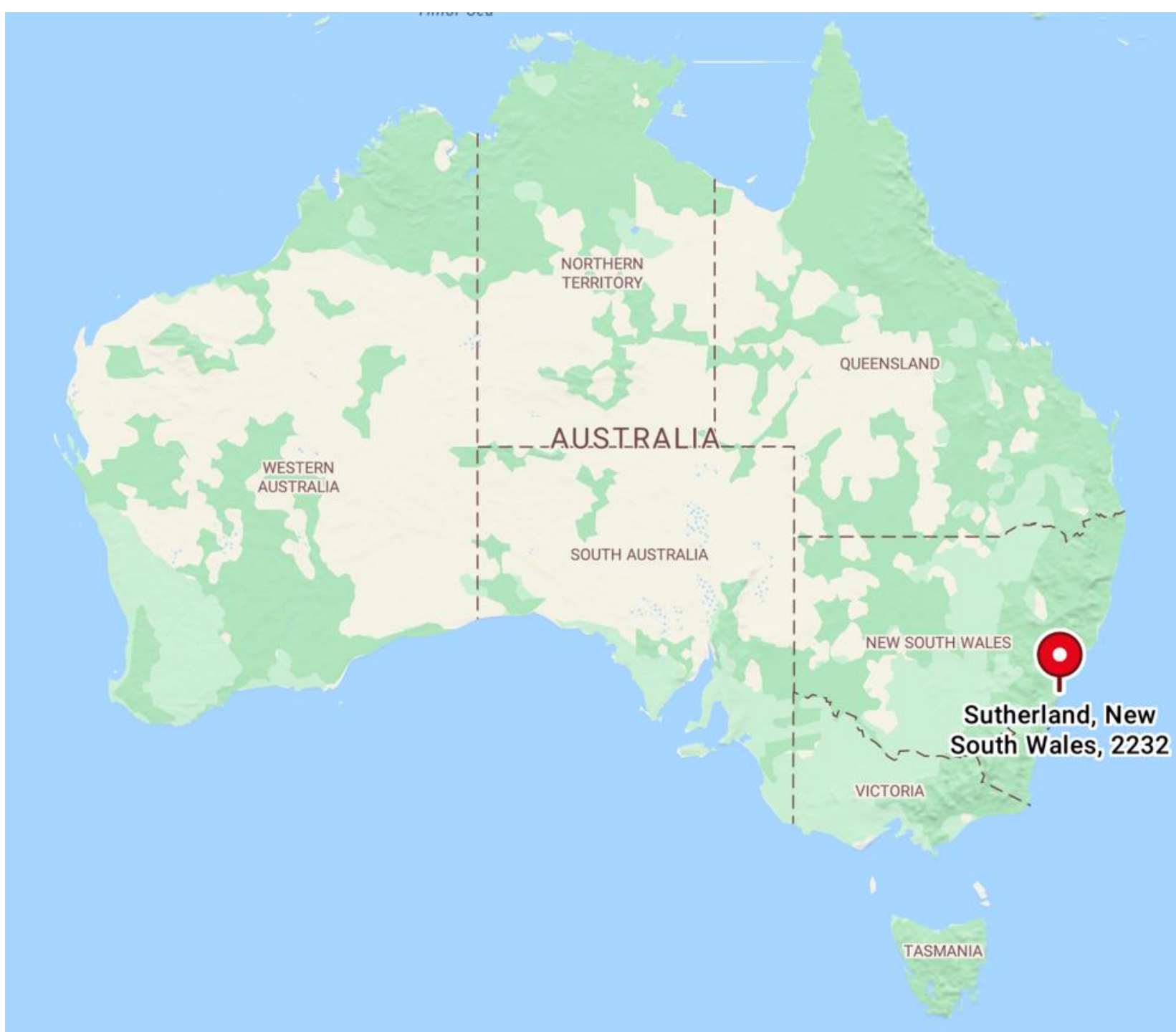


Secret Sauce: Cyber Governance Framework

Presented by:
Leanne Siveyer





Population
235,029

↑↑ **+12%**
by 2036

Population over 60
57,189

↑↑ **+15%**
by 2036



Youth (15-24)
26,974

↑↑ **+11%**
by 2036



Aboriginal and/
or Torres Strait
Islander
1.2%

5%



Living with
disability



Linguistically
diverse
14%



Overseas born
19%



↑↑ **+13%**
by 2036

Dwellings
90,922

Households with children
47%

↑↑ **+10%**
by 2036

Lone person households
22%

↑↑ **+20%**
by 2036



Rental
households
22%

1.9



Average number
of vehicles per
household

2.6



Average
number of
people per
household size

Gross
Regional Product
\$14.18b



Total
businesses
23,235



3.1%
Unemployment
rate



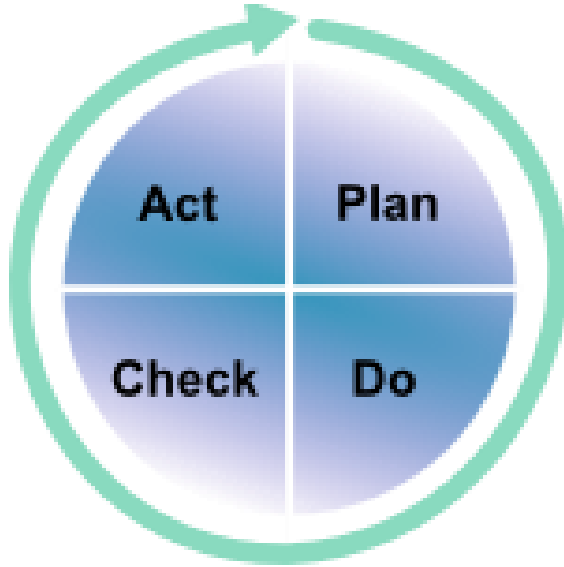
Ingredients & Method – What and How?

- Awareness and Desire
- Develop and Endorse
 - Framework
 - Crown Jewels
 - Security Objectiveness
- Implement and Operate
 - Deliver security initiatives
 - Run the forums
 - Write the reports
- Review and Improve

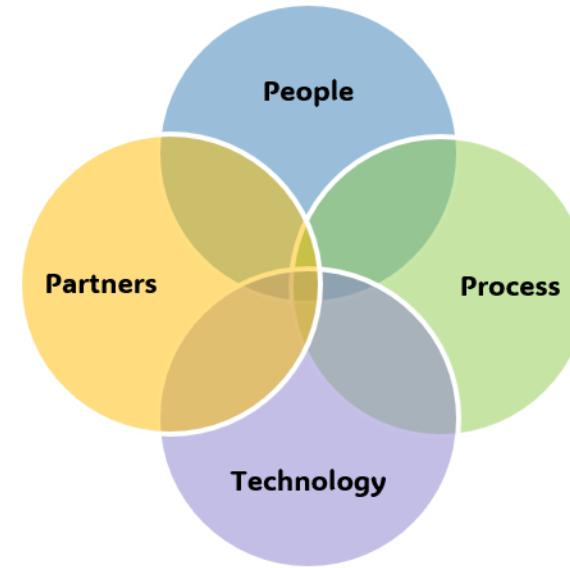


[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

What is an ISMS?



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)



Key artefacts:

- Cyber Security Policy (external)
- ISMS framework (Internal)
- ICT Acceptable Use determination
- Cyber security Standards
- Cyber security Incident Response Plan
- Cyber security plan/roadmap

ISMS Roles

Role	Key Responsibilities
Executive	Define councils risk appetite Resource and support cyber strategy
CIO/CISO 	ISMS Owner Ensure cyber roles and responsibilities are defined Ensure secure by design approach to projects Define cyber security plan Manage cyber security budget
Information Security Manager (IT Operations and Infrastructure Mgr) 	Manage response to cyber events, threats and risks Manage operational security activities, tools and platforms Manage cyber security partners Implement cyber security response plan Implement technical cyber security controls and initiatives
Cyber Security & Risk Mgt Lead 	Chair Security Working Group Co-ordinate and track ISMS activities Lead security risk assessments, cyber awareness campaign, audit co-ordination Prepare internal and external reports and presentations
Technical Cyber Security specialists 	Lead response to cyber events, threats and vulnerabilities Provide technical guidance on risks Perform operational security activities Implement new cyber controls eg E8
All staff with authorized access to SSC systems	Complete regular cyber awareness training Use SSC information assets in accordance ICT Acceptable Use determination eg MFA

ISMS Governance Framework



ISMS Steering Committee



Quarterly

Are we meeting our cyber security objectives?

Annual

Are our cyber security objectives right?

Executive Sponsor - Director Corporate

Membership (Enterprise Risk Committee)

- Manager Corporate Governance (Chair)
- CIO, CFO, Head of Safety and Well being
- Senior Manager – Community, Planning, Infrastructure, Corporate

Remit

- Ensure security objectives are aligned with the strategic direction of Council
- Ensure that security activities are carried out as per the ISMS Framework
- Ensure that the ISMS is implemented and resourced effectively
- make decisions on how to handle noncompliance
- Evaluate significant issues that may impact the operation of the ISMS
- Ensure the residual risk is within the tolerance of the organisation
- Monitor the effectiveness of the SWG
- direct the activities of the SWG

Scope = Crown Jewels + Objectives

Crown Jewels

Element	Level of Impact if the data was	Ratings
Confidentiality	Disclosed to the public?	Catastrophic Major Moderate Minor Insignificant
Integrity	Compromised or altered inappropriately?	
Availability	Unavailable for? (a) 24 hrs (b) 5 working days (c) Ever (Totally Lost)	

Method:

- Draft initial list (don't assume you know)
- Identify the system owner
- Consult the system owner
- Present findings to ISMS Steering Committee Update and endorse
- Review and improve



Crown Jewels

Critical Business Systems



Application	Function	Vendor	Confidentiality	Integrity	Availability
One Council	Financials, Enterprise Asset Management, Enterprise Content Management, Supply Chain Management	Technology One	Moderate	Major	Catastrophic
One Council	Request Mgt	Technology One	Major	Major	Catastrophic
Objective	Records Management	Objective	Moderate	Major	Catastrophic
TechOne P&R	Property and Rating	TechOne	Major	Major	Catastrophic
GIS/ESRI	Spatial	ESRI	Moderate	Major	Major - Catastrophic
Aurion Payroll	Payroll and Establishment	Aurion	Major	Major	Major
Figtree	Safety Management System	FigTree Systems	Major	Major	Major
AD/O365	Identity Mgt/Collaboration/Productivity	Microsoft	Catastrophic	Catastrophic	Catastrophic

Enterprise RISK MATRIX Ranking Tool (Dec 2024)

SUTHERLANDSHIRE



CONSEQUENCE									LIKELIHOOD				
									When we look at 'Likelihood', we are looking to identify the frequency or probability chance of the particular risk occurring. We are required to determine the most appropriate rating depending on the description.				
Financial & Assets	WHS	Environment	Reputation	Legal Liability	Service Delivery	Community Wellbeing & Safety	Information Security & Technology	Descriptor	Rare Unforeseeable or may occur in exceptional circumstances	Unlikely Could happen but probably won't	Possible Might occur at some time but not supported by data	Likely Experience / data suggests comparable events have occurred	Almost Certain Experience / data strongly suggests it will happen
													
Extensive financial or asset loss of > 1M or > 50% of revenue	Extensive multiple casualties or multiple fatalities	Extensive irreparable damage	Extensive public outcry. Potential international media attention.	Extensive litigation or indictable offence	Loss of a *Critical Service >1 month that may impact community safety	Extensive multiple casualties or multiple fatalities	Irretrievable loss of critical data	Catastrophic	Medium (8)	High (16)	Extreme (20)	Extreme (23)	Extreme (25)
Major financial or asset loss of 500k to 1M or up to 50% of revenue	Major casualty or single fatality	Localised irreparable damage	Major public outcry. Potential national media attention.	Major litigation, claim or prosecution	Loss of a *Critical Service > 2 weeks Non-critical service >1 Month	Major casualty or single fatality	Loss of critical IT services >2 weeks	Major	Medium (7)	Medium (12)	High (17)	Extreme (21)	Extreme (24)
Significant financial or asset loss of 50k to 500k or up to 25% of revenue	Moderate injury/illness requiring hospitalisation	Major damage requiring remediation	Serious public outcry. State media attention	Litigation, significant claim or fine	Loss of a *Critical Service < 2 weeks Non-critical service <1 Month	Moderate injury/illness requiring hospitalisation	Loss of critical IT services < 2 weeks	Moderate	Low (4)	Medium (10)	High (15)	High (18)	Extreme (22)
Minor financial or asset loss of 25k to 50k or up to 15% of revenue	Minor injury/illness requiring treatment by doctor	Moderate adverse effect requiring clean up	Significant community concern with local media attention.	Moderate claims or fine	Loss of a *Critical Service < 1 weeks Non-critical service <2 weeks	Minor injury/illness requiring treatment by doctor	Loss of critical IT services < 1 weeks	Minor	Low (2)	Low (5)	Medium (11)	High (13)	High (19)
Negligible financial or asset loss of <25k or <10% of revenue	Insignificant injury/illness requiring first aid treatment	Minor adverse effect with limited clean up	Heightened local community concerns and criticism	Minor claims, fine or action with short term significance	Loss of a *Critical Service < 1 day Non-critical service <1 weeks	Insignificant injury/illness requiring first aid treatment	Loss of critical IT services < 1 day	Insignificant	Low (1)	Low (3)	Low (6)	Medium (9)	High (14)

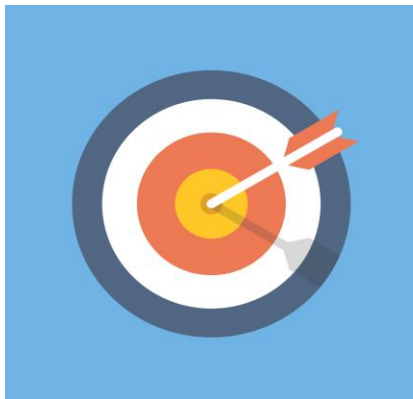
* Critical services are services that support the minimisation of harm to human health & the environment & the internal support services they depend on.

Risk Appetite Statement (RAS) the acceptable level of appetite for each risk category, once reached it triggers the need for further considerations/ mitigations/ monitoring of the risk

Medium Financial & Assets	Low WHS	Medium Environment	Medium Reputation	Medium Legal Liability	Medium Service Delivery	Low Community Safety	Medium IST
---------------------------	---------	--------------------	-------------------	------------------------	-------------------------	----------------------	------------

ISMS Objectives

Method



1. Draft objectives based on known risks

- a) Previous audits
- b) Environmental weaknesses
- c) Best practice eg E8, Cyber Guidelines for LG
- d) Industry knowledge
- e) Strategic Objectives

2. Consult with the ISMS Steering Committee

3. Formal endorsement

4. Define the strategy & measure for each objective

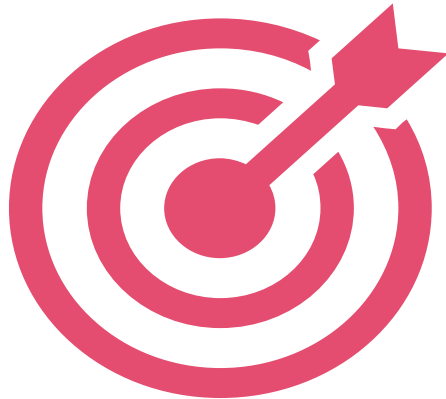
5. Execute the strategy

6. Report progress by objective

7. Review the objectives (annually)

ISMS Objectives

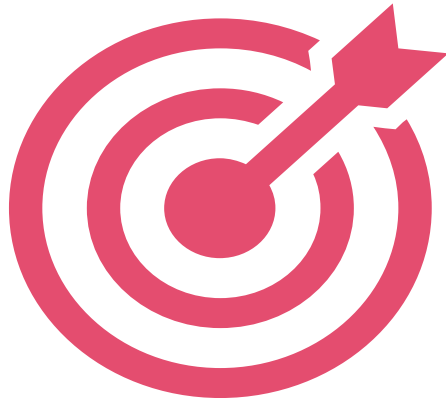
Year 1
2022/2023



Objective	Description
1	<u>Develop</u> information security management <u>capability</u> – internal staff and partners.
2	Apply appropriate risk-based controls to manage confidentiality, availability and integrity by focusing on sensitive information and <u>critical systems</u> .
3	Ensure continual improvement of <u>security controls</u> as defined by the Essential 8 in order to maintain an acceptable level of risk.
4	<u>Develop</u> associated policies, determinations and other needed <u>artefacts</u> to effectively operate, manage and govern the information security as an integral business activity process.
5	Increase the information <u>security awareness</u> across the organisation.
6	Provide appropriate management of internal and external <u>audit</u> issues.

ISMS Objectives

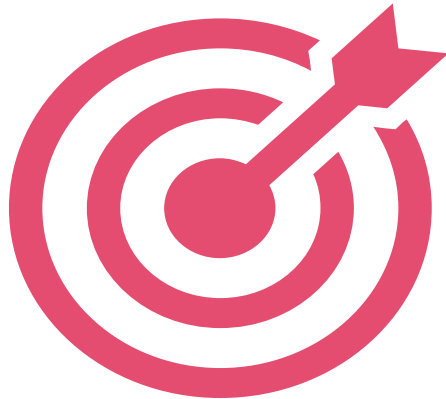
Year 2
2023/2024



Objective	Description
1	<u>Maintain</u> and continually improve information security management skills, capability and governing artefacts .
2	Identify, analyze and apply appropriate controls to manage the risk posed by vendors , suppliers and third parties.
3	<u>Maintain</u> and continually improve security controls including, but not limited to, the Essential 8 to an acceptable level of risk.
4	Identify and apply appropriate controls to manage the risk of over-collection and over-retention of private or sensitive information , considering legislative compliance, privacy, security and data practices.
5	Maintain and <u>increase</u> information security awareness and knowledge to mitigate the risk of compromise based on social engineering and other behavioural factors.

ISMS Objectives

2025/2026



Objective	Description
1	Develop a roadmap of activities to comply with the revised Cyber Security Guidelines for Local Government
2	Identify, analyze and apply appropriate controls to manage the risk posed by vendors , suppliers and third parties.
3	Maintain and continually improve skills, capability and security controls including, but not limited to, the Essential 8 to an acceptable level of risk.
4	Identify and apply appropriate controls to manage the risk of over-collection and over-retention of private or sensitive information, considering legislative compliance, privacy, security and data practices.
5	Maintain and increase information security awareness and knowledge to mitigate the risk of compromise based on social engineering and other behavioural factors.
6	Define and establish AI Guardrails

SWG Agenda

Monthly

- Detailed review of ISMS initiatives for each Security Objective.
- Review cyber risk register
- Review cyber incident register
- Review ISMS Standard exemptions
- Review audit items
- Cyber calendar and roadmap



ISMS Security Working Group MEETING AGENDA

Date:	25/10/23	Time:	2.30 pm – 4.30 pm
Chairperson:	Sherree List	Minute Taker:	Sherree List
Invited Attendees:	Sherree List, Steve Pirani, Dan Clarke, Savvas Eleutheriades, Wayne Cavanough, Leanne Siveyer		
Location:	LG Como		
Apologies:	n/a		
Meeting Cycle	Monthly.		

Objectives for 2023/2024

NO	Item	Presenter
1	Previous Minutes	Chair
2	Objective 1: Maintain and continually improve information security management skills, capability and governing artefacts. Roles/Recruitment Change Management and Risk Officer Cyber Trainee (commencing Feb 24) Cyber Acceleration Plan in 23/24 Budget 2nd Senior Technical Cyber Security Specialist (recruited)	Sherree Savvas
3	Objective 1 Maintain and continually improve information security management skills, capability and governing artefacts. Security Standard (update) ICT Acceptable Use Determination	Steven Sherree
4	Objective 2 - Identify, analyze and apply appropriate controls to manage the risk posed by vendors, suppliers and third parties. Monitoring Vendors - Crown Jewels – Cloud Providers - SOC Reports - Cyber Vendor Assessments -Procurement RFQs and Tenders	
5	Objective 3 Maintain and continually improve security controls including, but not limited to, the Essential 8 to an acceptable level of risk. CHIPS and Upguard – Breachlight Report - External Vulnerability Scan Remediation - Hazelhurst Website - Risks (IT Risk Register) Status updates - CSR 3.1 Remote Working Risk Review - CSR 4.8 OneCouncil – Auto BPay Upload - CSR 4.6 - Aurion Batch Plaintext Password	Dan/Sherree

NO	Item	Presenter
6	Objective 3 Maintain and continually improve security controls including, but not limited to, the Essential 8 to an acceptable level of risk. E8 Project Prioritization Priorities - Updates - CSP-11 Immutable Backup Solution - CSP-10 Multifactor Authentication Backlog - CSP-8 Windows Server Upgrade - CSP-9 Patch OS End Points - CSP-13 Vulnerability Assessment Scan VAS and Pen test - CSP-5 Microsoft Office Macros settings - CSP-163 365 Security Recommendations Other - Other Patching – DC - OC MFA – generic a/c's - Self Service + Laptop Local Password Change Procedure and Test – DC/SP - Patch My PC - Penetration Test (Savvas) - Internal Vulnerability Scan (Respiro) - Cyber NSW Voluntary Annual Reporting (Sherree)	Stephen Dan Dan and Stephen
7	Objective 4 Identify and apply appropriate controls to manage the risk of over-collection and over-retention of private or sensitive information, considering legislative compliance, privacy, security and data practices Update of ERC Action: Personal Details published on DA Tracker. - Update Digital Archivist project – update.	
8	Objective 5 Maintain and increase information security awareness and knowledge to mitigate the risk of compromise based on social engineering and other behavioural factors. Cyber Awareness Month -	Sherree
9	Objective 6: Provide External Audit	Sherree

ISMS Steering Committee & ARIC Updates

- High level status update for each ISMS Objective
- Cyber Security risk register
- Cyber security incident overview

Objective 1	Skills & Capabilities	Initiatives	
Maintain and continually improve information security management skills, capability and governing artefacts	Governance	ISMS Steering Committee Meetings – 2023 – April and August 2022 – 28 April, 19 August & December Security Working Group Meetings – monthly (March 22 to December 23)	
	Recruitment	- Cyber Security Technical Lead – Dan Clarke (permanent appointment) - Cyber Security and Risk Lead – Sherree List (permanent appointment) 1 x Digital Archivist – Jordan Lewis-Stark (temp appointment) - IT Change Management & Risk Officer (offer accepted – new employee starts Jan 2024) - Cyber Security Officer – (Cyber Academy student secured for Feb 2024) 1 x Senior Technical Cyber Security Specialists (Wayne Cavanough started 12/09/23) 2nd – Senior Technical Cyber Security Specialists (started Nov 23 – unfortunately resigned)	
	Upskilling and building capabilities	- Cyber Tech Lead – ACSC E8 Assessment Certificate (TAFE) Dec 23 - NSW Cyber Security Showcase Oct 23 - Cyber Security Summit Sept 23 - PSN Cyber Security Preparedness and Response for LG – Sept 23	

SUTHERLANDSHIRE

5

Objective 1	Artefacts	Status	
Maintain and continually improve information security management skills, capability and governing artefacts	Cyber Security Standard	Under draft and being reviewed.	
	ICT Acceptable Use Determination/Guideline	At Executive Forum on 12 Dec 24	
	Mandatory Data Breach Notification Scheme artefacts and compliance	Data Breach Policy – endorsed at Gov 27/11 – (on public exhibition for community consultation until early Jan 24)	
		Data Breach Guidelines – (approved by Executive Forum 24/10/23 – published on Compass)	
		Operational Readiness for Data Breach Policy – (conducted desktop simulation and collated DB toolkit for response)	

SUTHERLANDSHIRE

6

Objective 2	Initiative	Status	
Identify, analyze and apply appropriate controls to manage the risk posed by vendors, suppliers and third parties.	Vendor Security Assurance	Assurance Report Reviews – Crown Jewels	
		- OneCouncil (SOC2) - Figtree	
		Implemented UpGuard (CNSW) – Tool to monitor, assess and reduce vendor risk.	
		Vendor Cyber Security Reviews – embedded in Tenders, RFQ and through Portfolio Committee	
		Supply Chain Risk Management – presented to Procurement Team – awareness of data security and identify technologies vendors utilize for services (outside IT supplier solutions – Nov 23)	



SUTHERLANDSHIRE

7

Objective 3	Initiative		
Maintain and continually improve security controls including, but not limited to, the Essential 8 to an acceptable level of risk	Essential 8	Target = Maturity Level 2	
	M365	Security Assessment Conducted and remediation underway	
	Privilege User Access Review (Crown Jewels)	Q4 – December 23 review in progress:- Active Directory, One Council Finance, Aaron T1 Property and Rating, Objective CRM, legacy Q&S ESR, Farnes	
	CNSW Voluntary Reporting	Reported – Self Assessment of Cyber Security Maturity for FYE 22/23 Under OLG – Cyber Security Guidelines – Reporting for Local Government	
	Testing and Scanning	Vulnerability Scanning tool funded – baseline scan completed - analysing	
		Network Penetration Test – In progress 4 components – Internal, External, Network and WIFI	
		External Vulnerability scanning via Upguard (Monthly)	

SUTHERLANDSHIRE

10

Objective 4	Initiative	Business Unit	Status	
Identify and apply appropriate controls to manage the risk of over-collection and over-retention of private or sensitive information, considering legislative compliance, privacy, security and data practices.	Digital Information Retention and Disposal Project	Children's Services	Sentencing of PII and Health Data Complete	
			1st set of real data scheduled and approved for destruction Dec 23	
			Destruction of data complete	
			Over retention education	
		Risk and Insurance	Consulting to identify PII, Privilege and confidential information for sentencing	

SUTHERLANDSHIRE

12

Objective 5	Initiatives		
Maintain and increase information security awareness and knowledge to mitigate the risk of compromise based on social engineering and other behavioural factors.	Cyber Awareness Month October 2023	- Compass Comms - Deployed Screen Saver with key cyber hygiene messages - Teams – shared resources increase cyber hygiene practices. - Colouring Competition – Children & Adults – engagement awareness.	
	Artificial Intelligence	Using AI at work & confidentiality of Council information – staff education awareness piece:- Published Compass main page – (Sept 23) All Staff Email (Oct 23)	
		AI expert – David O'Keefe presented to Senior Managers (Nov 23)	
	Scam Awareness Week - November 23	How to identify Online Shopping Scams – resources and education via teams – (Cyber.gov)	
	External Cyber Security information	Website Content – under development	

SUTHERLANDSHIRE

13

Objective 6: Define and Establish AI Guardrails

Guardrails	Control/Mitigation	Status
Policy	Internal Policy (Determination)	Implemented
	External Policy	Planned
Usage governance	AI Register	Implemented
Education - staff	Responsible AI Training and Awareness ISO42001	Ongoing
Education - Councillors	Responsible AI Training and Awareness	Completed
		Planned
Data Governance	Permissions review and data security controls	In Progress
Education	Redirection to approved AI sites	Implemented
Procurement	All vendors must disclose AI use and meet security and ethical standards	Planned
Project Governance	AIAF applied to project lifecycle management. AIAF risk assessment required as part of CR submission	Implemented
Cyber Security	AI specific cyber security checks	Planned





Questions

Thank you