RELEASED 20 FEBRUARY 2023

ADELAIDE HILLS COUNCIL
AUDIT COMMITTEE MEETING
Monday 24 May 2021
CONFIDENTIAL AGENDA BUSINESS ITEM

Item:	**8.1**
Responsible Officer:	**James Sinden** **Manager Information Services** **Corporate Services**
Subject:	**Cyber Security Plan**
For:	**Decision**

1. Cyber Security Plan – Exclusion of the Public

Pursuant to section 90(2) of the *Local Government Act 1999* the Audit Committee (the Committee) orders that all members of the public, except:

- **Chief Executive Officer, Andrew Aitken**
- **Director Corporate Services, Terry Crackett**
- **Executive Manager Governance & Performance, Lachlan Miller**
- **Manager Financial Services, Mike Carey**
- **Manager Information Services, James Sinden**
- **Team Leader ICT, Daniel Souter**
- **Governance & Risk Coordinator, Steven Watson**

be excluded from attendance at the meeting for Agenda Item 8.1: Cyber Security Plan in confidence.

The Committee is satisfied that it is necessary that the public, with the exception of Council staff in attendance as specified in (a) above, be excluded to enable the Committee to consider the report at the meeting on the following grounds:

Section 90(3)(e) of the *Local Government Act 1999,* the information to be received, discussed or considered in relation to this Agenda Item is matters affecting the security of the council, members or employees of the council, or council property, or the safety of any person, the disclosure of which could reasonably be expected to create an awareness of Council's cyber security vulnerabilities and potentially lead to exploitation of those vulnerabilities resulting in loss/damage to information, breach of confidentiality and service continuity disruption.

Accordingly, on this basis the principle that meetings of the Committee should be conducted in a place open to the public has been outweighed by the need to keep the information and discussion confidential.

2. Cyber Security Plan – Confidential Item

SUMMARY

The purpose of this report is to provide a draft Cyber Security Plan ***(Appendix 1)*** to the Audit Committee for review in its capacity as advisors to Council resulting from a recent Cyber Security Audit that was completed in 2020 and addresses a CEO performance target for 2020-21.

The development of the draft Cyber Security Plan (CSP) has been completed with the assistance of CyberCX a specialist consultancy firm in the field of Information Security Management and Council staff.

The CSP addresses the Australian Cyber Security Centre's *Essential Eight Model* and the strategic recommendations, quick win audit findings and corporate risks identified in the Cyber Security Internal Audit.

RECOMMENDATION

The Audit Committee resolves:

1. That the report be received and noted

2. To recommend to Council that the draft Cyber Security Plan as contained in Appendix 1 and as reviewed by the Audit Committee, be adopted.

---

1. GOVERNANCE

➢ **Strategic Management Plan/Functional Strategy/Council Policy Alignment**

Strategic Plan 2020-24 – A brighter future

Goal 5	A Progressive Organisation
Objective O5	We are accountable, informed, and make decisions in the best interests of the whole community.
Priority O5.2	Make evidence-based decisions and prudently assess the risks and opportunities to our community before taking action.
Objective O6	Technology and innovation is utilised to better meet our community's expectations and deliver value for money.
Priority O6.1	Progressively strengthen Council's systems security to minimise the impact of cyber-attack.

➢ **Legal Implications**

Section 125 of the *Local Government Act 1999* (the Act) requires councils to ensure that appropriate policies, practices, and procedures of internal controls are implemented and maintained in order to assist the council to carry out its activities in an efficient and orderly manner to achieve its objectives, to ensure adherence to management policies, to safeguard Council's assets, and to secure (as far as possible) the accuracy and reliability of Council records.

- **Risk Management Implications**

The creation of a Cyber Security Plan will assist in mitigating the risks of:

> *Inability to discharge role and functions of a local government entity leading to a breach of legislation and loss of stakeholder confidence.*

Inherent Risk	Residual Risk	Target Risk
Extreme (5C)	High (E5)	Low

The creation of a Cyber Security Plan is one many controls involving the implementation of an Information Security Management System *(ISMS)*.

- **Financial and Resource Implications**

Funding for the project work of implementing the Cyber Security Plan has been provisioned in the draft budget 2021-22.

- **Customer Service and Community/Cultural Implications**

Council's information systems are fundamental to the provision of services to the community in addition to holding ratepayer's information. As such, there is likely to be a high expectation that Council's systems and information are appropriately protected from cyber security risks.

- **Sustainability Implications**

Not applicable.

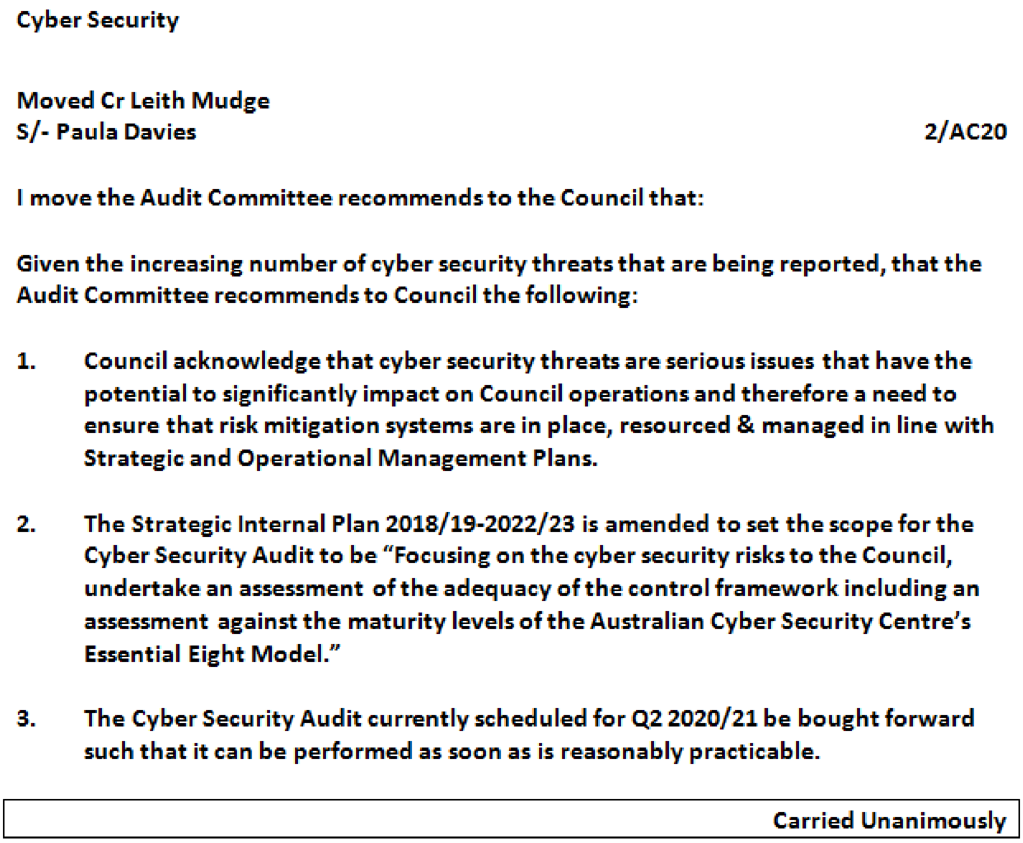
- **Engagement/Consultation conducted in the development of the report**

Consultation on the development of this report was as follows:

Council Committees:	The Audit Committee received a status report on the conduct of the Cyber Security Audit at its 19 October 2020 meeting.
Council Workshops:	Not Applicable
Advisory Groups:	Not Applicable
Administration:	Director Corporate Services Manager Information Services Team Leader ICT Executive Manager Governance & Performance Governance & Risk Coordinator
External Agencies:	CyberCX (formally CQR Pty Ltd)
Community:	Not Applicable

2. BACKGROUND

At its 17 February 2020 meeting on 17 February 2020, the Audit Committee resolved the following:



Cyber Security

Moved Cr Leith Mudge
S/- Paula Davies **2/AC20**

I move the Audit Committee recommends to the Council that:

Given the increasing number of cyber security threats that are being reported, that the Audit Committee recommends to Council the following:

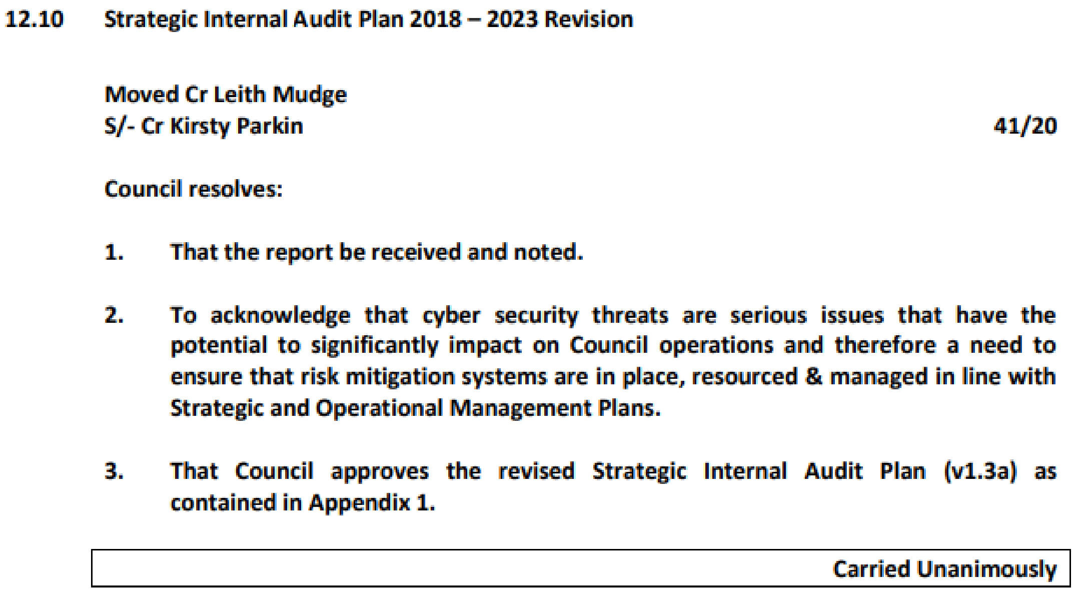
1. **Council acknowledge that cyber security threats are serious issues that have the potential to significantly impact on Council operations and therefore a need to ensure that risk mitigation systems are in place, resourced & managed in line with Strategic and Operational Management Plans.**

2. **The Strategic Internal Plan 2018/19-2022/23 is amended to set the scope for the Cyber Security Audit to be "Focusing on the cyber security risks to the Council, undertake an assessment of the adequacy of the control framework including an assessment against the maturity levels of the Australian Cyber Security Centre's Essential Eight Model."**

3. **The Cyber Security Audit currently scheduled for Q2 2020/21 be bought forward such that it can be performed as soon as is reasonably practicable.**

Carried Unanimously

In consideration of the Audit Committee's recommendation, Council at its 25 February 2020 meeting resolved as follows:



12.10 Strategic Internal Audit Plan 2018 – 2023 Revision

Moved Cr Leith Mudge
S/- Cr Kirsty Parkin **41/20**

Council resolves:

1. **That the report be received and noted.**

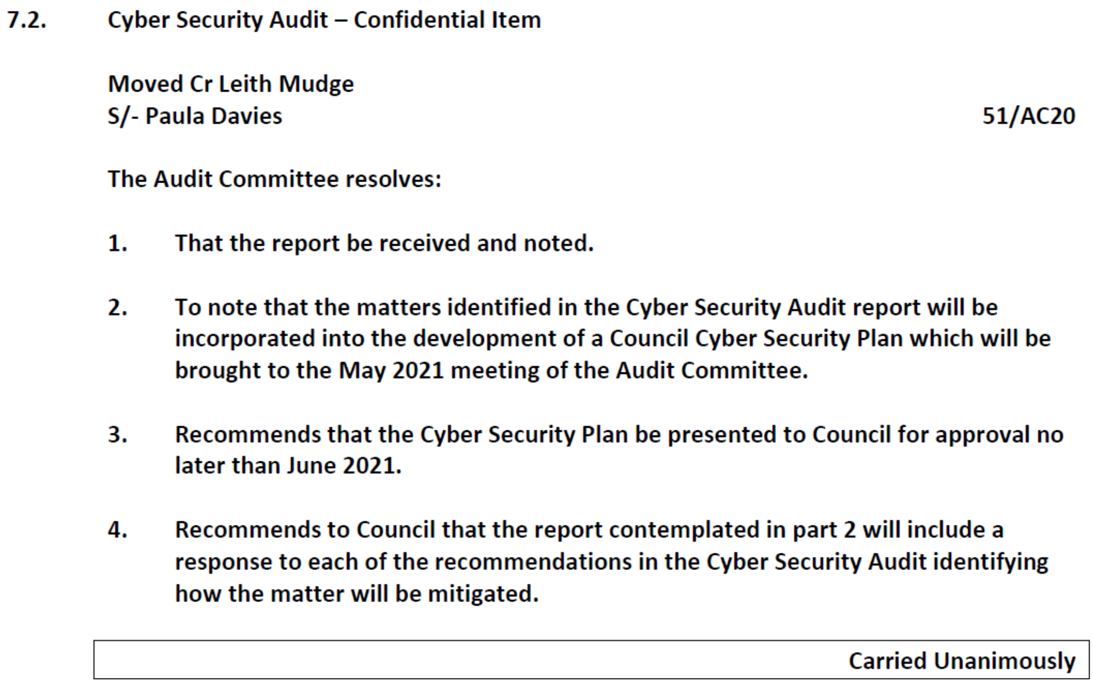
2. **To acknowledge that cyber security threats are serious issues that have the potential to significantly impact on Council operations and therefore a need to ensure that risk mitigation systems are in place, resourced & managed in line with Strategic and Operational Management Plans.**

3. **That Council approves the revised Strategic Internal Audit Plan (v1.3a) as contained in Appendix 1.**

Carried Unanimously

Council then engaged auditors to undertake an independent cyber security audit which identified several cyber security risks to Council and some notable information security control gaps where a report was prepared and presented to the Audit Committee on 19 October 2020.

The Audit Committee then resolved as follows:



7.2. Cyber Security Audit – Confidential Item

Moved Cr Leith Mudge
S/- Paula Davies **51/AC20**

The Audit Committee resolves:

1. **That the report be received and noted.**

2. **To note that the matters identified in the Cyber Security Audit report will be incorporated into the development of a Council Cyber Security Plan which will be brought to the May 2021 meeting of the Audit Committee.**

3. **Recommends that the Cyber Security Plan be presented to Council for approval no later than June 2021.**

4. **Recommends to Council that the report contemplated in part 2 will include a response to each of the recommendations in the Cyber Security Audit identifying how the matter will be mitigated.**

Carried Unanimously

The information contained in the Cyber Security Audit was then used to form a Cyber Security Plan to address the recommendations and risks from the Audit.

3. ANALYSIS

From the *Cyber Security Audit* ***(Appendix 2)*** Council engaged the services of CyberCX to assist with the development of a *Cyber Security Plan*. This Plan will implement an Information Security Management System *(ISMS)* framework which is a set of processes, controls and measures designed to protect the Councils systems from a cyber-security incident.

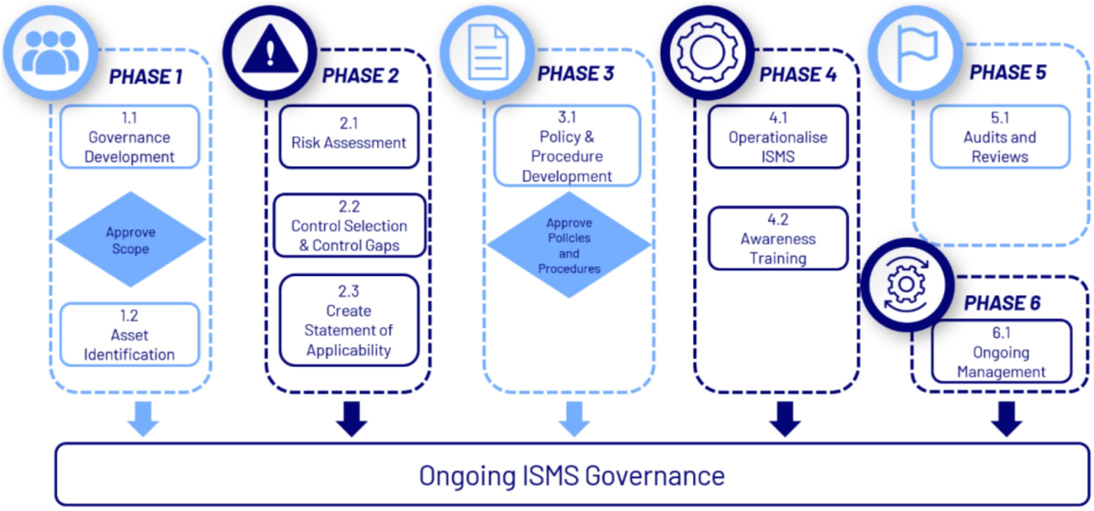
The Cyber Security Plan will implement and manage the ongoing operational ISMS that adheres to the *ISO/IEC 27001:2013 Information Security Management Standard* (ISO 27001) and uses an appropriate subset of the South Australian Cyber Security Framework (SACSF) as specific security controls.

The ISO 27001 standard takes a holistic approach to information security, ensuring Council can identify and manage information security risks for people, processes, and technology. This approach allows alignment of information security objectives and as a result improves the security posture of Council based on organisational risks and priority.

The objective of the *Cyber Security Plan* is to provide a practical and operational ISMS covering key Council operations to invest in security according to real risks.

The implementation of an ISMS mitigates the risks and recommendations identified in the *Cyber Security Audit* ***(Appendix 2)*** and, addresses the items in the Corporate Risk Register ***(Appendix 3)*** in relation *to Cyber Security Audit* and establishes an ISMS framework as an ongoing management system.

The diagram below shows the high-level phased approach to implementing the ISMS and full details of the Cyber Security Plan are within ***(Appendix 1).***



Progress on the implementation of the *Cyber Security Plan* will be reported to the Audit Committee to coincide with the bi-annual Audit Actions Implementation Update.

4. OPTIONS

The Committee has the following options:

I. To receive and note the report and recommend the Cyber Security Plan to Council for adoption. (Recommended)

II. To determine an alternate course of action. (Not Recommended)

5. APPENDICES

(1) Cyber Security Plan
(2) Cyber Security Audit
(3) Cyber Security Risk Register

Appendix 1

Cyber Security Plan

Adelaide Hills Council

Cyber Security Plan

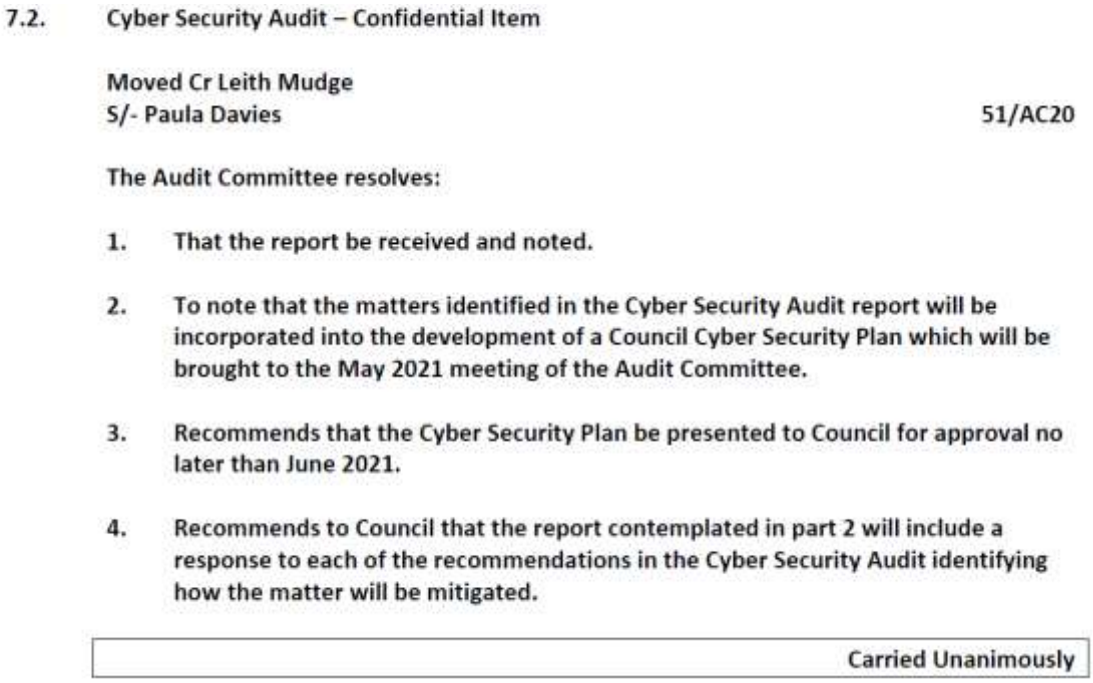
Information Security Management System (ISMS) Implementation

April 2021

Background

Adelaide Hills Council (Council) recently engaged CyberCX (CCX) to conduct an independent cyber security audit which identified several cyber security risks to Council and some notable information security control gaps.

The audit report was then presented to the Council Audit Committee for consideration where a Motion on Notice was unanimously carried as follows.



7.2. Cyber Security Audit – Confidential Item

Moved Cr Leith Mudge
S/- Paula Davies 51/AC20

The Audit Committee resolves:

1. That the report be received and noted.
2. To note that the matters identified in the Cyber Security Audit report will be incorporated into the development of a Council Cyber Security Plan which will be brought to the May 2021 meeting of the Audit Committee.
3. Recommends that the Cyber Security Plan be presented to Council for approval no later than June 2021.
4. Recommends to Council that the report contemplated in part 2 will include a response to each of the recommendations in the Cyber Security Audit identifying how the matter will be mitigated.

Carried Unanimously

Rather than addressing each individual risk discretely, in a reactive manner, the planed approach in developing a Cyber Security Plan (CSP) is to implement an **information security risk management framework** alongside a set of processes, controls and measures to protect Council information and systems that addresses the strategic recommendations and risks identified in the Cyber Security Audit.

Cyber Security Plan

The CSP has been developed using specialist consultancy services (CCX) to implement and manage an ongoing operational Information Security Management System (ISMS) based upon the South Australian State Government Cyber Security Framework (SACSF).

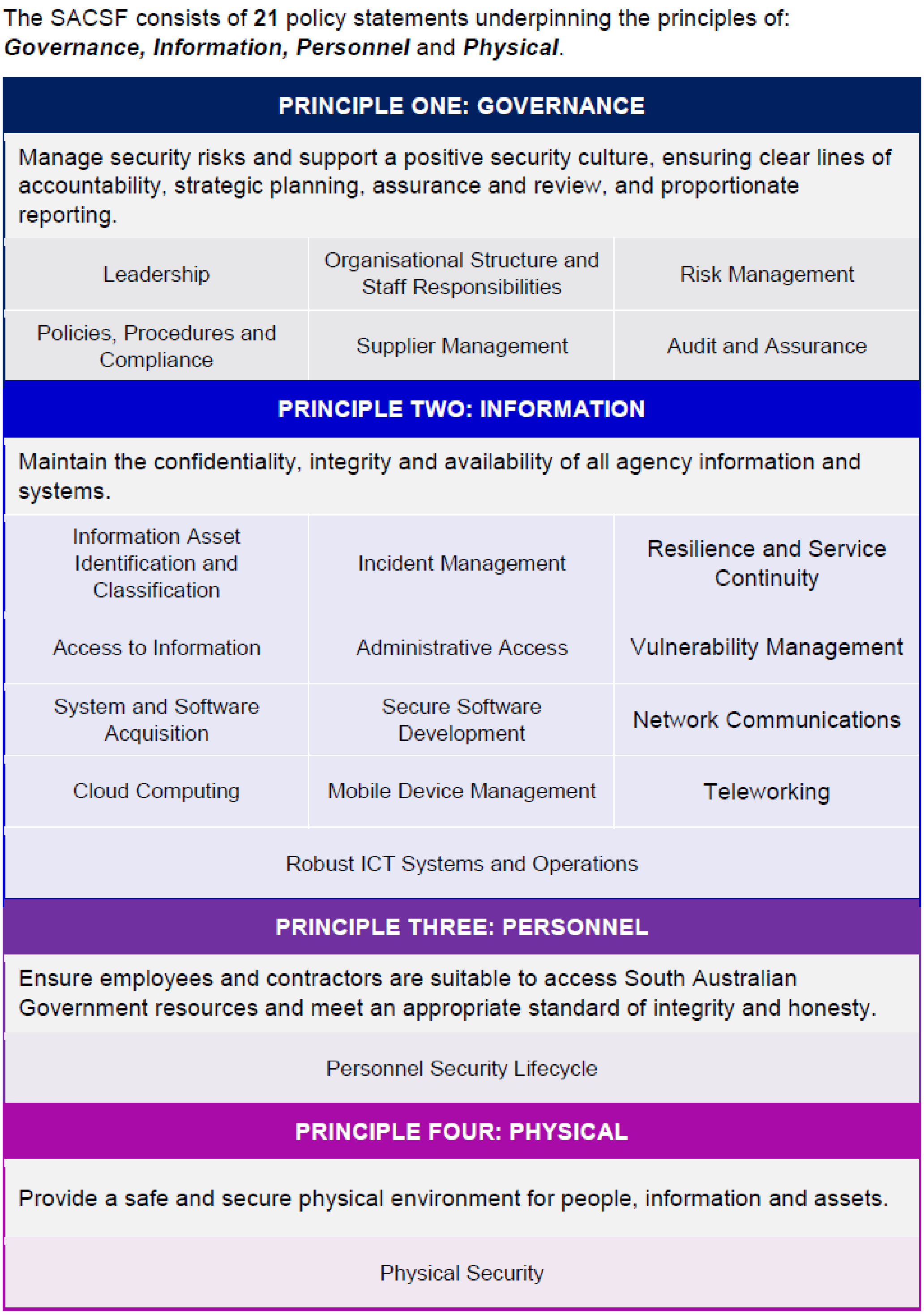
The Cyber Security Plan will implement and manage the ongoing operational Information Security Management System *(ISMS)* that adheres to the ISO/IEC 27001:2013 Information Security Management Standard *(ISO 27001)* and uses an appropriate subset of the South Australian Cyber Security Framework *(SACSF)* as specific security controls.

This will ensure that the current and newly identified information security risks are managed in an effective, structured manner.

The SACSF is set out tiering model to help provide guidance around the security controls and measure that should be considered based on the size, complexity, and criticality and as such, the tier level that Council will work towards will be confirmed during the first phase of implementation of the CSP.

For reference, the SACSF is outlined in the table below and the full document as ***(Appendix 1)*** that is licensed under Creative Commons Attribution (CC BY) 4.0 License of the Department of the Premier and Cabinet, Government of South Australia, 2019.

SACSF Framework



The SACSF consists of **21** policy statements underpinning the principles of: ***Governance, Information, Personnel*** and ***Physical***.

PRINCIPLE ONE: GOVERNANCE		
Manage security risks and support a positive security culture, ensuring clear lines of accountability, strategic planning, assurance and review, and proportionate reporting.		
Leadership	Organisational Structure and Staff Responsibilities	Risk Management
Policies, Procedures and Compliance	Supplier Management	Audit and Assurance
PRINCIPLE TWO: INFORMATION		
Maintain the confidentiality, integrity and availability of all agency information and systems.		
Information Asset Identification and Classification	Incident Management	Resilience and Service Continuity
Access to Information	Administrative Access	Vulnerability Management
System and Software Acquisition	Secure Software Development	Network Communications
Cloud Computing	Mobile Device Management	Teleworking
Robust ICT Systems and Operations		
PRINCIPLE THREE: PERSONNEL		
Ensure employees and contractors are suitable to access South Australian Government resources and meet an appropriate standard of integrity and honesty.		
Personnel Security Lifecycle		
PRINCIPLE FOUR: PHYSICAL		
Provide a safe and secure physical environment for people, information and assets.		
Physical Security		

Analysis of the Cyber Security Audit

The Cyber Security Audit also considered an assessment against the Australian Cyber Security Centre’s (ACSC) Essential Eight Model and a mapping exercise has been undertaken to ensure that implementing the SACSF also addresses the Essential Eight Maturity Model.

In its adoption Council is intending on meeting level 2 compliance as per the target levels highlighted in ***(Appendix D)*** of the Cyber Security Audit report.

The following table outlines the alignment of the ACSC Essential Eight Maturity Model to the controls of SACSF (pages 40-42 Cyber Security Audit):

Essential Eight Maturity Model	SACSF
7: Multi-factor authentication	**2.4:** Access to Information
5: Restrict administrative privileges	**2.5:** Administrative Access
1: Application control	**2.6:** Robust ICT Systems and Operations
3: Configure Microsoft Office macro settings	
4: User application hardening	
8: Daily backups	
2: Patch applications	**2.7:** Vulnerability Management
6: Patch operating systems	

The following table outlines the alignment the audit strategic recommendations to the controls of the SACSF (pages 11-12 Cyber Security Audit):

Strategic Recommendations Audit Findings	SACSF
Implement an access management policy	**1.4:** Policies, Procedures and Compliance
Enhance the suite of information security policies	
Develop a policy on cryptography	
Include management of contractors that gain access to Council information systems under the established OD process	

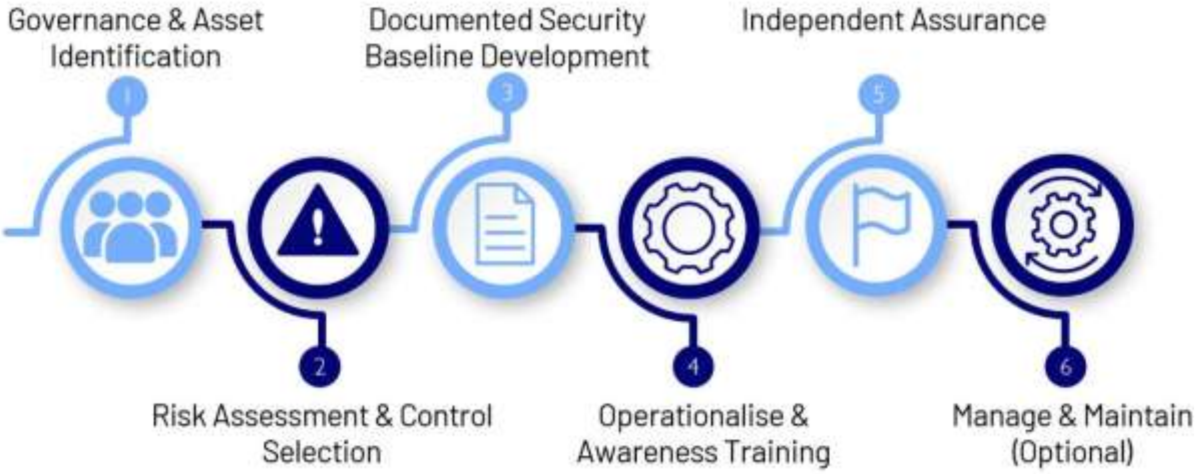
Develop a framework for managing supplier-related information security risks	**1.5:** Supplier Management
Conduct an independent penetration test	**1.6:** Audit and Assurance
Establish an information classification scheme with supporting handling procedures	**2.1:** Information Asset Identification and Classification

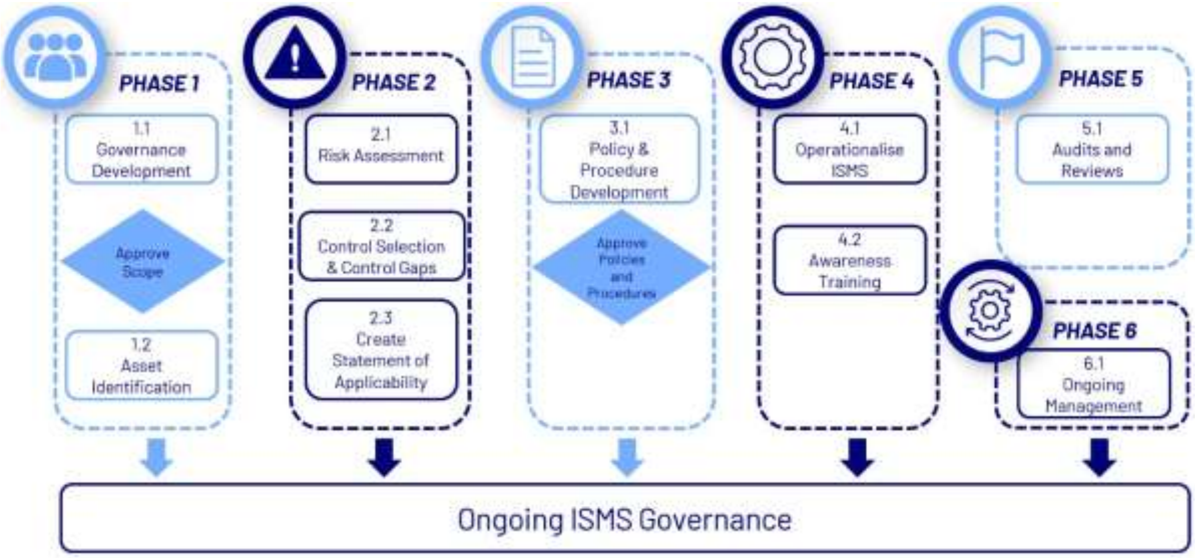
The following table outlines the alignment of the audit quick wins to the controls of the SACSF (page 13 Cyber Security Audit):

Quick Win Audit Findings	SACSF
Develop a top-level information security policy	**1.4:** Policies, Procedures and Compliance
Include a dedicated information security clause in the ICT usage agreement	
Include reiteration of confidentiality requirements during offboarding	
Council should document its access management processes in a procedure	
Enhance the acquisition plan template to consider security	
Update the existing password policy	**2.4:** Access to Information
Prohibit privileged users from conducting high-risk activities in policy (E8)	**2.5:** Administrative Access
Block web advertisements in browsers (E8)	**2.6:** Robust ICT Systems and Operations

Cyber Security Plan – Phased Implementation

The CSP will include the implementation and management of an ISMS in a phased approach across six phases as identified in the diagram below.


Governance & Asset Identification
1
Documented Security Baseline Development
3
Independent Assurance
5
2
Risk Assessment & Control Selection
4
Operationalise & Awareness Training
6
Manage & Maintain (Optional)



Timeframe & Resources Implications

The implementation of the ISMS can be expected to take approximately 8 months in elapsed time using consulting and internal resources to progress several key activities and will commence in July 2021.

For the successful completion of the Cyber Security Plan, the following commitment is required:

- Senior management support of the project;
- Staff attendance at regular ISMS steering committee meetings;
- Availability of personnel for scheduled workshops and interviews;

- Timely access to documentation and information;
- Timely approval of socialised documents and artefacts;
- Distribution and timely review of documentation provided;
- Completion of any remediation activities, to implement controls or procedures required for compliance with the standard; and
- attendance of all required staff at security awareness training

The diagram below indicates the phased approach to the work activity that will be undertaken.

Cyber Security Plan – Detailed Implementation work plan

The Cyber Security Plan will comprise of six phases and will implemented in a series of activities as indicated in the tables below.

Phase 1

Activity:	Month:	Key Activity:
Phase 1 – Governance & Asset Identification		
1.1 Governance Development	1	Project kick-off Run project briefing and scoping workshop Define ISMS objectives and policy Define governance structure Set up Steering Committee ***Deliverable: briefing presentation, information security governance policy***
1.2 Asset Identification	1	Agree information classification scheme Conduct workshop to identify and classify information assets ***Deliverable: information asset inventory***

Project Initiation

Initiate the project:

- Agree the project schedule
- Introduction to key resources
- Arrange scheduling of meetings

Phase 1 – Governance & Asset Identification

Development of the ISMS will commence with a workshop to define the scope and the governance structure required to support the ISMS. The outputs of this workshop will ensure the following aspects of the ISMS are identified and documented:

- The environment to be protected by the ISMS, i.e. logical and physical boundaries;
- Security objectives and potential issues or barriers for success;
- Roles and responsibilities and expected competencies of personnel within the ISMS;
- Stakeholders interested in having good information security practices; and
- Legal, regulatory, and contractual requirements.

After agreement on the scope and governance structure for managing information security, an information asset identification and classification workshop will be conducted. This workshop will identify the critical information, systems, applications and supporting infrastructure within the scope of the ISMS and classify these assets according to confidentiality, integrity, and availability requirements.

Estimated Completion Date: August 2021

Phase 2

Activity:	Month:	Key Activity:
Phase 2 – Risk Assessment & Control Selection		
2.1 Risk Assessment	2	Document risk management procedure Conduct risk assessment workshop Update existing risk register ***Deliverable: risk management procedure, ISMS risk register***
2.2 Control Selection & Control Gaps	2	Select controls within the ISMS scope Identify control gaps Determine what corrective actions are required ***Deliverable: improvements and actions register***
2.3 Create Statement of Applicability	2	Document applicable controls Determine status of implementation and how they are implemented Build Statement of Applicability (‘SoA’) ***Deliverable: Statement of Applicability (‘SoA’)***

Phase 2 – Risk Assessment & Control Selection

Leveraging information gathered within Phase 1, risk assessment workshops will be held to identify and assess information security risks.

The approach will allow the development of business-centric information security risks based on critical information, services provided and information assets. The advantage of this approach is that common risks across information assets can be treated holistically within the ISMS, making risk treatments more effective and pragmatic. Information security risks will then be documented within the ISMS risk register.

Identification of the applicable controls and document progress in implementing these controls within the Statement of Applicability ('SoA'). Where gaps are identified, these will be highlighted within the risk register and will be documented within the corrective actions register for action as the ISMS morphs from being a project into operational ISMS.

Estimated Completion Date: October 2021

Phase 3

Activity:	Month:	Key Activity:
Phase 3 – Documented Security Baseline Development		
3.1 Policy & Procedure Development	2-3	Create required security policies necessary to meet the selected controls Facilitate approval of policies ***Deliverables: information security policy and other policies as required*** Create the mandatory procedures required for the operation of the ISMS Facilitate approval of procedures ***Deliverable: documented information procedure, internal ISMS audit procedure, corrective actions procedure***

Phase 3 – Documented Security Baseline Development

The implementation of controls by developing necessary policies and procedures as required by the ISO 27001 standard and the Statement of Applicability. Policies and procedures will be tailored to meet needs and provide a benchmark for current industry good practices and processes for managing information security risks.

Note that existing policies and procedures will be leveraged where appropriate and a summary of all the policies and procedures that will be developed is listed in the Cyber Security Deliverables section of this document.

Estimated Completion Date: December 2021

Phase 4

Activity:	Month:	Key Activity:
Phase 4 – Operationalise & Awareness Training		
4.1 Operationalise ISMS	3-4	Construct supporting ISMS documents and procedures ***Deliverables: document and records registers, operational procedures, Security Calendar, measures and metrics, communications plan***
	Ongoing	Attend Security Steering Committee Meetings ***Deliverable: agendas, minutes***
4.2 Awareness Training	4	Prepare and deliver up to four face-to-face security awareness training sessions Council personnel. ***Deliverables: training materials and presentations***

Phase 4 – Operationalise & Awareness Training

The final phase of implementation drives the ongoing operation of the ISMS and is run in parallel with Phases 2 and 3. As ISMS development evolves, the ISMS security committee (initially convened in Phase 1) begins facilitating the management of information security risks.

The development of supporting material to assist in the ongoing management of the ISMS and establishment of ISMS security committee meetings. This is to ensure the ISMS is managed effectively, and as such recommend that the security committee meets regularly during implementation.

Successfully embedding your ISMS within Council will not be achievable without clear communication to personnel on their information security roles and responsibilities. As such, the development of a communication and training plan to facilitate appropriate messaging of the ISMS and to provide personnel with security awareness training.

Estimated Completion Date: January 2022

Phase 5

Activity:	Month:	Key Activity:
Phase 5 – Independent Assurance		
5.1 Audits & Reviews	5	Conduct management review Construct internal audit plan Perform independent internal audit Complete remedial action from audit ***Deliverables: internal audit plan, internal audit reports, management review report***

Phase 5 – Assurance Review

Performing reviews of the ISMS as required by the ISO 27001 standard, these being the ISMS audit and the ISMS management review.

The ISMS audit will ensure an understanding of any potential non-conformances or opportunities for improvement relating to the ISMS.

The ISMS management review will develop the scope, inputs and agenda of this review. The outputs and decisions from key personnel attending this meeting will be captured during the review to ensure any actions required are appropriately documented.

Implementation Finalisation on the completion of Phase 5, will begin the finalisation of the implementation project and begin the transition to 'business as usual'.

Within the finalisation stage the following will be completed:

- Finalise all material and deliver to project sponsor;
- Identify and develop program of activities for action within Phase 6 (Manage and Maintain); and
- Undertake an implementation close-out meeting.

Estimated Completion Date: March 2022

Phase 6

Activity:	Month:	Key Activity:
Phase 6 – Manage & Maintain		
6.1 Ongoing Management	Ongoing	Agree ongoing management scope Documented responsibilities for to manage within the Security Calendar Maintain ongoing operation of the ISMS ***Deliverable: ISMS security specialist resource***

Phase 6 – Manage & Maintain

To ensure the pragmatic and continuous operation of the ISMS, the program of activities will be guided by the security calendar on a scheduled (e.g. monthly, quarterly, annually) basis. Such tasks may include:

- Provide information security advice/guidance to Council and management;
- Ensure the effective controls in the following key areas:
  - Oversight of the ISMS committee schedules, meeting and outcomes;
  - Management reporting and metrics;
  - Information asset register management;
  - Access control;
  - Physical and environmental security;
  - Operations and network security;
  - Security in supplier relationships; and
  - Information security incident management.
- The tracking of progress of activities in the improvements and actions register and the periodic review of that register;
- The tracking of progress of treatment activities in the ISMS risk register;
- Staff awareness and briefings to interested stakeholders within the Council;
- Management of the information security calendar incorporating all activities designed to monitor the effectiveness of the ISMS;
- Review and updates to the ISMS policy and procedure suite.

Estimated Completion Date: Ongoing

Cyber Security Plan – Deliverables

The deliverables from the Cyber Security Plan are the following:

Phase 1 – Governance & Asset Identification	
Project briefing and presentation	Information security governance policy
Information asset inventory	
Phase 2 – Risk Assessment & Control Selection	
Risk management procedure	Improvements and actions register
ISMS risk register	Statement of Applicability ('SoA')
Phase 3 – Documented Security Baseline Development	
Information security policy	Operations security policy
Acceptable use policy	Physical & environmental security policy
Access management policy	Remote access & teleworking policy
Asset management & disposal policy	Supplier management policy
Network security policy	System acquisition & development policy
Resilience and service continuity policy	Documented information procedure
Information classification & handling policy	ISMS audit procedure
Mobile device policy	Information security incidents & actions procedure
Phase 4 – Operationalise & Awareness Training	
Communications plan	ISMS meetings agendas and minutes
ISMS security calendar	Third party risk register
ISMS audit program	Operational security procedures

ISMS measures and metrics	Incident response plan
Information security awareness training for Council staff with face-to-face delivery.	
Phase 5 – Independent Assurance	
ISMS audit report	ISMS management review report

Appendix 1

South Australian Cyber Security Framework

South Australian Cyber Security Framework

Government of South Australia

Document Control

ID	**SACSF**
Version	V1.0
Classification/DLM	OFFICIAL
Compliance	Mandatory
Original authorisation date	November 2019
Last approval date	November 2019
Next review date	November 2020

Licence

Table of contents

1. Foreword

The Government of South Australia manages, delivers and owns a range of information technology infrastructure, services and systems on behalf of the citizens of South Australia. In order to uphold citizen's trust and confidence, and to ensure services delivered to the community are reliable and resilient, it is imperative that government agencies safeguard infrastructure, digital assets and citizen information against cyber threats.

The South Australian Cyber Security Framework (SACSF) is a cabinet approved, whole of government policy framework which draws on international best practice for risk-based cyber security management. While the SACSF applies to all government agencies and their suppliers, it is not a one-size-fits-all or compliance approach to cyber security. Rather the SACSF reinforces the need for cyber security to be an enabler for government and drives this via a risk-based approach. This approach helps ensure risks are managed in a way that is commensurate with the risk appetite of the agency.

The objectives of the SACSF are to:

- Ensure cyber security risks are managed in an acceptable way.
- Provide assurance to the South Australian public and other interested parties that the information entrusted to the State Government is adequately protected.
- Maintain the confidentiality, integrity and availability of information assets in alignment with necessary policy, legal and regulatory requirements.
- Maintain the reputation of the individual agencies and the broader South Australian Government.
- Help embed cyber risk management as part of an agency's existing risk management framework.
- Demonstrate alignment to internationally recognised good practice in cyber risk management.

This approach will help deliver more responsible data sharing for social change, better protect the safety and prosperity of South Australians, and enhance the government's digital engagement with the business community.

2. Introduction

2.1 Background

The South Australian Cyber Security Framework (SACSF) has been developed to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of South Australian Government agencies.

For the purposes of this document cyber security refers to the measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.

The SACSF is a risk-based framework developed to assist with preserving the confidentiality, integrity and availability of information by applying risk management processes, with increasing control measures to be implemented based on increased likelihood or impact. A risk-based approach to cyber security management provides flexibility for an agency to implement controls based on its own risk profile, as opposed to a one-size-fits-all approach.

The SACSF is supported by a significant suite of supporting documentation, guidance and templates to help an agency implement the framework based on their risk profile and in line with an agency's existing risk management framework.

The SACSF is maintained by the Office for Cyber Security in the Department of the Premier and Cabinet (DPC) and is a subordinate document to the Protective Security Policy Framework.

2.2 Purpose

The SACSF outlines the mandatory requirements to which all SA Government agencies must adhere and as well as a set of supporting expectations. This document is designed to be used by all personnel within an agency including senior leadership, business unit managers, information technology staff, and audit and risk teams.

Relevant sections of the SACSF will also apply to suppliers to SA Government as well as non-government personnel that provide services to government agencies.

2.3 Authority

The SACSF is a Cabinet-approved document that describes 21 policy statements in support of contemporary practices for the security of information stored, processed, transmitted or otherwise manipulated by information and communication technology (ICT).

2.4 Applicability

The SACSF applies to:

- South Australian Government public sector agencies (agencies), that is, administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown. Refer: Public Sector Act 2009
- Suppliers to the South Australian Government and non-government personnel that provide services to government agencies.

Reliance upon this policy or standard by any other person is entirely at their own risk and the Crown in the right of South Australia disclaims all responsibility or liability to the extent permissible by law for any such reliance.

3. Implementation Approach

This section provides overview of key elements that must be considered as part of the implementation of the SACSF. Each section has underlying guidance and templates that agencies may utilise to assist with implementation of the SACSF.

3.1 Cyber Security Risk Appetite

The agency Chief Executive is required to approve the cyber security risk appetite statement for their agency. This statement defines, at a high level, the appetite that the agency has for cyber security risks.

As a minimum, it is expected that each agency defines their appetite toward cyber security risks that may impact:

- The health and safety of agency personnel and the South Australian community,
- The confidentiality and integrity of information held by the agency,
- The strategic objectives of the agency, and
- The reputation of the agency with key stakeholders

Additional information and guidance:

Cyber Security Risk Appetite Guidance

3.2 SACSF Tier Selection

The SACSF sets out a tiering model to help provide guidance around the security controls and measures that agencies should consider based on the size, complexity and criticality of their agency.

Agency Chief Executives are required to approve a tier level for their agency taking into consideration such factors as:

- The cyber security risk appetite of the agency;
- The classification of information held by the agency;
- The criticality of services provided by the agency;
- The agency’s size and resourcing capability; and
- The perceived overall risk of the agency.

The whole of government ICT and Data Board will note each agency’s tier selection.

Additional information and guidance:

Appendix C: Guidance on Tier Selection

3.3 The Cyber Security Program

Effective implementation of the SACSF requires the development of a cyber security program (CSP). The CSP work program helps demonstrate an agency’s ongoing commitment and approach to managing cyber security risk.

The program of work should take into consideration:

- The strategic cyber security objectives of the agency in alignment with the SACSF,
- The SACSF tier selected by the agency, including selection justification,
- The cyber security risk appetite of the agency,
- The cyber security governance model to be used by the agency including the key cyber security responsibilities of functions within the agency,
- The scope, boundaries and exclusions of the cyber security program,
- The interested parties (i.e. stakeholders) that require the agency to implement robust cyber security controls,
- Applicable legal, regulatory and contractual requirements of the agency.

Additional information and guidance:

Cyber Security Program Template

3.4 The Cyber Security Calendar

A cyber security calendar (may also be referred to as an Information Security Calendar, Information Assurance Calendar or similar) should be developed to support the cyber security work program and track key initiatives and ongoing operational tasks. This calendar will form a key component of the agency's annual attestation of their current alignment to the SACSF.

Additional information and guidance:

Security Calendar Template

3.5 Asset Identification & Classification

Agencies are to identify and document their critical processes and services, and the information assets used to support these processes. These information assets are to be classified for confidentiality, integrity and availability requirements thereby providing the agency with context for their risk assessment.

Additional information and guidance:

South Australian Information Classification System

SACSF Guideline 6.0 Integrity and Availability Classification using the SACSF

Information Asset Register Template

3.6 Risk Assessment

A risk assessment is to be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of personnel throughout the agency.

Cyber security is founded on risk management. Agencies must manage risk to reduce their likelihood and/or mitigate their business consequences, balancing the cost of security with its outcomes. Absolute security is unaffordable, often unachievable, and may impede business objectives and/or efficiencies.

Agencies are to identify and evaluate their cyber security risks and determine the required risk treatment activities in line with business requirements.

Additional information and guidance:

Risk Register Template

3.7 Framework Implementation Guidance

Each agency will implement controls to meet the requirements of each of the 21 policy statements. In addition to technical and procedural controls, this will include the development and implementation of a suite of approved cyber security artefacts, formalising the implemented controls and associated processes.

Additional information and guidance:

SACSF Implementation Toolkit

SACSF Guideline 3.0 Engaging Suppliers and Cloud Security

Measures and Metrics Guidance

Supplier Security Questionnaire

Supplier Register Template

Cyber Security Policy Template

Cyber Security Employee Handbook Template

Corrective Actions and Improvements Register

3.8 Independent Certification

Agencies are encouraged to consider certification of their Cyber Security Program and Framework to the ISO 27001:2013 Information Security Management Standard. This certification provides independent assurance that the agency is managing cyber security risks, whilst also satisfying a key policy statement of the SACSF (1.6: Audit and Assurance).

3.9 Annual Attestation

Each agency is to provide an annual attestation to the Department of the Premier and Cabinet which details its current state of alignment to the SACSF together with the plan to meet or maintain alignment to the requirements of the agency's selected tier level.

The attestation will be endorsed by the Agency Security Committee, reviewed by Senior Leadership, and approved by the Chief Executive.

At a high level, the attestation will cover:

- Tasks completed during the reporting period,
- Tasks to be completed during the new reporting period,
- Responsibility for completing the associated task, and
- Cyber security program funding model.

4. Functions and Responsibilities

This section provides overview of some of key roles, functions and responsibilities that are considered as part of the implementation of the SACSF.

4.1 Cabinet

Cabinet is responsible for:

- Approval of the SACSF and any updates to the Principles or Policy Statements.
- Noting annual SACSF attestation report.

4.2 Senior Management Council

Senior Management Council is responsible for:

- Noting the SACSF and approving its submission to Cabinet.
- Noting annual SACSF attestation report and approving its submission to Cabinet.

4.3 ICT and Data Board

The whole of government ICT and Data Board is responsible for:

- Endorsing the SACSF and overseeing the annual review of the SACSF and any subordinate documentation.
- Noting annual SACSF attestation report and approving its submission to the Senior Management Council.
- Noting agency Tier selection.

4.4 South Australian Government Cyber Security Steering Committee

The South Australian Government Cyber Security Steering Committee is responsible for:

- Endorsing the SACSF and overseeing the annual review of the SACSF and any subordinate documentation.
- Noting annual SACSF attestation report and approving its submission to the ICT and Data Board.

4.5 The Department of the Premier and Cabinet

The Department of the Premier and Cabinet's Office for Cyber Security are responsible for:

- Maintaining and communicating the SACSF across agencies.
- Providing expertise and guidance to agencies with regard to implementing the SACSF.
- Ensuring a consistent approach to the implementation of the SACSF.
- Administering the SACSF attestation process.

4.6 Agency Chief Executives

The agency Chief Executive (or equivalent) is ultimately accountable for the successful operation of the agency’s Cyber Security Program (CSP). The Chief Executive is accountable for:

- Definition of the agency’s cyber security risk appetite.
- Selection of the agency’s SACSF tier level.
- Assigning ownership of the agency’s CSP.
- Reviewing and approving the SACSF attestation.
- Assigning suitable and sufficient cyber security resources.

4.7 Agency Senior Leadership

Senior leadership comprising the agency’s executive leadership team or equivalent is responsible for providing support and resources for the CSP and championing organisational commitment to improving the cyber security culture of the agency.

4.8 Cyber Security Program Owner

The CSP owner is responsible for the successful operation of the CSP and is expected to:

- Provide CSP visibility as required to senior leadership.
- Monitor and report to senior leadership on the effectiveness of the CSP.
- Facilitate the provision of adequate training to ensure sound cyber security practices are understood by all personnel and effective cyber security controls are implemented.
- Review and approve Agency Security Committee recommendations on major security incidents, risks and risk treatment plans, adequacy of response and controls, security audits, and corrective actions and improvements taken.
- Review and approve core cyber security documentation and artefacts.

Note: *It is expected that the Cyber Security Program Owner function will be fulfilled by the Agency Security Executive (ASE), however this decision is to be based on the individual requirements of the agency.*

4.9 Cyber Security Program Coordinator

The CSP Coordinator is responsible for the operations of the CSP and coordination of cyber security activities including:

- Responding to the direction of the CSP owner.
- Organising and chairing the Agency Security Committee.
- Ensuring the activities documented in the cyber security calendar are scheduled, updated and performed.

- Escalating any issues, as necessary, to the CSP owner.
- Monitoring cyber security incident investigations and corrective actions.
- Highlighting major cyber security incidents to the Agency Security Committee.
- Ensuring operational cyber security activities are performed.
- Coordinating with external security vendors and specialists for expert advice.
- Reporting on various aspects of the CSP including security metrics, outstanding issues, and progress of the actions in risk treatment plans.

Note: *It is expected that the Cyber Security Program Coordinator function will be fulfilled by the agency Information Technology Security Adviser (ITSA), however this decision is to be based on the individual requirements of the agency.*

4.10 Agency Security Committee

The role of the Agency Security Committee is to act as the coordinator and adviser for all cyber security aspects in relation to the scope of the CSP, including:

- Responding to the direction of the CSP Owner.
- Ensuring the development and maintenance of, and adherence to, the agency's policies, procedures, work instructions and other operational documents to ensure compliance with the CSP.
- Reviewing security weaknesses and facilitating improvements to remediate cyber security risks identified by the agency risk management processes.
- Monitoring changes to services or deliverables for interested parties and reassessing any associated risks.
- Reviewing outcomes from cyber security incidents and associated corrective actions and improvements.
- Evaluating the results of internal and external audits and facilitating the required remedial actions.
- Communicating and providing guidance on implementation of cyber security policies, procedures, and other operational documents.

Membership may change based on operational requirements, and support and advisory groups can be invited as needed to attend Agency Security Committee meetings.

Note: *It is expected that the composition of the Agency Security Committee will be based on the individual requirements of the agency (e.g. an agency may have an existing governance committee in place that could consider security as part of its regular meetings).*

5. The Framework

The SACSF consists of **21** policy statements underpinning the principles of: ***Governance, Information, Personnel*** and ***Physical***.

PRINCIPLE ONE: GOVERNANCE		
Manage security risks and support a positive security culture, ensuring clear lines of accountability, strategic planning, assurance and review, and proportionate reporting.		
Leadership	Organisational Structure and Staff Responsibilities	Risk Management
Policies, Procedures and Compliance	Supplier Management	Audit and Assurance
PRINCIPLE TWO: INFORMATION		
Maintain the confidentiality, integrity and availability of all agency information and systems.		
Information Asset Identification and Classification	Incident Management	Resilience and Service Continuity
Access to Information	Administrative Access	Vulnerability Management
System and Software Acquisition	Secure Software Development	Network Communications
Cloud Computing	Mobile Device Management	Teleworking
Robust ICT Systems and Operations		
PRINCIPLE THREE: PERSONNEL		
Ensure employees and contractors are suitable to access South Australian Government resources and meet an appropriate standard of integrity and honesty.		
Personnel Security Lifecycle		
PRINCIPLE FOUR: PHYSICAL		
Provide a safe and secure physical environment for people, information and assets.		
Physical Security		

6. Principles and Policy Statements

Agencies and suppliers must consider and address each of the following 21 policy statements as part of their implementation of, and ongoing alignment to, the SACSF.

Appendix A lists each policy statement along with subordinate expectations and guidance that agencies and suppliers may consider. As referenced above, an implementation toolkit is also available that provides additional information, templates and tools that agencies can refer to.

PRINCIPLE ONE: GOVERNANCE
Manage security risks and support a positive security culture, ensuring clear lines of accountability, strategic planning, assurance and review, and proportionate reporting.
1.1: Leadership Senior leadership is ultimately accountable for the implementation and effectiveness of the agency's cyber security program. Senior leadership must be actively engaged in cyber security initiatives and champion cultural change. Senior leadership must demonstrate a commitment and understanding of the agency's cyber security program by providing an attestation of their current assessment against all mandatory requirements in the SACSF.
1.2: Organisational Structure and Staff Responsibilities A structure for managing cyber security must be embedded into the agency's governance framework. Roles and responsibilities for cyber security must be formally assigned by senior leadership, demonstrating commitment to providing suitable resources to manage the agency’s cyber security program. Personnel and contractors must be provided with information and training to support awareness of their collective responsibility to foster a positive security culture.
1.3: Risk Management The agency must take steps to identify, understand, assess and manage cyber security risks to its critical processes and information assets. Cyber security risk management processes must be embedded within the agency’s risk management framework and align to the risk appetite of the agency. Senior leadership must be aware of current and emerging cyber security risks to the agency.
1.4: Policies, Procedures and Compliance Cyber security policies and procedures must be in place and approved by senior leadership, providing management direction and support for cyber security in accordance with business requirements and relevant laws, regulations and contractual requirements, and the SACSF. The agency’s suite of cyber security policies, procedures, and working documents must be reviewed regularly and socialised throughout the agency.

1.5: Supplier Management

Cyber security requirements must be included in all agreements with suppliers.

Processes for assessing and managing the risks that suppliers introduce must be embedded within the procurement and contract management functions in alignment with the agency's risk management framework.

1.6: Audit and Assurance

A program of cyber security assurance activities must be in place to evaluate the effectiveness of the agency’s cyber security program and ensure cyber security controls are implemented and operated in accordance with the agency’s policies and procedures, relevant laws, regulations and contractual requirements, and the SACSF.

PRINCIPLE TWO: INFORMATION

Maintain the confidentiality, integrity and availability of all agency information and systems.

2.1: Information Asset Identification and Classification

Information assets supporting critical processes must be identified, recorded and classified.

Processes must be place for labelling, storing, handling and disposing of assets in alignment with their classification.

Agencies must comply with SACSF Ruling 2 – Storage and Processing of information in outsourced or offshore ICT arrangements.

2.2: Incident Management

Cyber security incident response plans must be in place and aligned with an overarching incident management process to enable a consistent approach to the management of cyber security incidents.

Agencies must report to the Office for Cyber Security in line with the requirements of PC042 – Cyber Security Incident Management

2.3: Resilience and Service Continuity

Cyber security requirements must be included as part of agency business resilience planning and incorporated into periodic business continuity and service recovery testing.

2.4: Access to Information

Access to agency systems, applications and information must be based on business need, authorised by the information owner or delegated custodian and be limited to the minimum required for personnel to undertake their duties.

Secure authentication mechanisms must be in place to control access to agency systems, applications and information.

2.5: Administrative Access

Administrative access to agency systems, applications and information must be restricted to personnel with a specific business need which is validated on a periodic basis.

2.6: Robust ICT Systems and Operations

Standard operating procedures and technical controls must be in place to provide a consistent and secure approach to system administration, maintenance and configuration activities.

2.7: Vulnerability Management

Security vulnerabilities in agency ICT equipment, systems and applications must be identified and managed.

2.8: Network Communications

Network communications must be secured, ensuring agency information traversing internal and external networks and must be appropriately protected based on its classification and can only be accessed by authorised parties.

2.9: System and Software Acquisition

Cyber security requirements must be considered throughout the acquisition lifecycle for acquiring new systems and software.

2.10: Secure Software Development

Procedures for secure software development must be embedded into the software development lifecycle.

2.11: Cloud Computing

Risk assessments must be performed by the agency prior to implementing any cloud computing service in order to assess the benefits of the service balanced with the additional jurisdictional, governance, privacy and security risks associated with the use of such services.

2.12: Mobile Device Management

Technical and procedural controls must be in place to address the risks associated with the use of mobile devices including mobile phones, smartphones, tablets, laptops, portable electronic devices, portable storage and other portable internet-connected devices.

2.13: Teleworking

Secure practices for teleworking must be established and understood by agency personnel, with technical controls implemented to enable secure remote access to agency information.

PRINCIPLE THREE: PERSONNEL

Ensure employees and contractors are suitable to access South Australian Government resources and meet an appropriate standard of integrity and honesty.

3.1: Personnel Security Lifecycle

Agencies must assess the suitability of new and existing personnel in alignment with the classification of information to be accessed during employment.

Separating personnel must be made aware of their ongoing cyber security obligations.

PRINCIPLE FOUR: PHYSICAL
Provide a safe and secure physical environment for people, information and assets.
4.1: Physical Security Protective security must be integrated in the process of planning, selecting, designing and modifying agency facilities for the protection of people, information and physical assets.

APPENDIX A: POLICY STATEMENTS AND TIER SPECIFIC EXPECTATIONS

In order to assist with implementation of the SACSF, each of the 21 policy statements are listed below along with tier specific expectations and guidance. The tier specific expectations outlined in this appendix are written as a set of increasingly complex treatments or controls spread across the four tier levels. For a tier one agency they should address the tier one expectations, whilst a tier four agency would be expected to consider the expectations of all the four tiers.

The following table provides an example of how to read the subsequent pages:

Policy Statement	Agency Tier Level	Expectations
1.1: Policy Statement Title Example Policy Statement (a)	One (b)	Example Expectation 1 (c) Example Expectation 2 (c) Example Expectation 3 (c)
	Two (b)	Example Expectation 1 (d) Example Expectation 2 (d) Example Expectation 3 (d)
	Three (b)	Example Expectation 1 (d) Example Expectation 2 (d) Example Expectation 3 (d)
	Four (b)	Example Expectation 1 (d) Example Expectation 2 (d) Example Expectation 3 (d)

1. This is the policy statement this is the top-level requirement that all agencies, regardless of size must address.
2. This is the agency tiering level that an agency will select based on their complexity, the criticality of their services, their risk appetite and a number of other factors as outlined in the SACSF Tier Selection section above.
3. This is the guidance and expectations on how a tier one agency would go about addressing the requirements of the policy statement. Agencies should consider the expectations. The Tier One expectations should also be considered as a baseline expectation for all agencies.
4. These are the increasingly complex standards or controls that should be considered by the higher tiered agencies. Importantly an agency at Tier Two should consider the Tier One expectations in addition to Tier Two. Whereas a Tier Three would consider Three, Two and One expectations and so on.

Principle One: Governance

Principle: The agency manages security risks and supports a positive security culture, ensuring clear lines of accountability, strategic planning, assurance and review, and proportionate reporting.

Policy Statement	Tier	Expectations
1.1: Leadership Senior leadership is ultimately accountable for the implementation and effectiveness of the agency's cyber security program. Senior leadership must be actively engaged in cyber security initiatives and champion cultural change. Senior leadership must demonstrate a commitment and understanding of the agency's cyber security program by providing an attestation of their current assessment against all mandatory requirements in the SACSF.	One	• Senior leadership provides an annual attestation of the agency's current state of alignment to the SACSF; together with a plan to meet or maintain alignment to the agency's required tier level. The attestation covers: o Tasks completed during the reporting period. o Tasks to be completed during the new reporting period. o Cyber security program funding model. o Responsibility for completing the associated task. • Senior leadership allocates roles, responsibilities and resources to support and enable the agency's cyber security program. • Cyber security is regularly included in the agenda of an appropriate senior leadership body, ensuring discussion is focused on the progress of the cyber security program; and cyber security risks to the agency, both existing and emerging.
	Two	**As above**
	Three	**As above**
	Four	**As above**

Policy Statement	Tier	Expectations
1.2: Organisational Structure and Staff Responsibilities A structure for managing cyber security must be embedded into the agency's governance framework. Roles and responsibilities for cyber security must be formally assigned by senior leadership, demonstrating commitment to providing suitable resources to manage the agency's cyber security program. Personnel and contractors must be provided with information and training to support awareness of their collective responsibility to foster a positive security culture.	One	**Management Structure** The management structure for cyber security is embedded into the agency's governance framework. Oversight of the agency's cyber security program is assigned to an Agency Security Committee with a direct report to senior leadership. **Cyber Security Responsibilities, Training and Awareness** The agency has appointed a senior leader accountable for cyber security to provide strategic level guidance for the agency's cyber security program and ensure compliance with cyber security policy, standards, regulations and legislation. Responsibility for day-to-day cyber security operations is assigned and documented in policy and relevant position descriptions. Cyber security education and awareness training is provided to all personnel and contractors during induction and at least annually thereafter, ensuring they are aware of their responsibilities regarding the appropriate use of agency information assets.
	Two	**Management Structure** A dedicated Agency Security Committee is in place to enable effective communication and oversight of the agency's cyber security program. The Agency Security Committee is attended periodically by a member of the agency's senior leadership. **Cyber Security Responsibilities, Training and Awareness** Additional security training is provided to agency personnel who are in positions of trust, have heightened security responsibilities, or have increased risk profiles. Personnel and contractors responsible for cyber security management and day-to-day operations maintain industry recognised certifications relevant to their role that have ongoing continuing professional education requirements or have been obtained within the prior five years. The agency evaluates the performance of all workers with reference to cyber security responsibilities and performance requirements.
	Three	**Cyber Security Responsibilities, Training and Awareness** Skills gap assessments are performed for cyber security and IT personnel responsible for implementing or managing technical security controls. Targeted training is provided for these personnel specific to the technologies in use within the agency. Where contractors or third-parties are used in place of internal resources, periodic vetting of competency is performed.

	Four	**Management Structure** • The agency operates an independently certified information security management system which covers the critical services of the agency and has implemented a formal business continuity management system. • The agency has formally appointed and defined responsibilities for an executive or senior manager solely responsible for cyber security.

Policy Statement	Tier	Expectations
1.3: Risk Management The agency must take steps to identify, understand, assess and manage cyber security risks to its critical processes and information assets. Cyber security risk management processes must be embedded within the agency's risk management framework and align to the risk appetite of the agency. Senior leadership must be aware of current and emerging cyber security risks to the agency.	One	Senior leadership has documented the agency's risk appetite. A risk management framework is in place and includes cyber security risk management processes. Cyber security risks are documented in an agency risk register; and are periodically reviewed by the Agency Security Committee. Cyber security risks are assessed and documented for all projects undertaken by the agency.
	Two	Cyber security risks are documented in a cyber security risk management tool maintained by security personnel and periodically reviewed by the Agency Security Committee.
	Three	**As above**
	Four	**As above**

Policy Statement	Tier	Expectations
1.4: Policies, Procedures and Compliance Cyber security policies and procedures must be in place and approved by senior leadership, providing management direction and support for cyber security in accordance with business requirements and relevant laws, regulations and contractual requirements, and the SACSF. The agency's suite of cyber security policies, procedures, and working documents must be reviewed regularly and socialised throughout the agency.	One	A suite of cyber security policies aligned to the requirements of the SACSF is in place and has been socialised throughout the agency. Significant changes to policies are communicated as they occur. Legal, statutory, regulatory or contractual requirements and the agency's approach to meet these requirements, including how they are monitored and kept up-to-date, are documented. Operating procedures supporting the agency's suite of cyber security policies are in place. Policies, procedures and working documents are version controlled. A cyber security calendar is maintained to schedule and track the status of the cyber security program**.**
	Two	Policies are reviewed every two years at a minimum.
	Three	Policies are reviewed annually at a minimum.
	Four	**As above**

Policy Statement	Tier	Expectations
1.5: Supplier Management Cyber security requirements must be included in all agreements with suppliers. Processes for assessing and managing the risks that suppliers introduce must be embedded within the procurement and contract management functions in alignment with the agency's risk management framework.	One	- A formal supplier register is maintained by the agency. - Processes for assessing and documenting cyber security risks that suppliers may introduce are embedded within procurement and contract management functions. - Cyber security obligations to address identified risks are documented within supplier agreements. - Agencies obtain assurance from suppliers that they have implemented controls to meet their cyber security obligations upon contract award and periodically thereafter.
	Two	**As above**
	Three	**As above**
	Four	- Agencies obtain independent assurance from suppliers that they have implemented controls to meet their cyber security obligations upon contract award and annually thereafter.

Policy Statement	Tier	Expectations
1.6: Audit and Assurance A program of cyber security assurance activities must be in place to evaluate the effectiveness of the agency’s cyber security program and ensure cyber security controls are implemented and operated in accordance with the agency’s policies and procedures, relevant laws, regulations and contractual requirements, and the SACSF.	One	Self-assessment assurance reviews of the cyber security program are performed at least annually by the agency. Independent reviews are performed periodically in line with agency requirements. Policy exemptions are formally requested, documented and monitored by the Agency Security Committee.
	Two	A formal internal audit program is in place to assess alignment to the requirements of the SACSF. Technical reviews of security of critical systems are planned and carried out using a risk-based approach.
	Three	**As above**
	Four	Formal independent reviews of the cyber security program are undertaken at least annually.

Principle Two: Information

Principle: Maintain the confidentiality, integrity and availability of all agency information and systems.

Policy Statement	Tier	Expectations
2.1: Information Asset Identification and Classification Information assets supporting critical processes must be identified, recorded and classified. Processes must be place for labelling, storing, handling and disposing of assets in alignment with their classification. Agencies must comply with SACSF Ruling 2 – Storage and Processing of information in outsourced or offshore ICT arrangements.	One	| Information assets supporting critical processes are identified and recorded in an information asset register. | Information assets are formally assigned an owner. | Information assets are classified by the asset owner in alignment with the South Australian Information Classification System.
	Two	| Processes are documented and followed for labelling, storing, handling and disposing of assets in alignment with their classification.
	Three	**As above**
	Four	**As above**

Policy Statement	Tier	Expectations
2.2: Incident Management Cyber security incident response plans must be in place and aligned with an overarching incident management process to enable a consistent approach to the management of cyber security incidents. Agencies must report to the Office for Cyber Security in line with the requirements of PC042 – Cyber Security Incident Management	One	- Cyber security incident response is included in the agency's incident management policy, documenting responsibility for cyber security incident management. - Incident management plans and processes are socialised throughout the agency periodically, and testing is included in assurance activities performed by the agency. - Post-incident review procedures are performed, and evidence relevant to cyber security incidents is recorded and retained. - Agencies have a formalised process for reporting cyber security events to the Office for Cyber Security Watch Desk and assisting in the assessment process as required.
	Two	- Response plans are developed for high impact or high likelihood cyber security risks as documented in the agency's cyber security risk register. - Cyber security specialists are identified and obtainable for cyber security incident response through internal capability or arrangements with third party specialists. - Post-incident review procedures are followed that include assessment of root cause, and evidence of learnings and corrective actions performed to reduce the risk of a recurrence.
	Three	**As above**
	Four	- Cyber security incident management is embedded in the agency's formal business continuity management system.

Policy Statement	Tier	Expectations
2.3: Resilience and Service Continuity Cyber security requirements must be included as part of agency business resilience planning and incorporated into periodic business continuity and service recovery testing.	One	- Business impact assessments have been performed. - Cyber security requirements are included in critical process continuity plans. - IT service recovery plans aligned to the outage limits identified in the business impact assessments are in place. - IT service recovery plans are tested periodically as part of the assurance activities performed by the agency.
	Two	- A detailed business continuity plan is implemented. - Business continuity and IT service recovery testing includes periodic testing against cyber security scenarios.
	Three	**As above**
	Four	- A formal business continuity management system is in place and includes: o Emergency and crisis management o Incident management o Business continuity o Business impact assessments o Disaster recovery o IT service recovery - Cyber security elements of the business continuity management system are tested annually at a minimum.

Policy Statement	Tier	Expectations
2.4: Access to Information Access to agency systems, applications and information must be based on business need, authorised by the information owner or delegated custodian and be limited to the minimum required for personnel to undertake their duties. Secure authentication mechanisms must be in place to control access to agency systems, applications and information.	One	**Access Provisioning** - Physical or logical access to agency information assets is provided based on business need. - The processes to provision access to systems and applications in use within the agency are documented. **Authentication and Traceability** - All users have unique accounts providing traceability of actions within critical systems and applications. - Secure virtual private networks and multi-factor authentication are used to remotely access the agency's IT environment. - Password standards (complexity, minimum length, maximum age) are documented and implemented on all systems and applications. **Access Reviews** - Reviews of general user access are performed at least annually for the network and all critical applications. **Termination of Access** - Terminated user's access is revoked within defined timeframes.
	Two	**Authentication and Traceability** - Multi-factor authentication is required to authenticate all users in positions of trust.
	Three	**Authentication and Traceability** - Multi-factor authentication is required to authenticate users to cloud based solutions such as Office 365. - Certificate based authentication is implemented to identify authorised workstations connected to the agency's network. **Termination of Access** - Access of terminated personnel is revoked immediately upon departure.
	Four	**As above**

Policy Statement	Tier	Expectations
2.5: Administrative Access Administrative access to agency systems, applications and information must be restricted to personnel with a specific business need which is validated on a periodic basis.	One	**Access Provisioning** - Users are assigned a dedicated privileged account to be used solely for tasks requiring privileged access. - Documented policies restrict the use of privileged accounts from reading emails, accessing the internet and obtaining files via online services. - Local administrative privileges on workstations are removed. **Access Reviews** - Reviews of privileged user access are performed at least every 6 months. **Authentication and Traceability** - Privileged account actions deemed high risk by the agency are logged and monitored for unusual activity. - Password standards (complexity, minimum length, maximum age) for privileged accounts are documented and implemented on all systems and applications. **Termination of Access** - Privileged access is revoked immediately once there is no longer a specific business need for it.
	Two	**Authentication and Traceability** - Multi-factor authentication is required to authenticate privileged users.
	Three	**Access Reviews** - Privileged user access reviews are performed at least every 3 months. - Technical controls are in place to restrict the use of privileged accounts from reading emails, accessing the internet and obtaining files via online services.
	Four	**Access Provisioning** - A process exists such that there is formal request and approval of access associated with tasks requiring privileged actions, and privileged access is revoked upon completion of the task.

Policy Statement	Tier	Expectations
2.6: Robust ICT Systems and Operations Standard operating procedures and technical controls must be in place to provide a consistent and secure approach to system administration, maintenance and configuration activities.	One	**Standard Operating Procedures** • Standard operating procedures have been developed for all primary cyber security functions performed by agency personnel. **Change management** • A change management process is developed and implemented that includes: o Identification and documentation of changes to be made, o Approval required for changes to be made, o Implementation and testing of approved changes, and o Any actions to be taken before and after approved changes are made. **Backups** • Backup, restoration and preservation strategies are developed and implemented as part of business continuity, disaster recovery and digital preservation planning. • Backups of important information, software and configuration settings are performed at least daily and stored for at least three months. • Backup and restoration processes are tested annually. • Backups are stored offline, or online in a non-rewritable and non-erasable manner. **System Configuration & Hardening** • Macro settings within Microsoft Office are as follows: o Only signed Microsoft Office macros can execute, o Microsoft Office macros in documents originating from the Internet are blocked, and o Microsoft Office macro security settings cannot be changed by users. • Web browsers are configured to block or disable support for Flash content, web advertisements and Java from the Internet. • Technical controls are in place to restrict non-privileged users from installing software.

	Two	**Backups** • Full back up and restoration processes are tested when fundamental IT infrastructure changes occur. **System Configuration & Hardening** • Application whitelisting is implemented on all workstations and servers to restrict the execution of executables and software libraries to an approved set. **Event Logging and Monitoring** • An event logging strategy is developed and implemented covering events to be logged, logging facilities to be used, event log retention periods and how event logs will be protected. • A centralised logging facility is implemented, and systems are configured to save event logs to the centralised logging facility as soon as possible after each event occurs. • An accurate time source is established and used consistently across systems and network devices to assist with the correlation of events. **System Redundancy** • Redundancy is built into systems commensurate with the system availability requirements identified as part of the business impact assessments.
	Three	**System Configuration & Hardening** • Application whitelisting is implemented on all workstations and servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.
	Four	**System Configuration & Hardening** • Controls are in place to isolate critical systems. • Critical system isolation is tested periodically.

Policy Statement	Tier	Expectations
2.7: Vulnerability Management Security vulnerabilities in agency ICT equipment, systems and applications must be identified and managed.	One	- Security vulnerabilities in applications and operating systems are patched or mitigated within **one month** of release for all workstations and servers. - Security vulnerabilities in applications and operating systems that are assessed as 'extreme' are patched or mitigated within **48 hours** of release for all workstations and servers. - There is a documented process for managing the risks associated with non-vendor supported applications and operating systems where they are required for a specific purpose. - A mechanism is in place to ensure compliance to patching requirements. Expected patching compliance rates are documented. - Malware detection and prevention tools are in place on workstations and servers.
	Two	- A vulnerability management strategy is in place that includes: o Conducting vulnerability assessments and penetration tests for systems throughout their lifecycle to identify security vulnerabilities o Analysing identified security vulnerabilities to determine their potential impact and appropriate mitigations or treatments based on effectiveness, cost and existing security controls o Using a risk-based approach to prioritise the implementation of identified mitigations or treatments o Monitoring information on new or updated security vulnerabilities in operating systems, software and ICT equipment as well as other elements which may adversely impact the security of a system. - Security vulnerabilities in applications and operating systems are patched or mitigated within **two weeks** of release for all workstations and servers.
	Three	**As above**
	Four	- Patching compliance reports are generated and provided to the agency by all relevant third parties.

Policy Statement	Tier	Expectations
2.8: Network Communications Network communications must be secured, ensuring agency information traversing internal and external networks and must be appropriately protected based on its classification and can only be accessed by authorised parties.	One	- The agency's network architecture is documented showing the internal network structure and incoming/outgoing egress points. - Information flows associated with critical processes are documented listing: o The type of information, o The classification of the information, o Who the information is being exchanged with, and o The controls in place to protect the information.
	Two	- Risk assessments are performed for all information flows associated with critical processes, and appropriate controls applied.
	Three	**As above**
	Four	- Information flow risk assessments are reviewed annually. - Network segregation is implemented throughout the agency's network.

Policy Statement	Tier	Expectations
2.9: System and Software Acquisition Cyber security requirements must be considered throughout the acquisition lifecycle for acquiring new systems and software.	One	- Security risks associated with system and software acquisition or significant system enhancements are identified, documented and managed as per the agency's risk management framework before the system and/or software is implemented into production. - Where system acquisition relates to a cloud service, the requirements of 2.11 Cloud Computing are applied.
	Two	**As above**
	Three	**As above**
	Four	**As above**

Policy Statement	Tier	Expectations
2.10: Secure Software Development Procedures for secure software development must be embedded into the software development lifecycle.	One	Software development, testing and production environments are segregated. Secure coding practices are documented and followed. Outsourced software development is supervised. Security functionality testing occurs throughout development and prior to implementation. Vulnerability assessments and penetration tests are conducted by suitably skilled personnel before systems are deployed, after significant changes have occurred, and at least annually or as specified by the system owner.
	Two	Platform-specific secure programming practices are used when developing software, including using the lowest privilege needed to achieve a task, checking return values of all system calls, and validating all inputs. Code reviews are performed by suitably skilled personnel prior to implementation. Software developers are provided additional training relating to secure software development. Workstations and accounts used for software development are managed in line with privileged access management procedures.
	Three	**As above**
	Four	**As above**

Policy Statement	Tier	Expectations
2.11: Cloud Computing Risk assessments must be performed by the agency prior to implementing any cloud computing service in order to assess the benefits of the service balanced with the additional jurisdictional, governance, privacy and security risks associated with the use of such services.	One	- A risk assessment is performed before implementing any cloud service. - Security risks associated with a cloud service are identified, documented and managed as per the agency's risk management framework before the cloud service is implemented.
	Two	**As above**
	Three	- Formal Independent assurance reports relating to the risks associated with the cloud service are obtained on an annual basis where the cloud service is supporting: o Critical services, o Services with high availability or integrity requirements, o Services storing sensitive information or higher, or o Services with a moderate or higher risk profile.
	Four	**As above**

Policy Statement	Tier	Expectations
2.12: Mobile Device Management Technical and procedural controls must be in place to address the risks associated with the use of mobile devices including mobile phones, smartphones, tablets, laptops, portable electronic devices, portable storage and other portable internet-connected devices.	One	• Procedural controls have been established, outlining the mechanisms for protecting agency information stored on or accessed from laptops, mobile phones and removable storage devices. • Processes exist for requesting and authorising the use of personal mobile phones to access agency information such as emails. • Passphrases and/or PIN codes are in place on laptops and mobile phones used for accessing agency information. • Secure virtual private networks and multi-factor authentication are used to remotely access the agency's IT environment. • Multi-factor authentication is required when configuring mobile phones to access agency email accounts on initial set up and each time the user's account password is changed. • Encryption of storage is enabled for all laptops, mobile phones, and removable storage devices.
	Two	• A mobile device management solution is in place to ensure that appropriate controls are applied to all mobile phones, including personal phones used for work. • Remote wipe functionality is enabled for all agency laptops and mobile phones, including personal phones used for work.
	Three	**As above**
	Four	**As above**

Policy Statement	Tier	Expectations
2.13: Teleworking Secure practices for teleworking must be established and understood by agency personnel, with technical controls implemented to enable secure remote access to agency information.	One	• Teleworking procedures are established and socialised with agency personnel working offsite. • Travel devices are provisioned to agency personnel for international travel in alignment with the risks associated with the destination country/countries. • Technical controls are implemented to enable secure remote access to agency information assets.
	Two	**As above**
	Three	**As above**
	Four	**As above**

Principle Three: Personnel

Principle: Ensure employees and contractors are suitable to access South Australian Government resources and meet an appropriate standard of integrity and honesty.

Policy Statement	Tier	Expectations
3.1: Personnel Security Lifecycle Agencies must assess the suitability of new and existing personnel in alignment with the classification of information to be accessed during employment. Separating personnel must be made aware of their ongoing cyber security obligations.	One	| Background verification checks on all candidates for employment are performed in accordance with relevant laws, regulations and ethics, and shall be proportional to the business requirements, the classification of the information to be accessed and assessed risks. | Agencies assess and manage the ongoing suitability of their personnel in relation to the information accessed as part of their role. | Separating personnel are made aware of their ongoing cyber security obligations, and have their access to agency resources withdrawn, per user access management processes.
	Two	**As above**
	Three	**As above**
	Four	**As above**

Principle Four: Physical

Principle: Provide a safe and secure physical environment for people, information and assets.

Policy Statement	Tier	Expectations
4.1: Physical Security Protective security must be integrated in the process of planning, selecting, designing and modifying agency facilities for the protection of people, information and physical assets.	One	Physical security measures are in place to protect agency physical assets including people, information and facilities based on the classification of the information that they are approved for processing, storing or communicating.
	Two	**As above**
	Three	**As above**
	Four	**As above**

APPENDIX B: GLOSSARY OF TERMS

Term	Description
Agency	South Australian Government public sector agencies (as defined in the Public Sector Act 2009), that is, administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown. Each agency retains ultimate responsibility for all aspects covered by the SA Cyber Security Framework as it relates to a particular agency and its information assets.
Agency governance framework	The management structure used by the agency. Cyber security management will be embedded within the overall governance framework. Governance may be further described as: the decision-making processes that define expectations, grant power, or verify performance. It consists either of a separate process or of a specific part of management or leadership processes.
Certification	The process by which an Accredited certifying body issues a certificate of conformance to a given Standard to an individual or organisation.
Classification	The process by which information assets are labelled according to their business importance and sensitivity. Classification markings are used to indicate the value of the information.
Critical process continuity plan	Documented work-around plans for maintaining critical processes during a period of disruption.
Critical processes	Agency processes that, if not performed, would eventuate in the highest level of risk to the agency. This could include meeting critical needs of the agency or satisfying mandatory regulations and requirements.
Critical Service	Services that, if compromised, would result in significant damage to the physical, social or economic wellbeing of the State. Critical Services are not typically ICT services, they are services that an agency delivers to the community on behalf of the State Government.
Cyber Security	Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means. (synonymous with ICT Security)
Cyber security program funding model	It is expected that there will be capital expenditure (CAPEX) during implementation of cyber security tasks and ongoing operational expenditure (OPEX) for ongoing maintenance and support.
Encryption	A process, which may be irreversible, of transforming information, particularly data, into an unintelligible form.
Exemption	Approval for exclusion from the implementation or use of a mandated document outlined in the SACSF.

Extreme vulnerability	Defined as: • the security vulnerability facilitates remote code execution, • critical business systems are affected, • an exploit exists in the public domain and is being actively used, and/or • the system is internet-connected with no mitigating controls in place.
Framework	A basic conceptual structure used to solve or address complex issues.
Governance	The exercising of authority or decision-making processes.
Guideline	A statement of desired, good or best practice.
Guidance	See Guideline.
ICT	Information and Communication Technology.
Incident	Any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service and/or loss or corruption of information resulting in a breach or privacy or security.
Information assets	Any information or asset supporting the use of the information that has value to the agency, such as collections of data, processes, ICT, people and physical documents.
Information custodian	The individual or group assigned responsibility for managing a set of information.
Information owner	The individual or group responsible and accountable for a set of information. The information owner may, at their discretion, assign responsibility for management of the information to another person or group, also known as an information custodian.
ITSA	Information Technology Security Adviser is a Position of Trust as defined in the PSMF. This role is appointed by an agency or organisation to manage the security of information and ICT systems. ISMF Guideline 4b provides information about this role, including guidance on the selection of suitable persons to fill the role.
IT service recovery plan	Documented plans for restoring IT services following a disruption.
Mobile device	Mobile phones, smartphones, tablets, laptops, portable electronic devices, portable storage and other portable internet-connected devices.
Multi-factor	A method of authentication using separate mutually dependent credentials, typically “something you have” and “something you know”.

Periodic (periodically)	An event or action that must occur at prescribed intervals.
Policy	A statement of principles and/or values that mandate or constrain the performance of activities used in achieving institutional goals.
Portable Device (electronic, storage and/or internet-connected portable device)	A small, lightweight, portable, easy to use device which is capable of storing and transferring large volumes of data.
Position of trust	Any position or role within the agency with heightened levels of access to sensitive information or otherwise have increased risk profiles.
Regular (regularly)	An event or action that should occur at consistent intervals and is typically determined by Standard Operating Procedures or a Security Schedule.
Risk appetite	The level of risk the agency is willing to accept. Agencies will need to define what level of management response is required for each risk level, for example *Extreme/High Risk – Senior leadership response.* *Moderate Risk – Agency Security Committee response.* *Low Risk – Security management response.*
Risk Profile	An outline of the risks to which an organisation, or business unit within an organisation, is exposed. Most Risk Profiles identify specific risks, associated mitigation strategies and an overall assessment or grading of each risk.
Ruling	An official interpretive statement of general applicability issued and published by a recognised authority.
Agency security committee	The management group responsible for security. It is expected that Tier one agencies will assign this responsibility to an existing group, whilst Tier two – four agencies will create a dedicated Agency Security Committee.
Senior leadership	Generic term that may encompass the Agency Board, Senior Executive Members, Chief Executive, Agency Security Executive or equivalent.
Standard	A formal document that establishes uniform criteria, methods, protocols, processes and practices to meet policy requirements.
Strategy	A long-term plan of action designed to achieve a particular goal.
Supplier	Suppliers are defined as any individual, contractor, business partner, or agent not directly employed by a South Australian Government agency. Supplier access is defined as any local or remote access made by a supplier to Government IT assets. In terms of arrangements with suppliers, the scope extends to the various service delivery interfaces with those suppliers, as defined in contracts and/or service level agreements. It includes auditing of security services implemented by suppliers that have a material impact on the

	security of information managed by the agency, but otherwise excludes the suppliers’ internal processes.
User	Anything, including persons and computer systems that access ICT resources.

APPENDIX C: GUIDANCE ON TIER SELECTION

Agency Chief Executives are ultimately accountable for their tier selection, and this tier selection will be noted by the whole of government ICT and Data Board on an annual basis as part of attestation processes.

The following table describes potential characteristics of agencies within each tier. These characteristics are not definitive and should be used as a guide only. Tier selection is aimed at providing additional guidance to help agencies to apply controls commensurate with the complexity and criticality of their agency.

Characteristics of a Tier Four Agency may include:

- Managing or maintaining information with a classification of Protected or higher.
- Providing services for the State of which an outage of more than four hours would result in catastrophic consequences for the State.
- Employing more than 2,000 personnel.
- Having a very low appetite for cyber security risk.

Characteristics of a Tier Three Agency may include:

- Providing technology services to other agencies.
- Managing or maintaining a large volume of information classified as Official: Sensitive, (e.g. personally identifiable information or health records).
- Providing services for the State of which an outage of more than 48 hours would result in catastrophic consequences for the State.
- Employing more than 500 personnel.
- Having a low appetite for cyber security risk.

Characteristics of a Tier Two Agency may include:

- Providing services for the State of which an outage of more than one week would result in catastrophic consequences for the State.
- Employing less than 500 personnel.
- Having a moderate or lower appetite for cyber security risk.

Characteristics of a Tier One Agency may include:

- Employing less than 200 personnel.
- Having a moderate or higher appetite for cyber security risk.

For more information:
Office for Cyber Security
Department of the Premier and Cabinet

T 1300 244 168
E officeforcybersecurity@sa.gov.au
W security.sa.gov.au

Appendix 2

Cyber Security Audit

Cyber Security Audit

Adelaide Hills Council

Contents

Report

Appendices

Executive Summary

Background

Adelaide Hills Council ('Council') operates an internal audit function to gain assurance of process effectiveness across different areas of the organisation. The areas to be audited are nominated following Council risk assessments, sector-wide issues and enquiries from other agencies (e.g. Auditor-General's Department).

Recognising the importance of managing cyber security risks, Council's Audit Committee incorporated a cyber security controls audit into its Strategic Internal Audit Plan and engaged CyberCX to conduct the audit following their response to the Review of Cyber Security Controls RFQ (60/20).

CyberCX is the largest Australian end-to-end information security provider. This project was delivered locally out of CCX's governance, risk and compliance practice who conduct cyber security audits as a primary service offering.

The key objective of this audit was to identify areas of cyber security risk and position Council to implement further controls to address those risks using the recommendations from a wholistic information security controls assessment.

Approach

To identify these risks, CyberCX conducted interviews with key personnel over three days to discuss Council processes and technologies, leveraging the wholistic ISO/IEC 27001:2013 information security standard which is comprised of 114 controls across 14 domains. Identified control gaps were explored with Council staff to determine if any risks were present, considering Council context as well as compensating controls.

Council was also assessed against the Australian Cyber Security Centre's Essential Eight Maturity Model and benchmarked against a sample of five similar sized Councils, at Council's request. Recommendations were provided for Council to achieve both a level two and three maturity where those maturity levels were not met.

ISO 27001 Annex A is comprised of a broad set of information security controls covering people, process, and technology in a holistic manner. It is intentionally non-prescriptive to facilitate a risk-based approach to managing information security and to capture non-technology related security aspects (e.g. human resource screening).

The Essential Eight complements the ISO 27001 control set as it's detailed in terms of specific technical controls that are useful in disrupting malicious hacking attempts. The Essential Eight's shortcoming is that it is only concerned with technical security domains, and does not consider other common mechanisms of compromise (e.g. social engineering). However, these standards used together provide appropriate coverage over Council operations (people and process – ISO 27001) and technical security controls (Essential Eight).

Overview Statement

The audit found that although some control gaps were identified, Council has a general awareness of its information security risk landscape and has implemented compensating controls to address many of the identified information security risks. It was also noted that several security uplift activities were underway and have been mentioned where appropriate in this report.

Strengths

Several areas of strength were identified within Council were primarily related to day-to-day IT security operations and physical security of Council's server room. Council ICT staff that were interviewed also demonstrated an adequate level of security awareness and technical security competence.

Executive Summary (cont'd)

Risks

Ten information security risks were identified from the controls audit. The Council risk owner evaluated one of these as High 2B (residual) which is related to ICT not having control over access to certain Council business applications.

Four were evaluated as Medium (residual) which relate to lack of multi-factor authentication (MFA) for remote access, lack of formality regarding supplier management, and inadequate documented process for information security incidents separate from data breaches (e.g. ransomware, website defacement, etc).

The five remaining risks were evaluated as Low (residual) by the Council risk owner, largely due to the presence of compensating controls.

Next Steps

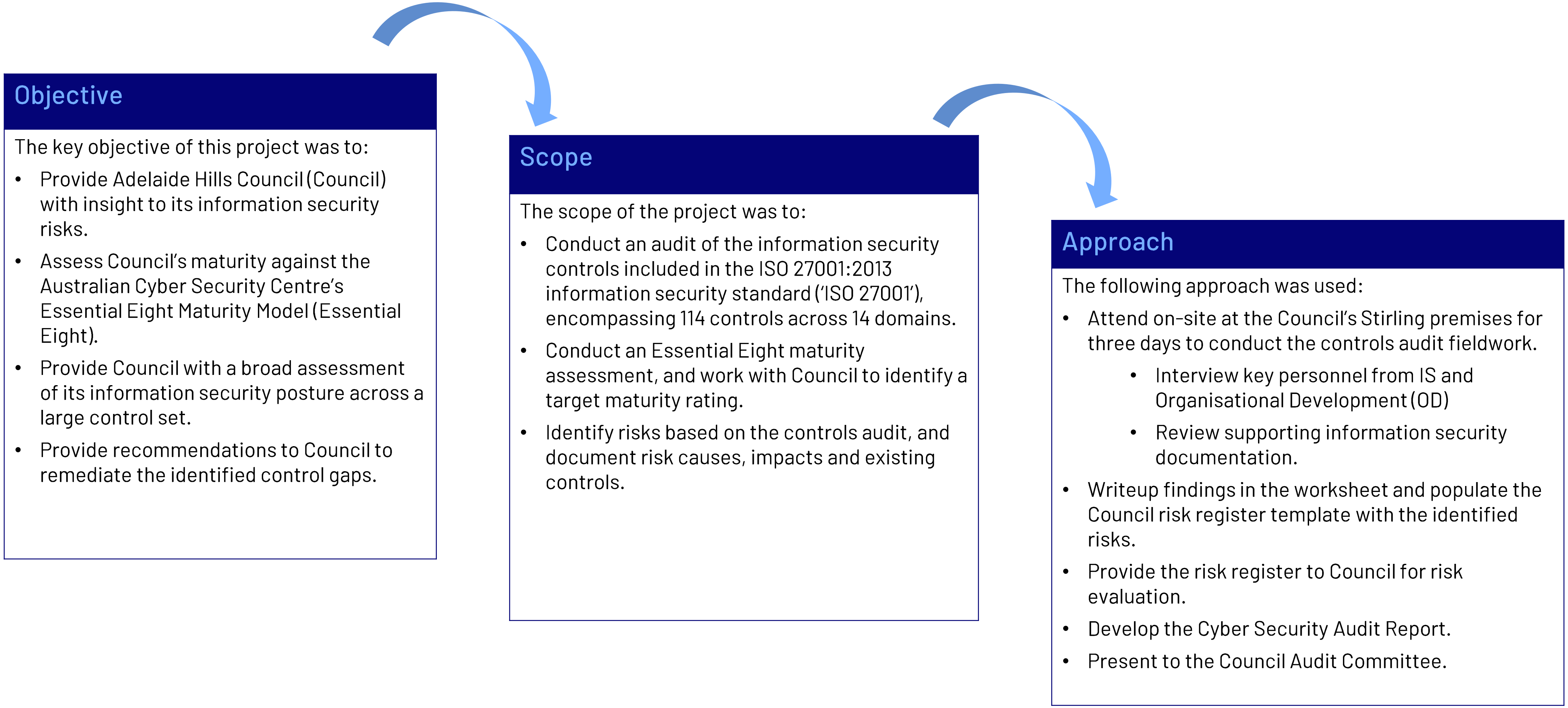
There are steps that Council should take to address the identified risks. Council should establish a framework for managing the information security risks associated with the use of contractors and vendors that gain access to Council systems. Council should consider establishing an information security classification scheme (e.g. Public, Internal, Restricted) to guide the implementation of security controls commensurate with the sensitivity or criticality of its information. Council should also enhance its information security policy suite to have coverage over additional key domains such as access management, network security, remote access, mobile devices and supplier management.

In the short term, there are several actions that can be readily addressed to provide some demonstrable progress. These include minor enhancements of existing security documentation and ICT agreements, the inclusion of key security considerations in the supplier management process, and the documentation of existing robust processes.

Further information on the above items can be found throughout this report. The detailed findings have been provided in Excel format to allow Council to track its progress against the recommendation.

CyberCX would like to thank all Council participants for their help and cooperation during this engagement.

Approach



Objective

The key objective of this project was to:

- Provide Adelaide Hills Council (Council) with insight to its information security risks.
- Assess Council's maturity against the Australian Cyber Security Centre's Essential Eight Maturity Model (Essential Eight).
- Provide Council with a broad assessment of its information security posture across a large control set.
- Provide recommendations to Council to remediate the identified control gaps.

Scope

The scope of the project was to:

- Conduct an audit of the information security controls included in the ISO 27001:2013 information security standard ('ISO 27001'), encompassing 114 controls across 14 domains.
- Conduct an Essential Eight maturity assessment, and work with Council to identify a target maturity rating.
- Identify risks based on the controls audit, and document risk causes, impacts and existing controls.

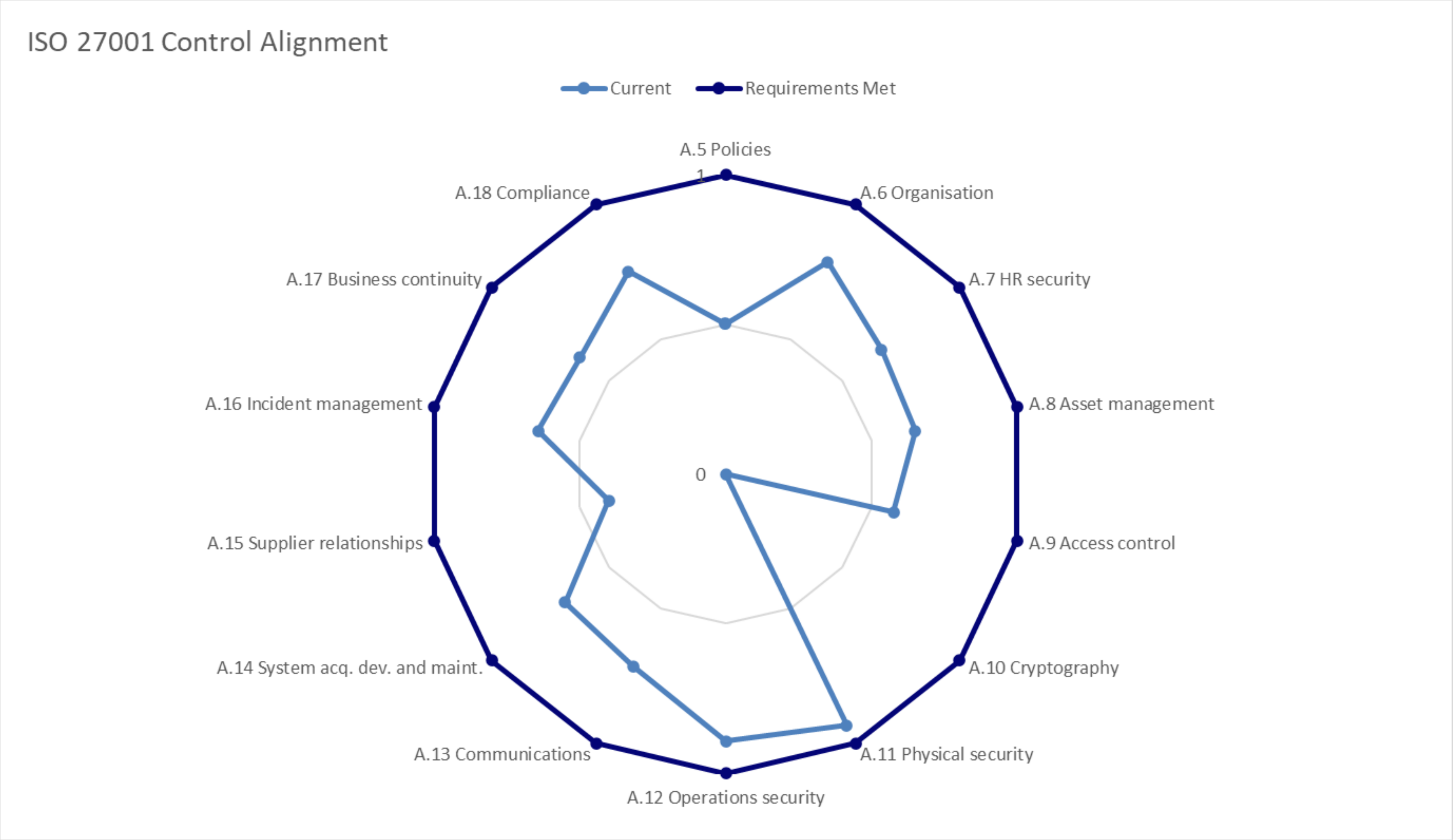
Approach

The following approach was used:

- Attend on-site at the Council's Stirling premises for three days to conduct the controls audit fieldwork.
    - Interview key personnel from IS and Organisational Development (OD)
    - Review supporting information security documentation.
- Writeup findings in the worksheet and populate the Council risk register template with the identified risks.
- Provide the risk register to Council for risk evaluation.
- Develop the Cyber Security Audit Report.
- Present to the Council Audit Committee.

Control Assessment Summary

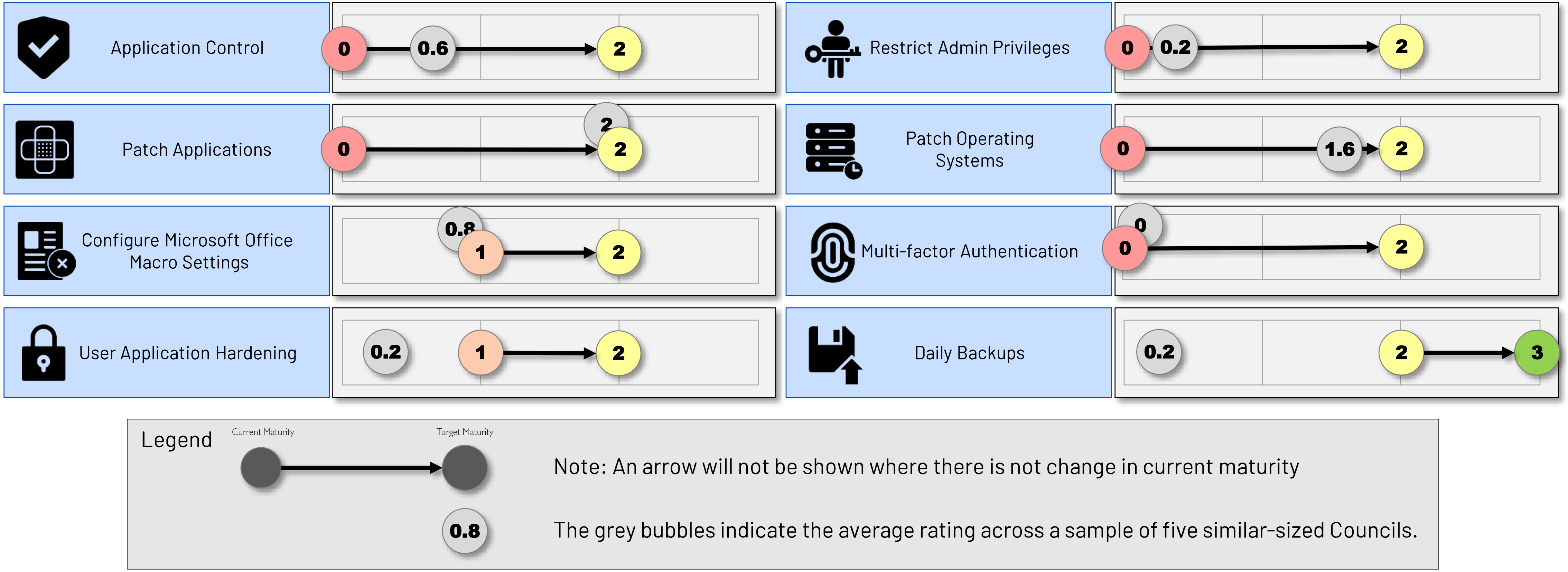
The following chart shows the level of alignment across the ISO 27001 Annex A control domains covered during the audit, where 2 indicates requirements are met, 1 indicates requirements are partially met and 0 indicates requirements are not met. Assessment details against each control can be found in Appendix C - ISO 27001 Controls Assessment.



Essential Eight Maturity Summary

The following illustrates Council's maturity against the Essential Eight. A detailed breakdown of the Essential Eight maturity assessment findings and recommendations can be found in the Appendix D – Essential Eight Controls Assessment. The target maturity ratings (marked with an arrow) were discussed with Council IT and determined to be an appropriate short-term target considering resources, difficulty of implementation, dependencies, etc.

It's important to note that although several requirements for a maturity level may be met, the standard requires all requirements to be met for the entity to achieve that maturity level. For example, Council patches vulnerabilities considered extreme within two weeks, which would achieve a maturity level two in both Patch Applications and Patch Operating Systems. However, Council relies on the TRIM records management system (and an outdated operating system version to support it) which is no longer supported by the vendor, and as such, Council cannot exceed a maturity level of zero. As such, achieving even a low level of maturity against the Essential Eight strategies can be difficult. This is supported by the average ratings in the grey bubbles, with most averages sitting below maturity level one.



Application Control: 0, 0.6, 2

Restrict Admin Privileges: 0, 0.2, 2

Patch Applications: 0, 2, 2

Patch Operating Systems: 0, 1.6, 2

Configure Microsoft Office Macro Settings: 0.8, 1, 2

Multi-factor Authentication: 0, 0, 2

User Application Hardening: 0.2, 1, 2

Daily Backups: 0.2, 2, 3

Legend

Current Maturity

Target Maturity

Note: An arrow will not be shown where there is not change in current maturity

0.8

The grey bubbles indicate the average rating across a sample of five similar-sized Councils.

Risk Summary

The following table outlines the risks identified during the audit alongside Council's evaluation of these risks. A detailed breakdown of each risk (e.g. causes, impacts, etc) can be found in Appendix E Risk Register.

Risk Statement	Inherent Risk	Control Effectiveness	Residual Risk
Lack of ICT control of certain cloud-based applications (Smarty Grants) may result in users being provided with or retaining access to systems after leaving the organisation.	High (2B)	Marginal	High (2B)
Lack of multifactor authentication resulting in unauthorised remote access for a user.	Medium (2C)	Marginal	Medium (2C)
No formal third-party supplier agreements in place resulting in potential compromise of Council data.	Medium (2C)	Poor	Medium (2C)
Internal labour hire (Contractors) are not always subject to the formal OD onboarding / offboarding process resulting in access to systems remaining in place after contractor agreements expire.	High (2B)	Marginal	Medium (2C)
The data breach response plan does not cover other types of information security incidents (e.g. ransomware, denial of service attacks, website defacement, etc) resulting in an ineffective or inefficient response during an information security incident.	Medium (2C)	Marginal	Medium (2C)
Lack of an information classification framework leading to the inappropriate release/management of corporate information.	High (2B)	Good	Low (1C)
Lack of identity verification may result in the compromise of Council credentials via vishing while processing a password reset (i.e. phone-based social engineering)	Low (2E)	Good	Low (1E)
Failure of staff to lock workstations when unattended resulting in unauthorised use of systems.	Medium (2C)	Marginal	Low (2D)
Lack of independent technical testing may result in vulnerabilities being undetected in Council systems.	Medium (3C)	Good	Low (2D)
Telecommunication service provider outage severing connection to Council data centres.	Low (3E)	Marginal	Low (3E)

Strengths

Strength Details

The following areas of strength were identified during the audit and should be recognised – note that this list is not exhaustive:

Security and IT operations

- Day-to-day IT and security operations are well managed including routine backups, management of changes at a technical level, capacity management, logging and monitoring of key user activities and management of technical vulnerabilities. The ICT Team Leader displayed competence in technical security operations and performs regular scanning of the network to identify vulnerabilities.

Physical and environmental security

- The physical security of Council's Stirling premises is robust. Key findings from the site survey were:
    - Despite being joined to the Stirling library, Council's perimeter was well-defined with locked doors requiring fob access. The internal door connecting Stirling library with the Council office has a concealed fob reader.
    - The server room is located well within the security perimeter and cannot be seen from outside. Access to room itself is further limited to individuals with a business requirement to have access.
    - A digital visitor sign-in system is used that prints a photo of the visitor on the badge itself.
    - Deliveries are managed from the library front desk, and delivery personnel are escorted if required.

IT asset management

- Council IT assets are leased, which ensures that several asset management controls meet the requirements of the standard including maintenance of equipment and supporting utilities as well as secure disposal of devices, drives and equipment.

Contact with special interest groups

- Two members from ICT, including the ICT Team Leader, maintain affiliations with the local SecTalks special interest group, subscribe to security news sources, and monitor DPC WatchDesk and RSS feeds to stay abreast of emerging threats and vulnerabilities.

Stand up awareness training

- The ICT Team Leader recently conducted stand-up awareness training to Council staff on password security. In-person training is an effective method of raising awareness and enthusiasm for information security. Council should expand this type of training into a program covering several areas to strengthen the human element of security.

Key Gaps

Gap Details

The audit has highlighted a number of areas where controls are not effectively implemented. This includes, but is not limited to the following:

Supplier / contractor management

- There were several gaps identified relating to Council's management of contractors and suppliers that gain access to Council information or systems (e.g. labour-hire):
  - OD are not always notified of contractors being onboarded and as such they may not be captured in the established onboarding and offboarding processes, resulting in:
    - Contractor access is sometimes managed outside of the established processes;
    - OD may not be aware of IT assets (e.g. devices, fobs) provisioned to contractors; and
    - Contractors do not sign ICT/IS agreements or read Council security-related policies
  - Management of information security risks are not formally embedded throughout the Council supplier management process. As a result, suppliers may be engaged without being subject to confidentiality clauses, having security related clauses in their contracts, acknowledging their security responsibilities.

Classification and labelling of information

- Council does not have a framework for classifying its information based on sensitivity. This makes it difficult to apply information security controls, both technical and non-technical, commensurate with risk.

Access management (outside of ICT)

- Although ICT has a controlled access management workflow – Council does not have an access management policy that outlines how access will be authorised, provisioned, reviewed, and revoked. There are other areas of Council where ICT does not manage access (e.g. for certain cloud applications), and inappropriate access may be provisioned and retained as a result.

Information security policy

- Council does not have information security policies that covers key domains (e.g. network security supplier management) which makes it difficult to enforce security controls throughout, especially in areas where security controls are not managed by ICT.

Independent reviews of information security

- Prior to this audit, Council has not had independent reviews of information security (technical or non-technical) for a number of years.

Policy on cryptography

- Council has not identified and documented its encryption requirements for information at rest or in transit – which is a core requirement of ISO 27001.

Strategic Recommendations

Detailed Recommendations

The following high priority actions are recommended to address the key gaps and risks:

Develop a framework for managing supplier-related information security risks

- Council should develop a framework to ensure that supplier-related information security risks are identified and managed throughout the supplier management lifecycle. This may include an initial risk assessment when onboarding a supplier or service, implementing controls to address risks (e.g. NDAs, security clauses in contracts, presenting suppliers with policies, implementing technical security controls relating to the service), and ensuring suppliers are maintaining good information security practices throughout the duration of the engagement (e.g. yearly attestations from the supplier).

Include management of contractors that gain access to Council information or systems under the established OD processes

- Further to the above, management of contractors that may have an impact on Council information security (typically those that gain access to information or systems) should be covered under the established OD processes to ensure their screening and management of access and IT assets are performed appropriately.

Establish an information classification scheme with supporting handling procedures

- A framework for classifying information can effectively guide the application of security controls. Council should define an appropriate information classification scheme (e.g. Public, Internal, Restricted) and design security controls (both technical and non-technical) based on the sensitivity of the information. Systems will inherit the classification of the information they contain and should be secured accordingly.

Implement an access management policy

- As there are areas of Council where ICT does not manage or have oversight of access (e.g. business unit cloud applications), Council should document its access management requirements (for authorisation, provision, review and revocation) in a policy and apply it across Council.

Enhance the suite of information security policies

- Council should expand its information security policies into a set of domain-specific policies. These can be contained in a single, larger policy or a suite of smaller policies. Policies define the 'what', and are the foundation of applying information security controls. Key policy domains for Council to develop are:
    - Access management;
    - Network security;
    - Remote access / mobile devices; and
    - Supplier / contractor management.

Strategic Recommendations (cont’d)

Detailed Recommendations

The following high priority actions are recommended to address the key gaps and risks:

Conduct an independent penetration test

- This audit is an independent assessment of information security practices. However, Council should conduct an independent technical test (e.g. penetration test) of technical security controls for additional assurance. An appropriate target may be the Council website or the virtual environment (from an external or internal perspective). Types of testing that may be suitable are:
    - External with no credentials - emulating a hacker targeting the Council website or internet gateway;
    - Internal with no credentials - emulating a competent hacker with physical access; and
    - Internal with a standard network account – emulating a disgruntled employee.

Develop a policy on cryptography

- To achieve full alignment in the Cryptography section of the ISO 27001 Framework (A.10) Council is required to develop a policy on encryption and the lifecycle of cryptographic keys. This should include where encryption is required within Council (e.g. when backing up to tape), how it will be applied and how the keys will be managed throughout their lifecycle.

Quick Wins

Quick Win Details

Changes made at the organisational level may require longer periods of time to be embedded, however the following "quick wins" are some of the areas that can be more readily addressed to demonstrate progress in the short term:

Develop a top-level information security policy

- Council may consider developing a top-level information security policy stating Council's cyber security objectives alongside a statement of commitment which is signed off by the CE. This policy can be a simple 'one-pager' and is useful for communicating the message throughout Council to facilitate awareness. This is also suitable for publication on the Council website to instil confidence in the community.

Include a dedicated information security clause in the ICT usage agreement

- The ICT and IS Usage Agreement should be enhanced with a dedicated information security paragraph outlining the responsibilities of the end-user.

Include reiteration of confidentiality requirements during offboarding

- The offboarding process should include a step to reiterate the confidentiality requirements that still apply to the departing employee after leaving Council.

Council should document its access management processes in a procedure

- Council has an established access management process for permanent staff which should be documented in an access management procedure. This can be generalised for other areas of the business to support the access management policy once developed.

Update the existing password policy

- Council should update its password policy to reflect modern standards and ensure that systems are configured in alignment with the policy where possible. For applications not managed by ICT, the policy should be communicated to system owners in other areas of Council to confirm that their systems meet the defined requirements.

Enhance the acquisition plan template to consider security

- To facilitate the management of supplier-related information security risks, Council should amend the system acquisition plan template to include a step for identifying potential security risks early in the procurement phase.

Prohibit privileged users from conducting high-risk activities in policy (E8)

- Council should amend the ICT Device and System Access Operational Policy to prohibit privileged users from browsing the internet, downloading files from the internet and reading emails. This will promote Council to maturity level two for 'Restrict administrative privileges' control of the Essential Eight.

Block web advertisements in browsers (E8)

- Council should investigate methods of blocking web advertisements in browsers. Doing so will achieve a maturity level of two for the 'User application hardening' control of the Essential Eight. However, a risk assessment of the method used to do so should be conducted. For example, blocking web advertisements using a browser plugin may introduce other areas of risk.

Appendix A – Interviewees

The following personnel were interviewed as part of this project:

Name	Position
James Sinden	ICT Manager
Daniel Souter	ICT Team Leader
Niamh Milligan	Organisational Development Advisor

Appendix B - Document Control

Date	Version	Description of Modification	Modified by
29 September 2020	1.0	Initial Release	Scott Belcher
9 October, 2020	1.1	Updated following feedback from Council	Scott Belcher

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.5	Information security policies				
A.5.1	Management direction for information security	Control Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.			
A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties	There is a collection of policies and agreements which have a level of coverage over information security domains. Staff acknowledge policies during onboarding and agreements (e.g. ICT usage) with a signature. However, contractors do not acknowledge policies or agreements. There are two formal approval process for Council policies. Council policies are reviewed by the elected Council and posted on the public website, and organisational policies are reviewed by the CEO and published on the HillsHub intranet.	Partially Meets Requirements	AHC should develop a top level (one page) information security policy with Council's cyber security objectives and a statement of commitment signed off by the CEO. This policy will form Council's official stance on information security, and is appropriate for the public website. AHC should require contractors to sign-off on Council information security policies. The operational (i.e. not public-facing) information security policy suite could be expanded to include: • Access Management Policy • Network Security Policy • Cryptography Policy • Information Classification and Handling Policy • Mobile Device Policy • Remote Access and Teleworking • Supplier Management Policy
A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Policy review dates are included on each individual policy. Governance and Performance manage the overall policy framework, and policy owners monitor their policy review dates. Policies are reviewed on a 3 year cycle at a minimum.	Partially Meets Requirements	AHC should review its security-related policies annually at a minimum to maintain controls in alignment with the rapidly-changing security landscape.
A.6	Organisation of information security				
A.6.1	Internal organization	Control Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation.			
A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Council staff are informed of their confidentiality requirements during onboarding by HR. There are ICT agreements that require Council staff to acknowledge before being provisioned access and a device, this includes: • Information Services - Internet, Email & Equipment Usage Form • ICT Usage Agreement • ICT Personal Devices Agreement Contractors are not informed of their information security responsibilities. Nor do they sign the above agreements.	Partially Meets Requirements	The ICT and IS usage agreement should be enhanced to include a section or clause dedicated to information / cyber security.

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibilities shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	Appropriate segregation of duties was observed to be in place where it's applicable. Access is managed through a workflow process from Manager to OD to helpdesk. Policies cannot be published without approval from the CE. Informal change management processes are in place with the appropriate approvals. The ICT Manager approves any material change.	Meets Requirements	N/A
A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Council maintains contact with DPC WatchDesk who are contactable during an incident. The Data Breach Policy contains steps to contacts SA Police and other authorities.	Meets Requirements	N/A
A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Council subscribes to DPC WatchDesk who collate and send threat and vulnerability notifications from several sources (e.g. AusCERT). Two members of ICT including the Team Leader, ICT are members of AISA and regularly attend the local SecTalks meetings.	Meets Requirements	N/A
A.6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of project.	The IISIP Panel is made up of key representatives within Council. A business / project plan is presented to the panel who must approve it. Key ICT / security personnel (inc. Manager, Information Services) are present on the panel, who highlight information security risks if they are present.	Meets Requirements	N/A
A.6.2	Mobile devices and teleworking	Control Objective: To ensure the security of teleworking and use of mobile devices.			
A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	A mixture of BYOD and Council-issued devices are used. However, it was noted that these devices are simply a means to connect to the virtual environment where desktops are hosted. There is no dedicated mobile device policy that's in place, but there is a level of coverage in the personal devices agreement and the ICT Device & Systems Access Operational Policy. Newly provisioned devices have BitLocker enabled.	Partially Meets Requirements	Due to the prevalent use of mobile devices, Council should consider developing a dedicated mobile device policy encompassing requirements for the use of mobile devices, physical security, and protection of information on the devices. Existing controls such as endpoint encryption should also be worked into policy. Council should install BitLocker on all devices if possible, for complete coverage.

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Council's end-user workstations are in a virtual desktop infrastructure (VDI) environment, all of which use a standard operating environment (SOE). Both Council-issued devices and BYOD devices are used to authenticate to the VDI environment via VPN through Council's internet gateway using Council domain credentials. An MFA solution is being investigated. A 15 minute mandatory lock screen time out has been implemented.	Partially Meets Requirements	To fulfil the requirement of this control, Council should develop a remote access and teleworking policy to stipulate how teleworking must be performed (e.g. only use the VDI, do not download information locally, do not leave workstation unattended, etc). Council should prioritise the implementation of MFA to address the risk of malicious actors compromising Council systems remotely.
A.7	Human resource security				
A.7.1	Prior to employment	Control Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.			
A.7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	There is a formal recruitment process in the form of the criminal and relevant history screening procedure. Reference checks are performed and typically ask for a current supervisor or direct reporting line. Police checks are not performed across all positions, but rather based on the nature of the position, risk, and legislative requirements. Customer service officers and ICT staff are required to have police checks. These are validated every 3 years.	Meets Requirements	N/A
A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organisation's responsibilities for information security.	Employee contracts contain statements regarding code of conduct, NDA / confidentiality and intellectual property.	Meets Requirements	N/A
A.7.2	During employment	Control Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.			
A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Staff are walked through their employment contract and applicable policies and procedures during onboarding. This is part of the 3-hour corporate induction. These contents are reiterated as part of a 6 months review process, a managers checklist is maintained to ensure these requirements are reinforced. If there is a change of the code of conduct, staff are required to acknowledge by re-signing.	Partially Meets Requirements	Council should expand the security awareness program as per A.7.2.2.

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant to their job function.	Awareness training was recently performed on password security, and a wider education piece is being developed. Security is occasionally on the agenda at the all Council stand-up meeting. HillsHub has daily announcement which are leveraged to spread security awareness. Awareness material is typically tailored to applicable attacks targeting the sector or attempts on Council itself.	Partially Meets Requirements	Council should formalise an information security awareness program to cover several topics in addition to password security, including: • Information security at a high level and why it's important • Council's information and why its valuable • Examples of impact cyber attacks have had on other Councils • Social engineering, and why hackers are targeting people • Identifying and reporting security events / control weaknesses • Phishing awareness • Safe security practices Awareness of Council's information security policies should be worked into the training where applicable.
A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	A formal HR disciplinary process is in place in the form of the coaching and performance management policy and procedure which sets out how poor performance will be managed. Breach of policy or agreements (including security) will be addressed by this process.	Meets Requirements	N/A
A.7.3	Termination and change of	Control Objective: To protect the organization's interests as part of the process of changing or terminating employment			
A.7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee, or contractor and enforced.	Personnel requirements for confidentiality in regards to Council information are not reiterated during the offboarding process.	Requirements Not Met	Council should update the HR offboarding procedure to include a step to reiterate the individuals confidentiality requirements (as signed during onboarding).
A.8	Asset management				
A.8.1	Responsibility for assets	Control Objective: To identify organisational assets and defined appropriate protection responsibilities.			
A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	An inventory of IT assets is maintained. The Helpdesk ticketing system has an asset management module. IT assets are tagged by make, model and service tag or serial number. The asset register is not formally reviewed. However, when IT staff visit Council premises, assets are checked to confirm they're being managed in alignment with the asset register.	Partially Meets Requirements	Council should consider developing a higher-level asset register which identifies key processes, information and systems managed by Council. These assets should then be classified by their confidentiality, integrity and availability requirements. The purpose of this is to maintain a visualisation of what information assets Council has, and what level of protection / controls they require. Council should conduct a due diligence review of the IT asset register annually at minimum.
A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	All devices have an assigned site and owner. Users acknowledge ownership of assets via the ICT agreement during the HR process. The onboarding process also records all items given to the employee (including access fobs).	Meets Requirements	N/A

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented, and implemented.	The ICT Device and Systems Access Operational Policy, supplemented by the ICT Usage Agreement have sufficient coverage over acceptable use.	Meets Requirements	N/A
A.8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Council IT equipment is leased, and thus is returned on a 3 year cycle which is tracked by the vendor. The HR exit process includes the retrieval of all assets (e.g. laptop, device, fobs etc) provisioned to the employee - as recorded during onboarding. It was noted that as contractors are not onboarded via the standard HR processes, the return of their assets is managed informally by the responsible business owner.	Partially Meets Requirements	Council should ensure the provision of assets to contractors is performed via the controlled HR process to ensure assets are retrieved during offboarding.
A.8.2	Information classification	Control Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation.			
A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification.	Council does not have a formal information classification scheme. 'CONFIDENTIAL' labels exist and are applied as necessary, however, there is no defined criteria for what constitutes CONFIDENTIAL information.	Partially Meets Requirements	An information classification scheme should be defined that is appropriate for the sensitivity of information processed and stored by Council (e.g. Public, Internal, Restricted). Criteria for Council's existing CONFIDENTIAL category should be defined and worked into the scheme. These classifications can then drive the implementation of information security controls (both process and technical).
A.8.2.2	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	The CONFIDENTIAL label is applied when directed by the ELT.	Partially Meets Requirements	Once the information classification scheme is developed, Council should develop a supporting procedure for labelling information in various scenarios (e.g. in documents, folders, printed, etc.)
A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Almost all information received by Council (except by email) is routed through the records team who have procedures for handling information when it is received. However, these procedures are limited to this specific unit and not for all staff.	Partially Meets Requirements	Once the information classification scheme is developed, Council should develop a supporting procedure for the handling of different types of information in various scenarios (e.g. Restricted must be encrypted while in transit).
A.8.3	Media handling	Control Objective: To prevent unauthorised disclosure, modification, removal or destruction of information on media			
A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	No procedures are defined for the management of removable media. However, due to the use of virtualisation and cloud applications, removable media are seldom used. The Library Information Kiosks has no write to USBs.	Requirements Not Met	Council should develop procedures for the handling of removable media if it deems necessary.

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	• As media is leased, it is wiped before being returned to vendors. • For servers, specialist vendors are engaged to do secure wipes. • The default OS wipe and factory default reset is used for laptops, as they do not retain data due to virtualisation.	Meets Requirements	N/A
A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse, or corruption during transportation.	It was noted that media containing Council information are seldom used and as such, are rarely transferred. Provisioned laptops have BitLocker end-point encryption enabled.	Meets Requirements	N/A
A.9	Access control				
A.9.1	Business requirements of access control	Control Objective: To limit access to information and information processing facilities			
A.9.1.1	Access control policy	An access policy shall be established, documented and reviewed based on business and information security requirements.	Although processes are in place an access management policy has not been developed. As there are areas of Council where certain access (e.g. to cloud applications) is managed outside of the established processes (i.e. without OD and ICT oversight), an access management policy would help Council manage the associated risks. For most Council business applications, baseline AHC access is required to have further access to business systems.	Requirements Not Met	Council should document its requirements for Council-wide access management in a policy, and implement supporting measures to ensure the policy is understood and followed.
A.9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use	The New Starter form identifies what access the new user requires. This access is then configured via groups maintained by ICT for VDI, network shares, O365, etc. Initial access requests are vetted by OD and then ICT before being configured.	Meets Requirements	N/A
A.9.2	User access management	Control Objective: To ensure authorized user access and to prevent unauthorized access to systems and services			
A.9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	For initial access, People Leaders fill out a New Staff form for OD (HR) to approve. Once approved, OD populate a SharePoint form which is then sent to Helpdesk to be configured. Helpdesk then vet the request to some extent before access is configured (i.e. any concerns are followed up with the People Leader). For deprovisioning, People Leader's notify OD that access is to be removed which is then sent to ICT for action. OD and ICT are not always notified of contractors who are provisioned with access (e.g. to cloud systems), and as such are not managed under the controlled process.	Partially Meets Requirements	Council should mandate (with policy and supporting controls, awareness) that all areas of Council (including management of contractors) follow the established access management process.

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Once the SharePoint form is delivered to ICT from OD, the ticketing system has workflows that control the access provisioning / deprovisioning process. ICT have scripts that both provision and revoke access automatically (with data from the SharePoint from). However, some systems require access to be configured and removed manually.	Partially Meets Requirements	Council should document access provision, review and deprovisioning of access in a formal access management procedure.
A.9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Privileged access for Council staff is managed as per the above process. Key actions of privileged users (e.g. authentication attempts) are caputred in the Splunk logs which are then shown in a dashboard that is viewed regularly. There are certain ICT contractors that retain privileged access rights. However, no generic privileged accounts are in use (i.e. third parties have to nominate individuals). Time-based access for privileged users is not implemented. Privileged user access is not reviewed in the traditional sense (e.g. reviewing a register of privileged users). However, a monthly 'AD account modification' report is generated which automatically highlights key changes to access which is reviewed every ICT monthly meeting. Privileged users have standard privileged accounts for day to day use. Privileged accounts have the same password requirements and are not restricted from high-risk activities (e.g. browsing the internet, opening email links, etc).	Partially Meets Requirements	Council should consider restricting privileged users accounts from conducting high-risk activities such as browsing the internet and accessing emails. This can be in the form of policy, supported by technical restrictions. This recommendation also relates to maturity level three for the 'Restrict admin privileges' control within the Essential Eight. Council should consider enhancing privileged account password requirements beyond that of standard user accounts. Council should conduct reviews of privileged user activity logs if feasible.
A.9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	A user's password is sent to their People Leader via email and is configured to change upon first login. A standard password is used for all initial passwords.	Partially Meets Requirements	Although the standard initial passwords are configured to be changed on first login, a randomised password should be used to mitigate possible hijacking of a user's account before they're able to login. Further, Council should investigate options to provide a user's account directly to them (e.g. in person or by phone) to ensure accountability - as currently, People Leaders have access to accounts that do not belong to them for a short period of time.
A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	As mentioned in A.9.2.3, the AD account modification report is reviewed at each ICT monthly meeting.	Partially Meets Requirements	As ICT do not manage access for all Council business applications, a process needs to be established by Council whereby access reviews are performed by system owners periodically.

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	The OD offboarding checklist includes a step to notify ICT of access to be removed. As mentioned, contractors may not be covered by the offboarding processes, and may retain unnecessary access. If instant dismissal, ICT is notified directly either in person or via phone. Access may be suspended when there is an allegation or ongoing investigation.	Partially Meets Requirements	As mentioned, Council should incorporate all contractors into the formal access management processes.
A.9.3	User responsibilities	Control Objective: To make users accountable for safeguarding their authentication information.			
A.9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	The ICT Team Leader recently conducted stand up training on the importance of password security. An outdated password policy is published which requires updating.	Partially Meets Requirements	Council should update the password policy to current standards and ensure systems are configured accordingly.
A.9.4	System and application access control	Control Objective: To prevent unauthorised access to systems and applications			
A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Although a policy is not implemented, access is restricted and controlled when managed by ICT (as per A.9.2). However, without an access management policy it is difficult to enforce proper access management across Council.	Partially Meets Requirements	As per A.9.2.2, the established access management process should cover access to all Council systems. The most appropriate way to enforce this may be to develop and socialise an access management policy.
A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be led by a secure log-on procedure.	Staff authenticate to systems with a set of credentials. AD integration is configured for business applications where available and appropriate. An MFA solution is being investigated and will be applied to remote access.	Meets Requirements	N/A
A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.	Systems that aren't integrated with AD cannot be configured by ICT in alignment with the password standards. Passwords currently reset every 90 days, users are able to reset at any-time via self-service (Ctrl, Alt, Delete). Users are able to reset their passwords via helpdesk using the internal or external phone number.	Partially Meets Requirements	Once the password policy is updated, a Council-wide task should be carried out to ensure all systems (managed by ICT or otherwise) are configured in alignment with the policy, and any exceptions documented. Council should investigate alternatives or compensating controls for conducting password resets over the phone. The helpdesk operator should be able to positively identify the person on the phone, or provide the password via a separate means (e.g. a follow-up phone call).
A.9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application standards shall be restricted and tightly led.	Local administrator privileges are disabled by default. Privileged accounts must be used to install software, even for ICT administrators. Privileged accounts capable of installing software are only used when needed (e.g. a separate standard account is used for day-to-day activities).	Meets Requirements	N/A
A.9.4.5	Access control to program source code	Access to program source code shall be restricted.	No source code is maintained by Council.	N/A	N/A

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.10	Cryptography				
A.10.1	Cryptographic controls	Control Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.			
A.10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic standards for protection of information shall be developed and implemented.	A policy on the use of cryptography within Council is not in place. The following were some identified uses of encryption within Council: • VPN is used for remote access. • Backups are encrypted by Veeam. • Encryption for web applications Kemp Load Balancer / Reverse Proxy which, allowed ciphers are limited to a best practices subset.	Requirements Not Met	To fulfil the requirement of this control, Council must document a cryptography policy which stipulates where encryption will be applied and how it will be managed within Council.
A.10.1.2	Key management	A policy on the use, protection, and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	KeyPass is used to store and manage cryptographic keys. An SSL key was sighted.	Requirements Not Met	To fulfil the requirement of this control, Council must document a cryptographic key management policy or procedure, specifying how cryptographic keys will be managed throughout their lifecycle, including: • Generation • Registration • Storage • Distribution / installation • Use • Rotation • Backup • Recovery • Revocation • Suspension / Destruction / Deletion / Termination • Logging and auditing
A.11	Physical and environmental security				
A.11.1	Secure areas	Control Objective: To prevent unauthorized physical access, damage, and interference to the organization's information and information-processing facilities			
A.11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information-processing facilities.	Physical security to Council's Stirling premises is controlled with limited points of entry which require a fob for access.	Meets Requirements	N/A
A.11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry standards to ensure that only authorized personnel are allowed access.	A fob is required to access the Council premises via the perimeter. There is a door from the Stirling library to the Council premises that also requires fob access, and the fob reader is concealed behind padding in the wall for added measure. Doors within the perimeter are unlocked during business hours but require fob access after hours. Visitors report to the library front desk where they are required to sign in using the tablet application which prints a badge with the visitor's picture on it.	Meets Requirements	N/A

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms, and facilities shall be designed and applied.	The only secure zone within the security perimeter is the server room, which requires fob access that is limited to a certain number of people. This access system also has logging functionality. The server room contains no windows and would not be recognisable as a sensitive location to an outsider.	Meets Requirements	N/A
A.11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack, or accidents shall be designed and applied.	Several fire extinguishers were observed around the Council premises. The server room has as HVAC system with under-floor cooling and a standard air-conditioning unit as a backup. The servers and network infrastructure are protected by a UPS.	Meets Requirements	N/A
A.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	The server room locks automatically when not occupied. Vendors coming on-site to perform maintenance are escorted and supervised while in the server room.	Meets Requirements	N/A
A.11.1.6	Delivery and loading areas	Access points such as delivery and loading areas, and other points where unauthorized persons could enter the premises, shall be led and, if possible, isolated from information processing facilities to avoid unauthorized access.	Deliveries are managed via the front desk in the library, the person having the package delivered is phone by the front desk person to come and collect. For larger deliveries the delivery person is escorted by a staff member to where the package needs to be delivered. Council has no dedicated loading areas as it is not required.	Meets Requirements	N/A
A.11.2	Equipment	Control Objective: To prevent loss, damage, theft, or compromise of assets and interruption to the organization’s operations.			
A.11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Servers and network infrastructure are located in the Stirling server room at the Stirling office with redundancy at AdamDC. Access to the Stirling server room is restricted to a few individuals, the room is located deep within the security perimeter and is not identifiable from the outside of the building. Printers are placed in appropriate locations within the security perimeter.	Meets Requirements	N/A
A.11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	A UPS and HVAC system (under floor cooling) supports the on-site infrastructure. This equipment is leased and maintained by the vendor.	Meets Requirements	N/A

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage.	Cabling was observed to be neat and concealed throughout the premises and within the server room.	Meets Requirements	N/A
A.11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Supporting equipment is covered under maintenance contracts, with the UPS and HVAC system undergoing checks / maintenance monthly. Servers and core infrastructure are leased and maintenance is performed by the vendor every six months.	Meets Requirements	N/A
A.11.2.5	Removal of assets	Equipment, information, or software shall not be taken off-site without prior authorization.	An established process is in place for when equipment is required to be taken off-site by the vendor. However, this is seldom used as vendor personnel come on-site and work with Council staff. Staff were recently authorised to take devices off-site due to COVID-19.	Meets Requirements	N/A
A.11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets, taking into account the different risks of working outside the organization's premises.	BitLocker is implemented on all new Council-provisioned devices. ICT agreements and policy also facilitate the security of assets taken offsite.	Meets Requirements	N/A
A.11.2.7	Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Disposal of equipment is handled in conjunction with vendors under the respective lease agreements. All equipment is leased.	Meets Requirements	N/A
A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Automatic lockout has been configured for systems after 15 minutes of inactivity.	Partially Meets Requirements	Although automatic lockout has been configured, Council should conduct awareness training that includes the locking of workstations while away - staff can also be informed of the Windows + L shortcut. Several staff workstations were observed to be unlocked and unattended while the audit was being conducted on-site.
A.11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	There is no formal clear desk / clear screen policy. Follow-me printing is used.	Partially Meets Requirements	To support A.11.2.8, a clear desk and clear screen policy must be documented to outline rules for locking workstations and clearing desks of sensitive information. This policy can be embedded in an existing one (e.g. acceptable use, once developed).
A.12	Operations security				
A.12.1	Operational procedures and	Control Objective: To ensure correct and secure operations of information-processing facilities			

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	Network Documentation' ICT SharePoint site has tracking spreadsheets to ensure tasks are being performed appropriately. It was noted that in ICT, there is a heavy emphasis on training. However, procedures are developed as needed (e.g. a procedure for updating SSL certificates was developed due to the complexity of the task). An operational procedure exists for performing backups. Other areas of Council (e.g. customer service) have several documented procedures for information processing, largely due to staff / volunteer intake and outgoing staff.	Meets Requirements	N/A
A.12.1.2	Change management	Changes to the organization, business processes, information-processing facilities, and systems that affect information security shall be controlled.	A SharePoint list is maintained to log notable ICT changes. Segregation of duties is in place, with a two phase approval process for notable changes. For more incidental changes, an assessment of impact is made by the ICT Team Leader who seeks informal (i.e. verbal) approval from the ICT Manager. All staff notifications are used to notify Council of changes that may result in outages. Backout plans are implemented for potentially impactful changes. ICT procurement milestones also restrict changes and control major system changes. Each virtual machine image has its own change log (i.e. logs of each changes to virtual desktops which can be rolled back).	Partially Meets Requirements	Council should formally document its change management process. Criteria for change tiers (e.g. major, minor, incidental) should also be defined and change controls applied commensurate with the category of change. This should include not only changes to IT, but also changes to business processes to ensure information security risks arising for process changes are appropriately managed.
A.12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	The Site24x7 dashboard is used to monitor server load and storage capacity. When procuring infrastructure and storage under the standard 3 year agreement cycle - a capacity prediction is made as to what storage / bandwidth will be required over the period. Reserve storage is kept just in case. Infrastructure is configured to simply add more storage drives if required.	Meets Requirements	N/A

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Entirely different VMs are used for testing. Different test environments are also maintained for key Council systems. Security controls for test environments are effectively the same both from a technical perspective (e.g. same group policies, logging) and at a process level (e.g. access management).	Meets Requirements	N/A
A.12.2	Protection from malware	Control Objective: To ensure that information and information processing facilities are protected against malware			
A.12.2.1	Controls against malware	Detection, prevention, and recovery standards to protect against malware shall be implemented, combined with appropriate user awareness.	EDR/AV solution Carbon Black is implemented on workstations and servers. Alerting is set up for the IT team when an alert is raised on a local workstation. Implementation of application whitelisting is starting imminently. Staff are made aware of trending or targeted attacks (against Councils) which are identified by DPC WatchDesk or by the ICT Team Leader (i.e. via news sources, twitter). No penetration testing or vulnerability scanning has been conducted for several years. A Fortigate Firewall is implemented that has a level of IDS/IPS functionality.	Partially Meets Requirements	Council should conduct a penetration test from an internal and external perspective to verify that security controls are operating effectively.
A.12.3	Backup	Control Objective: To protect against loss of data			
A.12.3.1	Information backup	Backup copies of information, software, and system images shall be taken and tested regularly in accordance with an agreed backup policy.	SharePoint is configured for backups every three hours and monthly off-site backups to tape. Storage-level snapshots (SAN) are taken twice per day and kept on-site for a week before moving to tape. Tapes are stored offsite at AdamDC. Partial restores are tested, and full restores of entire VMs are tested and working. Change backout plans use VM snapshots rather than the backup system.	Meets Requirements	N/A
A.12.4	Logging and monitoring	Control Objective: To record events and generate evidence			

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept, and regularly reviewed.	ACSC event logging recommendations have been worked into Group Policy and pushed out to all workstations. Centralised logging of key actions (e.g. authentication attempts, password fails, account creations) is provided via the SplunkLite dashboard. This dashboard is monitored throughout the day. Email alerts to the IT team are set up for suspicious actions. Network logging can be used to investigate whether connections are being made to malicious IPs (as notified by DPC). Monitoring is in place for network switches, when there is a configuration change on a switch, LibreNMS creates a new version of the config which can be used to identify discrepancies. Carbon Black also has robust logging for all types of events which is searchable.	Meets Requirements	N/A
A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Windows event logs cannot be modified by standard users. Splunk Greylog and NMS are protected by authentication. Logs are also captured in tape backups which are then stored off-site. Log retention periods vary based on system. Privileged users are able to edit log files. However, this action would generate an alert and a separate log entry which appears in SplunkLite.	Meets Requirements	N/A
A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Privileged account activity is logged. Although these logs are not reviewed, key actions are captured in the SplunkLite dashboard which is reviewed constantly.	Meets Requirements	N/A
A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Group Policy points all devices and VMs back to a single domain controller as the time source.	Meets Requirements	N/A
A.12.5	Control of operational software	Control Objective: To ensure the integrity of operational systems			

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Local administrator privileges are disabled by default to prohibit staff from installing software. There is an IT helpdesk process for users to request software installation. An approved software list is maintained (where there are limited licences). Unique software requires a business case and must be approved by the ICT Manager and IISIP panel before being installed.	Meets Requirements	N/A
A.12.6	Technical vulnerability management	Control Objective: To prevent exploitation of technical vulnerabilities			
A.12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.	DPC WatchDesk consolidates several notification sources including AusCERT. Two key individuals from IT including the Team leader are subscribed to DPC WatchDesk as well as RSS Feeds to stay informed of vulnerabilities. Once identified - vulnerabilities are discussed as a team, the applicability and severity is determined. Patches are applied commensurate with risk. If an outage is required, the Council is notified. Generally operating systems are patched within 48 hours. Network devices are patched after hours. Certain patches (e.g. registry changes) can be pushed out immediately.	Partially Meets Requirements	Council should consider documenting a patch management framework / procedure with different levels of criticality (e.g. low, moderate, critical). Criteria for each level of criticality should be defined, and a target timeframe attached to each level (e.g. 48 hours for critical, one week for moderate, etc.)
A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	The Information Services Internet, Email & Equipment usage form outlines the rule around installing software (prohibited unless explicitly approved by ICT).	Meets Requirements	N/A
A.12.7	Information systems audit considerations	Control Objective: to minimise the impact of audit activities on operational systems			
A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	Patches / updates that may result in an outage are communicated to Council. Council activities are reviewed to ensure there are no auspicious events that may be affected. There are legislative requirements that Council must ensure required systems are available within 48 hours of a meeting involving an elected member. Testing and updates are performed out of hours if required. Staff are able to object to notification outages, but a genuine business reason is required - which is then compared against the criticality of the patch.	Meets Requirements	N/A
A.13	Communications security				
A.13.1	Network security management	Control Objective: To ensure the protection of information in networks and its supporting information processing facilities.			

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications.	A VPN is used for remote users to access the Council environment. A fortigate firewall is implemented that includes IDS/IPS functionality and a level of AV and anti-spam mechanisms. Network diagrams are maintained. Switches act as routers between networks with rules that restrict access (i.e. segregation). Robust network logging is in place as per A.12.4.1.	Meets Requirements	N/A
A.13.1.2	Security of network services	Security mechanisms, service levels, and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Networks are managed by the Council (i.e. there is no external network provider). However, contractors are engaged to assist when required. There is no network documentation that defines what security mechanisms must be implemented on Council networks.	Partially Meets Requirements	Council should identify the security mechanisms and service levels that must be implemented on Council networks, and have them formally documented. This could be in the form of a network security policy.
A.13.1.3	Segregation in networks	Groups of information services, users, and information systems shall be segregated on networks.	Wireless access points are not segregated from Council network. However, they require AD authentication for devices to connect, so segregation (e.g. on a separate subnet / vlan) is not as relevant. Council networks are segregated from the Stirling library (managed by PLS), and a segmentation project is underway to further segment the Council network.	Meets Requirements	N/A
A.13.2	Information transfer	Control Objective: To maintain the security of information transferred within an organization and with any external entity			
A.13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures, and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Rules for information transfer have not been documented in policy or procedure. A secure file transfer solution is in place but only for limited use (i.e. not available for all of Council).	Requirements Not Met	Council should develop an information transfer policy and procedure in alignment with an information classification scheme as per A.8.2. Council should identify what information is transferred externally on a regular basis and apply security controls commensurate with the sensitivity of that information. An information transfer procedure can be in the form of a spreadsheet that includes the Council business unit, the information being transmitted, the direction (inward/outward/both), the entity with whom the information is being exchanged, method of transmission, frequency and the controls in place to protect the transmission (e.g. encryption), and whether or not a transfer agreement is in place (as per A.13.2.2). Council should make the secure file transfer solution available to all Council staff, and enforce its use where appropriate (e.g. for transferring CONFIDENTIAL information).

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	As per A.13.2.1, no formal rules are established for information transfer and as such, agreements with external parties for information transfer have not been established. Exfiltration by vendors is fairly uncommon. Council's records unit classifies incoming information as CONFIDENTIAL if required. The records unit processes all information coming inward to Council through formal channels.	Partially Meets Requirements	As per A.13.2.1, Council should identify the external parties it exchanges communication with and establish agreements outlining how that information will be transferred.
A.13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Skype for Business instant messaging is used within Council. These messages are encrypted using strong ciphers.	Meets Requirements	N/A
A.13.2.4	Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed, and documented.	As per A.7.1.2, employee contracts contain statements regarding code of conduct, NDA / confidentiality and intellectual property.	Meets Requirements	N/A
A.14	System acquisition, development and maintenance				
A.14.1	Security requirements of information systems	Control Objective: To ensure that information security is an integral part of information systems across the entire lifecycle; this also includes the requirements for information systems that provide services over public networks.			
A.14.1.1	Information security requirements analysis and specification	The information-security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	The IISIP panel identifies security requirements when new information systems are being procured / implemented. This includes backup retention requirements and other security requirements.	Partially Meets Requirements	Council could enhance the acquisition plan template to include a requirement for identifying security requirements. That way, the ISIP panel can vet / confirm security requirements rather than help define them.
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.	CRM FormStack forms (which the public use to submit information to Council) uses TLS encryption. The forms are managed by a third party, and Council uses an API call to retrieve the data which is also transmitted with TLS encryption.	Meets Requirements	N/A
A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or replay.	eCommerce functions / transactions on Council websites use a NAB processing portal (iFrame within the website). As such, AHC does not receive any cardholder data.	Meets Requirements	N/A
A.14.2	Security in development and	Control Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems			

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	Council does not perform software development, nor is development outsourced.	N/A	N/A
A.14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be led by the use of formal change procedures.	This control refers to change control during software development, for general change management refer to A.12.1.2.	N/A	This control refers to change control during software development, for general change management refer to A.12.1.2.
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Business applications are tested on test VMs when operating system changes are made. Any issues are fixed before the OS update are deployed to production VMs.	Meets Requirements	N/A
A.14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.	Modifications to standard software packages are never performed. If this were to be done, a specialist third party would be engaged.	Meets Requirements	N/A
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained, and applied to any information system implementation efforts.	Council does not perform software development, nor is development outsourced.	N/A	N/A
A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Council does not perform software development, nor is development outsourced.	N/A	N/A
A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	Council does not perform software development, nor is development outsourced.	N/A	N/A
A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.	No penetration testing is performed. Security configurations are tested for functionality, for example - separate internet connection is in place to verify firewall rules.	Partially Meets Requirements	Council should conduct penetration testing on key systems (whether internal or externally facing) to gain independent assurance of security control effectiveness.
A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades, and new versions.	Acceptance testing of the security requirements identified (e.g. by the ISIP) during planning are not tested.	Requirements Not Met	Council should ensure that security requirements identified during the planning phases of system procurement are tested throughout the procurement / deployment process.
A.14.3	Test data	Control Objective: To ensure the protection of data for testing			

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.14.3.1	Protection of test data	Test data shall be selected carefully, protected, and controlled.	Stale production data is used for testing within Council. Security controls are identical for testing environments / VMs. Contractors are given production data for testing which is then kept on their systems, with no control or oversight of Council.	Partially Meets Requirements	Council should consider masking the data it uses for testing. Council should refrain from providing suppliers with Council data sets for testing unless absolutely necessary.
A.15	Supplier relationships				
A.15.1	Information security in supplier	Control Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.			
A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed upon with the supplier and documented.	A policy for managing supplier-related information security risks has not been established, and no formal consideration given to information security requirements of suppliers. There is a level of supplier management through IISIP panel, and business units cannot procure cloud software without signoff by ICT Manager as the budget holder. Procurements (>$10K) must be managed in alignment with procurement process. There is a procurement officer that coordinates with the majority of suppliers. However, this person does not manage all engagements.	Partially Meets Requirements	Council should establish a policy for managing suppliers with respect to information security, and communicate it across Council. Management of information security should be embedded within the supplier management lifecycle, from specifying initial requirements, including those requirements in contracts, and receiving ongoing attestations from suppliers. Contractors gaining access to Council systems should be covered under the standard HR onboarding and offboarding processes to ensure their access and provisioned assets are managed as per the established processes. The procurement officer could be useful in implementing these supplier management practices. This person could be provided with an information security checklist that can be referred to when engaging with a new supplier.
A.15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed upon with each supplier that may access, process, store, communicate, or provide IT infrastructure components for the organization's information.	Information security requirements are not worked into supplier contracts by default. Confidentiality clauses exist in certain procurements templates, but not all.	Partially Meets Requirements	Council should ensure that the identified security requirements relating to each supplier are formally documented in contracts and agreements with those suppliers. Suppliers accessing Council systems and information should be subject to the relevant ICT and IS usage agreements. Council should adjust its procurement templates to ensure the confidentiality clause is worked into all templates, regardless of the size of the engagement.
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Information security risks associated with the supply chain are not considered by default.	Requirements Not Met	Council should work clauses into their contracts and agreements stating that the imposed requirements also apply to subcontractors and the supply chain. Or where possible, prohibit the use of subcontractors all together.
A.15.2	Supplier service delivery management	Control Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.			

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review, and audit supplier service delivery.	A list of software suppliers is maintained by the ICT Manager. Council suppliers are also registered in the finance system. ICT have regular meetings with their suppliers and contractors.	Partially Meets Requirements	Council should ensure (e.g. through policy / procedure) that supplier / contractor services across Council are monitored on an ongoing basis.
A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures, and standards , shall be managed, taking account of the criticality of business information, systems, and processes involved and re-assessment of risks.	ICT suppliers inform Council when there are any material changes to their service or terms and conditions. Such changes are discussed ad-hoc or at the regular meetings.	Partially Meets Requirements	As per A.15.2.1, Council should ensure that changes to supplier services that may impact Council's information security are communicated and accepted by Council. This can be imposed in the supplier using agreements.
A.16	Information security incident management				
A.16.1	Management of information security incidents and improvements	Control Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.			
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.	The data breach response procedure was developed following an incident. However, a wholistic information security incident response plan is not documented. The Data Breach Response Team / Committee is formed to manage incidents. External communications are managed by the CE as required. Specialist third parties are engaged on a case by case basis.	Partially Meets Requirements	The data breach response procedure should be updated to have a table outlining the roles and responsibilities of all parties (e.g. CE handles communication, ICT Team Leader drives technical response, etc). The data breach response plan should be enhanced to cover all types of information security incidents (e.g. ransomware, denial of service, website defacement, etc). Due to the sensitivity of digital forensics (e.g. from a legal perspective), Council should have a contact with a third party digital forensics specialist readily available.
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	WatchDesk notify Council of suspicious behaviour and indicators of compromise. Awareness training for staff to help them identify information security events has not been performed. Although ad-hoc email awareness of trending threats is communicated.	Partially Meets Requirements	Council should conduct awareness training for users to help them identify information security events (e.g. phishing emails, suspicious behaviour on systems, etc). This training should include the methods by which to report security events.
A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization’s information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	It was noted that unusual behaviour of systems are sometimes reported. However, staff have not been trained to identify and report security control weaknesses.	Partially Meets Requirements	Similarly with A.16.1.2, Council staff should be trained to identify security control weaknesses. These aren't security events, but more-so when an established security control is not functioning (e.g. authentication mechanisms not engaging, a secure process not being followed, etc).

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Reported events are assessed by ICT to determine if they're incidents. The data breach response procedure includes an step for evaluating the severity of events / incidents.	Meets Requirements	N/A
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	The data breach response procedure outlines the process for managing security incidents.	Meets Requirements	N/A
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	The "Prevent future breaches" guides the response team to determine what actions are required to ensure incidents do not reoccur.	Meets Requirements	N/A
A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.	The data breach response plan does not contain a process for collecting evidence. Contact with digital forensics experts is not maintained.	Requirements Not Met	Council should enhance the data breach response procedure to include a process for collecting digital evidence. Due to the sensitivity of this process (i.e. legal requirements around chain of custody), it is recommended that this process be performed by digital forensics specialists.
A.17	Business continuity management				
A.17.1	Information security continuity	Control Objective: Information security continuity shall be embedded in the organization’s business continuity management systems			
A.17.1.1	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	The strategic internal audit plan includes a component for ensuring BCPs accurately address business requirements. Business impact assessments identifying recovery requirements (e.g. Recovery Time Objective, Recovery Point Objective) for key Council systems have not been performed. However, it was noted that Councils DR capabilities (as documented under A.17.2.1) are robust, and would likely meet these recovery requirements.	Partially Meets Requirements	Council should perform a business impact assessment for key systems across Council to determine whether the current DR arrangement meets the business requirements.
A.17.1.2	Implementing information security continuity	The organization shall establish, document, implement, and maintain processes, procedures and standards to ensure the required level of continuity for information security during an adverse situation.	All Council laptops all have SIM cards and as such, do not need to connect to any wireless networks (including in their own home). In a BCP scenario where staff are required to work remotely, they connect to the VDI environment using the VMWare horizon client which is an encrypted session.	Meets Requirements	N/A
A.17.1.3	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity standards at regular intervals in order to ensure that they are valid and effective during adverse situations.	Council do not conduct tests of their BCP. However, the working from home arrangement during the COVID-19 pandemic provided assurance that information security controls implemented for BCP scenarios operate effectively.	Partially Meets Requirements	Council should consider conducting a BCP test (simulated or desktop scenario) to verify that the response process and information security controls are effective.

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.17.2	Redundancies	Control Objective: To ensure availability of information processing facilities.			
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Council has redundancy between two datacentres (at different geographical locations) connected by a 10GB dark fibre link. Each technology refresh (roughly every 3 years), DR capabilities are assessed and upgraded as necessary. Load is spread across both datacentres (i.e. staff may connect to their virtual desktops at either location). DR capabilities may be undermined by a Telco outage, a plan is in place to remove Fusion Broadband as a single point of failure.	Partially Meets Requirements	Council should investigate options to have a redundant telecommunications provider to help ensure that DR capabilities are not undermined by an service provider outage.
A.18	Compliance				
A.18.1	Compliance with legal and contractual requirements	Control Objective: Information security continuity shall be embedded in the organization's business continuity management systems			
A.18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements, and the organization's approach to meet these requirements shall be explicitly identified, documented, and kept up to date for each information system and the organization.	The strategic internal audit plan contains a Legislative and Regulatory Compliance component to identify and assess Council compliance with applicable legislation. Council tracks their PCI DSS compliance in conjunction with NAB, and populates a self-assessment questionnaire as required. Although not subject to it, consideration has been given to the Notifiable Data Breaches amendment to the Privacy Act, and Council may report accordingly if necessary. Council's governance area manages legal arrangements with an outsourced provider (i.e. no internal legal team).	Meets Requirements	N/A
A.18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products.	The ICT Manager maintains a software register to manage licences. There is a list of approved software, and requests for software outside of this list require a valid business case. The IS agreement states that staff cannot procure software without approval from ICT. Technical controls are in place to prevent users from installing unapproved (e.g. pirated) software. Staff contracts have clauses relating to intellectual property rights.	Meets Requirements	N/A

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access, and unauthorized release in accordance with legislatory, regulatory, contractual, and business requirements.	Council has a dedicated information management team who have formal processes developed in accordance with the State Records Act 1997. The records management system is configured with the legislated disposal schedules. Council retains digital and hard copy records. Physical records are scanned and stored within the records system hosted in the data centre. Records are protected by the DR arrangement and are also backed up to tape and stored at multiple sites.	Meets Requirements	N/A
A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	It was noted that the Notifiable Data Breaches scheme does not apply to Councils. The data breach response procedure includes consideration for reporting breaches of personally identifiable information. There is no nominated privacy officer. No privacy impact assessments have been performed.	Meets Requirements	Although Council meets its privacy requirements in line with legislation, consideration should be given to conducting an assessment of Council practices against the Australian Privacy Principles. Council may nominate an existing staff member to be a privacy officer for Council to ensure that these principles are being adhered to.
A.18.1.5	Regulation of cryptographic controls	Cryptographic standards shall be used in compliance with all relevant agreements, legislation and regulations.	Council applies encryption in line with legislation, and does not export any encryption hardware or software overseas.	Meets Requirements	N/A
A.18.2	Information security reviews	Control Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures			
A.18.2.1	Independent review of information security	The organization’s approach to managing information security and its implementation (e.g. Control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	This cyber security audit constitutes an independent assessment. The previous security audit was undertaken in 2015. Governance area undertakes a series of audits including financial which includes security related areas like access management.	Partially Meets Requirements	Council should look to conduct independent security assessments periodically. This could be technical (e.g. penetration testing) or non-technical (process reviews). The assessor must be independent of control design or operation, as such, third parties as well as independent internal personnel can be used for these reviews.
A.18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements.	Managers / People Leaders do not conduct reviews of their areas of responsibility for compliance with information security policies.	Requirements Not Met	Council should train its Managers / People Leaders to observe the operations in their area to ensure information security policies and procedures are being followed.

Control	Section	Control Detail	Findings	Assessment	Recommendation
A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.	The ICT Team Leader performs scans (nmap) from time to time to ensure security controls are applied correctly, and has the appropriate competence to do so. This is usually performed when a vulnerability arises.	Partially Meets Requirements	Council should consider conducting active penetration testing on its systems to determine the potential impacts of vulnerabilities being exploited.

Appendix D - Essential Eight Control Assessment

Control Area	Findings	Current Level	Target Level	Average Level	Recommendation For Level 2	Recommendation For Level 3
Application control	An application control solution was not implemented at the time of assessment. However, the AirLock Digital application control/whitelisting solution has been purchased. Discussions indicated that this solution is capable of achieving a maturity level of 3, but an assessment needs to be made as to whether implementing all of Microsoft latest recommended block rules (e.g. specific DLLs) will cause operational impacts. The Airlock solution will achieve a maturity level of 2 once implemented.	0	2	0.6	Once the Airlock application is switched to enforce mode (i.e. after adequate auditing and planning), Council will achieve a maturity level of 2 for this control.	To achieve a maturity level of 3 in this control, Council must implement Microsoft's recommended block rules, however, this may have a negative impact on Council business operation. As such, it is recommended that the feasibility of this application control function against current business practices is assessed before this option is enabled. However, ICT will explore whether implementing Microsoft's recommended block rules will cause operational impacts. If not, a maturity level 3 can be obtained.
Patch applications	Application vulnerabilities assessed as extreme are escalated immediately to the ICT Manager and are patched / remediated as soon as possible, based on what Council's current resources allow. For extreme vulnerabilities, Council engages contractors as an additional resource to help address the vulnerabilities as soon as possible. It was stated that these patches are addressed well-within two weeks, but not within 48 hours. Council's records management system (HP TRIM) is no longer supported, and thus Council is assessed as level 0 in maturity for this control. However, it was noted there is a project underway to migrate the records management function to SharePoint.	0	2	2	Once the records migration to SharePoint is completed and TRIM is decommissioned, Council will achieve a maturity level of 2 for this control provided there is no other unsupported business applications in use.	For Council to achieve a maturity level 3 in this control, it would need to employ a capability to patch vulnerabilities assessed as extreme within 48 hours. Discussions with ICT indicated this may be in the form of the following: • A specialist contractor on a retainer; • A third party managed service provider; or • A highly skilled internal resource.
Configure Microsoft Office macro settings	A Microsoft Office macro can only run once the user authorises it after being prompted. It was noted that areas of the Council (e.g. Finance) rely on macro-enabled documents. Although macros are permitted to run when approved, there are are compensating controls in place to mitigate the impact of any malicious macros being executed by mistake. An example of this is that Carbon Black blocks Office applications from executing a command line interpreter.	1	2	0.8	Maturity level 2 allows macros to run, as long as they have a digital signature. As such, Council should investigate where macros are used, sign those macros, and apply a technical control that allows only those signed macros to run. Council's financial auditor provides macro-enabled documents to Council's finance team to populate. As such, Council could have to discontinue this practice to achieve level 2.	To achieve maturity level 3, Council would need to establish a capability to vet macros at a technical level, which ICT expressed it does not currently have. Further, macros not only need to be signed by also restricted to a trusted location on the network which is tightly access controlled.

Control Area	Findings	Current Level	Target Level	Average Level	Recommendation For Level 2	Recommendation For Level 3
User application hardening	Flash is disabled. Java-enabled web applications are currently blocked. Council browsers do not currently block web advertisements (e.g. via a browser plugin). There is currently no controls to restrict OLEs from activating, however, it was noted that Carbon Black has a compensating controls that would mitigate the impact of malicious use, much like with macros above. It was noted by ICT that certain Council business units rely on OLEs for operational activities (e.g. spreadsheets referring to each other in a network location).	1	2	0.2	To achieve maturity level two, Council will need to block web advertisements in browsers by default.	To achieve maturity level 3, Council will also need to apply a technical control to restrict OLEs from being activated.
Restrict administrative privileges	The process for provisioning privileged accounts falls under the same ICT access management process, which includes validation of the appropriateness of the access request. This also follows the principle of least privilege (i.e. accounts are only provisioned with the minimum access they require). Restrictions for privileged accounts are not covered in Council policy.	0	2	0.2	Council can achieve maturity level two by prohibiting privileged user accounts from accessing email, browsing the internet and downloading files from the internet in Council policy. This could be incorporated into an acceptable use policy as recommended under A.5 of the ISO 27001 control assessment.	Council can achieve maturity level three by implementing technical controls to enforce the policy requirements as specified in the recommendation for level two. The ICT Team Leader indicated that an informal plan is in place to achieve maturity level three. Network segmentation followed by a firewall configured with AD would allow for a firewall policy to restrict privileged accounts conducting high-risk activities.

Control Area	Findings	Current Level	Target Level	Average Level	Recommendation For Level 2	Recommendation For Level 3
Patch operating systems	(Per application patching process) Operating system vulnerabilities assessed as extreme are escalated immediately to the ICT Manager and are patched / remediated as soon as possible, based on what Council's current resources allow. For extreme vulnerabilities, Council engages contractors as an additional resource to help address the vulnerabilities as soon as possible. It was stated that these patches are addressed well-within two weeks, but not within 48 hours. Further, ICT mentioned that patching of firmware for a key network switch may require a scheduled outage - which may not be possible within 48 hours due to operational constraints. The operating system supporting the non-supported TRIM are also no longer supported by Microsoft. Certain webservers running My Community are using non-supported server operating systems.	0	2	1.6	Council can achieve a maturity level of two by decommissioning the non-supported operating system required to run the TRIM application. As such, TRIM would also need to be decommissioned as mentioned in the 'patch applications' section above.	To achieve a maturity level of 3 in this control, Council would need to upgrade or decommission the non-supported versions of its operating systems. Further, Council would need to deploy an automated mechanism to facilitate patching and verify that the patch was applied effectively.
Multi-factor authentication	It was noted that although an MFA solution was procured, it was not implemented at the time of assessment. As such, Council was assessed as maturity level zero for this control.	0	2	0	The MFA solution currently being implemented will cover maturity level one in the first instance. However, to meet maturity level two the solution will need to be enhanced to authenticate privileged users for both remote and internal access. The planned second factor of authentication in the form of a mobile application on-time token is sufficient for maturity level two.	In addition to the recommendations for maturity level two, Council would have to implement MFA using a physical token (e.g. YubiKey) for all staff accessing important data repositories (to be determined by Council).
Daily backups	Restoration tests of entire VMs have been tested and work effectively. Such restores occur once every 6 months on average. VMs restorations from tape have also been successfully performed. Note: Council choses to interpret a full VM restore as a "full restoration" in this context, as ICT expressed a full restoration of all VMs at once is not a feasible task, and ICT has assurance that any and all VMs could be successfully restored via the tested, working process.	2	3	0.2	N/A	To achieve maturity level 3, Council would need to systemically test a full VM restoration whenever a fundamental infrastructure change occurs. While this is subjective, Council will need to make an assessment as to whether a change in infrastructure may have an impact on Council's ability to effectively restore data / VMs from backup, in which case a restoration test must be performed. These restores would also need to be performed on a quarterly basis at a minimum.

Work unit/activity being assessed: ICT & Council-wide processes | **Assessment conducted by: CyberCX, ICT and Governance & Performance** | **Assessment date: August - September 2020**

Context:

Section 1: Risk identification				Section 2: Inherent Risk				Section 3: Controls		Section 4: Residual Risk				Section 5: Risk Evaluation		Section 6: Risk Mitigation			
No	**Risk Statement (use the situation-consequence technique)**	**Causes & Impact**	**Risk Owner**	**Category**	**Consequence**	**Likelihood**	**Risk Rating**	**Details**	**Effectiveness**	**Consequence**	**Likelihood**	**Risk Rating**	**Date of assess-ment**	**Mitigation actions required**	**Next assess-ment no later than**	**Mitigation Action**	**Responsible Officer**	**Due Date**	**Target Rating**
1	Lack of multifactor authentication resulting in unauthorised remote access for a user.	**Cause**: • Credential for user found in a data breach •Password reuse between different systems • Single factor of authentication for remote access. • No formal phishing awareness training. **Impact**: • Compromise of information in the virtual environment. • Disruption of the virtual environment. • Hijacking of staff access, leading to accountability issues.	Manager Information Services	Service Continuity	Minor	Possible	Medium (2C)	• Established access management process. • Authentication for remote access. • VMWare Horizon sessions are encrypted. • Access reviews at ICT monthly meetings. • Password awareness training. • 'External' labels on inbound emails. •Authentication Logging systems.	Marginal	Minor	Possible	Medium (2C)	15/09/20	Minimum biannual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	14/03/21				
2	Lack of an information classification framework leading to the inappropriate release/management of corporate information.	**Cause**: • No formal information classification scheme. • No defined information labelling and handling guidelines outside of Council records unit. • No rules defined for information transfer. • No information transfer agreements with external parties. • Information is transferred with suppliers without restriction or user guidance. **Impact**: • Accidental information leakage. • Difficulty designing and applying information security controls.	Manager Information Services	Service Continuity	Minor	Likely	High (2B)	• Robust processes for handling incoming information through the records unit. • Secure file transfer software for limited areas of the business. • CONFIDENTIAL label is used. • Virtualised environment reducing the use of removable and local device storage.	Good	Insignificant	Possible	Low (1C)	15/09/20	Minimum annual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	15/09/21				
3	Lack of ICT Control of certain Cloud based applications (Smarty Grants) may result in Users being provided with or retaining access to systems after leaving the organisation.	**Cause**: • No formal process for access reviews of systems not managed by ICT (e.g. cloud applications). • No organisation wide access management policy. **Impact**: • Dormant accounts may remain after personnel departure • Users may retain access rights no longer required by their role.	Manager Information Services	Service Continuity	Minor	Likely	High (2B)	Nil	Marginal	Minor	Likely	High (2B)	15/09/20	Minimum quarterly assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan required.	14/12/20				

4	Lack of identity verification may result in the compromise of Council credentials via vishing while processing a password reset (i.e. phone-based social engineering)	**Cause**: • Passwords could be reset via phone calls with HelpDesk. No formal confirmation of identity beyond voice, and passwords are provided on the same call. • User passwords could be given verbally over the phone directly to hackers posing as Council ICT Staff. **Impact**: • Unauthorised access to Council systems.	Manager Information Services	Service Continuity	Minor	Rare	Low (2E)	• External helpdesk number isn't published. • 'External' labels on inbound emails, mitigating phishing risk. • Helpdesk personnel are familiar with Council staff.	Good	Insignificant	Rare	Low (1E)	15/09/20	Minimum annual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	15/09/21				
5	No formal third party supplier agreements in place resulting in potential compromise of Council data.	**Cause**: • Data is provided to suppliers which is managed outside of Council control, and with no assurance of supplier practices. **Impact**: • Theft of Council information via third party supplier breach. • Corrupted data uploaded by contractors	Manager Information Services	Service Continuity	Minor	Possible	Medium (2C)	Nil	Poor	Minor	Possible	Medium (2C)	15/09/20	Minimum biannual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	14/03/21				
6	Internal Labour hire (Contractors) are not always subject to the formal OD onboarding / offboarding process resulting in access to systems remaining in place after contractor agreements expire.	**Cause**: • Identification and management of information security risks is not embedded in Council's supplier management process. • Suppliers are not made aware of their security responsibilities • Suppliers do not sign ICT/IS agreements • Confidentiality clauses are absent from some procurement templates. **Impact**: • Compromise of Council information • Accidental or intentional misuse of Council systems by contractors	Manager Information Services	Service Continuity	Minor	Likely	High (2B)	• Managers are to advice ICT of start and finish of contractors.	Marginal	Minor	Possible	Medium (2C)	15/09/20	Minimum biannual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	14/03/21				
7	Failure of staff to lock workstations when unattended resulting in unauthorised use of systems.	**Cause**: • Unlocked workstations in shared areas at Council premises. **Impact**: • Increased likelihood of physical compromise of workstations. • Loss of accountability for user accounts.	Manager Information Services	Service Continuity	Minor	Possible	Medium (2C)	• Automatic lockout after 15 minutes. • Staff induction covers off on usage of systems.	Marginal	Minor	Unlikely	Low (2D)	15/09/20	Minimum annual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	15/09/21				

8	Lack of independent technical testing may result in vulnerabilities being undetected in Council systems.	**Cause**: • Independent technical testing (e.g. penetration testing) has not been performed for several years. **Impact**: • Compromise of systems via exploitation of vulnerabilities. • Certain vulnerabilities may result in ransomware deployment over Council system.	Manager Information Services	Service Continuity	Moderate	Possible	Medium (3C)	• ICT Team Leader scans networks frequently. • Changes to systems follow a controlled process. • DPC Watch Desk provides information on emerging vulnerabilities. • Patching is applied in a timely manner commensurate with risk. •Endpoint Detection Response (EDR) Software in use over Council systems.	Good	Minor	Unlikely	Low (2D)	15/09/20	Minimum annual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	15/09/21				
9	Telecommunication service provider outage severing connection to Council datacentres.	**Cause**: • Fusion Broadband is a single point of failure in terms of connectivity to Council datacentres. **Impact**: • Inability to access Council systems and information hosted in the datacentre.	Manager Information Services	Service Continuity	Moderate	Rare	Low (3E)	• Service Level Agreements with Telecommunications providers	Marginal	Moderate	Rare	Low (3E)	15/09/20	Minimum annual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	15/09/21				
10	The data breach response plan does not cover other types of information security incidents (e.g. ransomware, denial of service attacks, website defacement, etc) resulting in an ineffective or inefficient response during an information security incident.	**Cause**: • Roles and responsibilities for Council staff involved in the response process are not clearly articulated in the response plan. • Contact details for digital forensic specialists are not referenced in the response plan, should they be needed (e.g. if the incident becomes a legal matter). **Impact**: • A disorganised approach to responding to other types of information security breaches. • Disagreements within the response team regarding responsibilities. • Improper evidence collection that may void the evidence due to chain of custody ambiguity.	Manager Information Services	Service Continuity	Moderate	Possible	Medium (3C)	• Data breach response plan has a defined response group. • Contacts with authorities are maintained (e.g. SAPOL, DPC Watch Desk).	Marginal	Minor	Possible	Medium (2C)	15/09/20	Minimum biannual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	14/03/21				

Appendix 3

Corporate Risk Register Cyber Security Audit

Work unit/activity being assessed: ICT & Council-wide processes | Assessment conducted by: Information Services | Assessment date: April 2021

Context: items from Cyber Security Audit September 2020

Section 1: Risk identification				Section 2: Inherent Risk				Section 3: Controls		Section 4: Residual Risk				Section 5: Risk Evaluation			Section 6: Risk Mitigation			
No	Risk Statement (use the situation-consequence technique)	Causes & Impact	Risk Owner	Category	Consequence	Likelihood	Risk Rating	Details	Effectiveness	Consequence	Likelihood	Risk Rating	Date of assessment	Mitigation actions required	Next assessment no later than	Mitigation Action	Responsible Officer	Due Date	Target Rating
1	Lack of multifactor authentication resulting in unauthorised remote access for a user.	**Cause**: • Credential for user found in a data breach •Password reuse between different systems • Single factor of authentication for remote access. • No formal phishing awareness training. **Impact**: • Compromise of information in the virtual environment. • Disruption of the virtual environment. • Hijacking of staff access, leading to accountability issues.	Manager Information Services	Service Continuity	Minor	Possible	Medium (2C)	• Established access management process. • Authentication for remote access. • VMWare Horizon sessions are encrypted. • Access reviews at ICT monthly meetings. • Password awareness training. • 'External' labels on inbound emails. •Authentication Logging systems.	Marginal	Minor	Possible	Medium (2C)	30/04/21	Minimum biannual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	27/10/21	Current strategic initiative project being implemented to implement multifactor authentication for system users	Manager ICT	30/05/21	Low
2	Lack of an information classification framework leading to the inappropriate release/management of corporate information.	**Cause**: • No formal information classification scheme. • No defined information labelling and handling guidelines outside of Council records unit. • No rules defined for information transfer. • No information transfer agreements with external parties. • Information is transferred with suppliers without restriction or user guidance. **Impact**: • Accidental information leakage. • Difficulty designing and applying information security controls.	Manager Information Services	Service Continuity	Minor	Likely	High (2B)	• Robust processes for handling incoming information through the records unit. • Secure file transfer software for limited areas of the business. • CONFIDENTIAL label is used. • Virtualised environment reducing the use of removable and local device storage.	Good	Insignificant	Possible	Low (1C)	30/04/21	Minimum annual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	30/04/22	Addressed in Phase 3 & 4 of the Cyber Security Plan (ISMS) implementation with the creation of procedure	Manager ICT	30/05/22	Low
3	Lack of ICT Control of certain Cloud based applications (Smarty Grants) may result in Users being provided with or retaining access to systems after leaving the organisation.	**Cause**: • No formal process for access reviews of systems not managed by ICT (e.g. cloud applications). • No organisation wide access management policy. **Impact**: • Dormant accounts may remain after personnel departure • Users may retain access rights no longer required by their role.	Manager Information Services	Service Continuity	Minor	Likely	High (2B)	Nil	Marginal	Minor	Likely	High (2B)	30/04/21	Minimum quarterly assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan required.	29/07/21	Addressed in Phase 3 & 4 of the Cyber Security Plan (ISMS) implementation with the creation of procedure	Manager ICT	30/05/22	Low

4	Lack of identity verification may result in the compromise of Council credentials via vishing while processing a password reset (i.e. phone-based social engineering)	**Cause**: • Passwords could be reset via phone calls with HelpDesk. No formal confirmation of identity beyond voice, and passwords are provided on the same call. • User passwords could be given verbally over the phone directly to hackers posing as Council ICT Staff. **Impact**: • Unauthorised access to Council systems.	Manager Information Services	Service Continuity	Minor	Rare	Low (2E)	• External helpdesk number isn't published. • 'External' labels on inbound emails, mitigating phishing risk. • Helpdesk personnel are familiar with Council staff.	Good	Insignificant	Rare	Low (1E)	30/04/21	Minimum annual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	30/04/22	Addressed in Phase 3 & 4 of the Cyber Security Plan (ISMS) implementation with the creation of procedure	Manager ICT	30/2/22	Low
5	No formal third party supplier agreements in place resulting in potential compromise of Council data.	**Cause**: • Data is provided to suppliers which is managed outside of Council control, and with no assurance of supplier practices. **Impact**: • Theft of Council information via third party supplier breach. • Corrupted data uploaded by contractors	Manager Information Services	Service Continuity	Minor	Possible	Medium (2C)	Nil	Poor	Minor	Possible	Medium (2C)	30/04/21	Minimum biannual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	27/10/21	Addressed in Phase 3 & 4 of the Cyber Security Plan (ISMS) implementation with the creation of procedure	Manager ICT	30/05/22	Low
6	Internal Labour hire (Contractors) are not always subject to the formal OD onboarding / offboarding process resulting in access to systems remaining in place after contractor agreements expire.	**Cause**: • Identification and management of information security risks is not embedded in Council's supplier management process. • Suppliers are not made aware of their security responsibilities • Suppliers do not sign ICT/IS agreements • Confidentiality clauses are absent from some procurement templates. **Impact**: • Compromise of Council information • Accidental or intentional misuse of Council systems by contractors	Manager Information Services	Service Continuity	Minor	Likely	High (2B)	• Managers are to advice ICT of start and finish of contractors.	Marginal	Minor	Possible	Medium (2C)	30/04/21	Minimum biannual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	27/10/21	Addressed in Phase 3 & 4 of the Cyber Security Plan (ISMS) implementation with the creation of procedure	Manager ICT	30/05/22	Low
7	Failure of staff to lock workstations when unattended resulting in unauthorised use of systems.	**Cause**: • Unlocked workstations in shared areas at Council premises. **Impact**: • Increased likelihood of physical compromise of workstations. • Loss of accountability for user accounts.	Manager Information Services	Service Continuity	Minor	Possible	Medium (2C)	• Automatic lockout after 15 minutes. • Staff induction covers off on usage of systems.	Marginal	Minor	Unlikely	Low (2D)	30/04/21	Minimum annual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	30/04/22	Addressed in Phase 3 & 4 of the Cyber Security Plan (ISMS) implementation with the creation of procedure	Manager ICT	30/05/22	Low

8	Lack of independent technical testing may result in vulnerabilities being undetected in Council systems.	**Cause**: • Independent technical testing (e.g. penetration testing) has not been performed for several years. **Impact**: • Compromise of systems via exploitation of vulnerabilities. • Certain vulnerabilities may result in ransomware deployment over Council system.	Manager Information Services	Service Continuity	Moderate	Possible	Medium (3C)	• ICT Team Leader scans networks frequently. • Changes to systems follow a controlled process. • DPC Watch Desk provides information on emerging vulnerabilities. • Patching is applied in a timely manner commensurate with risk. •Endpoint Detection Response (EDR) Software in use over Council systems.	Good	Minor	Unlikely	Low (2D)	30/04/21	Minimum annual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	30/04/22	Addressed in Phase 5 of the Cyber Security Plan (ISMS) ongoing audits and reviews	Manager ICT	30/05/22	Low
9	Telecommunication service provider outage severing connection to Council datacentres.	**Cause**: • Fusion Broadband is a single point of failure in terms of connectivity to Council datacentres. **Impact**: • Inability to access Council systems and information hosted in the datacentre.	Manager Information Services	Service Continuity	Moderate	Rare	Low (3E)	• Service Level Agreements with Telecommunications providers	Marginal	Moderate	Rare	Low (3E)	30/04/21	Minimum annual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	30/04/22	Removal of single point of failure in terms of connectivity to Council Datacenters	Manager ICT	30/05/22	Low
10	The data breach response plan does not cover other types of information security incidents (e.g. ransomware, denial of service attacks, website defacement, etc) resulting in an ineffective or inefficient response during an information security incident.	**Cause**: • Roles and responsibilities for Council staff involved in the response process are not clearly articulated in the response plan. • Contact details for digital forensic specialists are not referenced in the response plan, should they be needed (e.g. if the incident becomes a legal matter). **Impact**: • A disorganised approach to responding to other types of information security breaches. • Disagreements within the response team regarding responsibilities. • Improper evidence collection that may void the evidence due to chain of custody ambiguity.	Manager Information Services	Service Continuity	Moderate	Possible	Medium (3C)	• Data breach response plan has a defined response group. • Contacts with authorities are maintained (e.g. SAPOL, DPC Watch Desk).	Marginal	Minor	Possible	Medium (2C)	30/04/21	Minimum biannual assessment of residual risk required or when causes or controls change or mitigations are implemented. Risk mitigation (treatment) plan optional.	27/10/21	Addressed in Phase 3 & 4 of the Cyber Security Plan (ISMS) implementation with the creation of procedure	Manager ICT	30/05/22	Low

3. Cyber Security Audit – Period of Confidentiality

Subject to the CEO, or his delegate, disclosing information or any document (in whole or in part) for the purpose of implementing Council's decision(s) in this matter in the performance of the duties and responsibilities of office, Council, having considered Agenda Item 8.1 in confidence under sections 90(2) and 90(3)(e) of the *Local Government Act 1999*, resolves that an order be made under the provisions of sections 91(7) and (9) of the *Local Government Act 1999* that the report, related attachments and the minutes of Council and the discussion and considerations of the subject matter be retained in confidence until the control deficiencies are mitigated but no longer than 30 June 2023.

Pursuant to section 91(9)(c) of the *Local Government Act 1999*, Council delegates the power to revoke the confidentiality order either partially or in full to the Chief Executive Officer.