[P.P.4P

Report of the Auditor-General

Report 1 of 2021

Examination of cyber security: City of Port Adelaide Enfield

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 1 of 2021 *Examination of cyber security: City of Port Adelaide Enfield*

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 Port Adelaide Enfield.

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 Port Adelaide Enfield.

Content of the Report

We examined the arrangements established by the City of Port Adelaide Enfield 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 Port Adelaide Enfield were not operating effectively. We do acknowledge that the City of Port Adelaide Enfield has implemented some controls over its core Enterprise resource planning system.

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

The City of Port Adelaide Enfield responded positively to our recommendations and commenced improvement activities during our examination. We also noted that the City of Port Adelaide Enfield maintains:

- a process where new starters are made aware of its ICT policies and some user awareness material is available on the intranet
- frequent security patching of its core Enterprise resource planning system
- a documented disaster recovery plan which also includes details of its backup arrangements
- fundamental security controls over its end user devices, including restricting administration privileges and using antivirus software and advanced endpoint protection.

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.

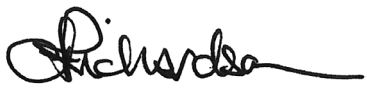
The examination was conducted in line with the Standard on Assurance Engagements ASAE 3500 *Performance Engagements*. We complied with the independence and other relevant ethical requirements for assurance engagements.

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 Port Adelaide Enfield.

Yours sincerely



Andrew Richardson
Auditor-General

Contents

1 Executive summary 1

1.1 Introduction 1
1.2 Conclusion 1
1.3 What we found 2
1.4 What we recommended 3
1.5 Response to our recommendations 4

2 Background 6

2.1 Cyber security overview 6
2.2 Cyber security questionnaire 6
2.3 City of Port Adelaide Enfield 8
2.3.1 Overview 8
2.3.2 Council challenges 8
2.3.3 Budget 9
2.3.4 Information and communications technology 10
2.3.5 Relevant law and guidance 11

3 Audit mandate, objective and scope 12

3.1 Our mandate 12
3.2 Our objective 12
3.3 What we examined and how 12
3.4 What we did not examine 13

4 Security governance 14

4.1 Detailed findings 14
4.1.1 Insufficient coverage of information security related policies, procedures and strategy 14
4.1.2 Gaps in security user awareness training program 15
4.1.3 Insufficient management of risks and contracts over third party service providers 16
4.1.4 ICT risk register and reporting does not exist 17
4.1.5 No ongoing review or assurance over ICT controls 18

5 System security 19

5.1 Detailed findings 19
5.1.1 Weaknesses in password and authentication controls 19
5.1.2 Weaknesses in privileged access management practices 20
5.1.3 Insufficient user access reviews 22
5.1.4 Security updates not regularly installed 23
5.1.5 Insufficient end user device security 24

6 Change management 26
6.1 Detailed findings 26
6.1.1 Insufficient change management controls 26
7 Backup operations, disaster recovery and incident response 28
7.1 Detailed findings 28
7.1.1 Gaps in backup and ICT disaster recovery arrangements 28
7.1.2 Information security incident response plans not established 29
8 Vulnerability assessment results 31
9 Explanation of terms used in this report 32

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 Port Adelaide Enfield (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 9 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 implemented some controls over its core enterprise resource planning (ERP)[1] system.

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 responded positively to our recommendations and commenced improvement activities during our examination. We also noted that the Council maintains:

- a process where new starters are made aware of its ICT policies and some user awareness material is available on the intranet
- frequent security patching of its core ERP system
- a documented disaster recovery plan which also includes details of its backup arrangements
- fundamental security controls over its end user devices, including restricting administration privileges and using antivirus software and advanced endpoint protection.[2]

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)	• Insufficient coverage of information security related policies, procedures and standards. • Gaps in security user awareness training program. • Insufficient management of risks and contracts 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 and authentication controls. • Weaknesses in privileged access management practices. • Insufficient user access reviews. • Security updates not regularly installed. • Insufficient end user device security.

[1] The ERP system is used by the Council in the management and integration of its financial, supply chain procurement, accounts payable, budgeting, records management, property and rating, development assessment, health inspections, expiations, receipting, performance planning and reporting, customer service requests, human resources and payroll activities.

[2] The practice of protecting endpoints or entry points of end-user devices (such as desktops and laptops) from being exploited by hackers.

Area	Findings
Change management (section 6)	• Insufficient change management controls.
Backup operations, disaster recovery and incident response (section 7)	• Gaps in backup and ICT disaster recovery arrangements. • 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. • The web application was using vulnerable software libraries and we identified exposures related to the administrative portal. Certain documents 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 related policies and develop a cyber security strategy. • Formalise an introductory and ongoing information security user awareness program. • Formalise a security risk management approach to identify and manage third party service provider risks, with an ongoing security performance review for high risk service providers. • Formalise the ICT risk register with risks periodically reviewed and reported to a governance committee(s) responsible for ICT. • Increase the frequency and scope of periodic security testing and audits with the results documented and tracked in the ICT risk register.
System security (section 5)	• Ensure password controls are applied to all accounts in line with the Council's password policy and strong password practices are encouraged. • Review, at least annually, the password settings configured in Active Directory and apply multi-factor authentication for all users with remote access.

Area	Recommendations
	• Review privileged accounts and ensure activities that require a heightened level of access are conducted using individual privileged accounts. • Restrict domain administration accounts from being able to access internet services and implement stronger password controls for privileged accounts. • Update the security management policy to ensure it includes user access review requirements for all Council ICT systems. • Conduct user access reviews regularly, and at least annually. • Apply more rigour to vulnerability management processes and regular patching of all Council systems. • Vulnerability assessments should be undertaken periodically to identify any potential missing patches. • Develop and implement a policy for securing end user devices and consider implementing a well configured mobile device management solution.
Change management (section 6)	• Develop a change management policy and procedure that is applicable to the Council's ICT environment. • Evaluate all changes and patches released by vendors in a separate test environment before releasing them into production. Segregate the duties of the developer, approver and promoter of system changes.
Backup operations, disaster recovery and incident response (section 7)	• Review the disaster recovery plan to ensure it accurately reflects the Council's current recovery arrangements, includes key recovery metrics and expands on its recovery procedures for all key business systems. • Ensure the business continuity plan includes identified Maximum Allowable Outage Times for all of the Council's key business systems. • Clearly define and implement a formal approach to test backup restorations and disaster recovery plans. • 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:

> *The City of Port Adelaide Enfield welcomes the report from the Auditor-General which will assist Council to further strengthen our existing cyber*

security controls. Although the Council has implemented a number of effective cyber security controls, the audit identified where Council can improve its cyber security across all systems and strengthen our strategy, policies and procedures.

A key finding in the audit was our risks and controls are not clearly documented within Council's policies, procedures and business continuity plans. As a result of the audit Council will be allocating an additional resource to fully document our cyber security controls and ensure that they are applied across all systems. As a result of the audit Council will develop a strategy which will be based on the maturity levels defined in the Australian Cyber Security Centre's essential eight maturity model.

Council agrees with the audit's recommendations to strengthen end user training and this aligns with Council's plans for 2020-21. Human error is often involved in cyber security attacks. Training our staff to understand and avoid common security threats will significantly reduce cyber security risks.

The Auditor-General's report, together with an action plan developed by the Administration has been presented to and reviewed by Council's Audit Committee and the Council. Council has endorsed the action plan to address the findings within the audit.

Council is committed to continual improvement of cyber security controls to mitigate the risk of damage to Council's information systems and operations and will implement the improvements using a risk based approach.

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 Port Adelaide Enfield

2.3.1 Overview

The Council area covers over 94 km^2 with a population of around 126 000 people. The area is located across the inner north and north-western suburbs of Adelaide and extends from the River Torrens to Outer Harbor. It is one of the largest metropolitan councils in South Australia and was established in 1996 by the amalgamation of the City of Port Adelaide and the City of Enfield.

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

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

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

2.3.2 Council challenges

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

In particular, the Council stated that it manages a large and diverse geographical area that has a range of internal and external challenges.

When compared to Greater Adelaide, the Council advised that its region has a higher proportion of low-income households, which requires it to deliver specific services and

[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.

programs that help strengthen community resilience. The Council is also currently seeking to stimulate the local economy and provide hardship support due to the impacts of the COVID-19 pandemic.

The region is home to unique natural environments including large constructed tidal wetlands, nature reserves, dolphin and bird sanctuaries, coastal beaches, extensive mangrove and samphire areas and freshwater rivers and creeks. The Council's preservation of its cultural environment is challenged by the impacts of climate change, heatwaves, coastal erosion and inundation and flooding.

The area also has a significant amount of strategic economic infrastructure, including port facilities, industrial land, commercial and retail areas and tourism assets. The Council advised us that it continues to support the economic growth of defence related industries by helping to secure local job opportunities.

In addition, due to changes to the waste management market, the Council advised us that it was collaborating with another council to construct a waste material recovery facility.

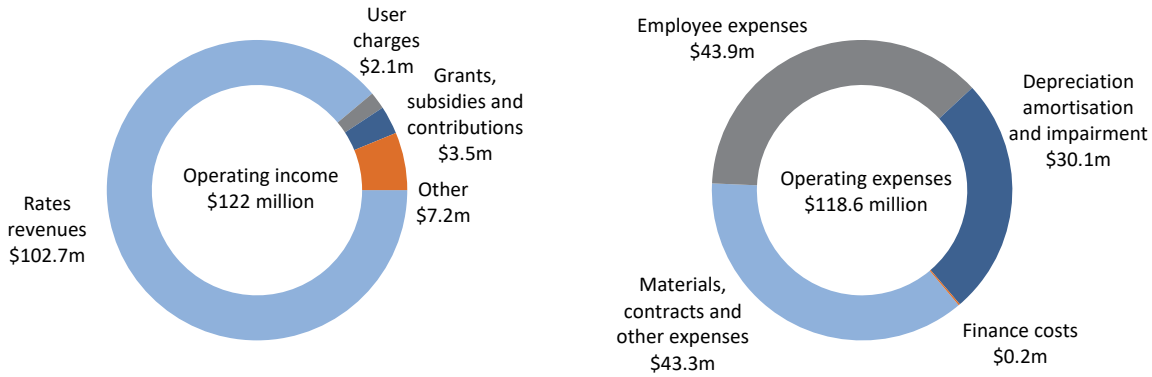
The SA Government is undertaking significant legislative reform in its planning system, which the Council considers will impact its urban development, heritage and environmental protection activities. The SA Government is also undertaking local government reform that aims to strengthen transparency and accountability, drive efficiency and deliver good governance.

2.3.3 Budget

The Council reported an operating surplus of $4.4 million in its 2018-19 audited financial statements. This was up from a surplus of $2.7 million in 2017-18.

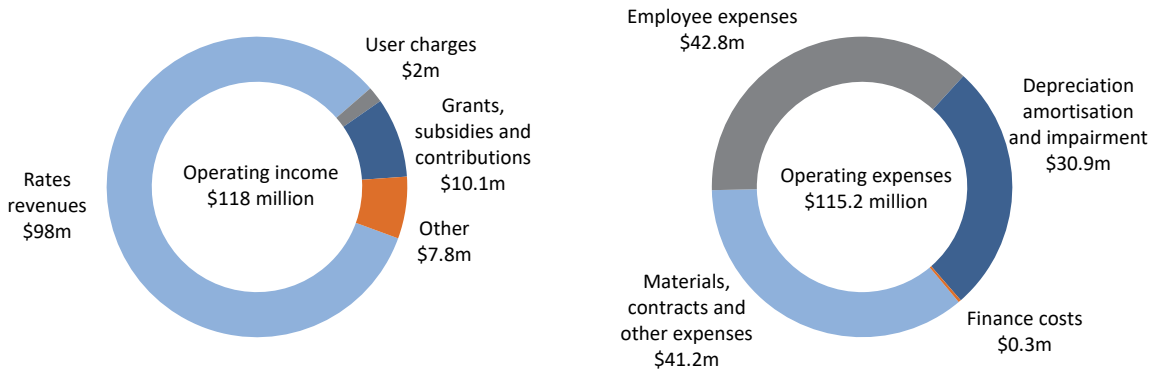
Figures 2.1 and 2.2 show the Council's sources of income and expenditure incurred to deliver services to its local community in the past two financial years.[7]

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



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

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



The Council's ICT spend for 2018-19 was $3.1 million which was down from $3.2 million in 2017-18.

In 2019-20, the Council allocated $3.99 million to ICT, split between operating expenditure ($3.44 million) and capital expenditure ($544 000).

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

2.3.4 Information and communications technology

The Council has approximately 465 staff for its general operations, of which the Information Technology (IT) team has 16 members. The Corporate Information 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.[8]

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.

Several ICT specific projects are currently in progress or completed, including a backup system refresh, implementing computer system monitoring alarms, a server and storage refresh, conversion of an internet content management system, replacing the email and web scanning service, replacing Council workstations including those used by the public in libraries, and upgrading a major line of business software system.[9]

In response to our 2019 questionnaire (discussed in section 2.2), the Council indicated that most of its key ICT systems are supported by external vendors while being hosted internally. The Council also said that it continues to work on several ICT areas that are posing a challenge operationally.

---

[8] Refer to City of Port Adelaide Enfield Annual Report 2018-19.

[9] Refer to Port Adelaide Enfield Council Annual Business Plan and Budget 2019-20.

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 Insufficient coverage of information security related policies, procedures and strategy

Recommendation

The Council should enhance its existing information security policies to address the 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 information security and risk management policies, including:

- an ICT systems security policy
- a business continuity plan
- a risk management policy and procedure
- an ICT disaster recovery plan.

The Council also has a manual that clearly defines the roles and responsibilities for managing its different application systems.

Despite this, we noted that there were no policies and procedures that adequately covered the following areas of information security control:

- details of the patch management process and scheduling
- change management
- incident management to address cyber security events such as phishing, unauthorised access or virus/malware
- third party ICT security risk management prior to procurement and throughout the contract life cycle
- requirements for auditing and monitoring security events
- security controls/requirements to reduce vulnerabilities
- testing of security controls to ensure they are operating effectively.

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

Why this is important

Without 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 assign accountability and responsibility 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 information security strategy helps ensure that the Council's objectives and direction are clearly documented to guide information security improvement initiatives and performance management. It also helps ICT controls to be consistently applied with the desired level of protection.

Council response

The Council advised us that management will review the existing ICT systems security policy to incorporate the additional controls we identified in our review.

The Council also advised us that management will develop and adopt a cyber security strategy. It will be based on the maturity levels defined in the Australian Cyber Security Centre's Essential Eight maturity model.

4.1.2 Gaps in security user awareness training program

Recommendation

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

Training participation by employees should be formally tracked.

Finding

Cyber security videos produced by Local Government Risk Services (LGRS)[10] are made available on the intranet for all Council employees to help build cyber awareness. In addition, a phishing email awareness quiz was conducted in mid-2019 to raise the awareness of all Council employees about detecting and responding to phishing emails.

The Council advised us that its new starters are required to sign its ICT systems security policy before being provided with their account login details. This policy defines certain controls the Council has implemented to manage security risks.

[10] Refer to <https://lgrs.com.au/>.

Despite this, the Council does not have a formal information security user awareness training program for new and existing employees.

Why this is important

While society's data dependency continues to rise, so do cyber incidents. Attacks are becoming more sophisticated and 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 are aware of their responsibilities and how to protect themselves and the Council from cyber threats.

Council response

The Council advised us that training was occurring but could be strengthened to deliver a more comprehensive program. Plans are underway to develop and deliver a security awareness program to further develop staff awareness and skills in cyber security.

The Council also advised us that records of completed cyber security training will be held in its human resource management system.

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 review of their security risk management performance.

Finding

The Council has a procurement procedure that requires procurement plans and risk assessments to be done.

The Council has contracts with its ICT vendors and service providers that contain defined roles and responsibilities and performance management processes. In addition, Council policy requires the IT team's approval before starting an ICT procurement process.

Despite this, the Council could not provide any evidence that 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 security risks associated with third party service providers over the life of the contract.

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 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 advised us that risk assessments of third party suppliers do occur however this will be strengthened in its procurement procedures. The procedures will be updated to include a cyber risk assessment and cyber security controls questionnaire in the requirements for assessing and evaluating third party service providers.

4.1.4 ICT risk register and reporting does not exist

Recommendation

The Council should formalise its ICT risk register to adequately capture and rate cyber risks. This should include clearly defining 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 which identifies a few ICT related risks. The risks are captured at a governance level with no assigned technical control owners.

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

The monthly strategic meetings held by the IT operations team do not include any regular discussions or checks on cyber security performance or the mitigation of ICT risks.

Why this is important

Without formal processes to capture and report information security risks, Council management'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 advised us that management will incorporate a specific ICT risk section in its

operational risk framework. This is to allow for the inherent and residual risk to be evaluated and also the target risk to be set.

4.1.5 No ongoing review or assurance over ICT controls

Recommendation

The Council should increase the frequency and scope of its periodic security testing and audits to evaluate the entire information security control environment. This should include penetration testing of internet facing services, asset vulnerability assessments 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 for ICT.

Finding

The Council conducted an ICT security review and health check in April and May 2016. This included a governance review, application security testing and a social engineering exercise. In May 2019 the Council completed a further independent ICT review in collaboration with two other metropolitan councils, which included a high-level cyber security review.

Annually the Council's internal audit, together with associated control owners, conduct a self-assessment of five finance related ICT controls. Despite these assurance activities for the core financial application, 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 advised us that security testing does occur but that there is no overarching plan to coordinate the testing and increase its frequency. Management will develop a plan for security testing (based on a risk assessment) over a number of years.

The Council also advised us that the Executive Leadership Team will oversee the effectiveness of ICT controls.

5 System security

5.1 Detailed findings

5.1.1 Weaknesses in password and authentication controls

Recommendation

The Council should ensure that password controls are applied to all user accounts in line with its password policy. Accounts should have passwords that are set to expire (maximum password age of 90 days), password complexity should be enabled within Active Directory and users should be requested to change their password on first login.

Strong password practices should be encouraged as part of the Council's ongoing information security user awareness program (refer to finding 4.1.2).

At least annually, the password settings configured in Active Directory should be reviewed to ensure they reflect the settings specified in the Council's ICT security policy.

Multi-factor authentication should be implemented for all users with remote access to the Council's network or other internet facing services.

Finding

We found that all elected Council members (email access only) and two employees had never expiring passwords in Active Directory. One of the employee accounts had administrator privileges. The Council advised us that there was an issue with the two employee accounts that was being diagnosed.

In addition, Active Directory passwords for new users and resets for existing users are generated and issued by the IT team. The Council advised us that users must change their password at first login, but this requirement is not documented in any policy or procedure.

We also conducted a password cracking exercise and were able to compromise 401 weak passwords across the Council within a short period of time. This was potentially due to a combination of:

- the Council's decision not to enable password complexity within Active Directory
- users not being aware of the importance of creating strong passwords, despite the advice provided in the Council's ICT security policy.

Further, multi-factor authentication is only enabled for selected members of the IT team and is not applied to all Council employees who access its systems remotely.

Why this is important

Passwords are often the only line of defence for an ICT environment. A lack of appropriate password controls weakens the Council's overall security posture. It increases the risk of

accounts being compromised and of 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, 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).

In addition, there is an increased risk of unauthorised access if first-time passwords are not changed and internet facing services or remote access connections are not secured with multi-factor authentication. Both risks have the potential to result in data loss and access to sensitive information.

Council response

The Council advised us that:

- all user passwords have been reviewed since our audit and now align with its password controls
- management will revise the ICT security management policy and include appropriate password controls in the security awareness training
- monthly reports are now being generated to identify non-compliance with the Active Directory settings. The requirement to review this is to be included in the ICT system security procedures
- management is supportive and will implement the recommendation for multi-factor authentication for all users with remote access to the Council's network or other internet facing services.

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, applications and cloud services to identify accounts that should be removed, or that should have reduced privileges. Implement an ongoing periodic review process
- conduct activities that require a heightened level of access using individual privileged accounts, which are separate to the user's standard account
- where shared accounts are required, explore options to improve the governance and monitoring of their use. This includes using a password manager and establishing audit logging
- restrict domain administration accounts from being able to access internet services
- implement stronger password controls for privileged user accounts, which includes longer and stricter passwords (such as non-dictionary words) and ensuring they are changed every 30 to 90 days.

Finding

Our testing of Active Directory privileged users identified 40 accounts and eight groups with domain level administrator privileges. A review of privileged access management practices identified the following weaknesses:

- 32 of the 40 accounts with domain level administrator privileges were either identified by the Council as inappropriate or the Council was not aware of their purpose
- employees performing privileged activities on Council servers either shared credentials or used their everyday user account instead of a unique individual administrative account
- shared privileged account passwords were not stored in a secure password manager
- stronger password controls were not applied to privileged accounts (shared accounts or everyday user accounts with elevated privileges)
- there was no logging and monitoring of individual or shared privileged account user activities
- there were no periodic user access reviews to confirm the appropriateness of privileged accounts.

Why this is important

Failing to adequately control privileged user accounts that have access to the Council's ICT environment reduces the Council's security posture. 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.

The absence of audit logs or periodic active monitoring and review of those logs reduces the likelihood of unauthorised or inappropriate access or system changes being identified promptly. It also compromises the ability to conduct forensic or root cause analysis of security incidents, if required.

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 advised us that:

- management will review and update its ICT system security procedures to reflect the requirement for a regular review
- management agrees with the recommendation that activities that require a heightened level of access should be conducted using individual privileged accounts, which are separate to the user's standard account. The Council is reviewing how best to implement this recommendation

- management agrees and will implement the recommendation that where shared accounts are required, options should be explored to improve the governance and monitoring of their use. This includes using a password manager and establishing audit logging
- management will review the recommendation to restrict domain administration accounts from being able to access internet services, and will assess the risk and the most effective controls.

5.1.3 Insufficient user access reviews

Recommendation

The Council should update its ICT system security management policy to ensure it includes user access review requirements for all ICT systems. User access controls should be established for roles and profiles to enable efficient verification by business unit managers.

User access reviews should be conducted regularly by all business units (at least annually). The Council should ensure that access and associated permissions are appropriately assigned for all users, particularly focusing on high risk functions. Any obsolete access identified should be promptly removed.

Finding

We found that periodic user access reviews were not conducted for all Council ICT systems to confirm the appropriateness of all current user accounts and associated privileges at the application, operating system and database level.

The Council's ICT system security management policy requires user access reviews to be performed for:

- its budgeting system
- the receipting roles and functions of its property and rating system
- delegate access to functions in the accounts payable and accounts receivable systems.

The Council could not provide us with any evidence that these reviews were conducted.

We did note that a user access review was conducted for its core ERP system in February 2020.

Why this is important

Not regularly and thoroughly reviewing user access increases the risk of users retaining inappropriate access to systems and potentially performing unauthorised activities. This could compromise the confidentiality, integrity or availability of sensitive information.

Council response

The Council advised us that management already reviews user access to core enterprise systems where these risks are high. Management will undertake risk assessments for the

remaining systems to determine if a user access review is warranted. For those systems that warrant the review, the Council will develop procedures and implement methods to undertake the review.

The Council also advised us that based on the risk assessments it will schedule the user access reviews and train business units on the method to be used.

5.1.4 Security updates not regularly installed

Recommendation

The Council should apply more rigour to its vulnerability management processes by formalising an established 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 release
- the requirement to document the rationale for deciding not to install a patch.

The Council should also review the results of the vulnerability assessment we performed in this examination (refer to section 8) and ensure that missing patches are tested and remediated. Consideration should be given to either upgrading or replacing unsupported software and underlying operating systems.

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

Finding

The Council advised us that its patching processes are often driven by external factors, including vendor time frames and other dependencies. We found that frequent security updates and patches are applied to the Council's enterprise resource planning (ERP) suite.

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

- The Council did not have a vulnerability and patch management policy and procedure.
- Microsoft Windows server patches were not consistently installed on Council systems, outside of the ERP suite.
- Our vulnerability assessment scans revealed numerous unsupported software applications and operating systems 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 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 advised us that:

- management will develop and implement a patch management policy
- management will review the vulnerability assessment scans using a risk based approach and take action as required
- management agrees with the recommendation to periodically perform vulnerability assessments to identify any missing patches in system software and applications and will update its ICT system security procedures to reflect the assessment procedures.

5.1.5 Insufficient end user device security

Recommendation

The Council should develop and implement a policy that defines an approach to securing end user devices. Workstations, servers, databases and network devices should be subject to security controls, in line with industry standards (such as the Centre for Internet Security standards[11]).

Further, a well configured mobile device management solution should be installed and configured on all mobile devices that can access Council systems or data, to reduce the likelihood of data leakages associated with mobile devices.

Finding

Council user workstations and laptops (end user devices) are protected by some foundational security controls, including restricting administration privileges and the use of antivirus software.

Despite this, we noted that more advanced endpoint protection techniques have not been implemented to further reduce the ability of malicious software to execute. For example:

- the Council uses System Centre Configuration Manager to prevent standard users from installing applications, but does not use application whitelisting to prevent applications from executing
- the Council does not have a mobile device management solution, after it stopped using one in 2018.

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

We also noted that the Council does not have a formal policy 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.

Application whitelisting is a technique recommended in the Australian Signals Directorate's Essential Eight controls. It prevents unauthorised or malicious software (including many forms of ransomware) executing on a workstation or server.

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 not properly secured. They may be exploited by attackers to gain unauthorised access to Council information and systems or to cause disruption, through methods like ransomware.

A well configured mobile device management solution is key to enforcing mobile security requirements and device security controls. It reduces the risk of data leakages associated with mobile devices.

Council response

The Council advised us that a policy defining an approach to securing end user devices will be incorporated into its cyber security strategy. This will be based on the maturity levels defined in the Australian Cyber Security Centre's Essential Eight maturity model.

The Council also advised us that management will conduct a procurement process to assess mobile device management solutions and implement the preferred option.

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 suits its ICT environment. The procedure should be formally endorsed by management and agreed by both business units (including vendors) and the IT team. It should also include how security risks will be addressed in any system acquisition and implementation.

In addition, all 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. We noted that the Council has a manual that includes some change management roles and responsibilities.

Despite this, we noted the following shortfalls:

- The Council did not have formalised change management policies and procedures to control changes applied to its ICT environment. This included its approach to security risk assessments, system testing, backout plans and formal approval prior to promoting changes to the production environment.
- There was no central repository to record all approved system changes.
- There was no consistent change management approach applied to Council systems outside of its core ERP suite. The Council considers that the risk is reduced as the other systems are not key business systems.
- There was no separate environment available to test system changes and patches applied to the Council's Active Directory and Microsoft Exchange before they were implemented in the production environment. Changes were instead applied directly into production. We note that the Council does maintain several Active Directory domain controllers for redundancy.

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 changes to systems 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 introduce security vulnerabilities into the ICT environment.

Council response

The Council advised us that management will develop a change management policy and procedure. The procedure will incorporate the use of the service desk change management tools.

The Council also advised us that management already has a separate test environment for core enterprise systems where the risks are high. Management will conduct risk assessments for the remaining systems to determine if further test environments are warranted.

7 Backup operations, disaster recovery and incident response

7.1 Detailed findings

7.1.1 Gaps in backup and ICT disaster recovery arrangements

Recommendation

The Council should review its disaster recovery plan to ensure it accurately reflects its current recovery arrangements and includes key recovery metrics. It should also expand its recovery procedures for all key business systems, including details about how to recover or switch business processes to a standby system in the disaster recovery site if required. Procedures should cover applications as well as supporting infrastructure, databases and networks.

The Council should also ensure its business continuity plan (BCP) includes identified maximum allowable outage (MOA) times[12] for all of its key business systems.

The Council should clearly define and implement a formal approach to test backup restorations and ICT disaster recovery plans. This testing should be conducted regularly.

Finding

The Council has a BCP that was last updated in October 2018. It includes MOA times for some of its business systems.

The Council also has an ICT disaster recovery plan that was last reviewed in January 2019, which is intended to provide an approach to addressing the failure/loss of any ICT system. The plan involves transferring operations of its production environment to its secondary site. The Council advised us that in the event of a disaster or system failure, there are several detailed processes that need to be completed for the Council to continue its operations from the secondary site.

We noted that the disaster recovery plan only contains some high-level recovery procedures and does not include the following:

- Recovery Time Objectives (RTOs) – the length of time it will take to restore a key business system after a failure or disaster occurs
- Recovery Point Objectives (RPOs) – the amount of data that could potentially be lost during a disaster
- detailed procedures to recover in the event of a disaster or system failure.

[12] MOA is the maximum length of time that can elapse before a business process outage is considered unacceptable or intolerable.

The Council conducted a failover test in December 2019 but it had not tested whether all major components of the disaster recovery plan could be completed within any RTOs and RPOs (not identified) and the MOA times documented in the BCP. In addition, there is no periodic testing scheduled.

For backups, we noted that the disaster recovery plan contains detailed backup scope, schedules, frequency, retention and testing requirements. The Council advised us that in 2019-20 it conducted a major upgrade of its Storage Area Network which included restructuring its backup and restore processes.

The Council's backup processes were tested on initial implementation and some ad hoc restores are conducted as part of business-as-usual operations. Despite this, the Council does not conduct scheduled backup restoration testing.

Why this is important

Where detailed recovery procedures do not exist for all key business systems, there is a risk that they cannot be recovered within agreed recovery objectives in the event of a disaster or system failure. There is also a greater risk of knowledge loss if key IT staff leave the Council.

Without conducting regular backup and disaster recovery testing, the Council has insufficient assurance of its ability to restore systems and data in the event of a disaster, system failure or data loss (for example, as a result of a ransomware security incident).

Council response

The Council advised us that management will review and update the disaster recovery plan to include recovery metrics and procedures.

The Council also advised us that management will develop a test plan and schedule, and will include this in the disaster recovery plan.

7.1.2 Information security incident response plans not established

Recommendation

The Council should establish 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

Information security incident response plans to key scenarios and security threats have not been established.

Why this is important

Without an established, understood and tested cyber 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 in the 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 defined 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 quickly 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 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 us that cyber attacks are covered in general terms in its BCPs.

The Council advised us that it has an ICT disaster recovery plan and a cyber security incident response plan, which it will incorporate into its BCP.

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. Some underlying software disclosures needed to be reduced, and documents created and hosted by the Council required greater security to be applied. These documents could contain information that could be used by an attacker.

Further, some fundamental security aspects also required strengthening so that other potential vulnerabilities were not exploited.

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