north of the centre of Adelaide. It includes all or parts of the suburbs of Collinswood, Medindie Gardens, Fitzroy, Prospect, Ovingham, Thorngate, Broadview, Nailsworth and Sefton Park.

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

- parks and reserves, sports facilities, venues and halls
- library, information and children's services
- bus services and other support programs
- roads, footpaths, street trees, street lighting
- stormwater drainage
- rubbish collection and disposal.

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

2.3.2 Council challenges

In conducting this examination, the Council wanted to highlight some of the challenges and competing priorities that it experiences in its daily operations. They can impact the available resources and funding it can apply to managing its ICT environment.

In particular, the Council advised us that it recently went through a major change in relocating from the Thomas Street Centre in Nailsworth (main office), the Nailsworth Community Hall in Collinswood and the Prospect and Walkerville Depots to a new Council and community building, Payinthi,[8] on Prospect Road. The new building opened in mid-October 2019.

The Council is also working through several challenges relating to ICT operational and support resources, ICT projects and security.

---

[6] 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.

[7] Refer to <www.prospect.sa.gov.au>, viewed March 2020.

[8] Payinthi was the project that consolidated the Council's administration, library and art gallery.

2.3.3 Budget

The Council reported a net surplus of $1.4 million in its 2018-19 audited financial statements. This was up from a deficit of $214 000 in 2017-18. The surplus was largely attributed to amounts received specifically for new or upgraded assets.

Commitments due to the construction of Payinthi have impacted the Council's long-term financial plan in recent years. Payinthi was funded through loan borrowing, existing working capital and projected asset sales. Based on a set of adopted assumptions, a short-term operating deficit has now been forecast, returning to operating surpluses in later years.[9]

Figures 2.1 and 2.2 show the Council's sources of income and expenditure incurred to deliver services to the local community in the past two financial years.[10]

Figure 2.1: Sources of income and expenditure incurred in 2018-19

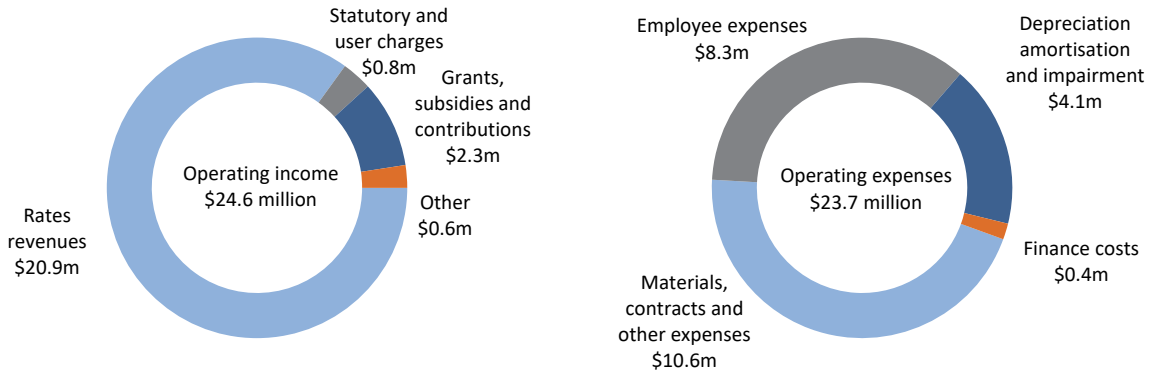
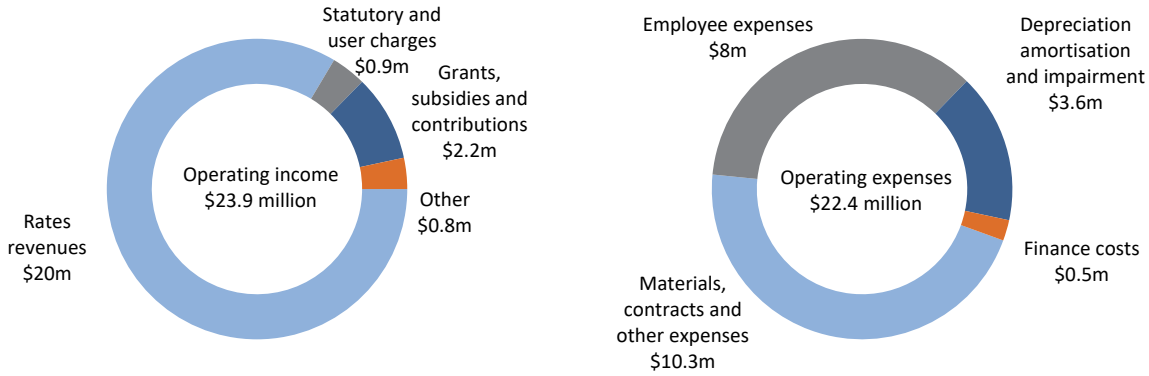


Figure 2.2: Sources of income and expenditure incurred in 2017-18



The Council's ICT spend for 2018-19 was $944 000, which was up from $814 000 in 2017-18.

[9] Data sourced from the Council's 2020-21 annual business plan.

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

In 2019-20 the Council allocated $1.13 million to ICT, split between operating expenditure ($982 000) and capital expenditure ($146 000).

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

2.3.4 Information and communications technology

The Council employs approximately 90 staff of which the Information Technology (IT) team has two team members (includes one vendor support person). The IT team focuses on services internally managed by the Council and is led by the Information and Customer Service Manager, who is also responsible for information security management.

The Council's ICT services, including help desk and local infrastructure support, are outsourced to an external service provider. Service agreements are also in place to support the Council's EDRMS, database administration and complex ERP system issues. Other Council systems are also supported by software vendors.

The IT team performs a range of critical functions to provide support, management and control of multiple computer systems (ICT applications and hardware) used by various Council departments. These functions include maintaining and upgrading the Council's website, software applications, information databases and hardware. They also help provide the community with the ability to interact with Council electronically.[11] The Council's website is maintained by an external service provider and is hosted by the LGA.

Several ICT projects were recently completed, including migrating to a new email service, replacing and implementing new scanning tools and reviewing the Council's Geographic Information System and associated data. The Council also conducted significant ICT infrastructure planning when preparing for its move to Payinthi.

Several projects previously delayed by the move and the COVID-19 pandemic are now regaining momentum. These include major upgrades to the Council's ERP, EDRMS and infringements systems. The Council is introducing a SharePoint intranet site to enhance existing processes and implementing additional tools to help with report writing and dissemination. Work is also being done to complete the implementation of additional cyber security measures.

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*

[11] Refer to City of Prospect Annual Report 2018-19.

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, procedures and strategy

Recommendation

The Council should enhance its existing information security policies to address missing control aspects.

The Council should also develop a cyber security strategy that has a clear action plan to track and mitigate its cyber risks.

Finding

The Council has several ICT policies, including:

- Knowledge and Information Management Policy
- Council Members Records Management Policy
- Corporate Risk Management Policy
- Information Technology Disaster Recovery Plan
- Information Security Incident Response Plan
- Mobile Phones and Devices Policy.

Despite this, we noted that these policies did not address:

- patch and vulnerability management
- change management
- third party risk management
- network security
- user access management.

We also noted that there was no information security strategy or roadmap establishing the Council's capabilities, direction and cyber security priorities.

Why this is important

Without complete established policies or strategies there is a high reliance on the experience and skills of key personnel for the implementation and management of cyber security controls. This could result in the Council's cyber security risks, business objectives and security controls being misaligned.

Policies also help to establish a clear direction on how information security should be consistently managed within the Council. They should include an appropriate definition of accountability and responsibilities for information security.

Having an information security strategy ensures that the Council's ICT objectives and direction are clearly established to guide information security improvement initiatives and performance management. An established and consistently implemented approach to managing information security is important so that controls are consistently applied to provide the desired level of protection across the Council.

Council response

The Council acknowledged our recommendation to improve its information security policies.

The Council advised that rectification work had been planned for completion last financial year, however the project was delayed due to the reprioritising of ICT resources for the move to the new building and COVID-19.

The Council advised us that our findings would be addressed as part of the review of current policies and the development of the following focussed policy documents:

- ICT security
- user access management
- internet and email
- network security (including remote access)
- change management
- third party risk management
- patch and vulnerability management.

The Council also advised that an Essential Eight framework review was planned to be completed by its ICT service provider. However, this project was also delayed due to reprioritising ICT resources for the move to the new building and COVID-19.

The completion of the Essential Eight framework review has now been scheduled for November 2020. A formal cyber security roadmap will then be developed in December 2020. The maturity level of each mitigation strategy will be assessed.

4.1.2 Insufficient cyber awareness training during induction

Recommendation

The Council should formalise introductory information security user awareness training for all new employees as part of their induction. This should include a balance of both personal and Council cyber security considerations.

Finding

With help from an outsourced security provider, the Council conducts an ongoing user awareness program. Typically, sessions are held every 18 months with detailed results provided to the Council. Two sessions were held in the past 18 months, with the most recent one run during our examination in February 2019. This training included phishing awareness and recorded a 95% employee attendance rate.

Additionally, cyber awareness emails sent periodically provide security information to Council employees. This includes advising employees of known phishing email attempts, password security and information handling.

Despite these proactive measures we noted that new employees are not required to participate in cyber awareness training sessions or e-learning activities during their induction.

Why this is important

While society's data dependency continues to rise, so do cyber 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 the Council's cyber security awareness efforts continue and improve to ensure all employees, including new employees, are aware of their responsibilities and how to protect themselves and the Council from cyber threats.

Council response

The Council stated that in addition to the proactive measures promoting cyber awareness that we identified, formal information security awareness training will be included in the induction of all new employees in future. New staff will also be provided with a cyber resilience guide.

Broader general awareness training will be provided annually to all staff. A program will be established with help from specialist vendors registered on the Local Government Information Technology Procurement Panel.

Further, the Council stated that it is planning to develop a SharePoint workflow for onboarding and inducting new employees. The functionality will help to formalise the induction process. This was expected to be completed last financial year, but was also delayed when ICT resources were reprioritised.

4.1.3 Insufficient management of risks over third party service providers

Recommendation

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

Finding

The Council uses the Local Government Procurement Panel to choose its third party ICT vendors and service providers. It maintains contracts with these third parties that contain

clearly defined roles and responsibilities. It is also supported by performance management processes.

Despite this, we found that no formal cyber risk assessments were conducted or documented prior to procuring third party services.

There was also no formal approach established to identify, manage and monitor third party service providers over the life of the contract, including contract compliance and security risk management 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 sensitive data, the exposure to potential cyber threats is likely to increase. Numerous industry studies of 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 critical to reducing the likelihood of new security threats being introduced to the Council and to ensuring that services are provided in line with the Council's risk appetite.

Council response

The Council stated that a cyber security risk assessment of vendors on the ICT vendor panel is not conducted by the Local Government Procurement Panel to determine the level of risk for councils when the vendor is engaged. Recent advice from the Panel is that councils should conduct this assessment as part of their own internal due diligence.

The Council acknowledged this finding and stated that it will collaborate with the LGA and other councils that have agreements with the same service provider to investigate sharing the cost of an independent cyber security consultancy to help assess the provider.

The Council advised us that initial and very early discussions at a local government ICT Conference in October 2020 suggested providing a specialist resource to help develop a framework and assist councils with assessments and/or addressing cyber security issues. This expertise could potentially be sourced for specialist cyber security advice.

4.1.4 ICT risk register and reporting does not exist

Recommendation

The Council should implement an ICT risk register that adequately captures and tracks key cyber risks. This should include clearly defined ownership and treatment plans for all risks.

Risks should be periodically reviewed and reported to a governance committee responsible for ICT.

Finding

The Council maintains a strategic risk register that refers to cyber crime/fraud risk at a high level. This register does not have assigned technical owners for each ICT risk.

There is no ICT specific risk register to capture and track ICT risks or instances of non-compliance with information security policy requirements, and the related treatment plans.

Why this is important

Without processes to capture, track 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. It also reduces the Council's ability to effectively demonstrate that it has reduced its ICT risks over time.

Council response

The Council stated that in addition to its existing strategic risk register, a specific ICT risk register will be developed concurrently with the development of or after developing its focused ICT security policies.

The Council also stated that some risks are reported by staff through the Council's help desk. They are documented and advice about them is communicated to other staff by email.

Finally, the Council stated that an ICT risk register will be developed to record and track risks and their treatment plans. A process will be developed to ensure that each risk identified has a treatment plan or action to complete a treatment plan. Risks and plans will be reviewed and updated quarterly. The ICT risk register will be maintained by the IT team and updated as additional risks are identified. It will also be reviewed annually as part of the engagement of an independent cyber security vendor to conduct annual penetration testing and vulnerability assessments of the Council's environment.

4.1.5 No ongoing review or assurance over ICT controls

Recommendation

The Council should conduct periodic security testing and audits to evaluate its information security control environment. This should include penetration testing of all internet facing services, an asset vulnerability assessment and security control audits.

The results of these activities should be documented and tracked in the ICT risk register and reported to the governance committee responsible for ICT.

Finding

The Council's ICT provider reviews its managed ICT controls on an ongoing basis, with regular performance reports provided to the Council.

Despite this, the Council does not conduct any periodic testing or assurance reviews of its overall information security control environment.

Why this is important

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

Council response

The Council stated that its ICT service provider reviews its managed ICT controls on an ongoing basis and provides regular performance reports. It said that formal security testing, however, has been delayed since late 2018 due to the preparation and maintenance of three temporary work sites and planning for the move to the new building. An independent cyber security vendor will be engaged to conduct annual formal penetration testing and vulnerability assessments of its environment.

5 System security

5.1 Findings

5.1.1 Weaknesses in password controls

Recommendation

The Council should ensure that password controls are applied to all user accounts in line with its password policy. This includes ensuring that the minimum password length is increased (10 characters with complexity enabled) and passwords are set to expire.

Strong password practices should be encouraged as part of the Council's ongoing information security user awareness program.

Finding

We identified 22 Active Directory user accounts, which included elected Council members and several domain administrators, with passwords that did not expire. In addition, the password minimum length was only eight characters.

We conducted a password cracking exercise and identified the following:

- 136 weak passwords were compromised out of 533 accounts, two with Domain administration privileges
- despite meeting the minimum Windows default complexity requirements, we were able to crack 99% of the passwords we tested (134 out of 136).

Why this is important

A lack of appropriate password controls weakens the Council's overall ICT security. It increases the risk of accounts being compromised and unauthorised access to the Council's ICT systems.

Strong password rules should be enforced to improve the uniqueness of passwords, which should include 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 stated that it had reviewed accounts with non-expiring passwords. It also implemented a separate process for password change for users who do not log into the Council's domain. This will be a manual process carried out on a three to six month basis and will involve the IT team and the user.

The Council stated that non-expiring passwords were provided to specific users who could not log into its domain to change their password.

The Council also stated that its password policy was updated in August 2020 as part of the planned work to strengthen its security profile. The password length requirement has been increased beyond the recommended length. Approximately 95% of users have been forced to change their passwords, with the remaining users needing to change their passwords before mid-November 2020.

The Council stated that the rollout of two-factor authentication with Office 365 in 2019 was delayed and interrupted by COVID-19. Configuring two-factor authentication for each user was planned for completion in October 2020.

Finally, the Council advised us of some additional measures that it will introduce to strengthen its security profile.

5.1.2 Weaknesses in privileged access management practices

Recommendation

The Council should consider the following control improvements:

- review privileged user accounts across Active Directory, databases and applications and cloud services to identify accounts that should either be removed or have reduced privileges reduced. Implement an ongoing periodic review process
- conduct activities that require a heightened level of access using individual privileged accounts that are separate to a user's standard account
- implement stronger password controls for privileged accounts, which includes longer and stricter passwords (such as non-dictionary words) and ensuring they are changed every 30 to 90 days.

Finding

Testing of Active Directory privileged users identified 25 accounts and eight groups with domain level administrative privileges. A review of privileged access management practices identified the following weaknesses:

- 13 of the 25 accounts with domain level administrator privileges were identified by the Council and the third party vendor as inappropriate
- employees performing privileged activities on Council servers used their everyday user account instead of a unique individual administrative account
- a former employee's Active Directory account with domain level administrator privileges was still enabled
- there were several active vendor shared privileged accounts
- there were no periodic user access reviews to confirm the appropriateness of privileged accounts.

Why this is important

Weaknesses in managing privileged user accounts with access to the Council's ICT environment reduce the Council's security controls. The credentials of privileged accounts

which includes the ability to make system changes and access sensitive data, potentially increases the severity of any compromise. The use of generic/shared accounts reduces individual accountability and the traceability of actions performed through these accounts.

In addition, not regularly and thoroughly reviewing privileged accounts increases the risk of inappropriate or unauthorised access to Council systems. This could compromise the confidentiality, integrity or availability of sensitive information.

Council response

The Council stated that it is important to note that staff who have terminated their employment with the Council do not have access to any systems as their password is changed immediately by the IT Administrator.

The Council acknowledged our findings and advised us that the following issues have been addressed by the Council's ICT service provider:

- Privileged accounts were reviewed – accounts have been removed or privileges updated.
- Unique individual administrative accounts were created for employees performing privileged activities on Council servers.
- The former employee's Active Directory account with domain level administrator privileges was removed.
- Privileged accounts will be reviewed bi-annually and privileges updated if needed.
- Its password policy was updated in August 2020.
- Password length has been increased beyond the recommended length.
- The Password complexity requirement has been increased.
- Two-factor authentications for remote access used by service providers (using individual accounts) was implemented in September 2020.
- SecureLink will be implemented for third party access.

5.1.3 Insufficient user access management

Recommendation

The Council should establish a user access management policy and procedure that explains the process for adding, modifying and removing user access.

Given the termination exceptions we identified, more emphasis should be placed on this process to improve its effectiveness. The policy and procedure should also document the 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
- simplified by documenting system roles and profiles and mapping them to job roles.

The Council should also review the terminated user exceptions and investigate any activities performed after a user's termination date. Terminated employee accounts should typically be removed no later than three to five working days from termination date. To support the process, a monthly review should be performed of terminated employees against systems access listings. Where the Council requires access to a terminated user's account, the level of access should be minimised to only what is necessary.

Finding

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

We conducted sample testing of new users added to Council ICT systems over nine months. We found that there was no consistent approach to provisioning new user access. Several accounts created did not have a supporting access request or approval.

Similarly, through our sample testing of the employee termination process, we could not identify a consistent approach to removing user access from the Council's ICT systems. Our sample testing identified that:

- five of nine terminated employee accounts were still enabled in Active Directory. The Council advised us that it had documented evidence of the reasons why some access to these accounts should remain active, such as to maintain access to a user's email account. We noted, however, that not all access assigned to these terminated accounts was still required
- of these accounts, three had been logged into after the user's 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 in cyber attacks. If terminated employee or contractor accounts are not removed promptly, there is an increased risk that an obsolete user account could be used to perform inappropriate or unauthorised activity. This may result in the confidentiality, integrity or availability of sensitive information being compromised.

Council response

The Council stated that it is important to note that staff who have terminated their employment with the Council do not have access to any systems as their password is changed immediately by the IT Administrator. Access to systems that the terminated employee would use is then removed.

The Council also stated that it would develop a user access management policy. This was planned for completion last financial year, but was delayed by the reprioritising of ICT resources for the move to the new building and COVID-19.

The Council plans to develop a SharePoint workflow for new and existing employees that will help to formalise this process, including determining the appropriate level of access to corporate applications. Work on this is in progress.

The Council stated that a review of user access to modules in its ERP is conducted annually as part of its external audit. A review of user access to its EDRMS was conducted and updated as part of the development of a new Business Classification Scheme in late 2018.

Finally, the Council stated that despite being scheduled in its work program, an annual review was deferred by the preparation and maintenance of three temporary work sites and planning for the move to the new building, COVID-19 and resource constraints. A review of access to all systems will be conducted annually and a process will be developed as part of the work program for a new business analyst who was starting in October 2020.

5.1.4 Weaknesses in patch management

Recommendation

The Council should apply more rigour to its vulnerability management processes by establishing a 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 time frame after their release
- the requirement to document the rationale for deciding not to install a patch.

The Council should review the results from the vulnerability assessment we performed and ensure that missing patches are tested and remediated. It should also consider either upgrading or replacing legacy unsupported software and underlying components.

Finding

We identified that the Council's ICT service provider applies patches and security updates to the Council's Active Directory environment. The timeliness of this can be subject to the readiness of the vendor and other dependencies.

Despite the consistent monthly updates, we identified the following weaknesses in the Council's vulnerability patching of its systems:

- although the Council advised us that some patching requirements are contained in its vendor contract arrangements, overall the Council did not have a vulnerability and patch management policy and procedure
- our vulnerability assessment scans revealed there was a considerable amount of unsupported legacy software installed within the environment.

Why this is 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. Unreliable system patching also increases the risk of ransomware attacks.

Further, a lack of vendor support for legacy systems 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 will not be identified and remediated promptly and efficiently.

Council response

The Council acknowledged our findings and stated that the missing patches and security updates we identified have now been installed. Windows Server machines have been upgraded and are fully patched and under full vendor support, and a non-production server identified as having vulnerabilities was decommissioned. A time delay exists between the release of patches and updates and applying them to its environment to allow for testing by the Council's ICT service provider.

The Council also stated that a review of patching and security updates and the details of any delay in applying them and any resulting impacts will be documented and communicated in regular internal account management meetings. This finding has been highlighted with the Council's ICT service provider. The vendor will compile this information as a regular agenda item in each meeting

The Council's production server running ERP is being decommissioned as part of an upgrade planned for completion in December 2020. Shortcomings identified in the Council's Geographic Information System environment are planned to be addressed by the new business analyst starting in October 2020 as part of planned work identified in the Council's ICT strategy. This project was delayed due to resource constraints.

Finally, the Council stated that it will develop a vulnerability and patch management policy and it is currently in discussions with its ICT service provider about this.

5.1.5 Insufficient end user device security

Recommendation

The Council should develop and implement a policy that establishes an approach to securing workstations and laptops (end user devices). These devices should be subject to security controls, in line with industry standards (such as the Centre for Internet Security standards).

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

Finding

The Council's end user devices are protected by several security controls. These include restricting local administration privileges, using an antivirus product and the Windows antivirus solution (Windows Defender), hard drive encryption, email security and a mobile device management solution.

Despite this, we noted that more advanced endpoint protection techniques were not implemented to reduce the ability for malicious software to execute. Such techniques include enabling:

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

We also noted that the Council did not have any policies 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 in the Windows 10 antivirus solution designed to combat the threat of malware exploiting legitimate functionality in Microsoft Office applications.

Application whitelisting is a technique recommended in the Australian Signals Directorate's Essential Eight controls. It helps prevent 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, through methods like ransomware.

Council response

The Council stated that its end user devices are currently protected by several security controls and will be further strengthened as we recommended.

The Council also stated that:

- advice it received from its current antivirus solution vendor is that the antivirus product currently deployed has very comparable controls to Windows Defender ASR (attack surface reduction). This feature is not enabled and is subject to additional licensing as it is not available by default in Windows
- the development of a focused end user device security policy will be addressed as part of the review of current policies and the development of a focused policy document (refer to section 4.1.1)
- application whitelisting will be determined and executed once the Essential Eight framework review is completed.

6 Change management

6.1 Detailed findings

6.1.1 Gaps in change management controls

Recommendation

The Council should establish a change management policy and procedure that is applicable to its ICT environment. The procedure should be endorsed by management and agreed by both business and the IT team. It should also include how security risks will be addressed in any 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 of the system owner's approval to release should be documented and tracked in a centralised change management repository. Segregation of duties should be applied between the developer, approver and promoter of system changes.

Finding

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

- The Council does not have change management policies or procedures to control changes that are applied to its ICT environment.
- No records are retained of system testing and approval of major changes prior to implementation for systems other than the Council's ERP suite and EDRMS.
- Records, including approvals, are not stored in the Council's centralised repository (EDRMS) for system changes other than for its ERP suite and EDRMS.
- For all systems other than the Council's ERP suite and EDRMS, there is no separate environment available to test system changes and patches before they are implemented into the production environment. An example is changes made to the Council's Active Directory 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 critical to ensuring consistency in change management across all ICT systems and that changes are effective and in line with the Council's expectations.

Not having 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. There is also an increased risk that new systems or services will be inadvertently implemented, which could introduce additional security vulnerabilities into the ICT environment.

Council response

The Council acknowledged our recommendation to enhance its information security policies. The development of a change management policy and formalised process has been recommended by its external auditor and was planned for completion last financial year, but was delayed by the move to the new building and COVID-19.

The Council also stated that:

- a formal change management process is used by its ICT service provider for the maintenance of its infrastructure. Records of system testing and approval of major changes to the Council's core ERP and records management systems are retained
- the current and ongoing change management procedures involving its ICT service provider are being revised to improve the change management process
- our findings regarding separate test environments are acknowledged and have been subject to budget constraints and timelines for the refresh of the Council's infrastructure
- separate integrated test environments are being planned as part of the refresh of its server environment
- a change management policy will be developed (refer to section 4.1.1).

7 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 forms 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 could contain additional information that could be used by an attacker. Further, some fundamental security aspects also required strengthening so that other potential vulnerabilities were not exploited.

The Council responded with details of its remediation activities and time frames.

8 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 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 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	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

Term	Description
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 staff 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