

Cyber Security Initiative Update

MITIGATING A SIGNIFICANT BUSINESS RISK

LGITSA CONFERENCE 5 MAY 2022 LGITSA Cyber Security Strategy: A coordinated and collaborative approach to cyber resilience



Cyber Security Strategy 2021-2024



Taking a truly coordinated and collaborative approach to sharing resources and establishing practices to increase cyber maturity and resilience across the Local Government sector.

Common Gaps ¹	Strategic Priorities	Initiatives	Potential LGITSA Partners	Existing Capabilities & Resources
Security Governance Strategy Policies & procedures Cyber awareness Third parties Risk management Audits	1. Protect what matters Formalise and implement business driven and risk-based processes and procedures for protection	 Governance – Leverage existing government resources to develop a fit for purpose toolkit including strategy, framework, and policies for the sector Third parties – Develop clauses for standard tendering, procurement documentation, and certification of purchased items Supplier panel – Provide a cyber panel for purchasing of software, hardware and services Insurance coverage – Tailor insurance policy needs to risk levels 	LGA LG Procurement LGRS LG R&D Scheme	 Existing frameworks (DPC SA Cyber Security Framework, ACSC – Essential 8 and ISM) Model policies (LGA) Advocate, assist & advance (LGA)
System Security Passwords Privileged accounts User access Vulnerability management Change Management Change management policy	 Create a cyber aware culture Promote cybersecurity awareness through fit for purpose governance and an ongoing and engaging training program 	 General awareness – Promote the cyber security toolkit and common terminology Training and skills development – Provide training for Executive awareness, and skills development for end users, Elected Members and IT staff Testing – Regularly assess the cyber security and policy awareness of council staff Education - Facilitate sector-wide education on cyber security threats and mitigation strategies 	LGA LGRS LG Professionals AGD	 Procurement (LGAP) ICT Vendor Panel (LGAP) Insurance (LGRS) Skytrust (LGRS) VOCAM LMS (LGRS) Examination reports (AGD) IT expertise (LGITSA)
Vendor change management Patch management Backup Operations, Disaster Recovery & Incident Response Disaster recovery	3. Proactively identify vulnerabilities Tighten our monitoring and testing regimes for early identification of cybersecurity threats	 Baseline audit – Undertake audits to identify individual council improvement plans Improvement plans – Support the implementation of improvement plans to increase maturity Critical infrastructure – Identify key community infrastructure (e.g. pumping stations, traffic control, monitoring devices, etc) and certification of the systems for cybersecurity 	LGRS LGA	 Yammer network (LGITSA) Special Interest Group (LGITSA) Conferences & workshops (LGITSA) Watch Desk (DPC) Joint operating guideline
Business Continuity Plan Incident response Vulnerability assessment External website	4. Increase resilience and responsiveness Strengthen our ability to respond and recover from cybersecurity threats and incidents	 Threat intelligence – Form partnerships with government agencies for subscription alerts Responsiveness - Share real-time updates on threat intelligence Incidents – Develop relationships with relevant cybersecurity agencies and promote reporting of incidents, and include incident response playbooks in the cyber security toolkit 	LGA DPC LGFSG ACSC	(LGSFG/DPC) • Funding (LGRS, LG R&D Scheme)

STRATEGIC PRIORITIES & KEY INITIATIVES

I. Protect what matters

Formalise and implement business driven and risk-based processes and procedures for protection.

 Local Government Cyber Security Framework funded by R&D Scheme

2. Create a cyber aware culture

Promote cyber security awareness through fit for purpose governance and an ongoing and engaging training program.

 LGA/LGITSA engagement with other agencies to coordinate an education and training program

3. Proactively identify vulnerabilities

Tighten our monitoring and testing regimes for early identification of cyber security threats.

LGRS/LGAAMF cyber security uplift program

4. Increase resilience and responsiveness

Strengthen our ability to respond and recover from cyber security threats and incidents.

 LGFSG, LGA and LGITSA engaged with DPC to streamline cyber threat notifications and intelligence LG Cyber Security Framework: A foundational initiative to identify and protect what matters

CYBER SECURITY GOVERNANCE STRUCTURE

Project Steering Group Monthly meetings	 Project Sponsor: Karin Swiatnik Product Owner: Daniel Brinkworth Project Manager: Richard Tyrcha (Cyber CX) Senior Supplier: Sarah Taylor (CyberCX) Advisor: Michael Billett (DPC) IT Auditor: David Powell (indept evaluation)
Project Team Fortnightly meetings	 Project Manager: Richard Tyrcha Project Officers: Alex, James Working Group Lead: Daniel Brinkworth Working Group: LGITSA members, Emily Wingard & Daniel Souter (DPC)
Project Assurance Meetings as needed	 LGITSA Committee LGITSA Special Interest Group Local Government Cyber Security Steering Group: LGA, LGRS, LGFSG, LGITSA IT Auditor: David Powell

LG Cyber Security Steering Group:

LGA (Nathan Petrus) LGRS (Anthony Genovese) LGFSG (Scott Loechel) LGITSA (Karin Swiatnik, David Carroll)

~ Quarterly meetings

LOCAL GOVERNMENT CYBER SECURITY FRAMEWORK PROJECT

Developed for Councils, by Councils

We know our Councils and our security challenges better than anyone else.

Standardised Language and Approach

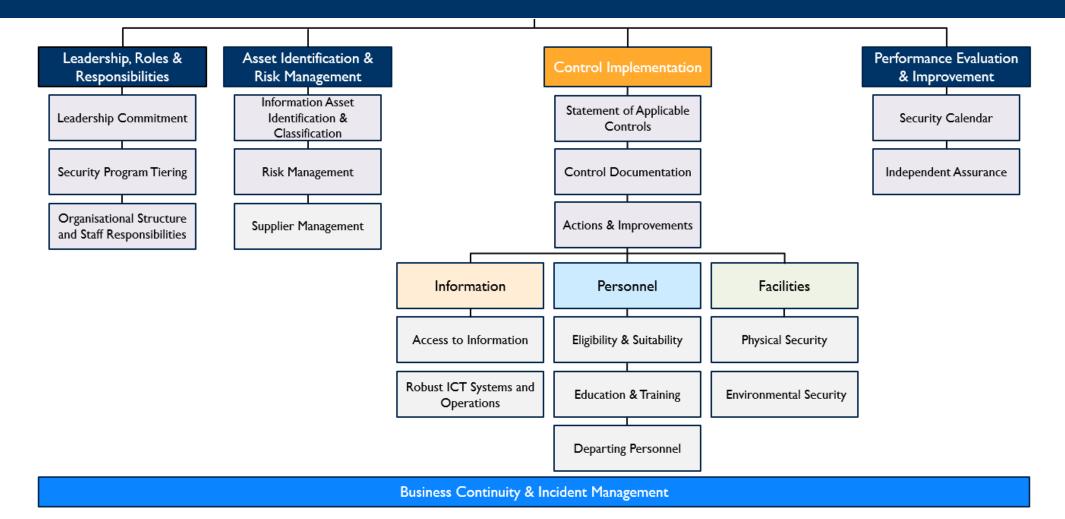
Creating consistency in security risk management practices between Local, State and Federal Government.

Demonstrable and Defensible Security Measures A guided approach to enable better visibility and tracking of our security risk posture

Project outcomes at a glance:

- A working group of representatives from Councils, the SA Department of the Premier and Cabinet, and our industry partner.
- A tiering model, giving us the flexibility to right-size our security controls based on the context and characteristics of our Councils.
- A simplified framework and guidelines for implementing and managing our security risks, based on proven industry standards.
- A toolkit and templates that we can leverage to document our security posture.

LOCAL GOVERNMENT SECURITY FRAMEWORK



LOCAL GOVERNMENT SECURITY TOOLKIT SUPPORTING DOCUMENTS, GUIDELINES AND TEMPLATES

Core Toolkit Documents:

- Implementation Toolkit
- Actions and Improvements Register
- Security Calendar
- Asset Inventory

'Model' Policies:

- Information Security Policy Manual
- Security Governance Policy
- End User Security Policy

		CONTROL IM	PLEMENTATION					
Statement of Applicable Controls	Controls necessa level should be o		or mitigate identified risks to an acceptable					
Control Documentation	Policies reflectin documented in t approved by ma employees and e	he Statement nagement, pu	Guidelines					
Actions & Improvements	Record and track improvement in		ired to address gaps or opportunities for rogram.					
Information	Maintain		iality, integrity and availability of all council formation and systems.					
Access Management	Enable appropria	ite access to o	council information.	Gui				
Robust ICT Systems & Operations			cesses supported by ICT systems through ation and operation of ICT systems.	Guidelines	toward expectations for han			
Personnel		Australian co	s, elected members, and volunteers are suit uncil resources and meet an appropriate star		classified as OFFICIAL: Sensit			
Eligibility & Suitability			bility of personnel who have access to prmation and assets) on an ongoing basis.					
Education & Training			ctors with information and training to liective responsibility to foster a positive	Guidelines	ion (including emails) within the council or externa			
Departing Personnel			sources when no longer required and cors of ongoing security obligations upon	35	neral. of this information could I			
Facilities	Provide a safe a assets.	nd secure phy	sical environment for people, information a	nd	ssets, or individuals. Example			
Physical Security		ouncil resour	easures that minimise the risk of harm to ces being accessed, used or removed	Guid	emails); ocedures;			
Environmental Security			urity measures that minimise the risk of il resources being made inoperable or	Guidelines	ases;			
			Information that is only available to auth relates to their job function or externally to which it relates. Unauthorised release could reasonably bi individual, organisation or government ge	with th	e relevant and specific third particular ted result in limited damage to			
	Se	FICIAL: nsitive onfidential)	information include: Financial information; Credic card information; Personal information of citizens; Personal information of council e Strategic jenning information (p Data protected by state or federa Data protected by non-disclosure Security assessment material (eg	mploye re-relea I regula	tes; ase); titions; fidentiality agreements; and			

Security Governance																		
vernance Model				- 11														
				- 84														
urity risk management is everyone's responsibility. rseen by the [Security Working Group] with a direct				ve able	of Conte													
ponsibility for security].				able of a	ontents								2					
diagram below shows the security governance stru	ture together with the inte	erfaces and		arpose.														
endencies within [Council]'s security program.					rsponsibilitie													
<example governance="" st<="" td=""><td>RUCTURE DIAGRAM></td><td></td><td></td><td></td><td>on Classifica fication and</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></example>	RUCTURE DIAGRAM>				on Classifica fication and													
	NOCTONE DIMONTANT				ity													
Local Government Se	nior Leadership			grity									6					
					Labeling													
Security Workir	g Group				ioning													
					Assets and b Media & M													
Security Pro					Mecha & M													
Owner				mation	Asset Handl	ing Guide	lines						9					
					entication P inistration													
Security Program Coordinator	Support & Advisory Groups				coess Manag													
Coordinator	Groups			tentica	ion								11					
					Standards													
gal and Regulatory Requirements				System	s Security								13					
uncil]'s legal and regulatory requirements for securi	ty risk management, and in	formation p	rivacy	work an	d Infrastruct													
d protection are documented in [Register].					tworks													
					ess													
					iselines													
				Server Base Mobile Dev														
				Mobile Dev Equipment	ce Baselines Maintenance	Baseline	5						15					
				Mobile Dev Equipment Threat & Vi	ce Baselines Maintenance Inerability N	Baseline lanageme	s							I				
				Mobile Dev Equipment Threat & Vi System Red Logging & P	ce Baselines Maintenance Inerability N andancy & D Ionitoring	Baseline Ianageme Igital Pres	s int servation							l				
				Mobile Dev Equipment Threat & Vi System Red Logging & P Cryptograp	ce Baselines Waintenance Inerability N andancy & D Ionitoring Y	Baseline lanageme igital Pres	ss int						15 15 16 16 16	l				
				Mobile Dev Equipment Threat & Vi System Red Logging & P	ce Baselines Waintenance Inerability N andancy & D Ionitoring Y	Baseline lanageme igital Pres	ss int						15 15 16 16 16	l				
				Mobile Dev Equipment Threat & Vi System Red Logging & P Cryptograp	ce Baselines Waintenance Inerability N andancy & D Ionitoring Y	Baseline lanageme igital Pres	ss int						15 15 16 16 16	l				
TSA Information Security Calendar				Mobile Dev Equipment Threat & Vi System Red Logging & P Cryptograp	ce Baselines Waintenance Inerability N andancy & D Ionitoring Y	Baseline lanageme igital Pres	ss int						15 15 16 16 16	l				
Tesk	/insponsibility	frequency		Mobile Dav Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Par	ce Baselines Meintenence Inerability IV andancy & D Jonitoring Y y Security IV	: Baseline lanageme igital Pres	sservation						15 15 16 16 16 17		War-23	Apr-23 1	May-23	Juni
Tesk Security Program Management Review Cyber Security Governance Framework	Insponsibility	Annual		Mobile Dav Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Par	ce Baselines Meintenence Inerability IV andancy & D Jonitoring Y y Security IV	: Baseline lanageme igital Pres	sservation		iep-22 (15 15 16 16 16 17		War-23	Apr-23	May-23	Juni
Task Security Program Manupament Environ Cyber Executly Governance Framework Review Information Asset Register Review Society Risk Register	/trepons dotty			Mobile Dav Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Par	ce Baselines Meintenence Inerability IV andancy & D Jonitoring Y y Security IV	: Baseline lanageme igital Pres	sservation						15 15 16 16 16 17		War-23	Apr-23 1	May-23	Juni
Table Security Program Management Review Cyber Security Governance Framework Pervew Information Asset Degater Frameworksert/Pikal Register	Tergoon killy	Annual Annual		Mobile Dav Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Par	ce Baselines Meintenence Inerability IV andancy & D Jonitoring Y y Security IV	: Baseline Ianageme Igital Pres	sservation		lep-22 (15 15 16 16 16 17		Wer-23	Арт-23	May-23	Juni
Tesk Second Pergram Merconnect Second Pergram Merconnect Nerver (Que Second public Nerver (Second And Pergram Nerver Second Pergram Nerver Second Pergram Second Pergram Set Assessment Second Pergram Set Assessment	Inspendelly	Annual Annual Annual Annual Annual 2-years		Mobile Dav Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Par	ce Baselines Meintenence Inerability IV andancy & D Jonitoring Y y Security IV	: Baseline Ianageme Igital Pres	sservation		іер-22 (Р Р	et-22 No			15 15 16 16 16 17		Mar-23	Apr-23	May-23	Jan;
Test Constry Program Management Neuron Coper Security Sovemans of Thermonics Neuron Variandia Anna Margane Neuron Sovement The Apolathy Neuron Theorem The Apolathy Neuron Theorem The Apolathy Neuron Theorem Theorem Theorem Theorem Theorem Theorem Neuron Actions of Apolatory Neuron Actions of	Inspectability	Annual Annual Annual Annual Annual 2-years Monthy Monthy		Metalle Dev Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Pari	ce Baselines Maintenance Interability IV andancy & D Ionitoring ry y Security IV 32 May-22 P P	: Baseline Ianageme Igital Pres	5 servation Jul-32 P P	Aug-22 1	іер-22 (Р Р	et-22 No P		-22 Jan			Mar-23	Apr-23 1 P P	P P	Jun-i P P
Exis Concryt Program Management Exempt Operating Management		Annual Annual Annual Annual Annual Annual 2-years Meethy Meethy Mosthy	Peti-22	Mobile Dev Equipment Threat & Vi System Rec Logging & P Cryptograps 5. Third Part	ce Baselines Maintenance Interability IV andancy & D Ionitoring ry y Security IV 32 May-22 P P	Baseline lanageme lanageme Jam22	Jail-22 P	Aug-22 1	P P P	et-22 No		-22 Jan		6-23 M		•	P	•
Text Concern Sprage Management Concern Concern Sprage Concern Conce	Policy Owners	Annual Annual Annual Annual Annual Annual Zyeers Meethy Meethy Meethy Yeary	Peti-22	Metalle Dev Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Pari	ce Baselines Maintenance Interability IV andancy & D Ionitoring ry y Security IV 32 May-22 P P	Baseline lanageme lanageme Jam22	5 servation Jul-32 P P	Aug-22 1	P P P	et-22 No		-22 Jan		6-23 M		•	P	•
Test Details Advancement Details Advancement Reverse Security Wards Reverse Security Wards Reverse Security Wards Reverse Advancement Reverse Advance		Annual Annual Annual Annual Annual Annual 2-years Meethy Meethy Mosthy	Peti-22	Metalle Dev Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Pari	ce Baselines Maintenance Interability IV andancy & D Ionitoring ry y Security IV 32 May-22 P P	Baseline lanageme lanageme Jam22	S	Aug-22 1	P P P	et-22 No		-22 Jan		6-23 M		•	P	•
Source for prevent the encourse of the en	Palay Owners Procedure Owners	Annual Annual Annual Annual 2-years Meetiky Meetiky Meetiky Vearly Vearly Vearly	Peti-22	Metalle Dev Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Pari	ce Baselines Maintenance Interability IV andancy & D Ionitoring ry y Security IV 32 May-22 P P	Baseline lanageme lanageme Jam22	s	Aug-22 1	P P P	et-22 No		-22 Jan		6-23 M	P P P	•	P	•
test Execution Secure Associated Event Security Securi	Palay Owners Procedure Owners	Annual Annual Annual Annual Annual 2-yeedy Monthy Monthy Monthy Monthy Monthy Monthy Monthy Yearty Yearty	Peti-22	Metalle Dev Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Pari	ce Baselines Maintenance Interability IV andancy & D Ionitoring ry y Security IV 32 May-22 P P	Baseline lanageme lanageme Jam22	s	Aug-22 1	P P P	к(-22 Мо Р Р Р Р Р Р		-22 Jan		6-23 M	P P P	•	P	•
test testers fasters and kandpasses testers fasters and kandpasses testers fasters and kandpasses testers fasters fasters testers fasters fasters testers fasters fasters testers tester	Palay Owners Procedure Owners	Annual Annual Annual Annual Annual 2-years Meethy Meethy Vearty Vearty Vearty Vearty Wearty Meethy Meethy Guidenty Custerity	Peb-22	Metalle Dev Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Pari	ce Batelines Weitenen Innarabily B. De Ionitoring Y. Y. ZZ Mer-ZZ Mer-ZZ P P P P P P	Baseline lanageme lanageme Jam22	s	Алд-22 1 Р Р Р Р Р	P P P	P P P P P P P P P P P P P P P P P P P	P P P P P P P P P P P P P P P P P P P	-22 Jan		P P P	P P P	•	P P	•
Internet Control Contr	Petry Desers Product Ownes Product Ownes Petry & Cuber / Durin Resercts	Annual Annual Annual Annual Annual Annual Annual Meethy Meethy Meethy Veery Veery Veery Veery Veery Annual Custony a Custony a Custony	Peb-32	Metalle Dev Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Pari	ce Baselines Wintensnen Indrahry & D Iontoning, Y,	Baseline lanageme lanageme Jam22	s	Аюд 22 [Р Р Р Р	P P P	P P P P P P P P P P P P P P P P P P P	P P F	-22 Jan		P P P	P P P	•	P P P	•
International Control	Palay Overas Presidenti Overas Presidenti Overas	Annual Annual Annual Annual Annual Annual Annual Meethy Meethy Yearly Yearly Yearly Weethy Yearly Meethy Quartedy Guartedy Boundary Counterfy Boundary	Peb-32	Metalle Dev Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Pari	ce Baselines Wintensnen Indrahry & D Iontoning, Y,	Baseline lanageme lanageme Jam22	s	Аюд 22 [Р Р Р Р	P P P	P P P P P P P P P P P P P P P P P P P	P P F	-22 Jan		P P P	P P P	•	P P P	•
Heat Market Start Start Start Start Start Start Start Start Start Start Start Start Start Start	Petry Desers Product Ownes Product Ownes Petry & Cuber / Durin Resercts	Annual Annual Annual Annual Annual 2-years Meethy M	Peb-32	Metalle Dev Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Pari	ce Baselines Wintensnen Indrahry & D Iontoning, Y,	Baseline lanageme lanageme Jam22	s	Аюд 22 [Р Р Р Р	P P P	P P P P P P P P P P P P P P P P P P P	P P F	-22 Jan		P P P	P P P	•	P P P	•
Here Example of the second s	Petry Desers Product Ownes Product Ownes Petry & Cuber / Durin Resercts	Annual Annual Annual Annual Canadi Canadi Beethy Beethy Beethy Beethy Veary Veary Veary Veary Veary Veary Nearly Ouestedy Annual Annual Annual Ouestedy	Peb-22	Möbis Den Kaya (1996) Mari 20 (1996) Mari	ce Baselines Mainteannes Jacobie Jacob	Baseline lanageme lanageme Jam22	S	A0322 1 P P P P P	P P P P P P P P P P P P P P P P P P P	еt-22 Вю Р Р Р Р Р Р Р	A-22 Dec		-23 Pe	0-23 F P P P P	P P P	р Р Р	P P P P P	•
	Petry Desers Product Ownes Product Ownes Petry & Cuber / Durin Resercts	Annual Annual Annual Annual 2-years Meethy Neethy Veary Veary Veary Veary Veary Neethy Annual	Peb-32	Metalle Dev Equipment Threat & Vi System Red Logging & P Cryptograp 5. Third Pari	ce Baselines Mainteannes Jacobie Jacob	Baseline lanageme lanageme Jam22	s	A0322 1 P P P P P	P P P P P P P P P P P P P P P P P P P	еt-22 Мо Р Р Р Р Р Р	P P F		-23 Pe	0-23 F P P P P	P P P	•	P P P	•
	Petry Desers Product Ownes Product Ownes Petry & Cuber / Durin Resercts	Annual Annual Annual Annual 2-yens Meethy Heethy Veary Veary Veary Veary Veary Veary Veary Annual An	Peb-22	Möbis Den Kaya (1996) Mari 20 (1996) Mari	ce Baselines Mainteannes Jacobie Jacob	Baseline lanageme lanageme Jam22	S	A0322 1 P P P P P	P P P P P P P P P P P P P P P P P P P	еt-22 Вю Р Р Р Р Р Р Р	A-22 Dec		-23 Pe	0-23 F P P P P	P P P	р Р Р	P P P P P	•
	Petry Desers Product Ownes Product Ownes Petry & Cuber / Durin Resercts	Annual Annual Annual Annual Annual 2-yaws Meethy Meethy Yeavy Yeavy Yeavy Yeavy Yeavy Yeavy Yeavy Yeavy Yeavy Yeavy Annual Annua	Peb-22	Möbis Den Kaya (1996) Mari 20 (1996) Mari	ce Baselines Mainteannes Jacobie Jacob	Baseline lanageme lanageme Jam22	S	P P P P P P P P P P P P P P P P P P P	P P P P P P P P P P P P P P P P P P P	еt-22 Вю Р Р Р Р Р Р Р	A-22 Dec		-23 Pe	0-23 F P P P P	P P P	р Р Р	P P P P P	•
	Petry Desers Product Ownes Product Ownes Petry & Cuber / Durin Resercts	Annual Annual Annual Annual Annual Annual Veary Veary Veary Veary Veary Veary Annual Annual Annual Annual Annual Annual	Peb-22	Möbis Den Kaya (1996) Mari 20 (1996) Mari	ce Baselines Mainteannes Jacobie Jacob	Baseline lanageme lanageme Jam22	S	A0322 1 P P P P P	P P P P P P P P P P P P P P P P P P P	еt-22 Вю Р Р Р Р Р Р Р	A-22 Dec		-23 Pe	0-23 F P P P P	P P P	р Р Р	P P P P P	•
	Petry Desers Product Ownes Product Ownes Petry & Cuber / Durin Resercts	Annual Annual Annual Annual Annual Annual Annual Veary Veary Veary Veary Veary Veary Veary Annual Annual Annual Annual Annual Annual Annual	Peb-22	Möbis Den Kaya (1996) Mari 20 (1996) Mari	ce Baselines Mainteannes Jacobie Jacob	Baseline lanageme lanageme Jam22	S	P P P P P P P P P P P P P P P P P P P	P P P P P P P P P P P P P P P P P P P	еt-22 Вю Р Р Р Р Р Р Р	A-22 Dec		-23 Pe	0-23 F P P P P	P P P	р Р Р	P P P P P	•

Council Case Study: Experiences in establishing a cyber security framework at <u>CoPAE</u>

NEXT FOCUS AREAS

I. Protect what matters

 Third parties: inclusion of cyber security clauses and protections into ICT Panel supplier contracts (LGITSA/LGAP)

2. Create a cyber aware culture

 Framework adoption: training sessions, further promotion, and support for implementation (LGITSA/LGRS/CyberCX)

 Education and training program: including Executive preparedness (LGA/LGITSA/JCSC)

3. Proactively identify vulnerabilities

- Shared delivery: exploring a coordinated approach to cyber security activities and platforms (LGITSA/LGAP)
- Seeking to onboard Local Government to the Australian Protected Domain Service (LGITSA/DPC)
- Monitoring the critical infrastructure bill (JCSC/LGA/LGITSA)

4. Increase resilience and responsiveness

Exploring a potential Local Government deed for all councils to access to the JCSC network partnership

Ongoing guidance, support and collaboration

Formation of LGITSA Cyber Security Special Interest Group

THANKYOU TO OUR PARTNERS AND CONTRIBUTORS

Adelaide Hills Council Adelaide Plains Council City of Adelaide City of Charles Sturt City of Holdfast Bay City of Marion City of Onkaparinga City of Playford City of Port Adelaide Enfield

City of Prospect City of Tea Tree Gully City of Unley City of Victor Harbor Mount Barker District Council Port Augusta City Council Tatiara District Council The Rural City of Murray Bridge Whyalla City Council

LGA, R&D Scheme LG Professionals LGRS / LGAAMF LGFSG LGA Procurement LGITSA CyberCX IT Auditor. David Powell Office for Cyber Security, DPC Auditor-General's Department Joint Cyber Security Centre (JCSC)



CYBER SECURITY IS EVERYONE'S RESPONSIBILITY