



**LGITSA**

---

# 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*





*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 <sup>1</sup>	Strategic Priorities	Initiatives	Potential LGITSA Partners	Existing Capabilities & Resources
<b>Security Governance</b> Strategy Policies & procedures Cyber awareness Third parties Risk management Audits  <b>System Security</b> Passwords Privileged accounts User access Vulnerability management  <b>Change Management</b> Change management policy Vendor change management Patch management  <b>Backup Operations, Disaster Recovery &amp; Incident Response</b> Disaster recovery Business Continuity Plan Incident response  <b>Vulnerability assessment</b> External website	<b>1. Protect what matters</b>  Formalise and implement business driven and risk-based processes and procedures for protection	<ul style="list-style-type: none"> <li>• Governance – Leverage existing government resources to develop a fit for purpose toolkit including strategy, framework, and policies for the sector</li> <li>• Third parties – Develop clauses for standard tendering, procurement documentation, and certification of purchased items</li> <li>• Supplier panel – Provide a cyber panel for purchasing of software, hardware and services</li> <li>• Insurance coverage – Tailor insurance policy needs to risk levels</li> </ul>	LGA LG Procurement LGRS LG R&D Scheme	<ul style="list-style-type: none"> <li>• Existing frameworks (DPC – SA Cyber Security Framework, ACSC – Essential 8 and ISM)</li> <li>• Model policies (LGA)</li> <li>• Advocate, assist &amp; advance (LGA)</li> </ul>
	<b>2. Create a cyber aware culture</b>  Promote cybersecurity awareness through fit for purpose governance and an ongoing and engaging training program	<ul style="list-style-type: none"> <li>• General awareness – Promote the cyber security toolkit and common terminology</li> <li>• Training and skills development – Provide training for Executive awareness, and skills development for end users, Elected Members and IT staff</li> <li>• Testing – Regularly assess the cyber security and policy awareness of council staff</li> <li>• Education - Facilitate sector-wide education on cyber security threats and mitigation strategies</li> </ul>	LGA LGRS LG Professionals AGD	<ul style="list-style-type: none"> <li>• Procurement (LGAP)</li> <li>• ICT Vendor Panel (LGAP)</li> <li>• Insurance (LGRS)</li> <li>• Skytrust (LGRS)</li> <li>• VOCAM LMS (LGRS)</li> <li>• Examination reports (AGD)</li> <li>• IT expertise (LGITSA)</li> </ul>
	<b>3. Proactively identify vulnerabilities</b>  Tighten our monitoring and testing regimes for early identification of cybersecurity threats	<ul style="list-style-type: none"> <li>• Baseline audit – Undertake audits to identify individual council improvement plans</li> <li>• Improvement plans – Support the implementation of improvement plans to increase maturity</li> <li>• Critical infrastructure – Identify key community infrastructure (e.g. pumping stations, traffic control, monitoring devices, etc) and certification of the systems for cybersecurity</li> </ul>	LGRS LGA	<ul style="list-style-type: none"> <li>• Yammer network (LGITSA)</li> <li>• Special Interest Group (LGITSA)</li> <li>• Conferences &amp; workshops (LGITSA)</li> <li>• Watch Desk (DPC)</li> <li>• Joint operating guideline (LGSFG/DPC)</li> </ul>
	<b>4. Increase resilience and responsiveness</b>  Strengthen our ability to respond and recover from cybersecurity threats and incidents	<ul style="list-style-type: none"> <li>• Threat intelligence – Form partnerships with government agencies for subscription alerts</li> <li>• Responsiveness - Share real-time updates on threat intelligence</li> <li>• Incidents – Develop relationships with relevant cybersecurity agencies and promote reporting of incidents, and include incident response playbooks in the cyber security toolkit</li> </ul>	LGA DPC LGFSG ACSC	<ul style="list-style-type: none"> <li>• Funding (LGRS, LG R&amp;D Scheme)</li> </ul>

Provide ongoing guidance, support and collaboration for continuous improvement

# STRATEGIC PRIORITIES & KEY INITIATIVES

## 1. 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

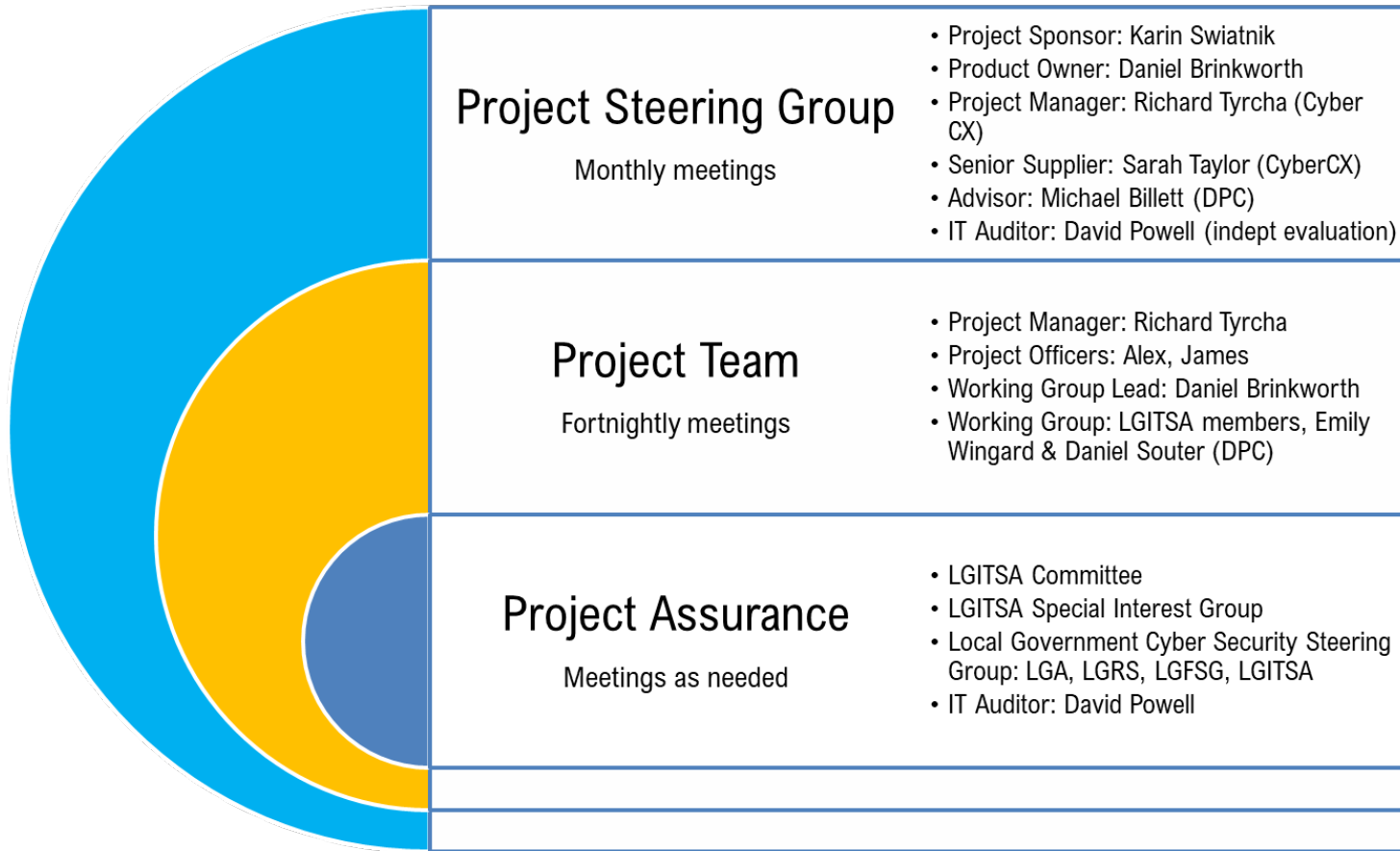


# LG Cyber Security Framework:

*A foundational initiative to identify  
and protect what matters*



# CYBER SECURITY GOVERNANCE STRUCTURE



**LG Cyber Security Steering Group:**

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

*~ Quarterly meetings*

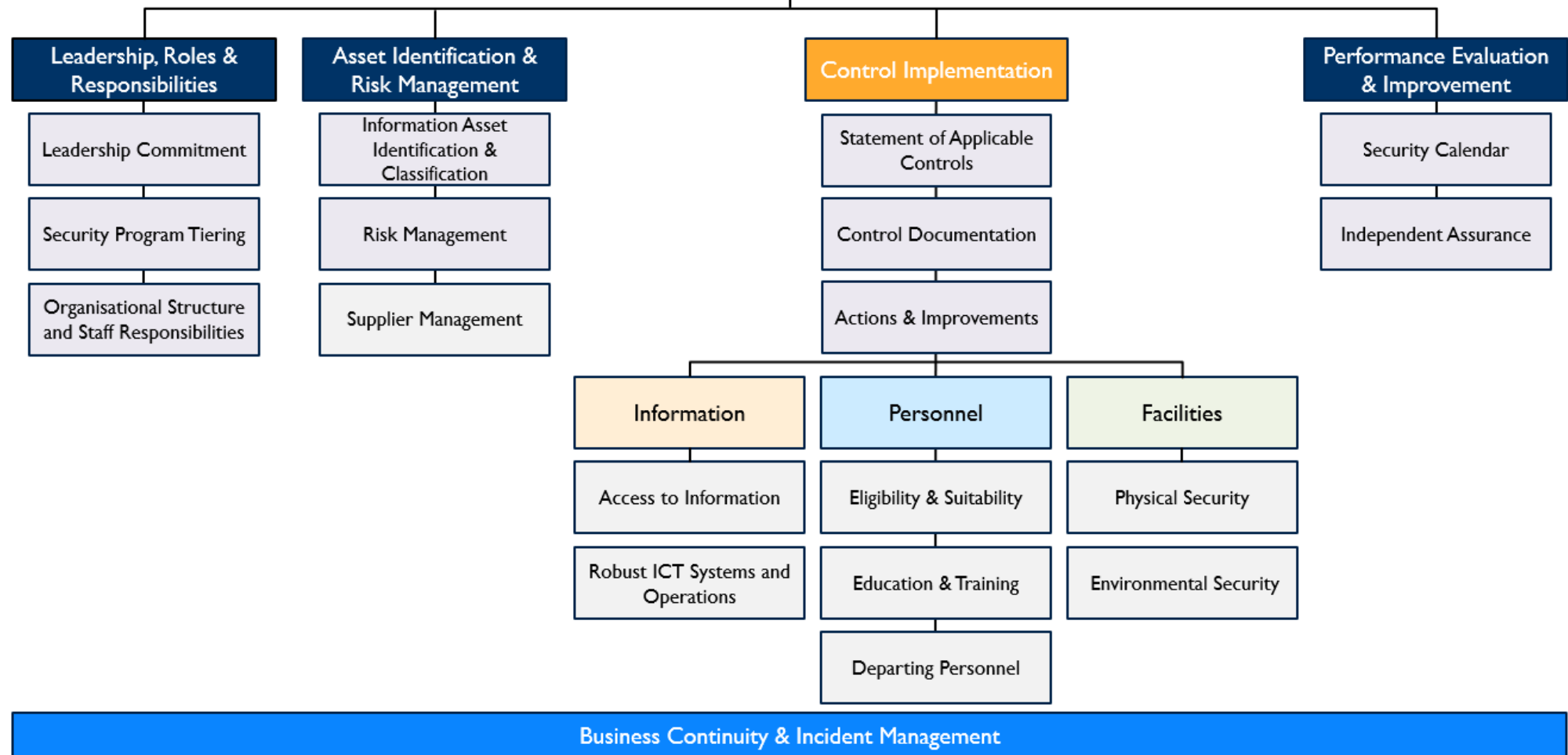
# LOCAL GOVERNMENT CYBER SECURITY FRAMEWORK PROJECT



## *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










**Council Case Study:**  
*Experiences in establishing a cyber  
security framework at CoPAE*



# NEXT FOCUS AREAS

## 1. 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)  
A3C



**LGITSA**

---

CYBER SECURITY IS  
EVERYONE'S RESPONSIBILITY