



ICT, Cyber Security and Digital Government Strategy plan for 2020 to 2025

Progress update for 2023



Government
of South Australia

Department of the
Premier and Cabinet

ICT, Cyber Security and Digital Government Strategy Reporting

Status update for 2023

The Office of the Chief Information Officer (OCIO), within the Department of the Premier and Cabinet (DPC), leads the South Australian (SA) Government's technology, cyber security and digital government strategies and policies and is the central service provider for whole of government technology and cyber security services and platforms.

The ICT, Cyber Security and Digital Government Strategy outlines the aspirations and deliverables for South Australia over five years, from 2020 to 2025. The strategy is presented through the lens of four key principles that guide our actions, and three priorities to enable the state to be: 1) accessible and inclusive, 2) collaborative, and 3) secure and trusted. These priorities are underpinned by internal enablers.

In August 2023, DPC conducted an internal review of their structure to better reflect the state's Strategic Direction. As a result, the Major Programs division became the Chief Operating Officer division within DPC, with Digital Programs leading a transformation program that revolutionises the provision of digital services to citizens and businesses.

This report provides a status update on achievements made by OCIO and Digital Programs against the strategy in 2023 and outlines the priorities for 2024.

Priority areas 2022/23

The priority areas for Office of the Chief Information Officer and Digital Programs (formerly Major Programs Division) and the achievements as of December 2023.



Priority area	Update
1. Provide more inclusive access and seamless service delivery for citizens and businesses to securely interact with government online.	This priority was achieved and reported on in the 2021 Progress update report.
2. Build resilience and improve protection of government assets and data.	<p>Achieved</p> <p>In collaboration with the Department of Home Affairs, the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC), supported the 'Act Now, Stay Secure' initiative. This joint initiative features a co-branded awareness campaign developed by the South Australian Government and the ACSC. The campaign provides straightforward cyber security advice for government, business and individuals.</p> <p>Recruited positions in the field of Cyber Threat Intelligence to manage and enhance our cybersecurity intelligence function to increase the security posture of the SA Government.</p> <p>To support SA Government agencies in effectively managing their cybersecurity risks, new guidance documents and templates have been released under the SA Cyber Security Framework (SACSF).</p> <p>Department of the Premier and Cabinet (DPC) appointed the Cyber Hazard Risk Reduction Leader under the state emergency management arrangements and completed a state-wide risk assessment for cyber risks.</p>

Priority area	Update
	<p>In progress and Ongoing</p> <p>Development of the South Australian Government Cyber Threat Intelligence Framework to empower intelligence lead risk decision making for safeguarding South Australia from cyber threats.</p> <p>Approval of the Cyber Crisis Hazard Risk Reduction Plan in June 2023, which is the overarching framework for cyber hazard mitigation.</p> <p>Major review of the SACSf is in progress with work continuing to support agencies with their implementation of the Framework.</p> <p>Designed and delivered a series of cyber attack exercises to help agencies get ready for real-life cyber attacks. These exercises tested agencies' ability to plan, prepare, and respond to cybersecurity incidents.</p> <p>Maturity uplift for the Cyber Security Watch Desk including delivery of an Annual Training program (cyber crisis planning, preparedness and response exercises).</p> <p>Significant progress on improving SA Government's security posture through increased monitoring and incident response capabilities to protect government data.</p> <p>Formed a whole of government cyber security Community of Practice to bring together cyber security practitioners at all levels of seniority to share work and information and collaborate on issues.</p> <p>Facilitated configuration reviews and risk assessments on some whole of government services provided by OCIO which helped to fix vulnerabilities and implement good security processes for ongoing management.</p>
<p>3. Enable a connected, productive government, underpinned by the central M365 tenancy.</p>	<p>Achieved</p> <p>Approval of the State's Connectivity Infrastructure Strategy by the Chief Executive Council in November 2021.</p> <p>Further deployment of M365 capabilities to protect the state's people and information assets.</p>

Priority area	Update
	<p>Power Platform resources including the Governance Framework, Security Baseline Standard, Monitoring and Compliance guideline and supporting documents have been endorsed and made available for use by agencies.</p> <p>In progress</p> <p>Implementation of the M365 Operating Model to automate and improve security, productivity and collaboration in the central M365 tenancy, as part of Aspirations 1.3 and 2.8.</p> <p>High-level and detailed reporting for agency resource utilization of M365, cloud computing and MBCS resources.</p> <p>Ongoing</p> <p>Establishment of M365 Operating Model Working Group, comprising agency IT and service desk staff</p> <p>Design and implementation of data retention, loss prevention and associated M365 information management products and services. Remediation of identified risks and issues.</p> <p>Working in partnership with agencies to leverage whole of government licences increasing agency usage of M365 capabilities and tools across agencies.</p>
4. Enable modern communications services.	Refer to Aspirations 1.4 and 2.8 Deliver Enterprise Voice solutions based on agency user personas for consolidated investment, economy of scale and value realisation.
5. Enable government with modern network architecture and capabilities.	This priority was achieved and reported on in the 2021 Progress update report.

1. Accessible and Inclusive

Design and deliver technology, cyber security and digital services that are accessible and meet the needs of South Australian businesses, community and government.



Services to SA's Businesses and Community by 2023

Aspiration	Status
<p>1.1 Deliver improved citizen and business interactions with Government via Serving South Australia – One Stop Shop for Government Services, in partnership with agencies.</p> <p>(Digital Programs)</p>	<p>In Progress</p> <p>The Major Programs division became the Chief Operating Officer division within DPC, with Digital Programs leading a transformation program that revolutionises the provision of digital services to citizens and businesses.</p> <p>As part of the One Stop Shop initiative (previously SA Government Services Portal initiative), Digital Programs have progressively improved citizen and business interactions with Government through the delivery of:</p> <ul style="list-style-type: none"> • 12 government services that have been digitised following the consistent application of best practice user experience principles. • 32 new pages linking to services in SA.GOV.AU, the central whole of government website, reducing duplication and improving trust in the services the Government provides. • A beta SA.GOV.AU dashboard has been launched providing citizens a central location to view credentials and the status of their applications in real time. • A whole of government digital identity exchange has been launched into production providing the foundation for connection to myGovID. • Housing SA is now the first South Australian Government agency to connect to myGovID, allowing customers to access the Housing Connect portal using the federal identity.

Aspiration	Status
<p>1.2 Support agencies to design new services incorporating digital inclusion, architecture principles and security from the start. (Office of the Chief Information Officer and Digital Programs).</p>	<p>Ongoing</p> <p>Whole of Government Architecture Review Group (ARG) sessions are held weekly with SA Government agency architects to review solution designs and ensure systems are developed using best practices that align with whole of government ICT strategy, cyber security and architecture standards.</p> <p>Agencies are adopting endorsed enterprise architectural patterns, reference architectures, standards and guides within their own agencies to benefit from tested and robust patterns and comply with best practice approaches which are available for whole of government use.</p> <p>New communication and governance forums are being established as the need arises to support adoption, knowledge sharing and rapid maturity across agencies. This includes:</p> <ul style="list-style-type: none"> • A Domain Architects community of practice as well as an Enterprise Architects community of practice for IT and Enterprise Architects across SA Government to share knowledge and practices. • A Microsoft 365 Power Platform community of practice was launched in August 2022 and is open to all SA Government staff with an interest in leveraging the benefits of the Power Platform suite of products. This group now has over 360 active members. <p>The Power Platform Governance Framework was approved by the Chief Information Officers Steering Committee in November 2022 and is designed to provide an overarching governance structure for the Power Platform within the SA Government M365 Central Tenancy. Agencies can build upon the Framework by developing their own supplementary agency-level Power Platform governance that aligns with their existing digital and data transformation strategies.</p> <p>Through the One Stop Shop initiative, a design system has been established for digital transactions, following the look and feel of SA.GOV.AU. The design system leverages industry best practice for digital user experience and has been user-tested. The design system has been implemented in the whole-of-government forms platform and is available for agency use in other technologies.</p>

Aspiration	Status
	<p>The whole-of-government identity broker is in production with the first South Australian agency onboarded to myGovID. Other agencies are expected to onboard this identity provider to provide customers with a consistent and secure method to verify themselves digitally to access services.</p>
<p>1.3 Deliver high speed, low cost, ubiquitous connectivity across more of South Australia. (Office of the Chief Information Officer)</p>	<p>In progress</p> <p>To complement the State's Connectivity Infrastructure Strategy, the draft State Connectivity Investment Strategy has been developed to align connectivity investment prioritisation and decision making across the state. The strategy will inform future funding requests and decisions from a variety of sources including Commonwealth, state and local government and telecommunications service providers, to deliver better access to internet, data and voice in our communities across the state.</p> <p>The Telecommunications Services Marketplace new panel arrangements have been established to deliver better outcomes for government's connectivity across the state and contribute to ubiquitous and seamless delivery of services.</p> <p>The State core data network is being upgraded to enable adoption of modern applications and systems by agencies.</p> <p>Consolidation of firewalls and gateway upgrades are significantly increasing the internet bandwidth to reflect a growing demand and reliance on external services including cloud based services.</p> <p>The SD-WAN business case was approved by the Chief Information Officers Steering Committee in September 2023 and implementation is underway. This, together with Secure Access Service Edge (SASE), will provide a common connection point between carrier providers and SA Government networks affording greater business certainty.</p> <p>SA Government's progression towards a Zero Trust network, as part of the SD-Wan pilot, is contributing to more mature security posture and secure mobility for staff in regional and remote locations to access core government services.</p>



Accessible and Inclusive – Services to SA Government by 2023

Aspiration	Status
<p>1.4 Consistent user experience in transacting with government (between in-person, online etc), including the extension of operating hours in Service SA centres</p>	<p>Ongoing</p> <p>Through the One Stop Shop initiative, a design system has been established for digital transactions, following the look and feel of SA.GOV.AU. The design system leverages industry best practice for digital user experience and has been user tested. The design system has been implemented in the whole of government forms platform and is available for agency use in other technologies.</p> <p>The whole of government identity broker is in production with the first South Australian agency onboarded to MyGovID. Other agencies are expected to onboard to this identity provider to provide customers a consistent and secure method to verify themselves digitally in order to access services.</p> <p>Service SA have extended operating hours to open on Saturdays in May 2023 across Service Centres in Elizabeth, Marion, Modbury, Prospect and Seaford Meadows offering more convenience for customers.</p>
<p>1.5 Deliver Enterprise Voice solutions based on agency user personas for consolidated investment, economy of scale and value realisation.</p> <p>(Office of the Chief Information Officer)</p>	<p>Ongoing</p> <p>Continue to modernise solutions and look to retire ageing on-premise equipment, migrate agencies to platforms that allow for flexible working arrangements and improve engagement with customers.</p> <p>Continuing the migration of traditional on-premise PBX to a Microsoft Teams Voice service together with the adoption of online contact centres for agency service desks. The Microsoft Teams Phone system consumption continues to grow for knowledge worker base whilst on-premise PABX services the Health and emergency services sector. Long term support arrangements are being established for these services.</p>

Aspiration	Status
	<p>The Enterprise Voice Strategy (EVS) has been implemented and continues to be an ongoing process to expand to 12,000 Teams Voice services.</p> <p>EVS service resilience assessments will be redeveloped, with a focus on business continuity planning and investment requirements.</p>
<p>1.6 Active communities of practice across government, informing better ways of delivering services.</p> <p>(Office of the Chief Information Officer and Digital Programs)</p>	<p>Ongoing</p> <p>Communities of practice (CoP) have been established to bring together groups of people with a common interest to connect, share knowledge and best practice. OCIO supports several information technology Communities of Practice (CoP), sharing capabilities between employees, contractors, vendors and partners. These include:</p> <ul style="list-style-type: none"> • Azure CoP • Cyber Security CoP • Data centre exit planning CoP • Domain Architects CoP • Enterprise Architects CoP • Intune Endpoint Management CoP • Microsoft 365 adoption CoP • Microsoft 365 Power Platform CoP • Microsoft 365 SharePoint CoP • Secure collaboration CoP • Online Accessibility CoP • Online Forms CoP <p>OCIO will continue to add more Communities of Practice as required.</p> <p>This is also an enabler – refer to enabler 8.</p>

Aspiration	Status
<p>1.7 Provide a robust set of whole of government digital platforms, including surveys, community engagement, forms, websites and others as required.</p> <p>(Office of the Chief Information Officer and Digital Programs)</p>	<p>Ongoing</p> <p>OCIO provides services so that South Australian Government agencies can better service our community – we deliver resilient and innovative ICT services:</p> <ul style="list-style-type: none"> • YourSAy – community collaboration platform • iApply – online forms platform (Digital Programs) • SA government website design system (Digital Programs) • Accessibility toolkit (Digital Programs) • An existing platform tool to undertake surveys. <p>This item is also an enabler – refer to enabler 9.</p>



2. Collaborative

Enable government innovation, efficiency and effectiveness through the provision of the latest digital collaboration tools, to produce better outcomes and services for citizens and businesses.

Services to SA's Businesses and Community by 2023

Aspiration	Status
<p>2.1 Meaningful and streamlined engagement with the ICT industry through presentations at various forums to share SA Government's priorities and opportunities, aligned with an outcomes-based, early engagement approach.</p> <p>(Office of the Chief Information Officer)</p>	<p>Ongoing</p> <p>An OCIO Industry Forum was held in December 2022 – 'Progress against the ICT, Cyber Security and Digital Government Strategy 2020-2025'. An Industry Forum was held in November 2023 – 'Priorities update'. These forums provide opportunities for industry and government to continue to build and develop partnerships.</p> <p>Department of the Premier and Cabinet (through OCIO) partnered with the Public Sector Network to support their Innovate SA event in June 2023, which brought together public sector leaders in data, ICT, digital, and cyber security with technology providers to share recent challenges and successes and to explore the innovative work being delivered across the state.</p> <p>OCIO periodically invites partners and suppliers to SA Government to present at Executive Briefings to ensure awareness of their latest offerings and services. As the largest single customer in SA, it is critical that we are a well informed and respectful customer and take the effort to understand and learn what is possible so that we can be better informed as we make decisions about the services we deliver to the community. Multiple Executive Briefings were facilitated by OCIO in 2023. Note that partners and suppliers must be on at least one SA Government procurement panel in order to be eligible to deliver an executive briefing to SA Government in consultation with OCIO.</p> <p>OCIO uses the YourSAy platform to seek feedback on our initiatives and consultations.</p>

Aspiration	Status
<p>2.2 Co-design initiatives with strategic ICT, digital and/or cyber security suppliers to deliver social and economic benefit to the state. (Office of the Chief Information Officer)</p>	<p>Ongoing</p> <p>OCIO continues to engage with industry and suppliers across the State and in Australia more broadly.</p> <p>Subject to procurement policy, OCIO contract with many organisations across the Nation and especially in South Australia.</p> <p>OCIO holds regular 'Industry Forums' where we engage with our Industry colleagues about matters of interest to Government. OCIO also regularly hosts of 'Industry briefings' to enable suppliers to advise the State on the services it provides.</p> <p>OCIO uses a variety of project methodologies to undertake its strategic and business goals. Our ICT and Cyber program co-designs solutions together with suppliers and with the involvement of our customers/users, mostly SA Government agencies.</p> <p>The draft Statewide Connectivity Investment Strategy presents a coordinated strategic and whole-of-government approach to connectivity investment decisions in South Australia to address existing connectivity gaps and to leverage and benefit from state and federal government and private sector funding sources including First Nations people.</p> <p>An Artificial Intelligence (AI) Working Group has been established to provide recommendations to the Chief Information Officers Steering Committee about an appropriate AI governance approach for SA Government.</p> <p>This Group is engaging with third parties to understand and inform the requirements for a whole of government AI Strategy, AI Ethics policy and AI Assurance Framework and leverage insights and expertise of industry.</p> <p>OCIO, in partnership with five nominated agencies and two vendors, conducted a SD-WAN pilot to assess SD-WAN technology platforms and SASE technology to determine the most suitable solution for agencies.</p>

Aspiration	Status
<p>2.3 Lead the development of easily consumable services that make it easy for businesses to use a digital identity (partner with Commonwealth, agencies, business etc. to develop).</p> <p>(Office of the Chief Information Officer and Digital Programs)</p>	<p>In progress</p> <p>A beta SA.GOV.AU dashboard has been launched providing citizens a central location to view credentials and the status of their applications from a range of Government agencies in real time.</p> <p>A whole of government digital identity exchange has been launched into production providing the foundation for connection to myGovID.</p> <p>Housing SA is now the first South Australian Government agency to connect to myGovID, allowing customers to access the Housing Connect portal using the federal identity. Further agencies are expected to onboard.</p>



Collaborative - Services to SA Government by 2023

Aspiration	Status
<p>2.4 Continue to mature the model for service transformation to enable widespread agency adoption of and capability to transform service delivery for citizens and businesses.</p> <p>(Digital Programs)</p>	<p>In progress</p> <p>SA.GOV.AU continues to be developed as a single, online entry point for the digital delivery of a range of government services.</p> <p>32 new pages linking to services have been created within the website, reducing duplication and improving trust in the services the Government provides.</p> <p>A whole of government online forms design uplift has been implemented which aligns the online forms platform with best practice and is available for use in other form building technology platforms.</p>
<p>2.5 Expand the identity ecosystem to encompass other sectors, including finance and retail.</p> <p>(Digital Programs)</p>	<p>In progress</p> <p>A whole of government digital identity exchange has been launched into production providing the foundation for connection to myGovID.</p> <p>Housing SA is now the first South Australian Government agency to connect to myGovID, allowing customers to access the Housing Connect portal using the federal identity. Further agencies are expected to onboard.</p>
<p>2.6 Widespread agency adoption of contemporary network security approaches, including zero trust network principles for government systems and applications.</p>	<p>In progress</p> <p>OCIO is working to deliver a SD-WAN service in the first quarter of 2024, with a business case having been approved by the CIO Steering Committee in September 2023.</p>

Aspiration	Status
(Office of the Chief Information Officer)	<p>OCIO will build a 'landing zone' that is a centralised service for SD-WAN and Secure Access Service Edge (SASE) that provides a common connection point between carrier providers and SA Government networks. It will also provide visibility where direct internet access is deployed. This will allow SA Government agencies to leverage any combination of transport services to securely connect users to applications and data in hybrid cloud platforms and on-premises.</p> <p>Zero-Trust has progressed through various stages of governance to transform from traditional VPN to a SASE environment. These networking technologies provide a much higher degree of granularity and control over how users and agencies interact with technology, both inside their own organisations and across the SA Government.</p> <p>The StateNet Conditions of Connection (Version 5.0) and related appendices have been updated to better reflect new and emerging threats to the StateNet environment when agencies, third party organisations and internet based users connect networks and/or ICT systems.</p>
<p>2.7 Continuously develop easily customisable toolkits to enable agencies to adopt new functionality as conveniently and quickly as possible (Microsoft 365).</p> <p>(Office of the Chief Information Officer)</p>	<p>Ongoing</p> <p>A new M365 operating model has been implemented, together with supporting documentation for all M365 services to provide agencies with more autonomy and flexibility in managing their users and environments.</p> <p>All Service Toolkits are being published in the Service Catalogue which are supported by detailed service specifications.</p> <p>IT Service Management (ITSM) is being upgraded to provide a platform enabling better support to agencies and vendors relying on OCIO's central services.</p> <p>OCIO provides a library of architectural patterns, reference architectures, standards and guides for different services, to enable agencies to quickly and easily implement their own services using robust, tested, best practice approaches that are consistent with whole-of-government enterprise architecture and strategy.</p>

Aspiration	Status
	<p>OCIO develops and maintains over 120 whole of government frameworks, strategies, policies, standards, guidelines, toolkits and rulings.</p> <p>In 2022/23, OCIO developed 31 new documents, updated a further 15 documents as part of their biennial review and retired 6 technology-based documents that were no longer relevant.</p> <p>A roadmap has also been developed to capture future business needs and agency requirements around cyber security, cloud, Microsoft 365 and other emerging technologies.</p>
<p>2.8 Deliver Enterprise Voice solutions based on agency user personas for consolidated investment, economy of scale and value realisation.</p> <p>(Office of the Chief Information Officer)</p>	<p>Refer to Aspiration 1.5 above.</p>
<p>2.9 Exit government hosting services business.</p> <p>(Office of the Chief Information Officer)</p>	<p>In Progress</p> <p>Glenside will cease to be a whole of government hosting facility by 1 February 2024.</p> <p>The decommissioning of the Glenside Hosting Facility and the Infrastructure as a Service (IaaS) platform (at multiple sites) continues with agencies removing equipment and services.</p> <p>OCIO has been working closely with agencies over the last 3 years to migrate both agency workloads and whole of government services to alternate data centres. Agencies are migrating services and removing equipment from the Glenside Hosting Facility in line with the exit date of 30 November 2023 and their declared project plans.</p>

Aspiration	Status
<p>2.10 OCIO provides leadership to SAG in the adoption of new and emerging technologies</p>	<p>Development of AI tools and guidelines (May 2023) to equip agencies with the clarity to responsibly and safely adopt and use new technologies such as generative AI (Chat GPT, Bard)</p> <p>Established an across government AI governance working group to:</p> <ul style="list-style-type: none"> • Understand what agencies are doing with AI • Understand AI benefits and risks • Develop an AI governance approach. <p>This Group is engaging with third parties to understand and inform the requirements for a whole of government AI Strategy, AI Ethics policy and AI Assurance Framework and leverage insights and expertise of industry.</p> <p>In November 2023, a two part survey covering AI implementation and awareness and embedded AI was released to collect data about the current state of AI in SA Government agencies. This same survey will be repeated in 2024.</p>
<p>2.11 Lead the development of a statewide connectivity investment strategy</p>	<p>Lead an across government working group to develop a strategy prioritisation framework and connectivity coverage map in close collaboration with numerous third party stakeholders including First Nations people.</p>



3. Secure and Trusted

Protecting the safety and prosperity of South Australians online.

Services to SA's Businesses and Community by 2023

Aspiration	Status
<p>3.1 Build community trust in transacting with government online. (Office of the Chief Information Officer)</p>	<p>Ongoing</p> <p>Ongoing initiatives to drive the strategic imperative for cyber security across government based on the greatest areas of emerging risk, changes in the technology landscape and industry developments. The strategic imperative enables strategic integration on the cyber agenda for SA Government to support the cyber resilience of South Australia.</p>
<p>3.2 Increase South Australia's cyber security capacity through Australian Cyber Collaboration Centre (A3C), Joint Cyber Security Centre (JCSC) and AustCyber supported programs. (Office of the Chief Information Officer)</p>	<p>Ongoing</p> <p>In line with the Department of the Premier and Cabinet's (DPC) Strategic Direction 2022-2025, the department aims to "Invest in trusted cyber strength to underpin security, resilience and uptake by developing a 'Cyber Hazard Lead Program' to ensure SA is prepared for cyber emergencies in partnership with Industry.'</p> <p>To maintain robust cyber security measures, the state continues to work close with the Department of Home Affairs - Cyber and Infrastructure Security Centre, Australian Cyber Security Centre, to assist the DPC in effectively addressing the state's cyber crisis preparedness under the State Cyber Crisis Hazard Leader Risk Reduction Plan.</p>

3.3 SA Government to be a significant employer of new cyber security trainees.

(Office of the Chief Information Officer)

Ongoing

SA Government Cyber Security Graduate Pool has been launched which assists TAFE and university graduates in launching their cyber careers in government and streamlines the recruitment process of cyber graduates for all government agencies.

This aspiration has been revised and merged with 'Contribute to the implementation of the SA Cyber Capability Strategy for industry (cyber action plan to support economic growth, skills, protecting defence and SMEs)' in the ICT, Cyber Security and Digital Government Strategy.



Secure and Trusted - Services to SA Government by 2023

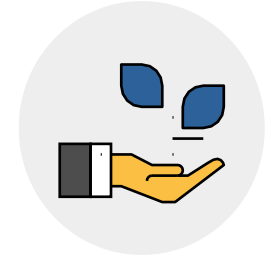
Aspiration	Status
<p>3.4 Deliver mature analysis of events and forecasts of cyber risks. (Office of the Chief Information Officer)</p>	<p>Ongoing</p> <p>The Cyber Crisis Hazard Risk Reduction Plan has been approved as the overarching framework for cyber hazard mitigation.</p> <p>The State Cyber Hazard Lead Program outlines specific, high-impact actions that will drive the State and DPC to fulfill their respective roles in leading cyber hazard risk reduction efforts.</p> <p>Enhance the government's cyber threat capabilities to empower intelligence lead risk decision making for safeguarding South Australia from cyber threats, with development of the South Australian Government Cyber Threat Intelligence Framework.</p>
<p>3.5 Monitor user behaviour to minimise risk of insider threat and address when it occurs. (Office of the Chief Information Officer)</p>	<p>Ongoing</p> <p>Cyber Security Expertise at the Executive Level: Investing in executive-level education and awareness programs will enhance their understanding of cyber security threats, enabling them to provide better support to agencies in the event of an incident (AICD).</p> <p>Enhancing Cyber Security Maturity through Threat Simulations: OCIO-facilitated discussion based threat exercises involving multiple agencies will serve as a valuable tool for refining cyber security maturity.</p> <p>Insider Threat Program: A proof-of-concept for an Insider Threat program will be executed, encompassing the development of a risk matrix and a response procedure.</p>
<p>3.6 SA's Cyber Security Framework embedded and embraced as security standard.</p>	<p>Ongoing</p>

	(Office of the Chief Information Officer)	2022 attestation completed and reported to Cabinet. 2023 attestation reporting in progress. Minor review of the SACSf completed, with 13 supporting documents being updated or developed. Major review of the framework in progress. Work continues to support agencies with their implementation of the framework.
3.7	Enterprise security architecture framework embedded across government (secure by design). (Office of the Chief Information Officer)	This aspiration has been moved to 'Enablers' in the ICT, Cyber Security and Digital Government Strategy.
3.8	Bolster security operational capability for whole of government services managed by OCIO. (Office of the Chief Information Officer)	<p>Ongoing</p> <p>A Security Operations Centre (SOC) for OCIO will be commissioned early in 2024. This new SOC follows a scalable technological and procedural pattern which enables strong interoperability between security practices across government. In this way, a cohesive network of cyber security capability can be achieved.</p> <p>Analysts for the new SOC are being trained.</p> <p>OCIO is in the process of procuring an industry partner.</p> <p>Supporting technologies have been put in place.</p> <p>Further refinement of model to occur.</p> <p>Facilitated configuration reviews and risk assessments on some WoG services provided by OCIO which helped to fix vulnerabilities and implement good security processes for ongoing management.</p>
3.9	Widespread agency adoption of contemporary network security approaches, including zero trust network principles for government systems and applications. (Office of the Chief Information Officer)	<p>In progress</p> <p>Refer to priority 5 for 2020/21 - Enable government with modern network architecture and capabilities.</p> <p>Refer to Aspiration 2.6 above.</p>

<p>3.10 Deliver a comprehensive, statewide Cyber Hazard Risk Reduction program for SA that aligns with the state's emergency management arrangements.</p>	<p>In a significant step forward in cybersecurity, the Chief Executive of the Department of Premier and Cabinet (DPC) formally endorsed the Cyber Crisis Hazard Risk Reduction Plan on June 30, 2023. This plan establishes a comprehensive roadmap for preventing, preparing for, and effectively responding to Cyber Crisis in South Australia.</p> <p>The formulation of this plan drew upon insights from the State Strategic Cyber Risk Assessment, a collaborative involving critical infrastructure sectors across South Australia.</p> <p>The Cyber Crisis Hazard Risk Reduction Plan serves as the overarching framework for cyber hazard mitigation, while the State Cyber Hazard Lead Program outlines specific, high-impact actions that will drive the State and DPC to fulfill their respective roles in leading cyber hazard risk reduction efforts.</p>
<p>3.11 Schedule 22 and ALL supplier security expectations (supply chain risk management)</p>	<p>In progress</p> <p>The first stage of a multistage project to uplift supplier cyber risk management for SA Government was completed, looking at the current state across legislation, policy, central and agency procurement and contract management, and outlining a set of evidence-based recommendations to uplift for the whole of government. Stage 2 findings implementation in progress.</p>

Enablers by 2023

We facilitate a whole of government governance structure that provides leadership, direction and advice to set the standards, policies and frameworks for the development of ICT, digital and cyber security solutions for SA Government, connecting agencies to share information and best practices.



Aspiration	Status
1. Engage with agencies through surveys, briefings, communities of practice, CIO forums etc to inform improvements and priorities. (Office of the Chief Information Officer)	<p>Ongoing</p> <p>OCIO provides fortnightly updates to an across government distribution list of more than 400 recipients. It also undertakes quarterly forums with SA Government agencies where the work of the Division and that of agencies can be showcased.</p> <p>OCIO presented three SA Government Tech, Cyber and Digital Forums in 2023, on 16 March, 28 July, and 26 October. These forums are designed to support information sharing and collaboration across government. They showcase the interesting, inspiring and innovative work happening in agencies to support South Australian communities and businesses. Note: these events are open to SA Government employees only.</p> <p>The Chief Information Officer Steering Committee meets monthly and there are at least 6 working groups reporting into the Steering Committee on particular matters.</p> <p>Our Communities of Practice now number more than 13 and involve many hundreds of agency representatives from all parts of government.</p> <p>Individual agencies have a formal meeting with OCIO Executives quarterly to discuss individual matters.</p> <p>The Customer Satisfaction survey is scheduled to be run in Feb/March 2024 with all actions (one time or ongoing) completed from the 2022 Action Plan.</p> <p>An Artificial Intelligence (AI) Working Group has been established to provide recommendations to the Chief Information Officers Steering Committee about an appropriate AI governance approach for SA Government.</p>

Aspiration	Status
	<p>This Group is engaging with third parties to understand and inform the requirements for a whole of government AI Strategy, AI Ethics policy and AI Assurance Framework and leverage insights and expertise of industry.</p>
<p>2. Digital government roadmap to inform government service improvements. (Digital Programs)</p>	<p>Ongoing</p> <p>A forward procurement plan has been published with upcoming initiatives.</p> <p>The One Stop Shop initiative roadmap has been informed by the user testing of over 1,000 South Australians using qualitative and quantitative methods.</p> <p>The One Stop Shop initiative continues to encourage Government agencies to leverage the investment made for whole of government services such as myGovID, the SA.GOV.AU website, the established design system and the SA.GOV.AU dashboard.</p>
<p>3. Resourcing profile to articulate where increased capability is required. (Office of the Chief Information Officer)</p>	<p>In progress</p> <p>Work has continued to develop an SA Government resourcing profile with the plan to deliver upon the goals in 2024.</p>
<p>4. Continually update OCIO Service Catalogue providing a comprehensive overview of services to agencies. (Office of the Chief Information Officer)</p>	<p>Ongoing</p> <p>The Service Catalogue is maintained and updated on a regular basis. Work is underway to deliver the Catalogue in a more user-friendly way with a plan to launch in early 2024.</p>
<p>5. Optimise the maturity of product portfolio development and delivery.</p>	<p>In progress</p> <p>Maturity is being achieved by the creation of new management information delivered at a Divisional level by the OCIO Performance Unit. All Programs, Projects and Initiatives are regularly reported on, along with risks and issues. Monthly workforce reporting contributes to our workforce planning approach which formally occurs twice per year.</p> <p>Our work program is also provided to agencies by the production of the 'initiatives roadmap' which is produce quarterly.</p>

Aspiration	Status
	For employees, information is available online, and in person via story boards and the Initiatives Wall located in the common area with links to the OCIO Strategy and DPC strategic objectives more broadly.
6. Active communities of practice across government informing better ways of delivering services. (Office of the Chief Information Officer)	Ongoing Refer to Aspiration 1.5.
7. Provide a robust set of whole of government digital platforms, including surveys, community engagement, forms, websites and others as required. (Office of the Chief Information Officer)	Ongoing Refer to Aspiration 1.6.



**Government
of South Australia**

Department of the
Premier and Cabinet

W dpc.sa.gov.au

E OfficeoftheCIO@sa.gov.au