WALGA

THE STRATEGY GROUP

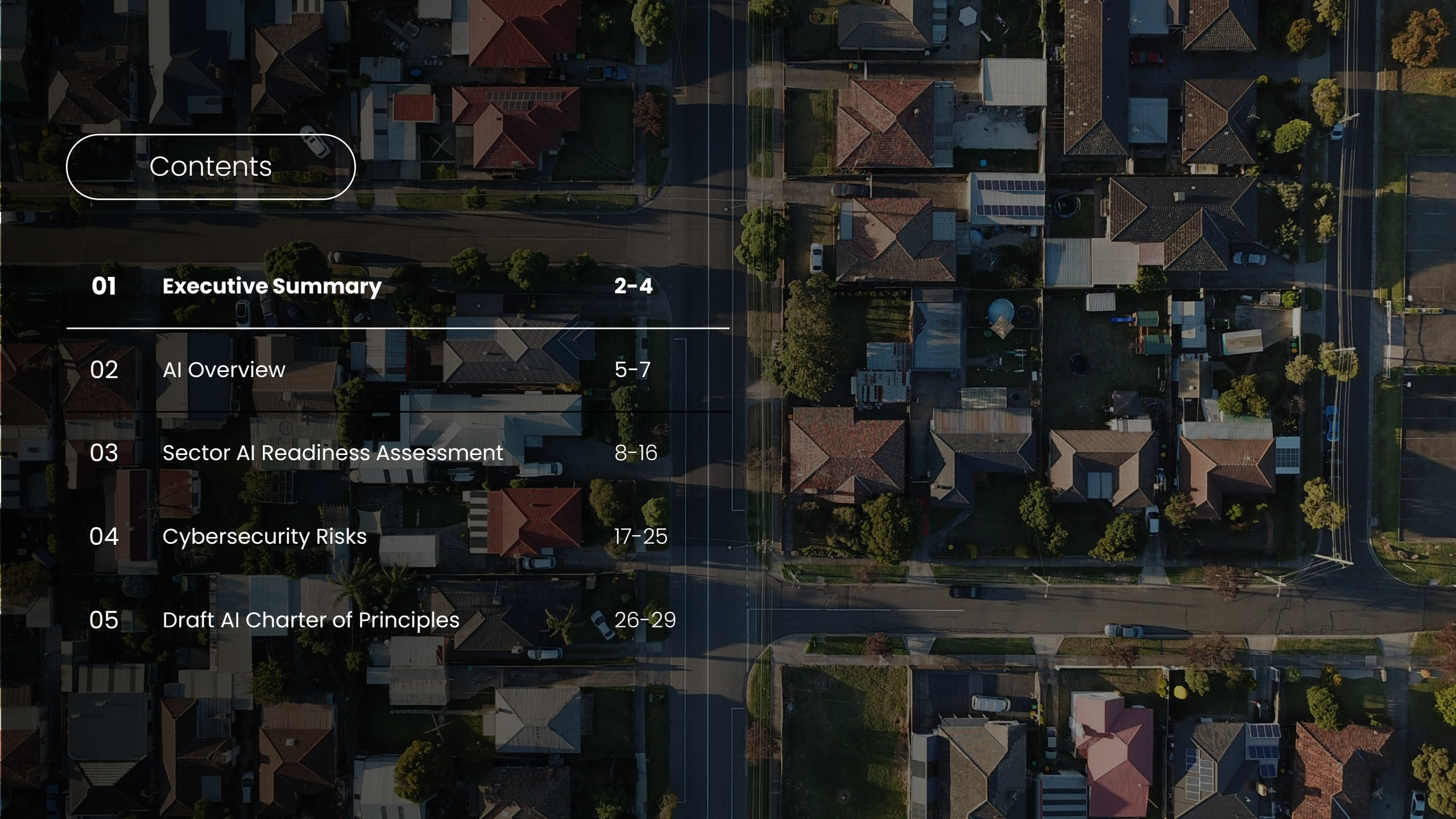
WA Local Government Sector **AI Readiness Assessment**

AI Readiness Assessment Report

Developed by WALGA in collaboration with The Strategy Group and Cygence

April 2026

Contents



The WA Local Government Sector has started its transformative AI readiness journey

Background and Context

With 139 Local Governments serving diverse communities from remote shires to metropolitan centers, the Sector faces both unprecedented opportunities and challenges in adopting Artificial Intelligence (AI) technologies. The WA Local Government Association (WALGA) identified the need for this AI readiness assessment that provides the first Sector-wide baseline understanding of current capabilities, barriers, and support needs across WA Local Governments.

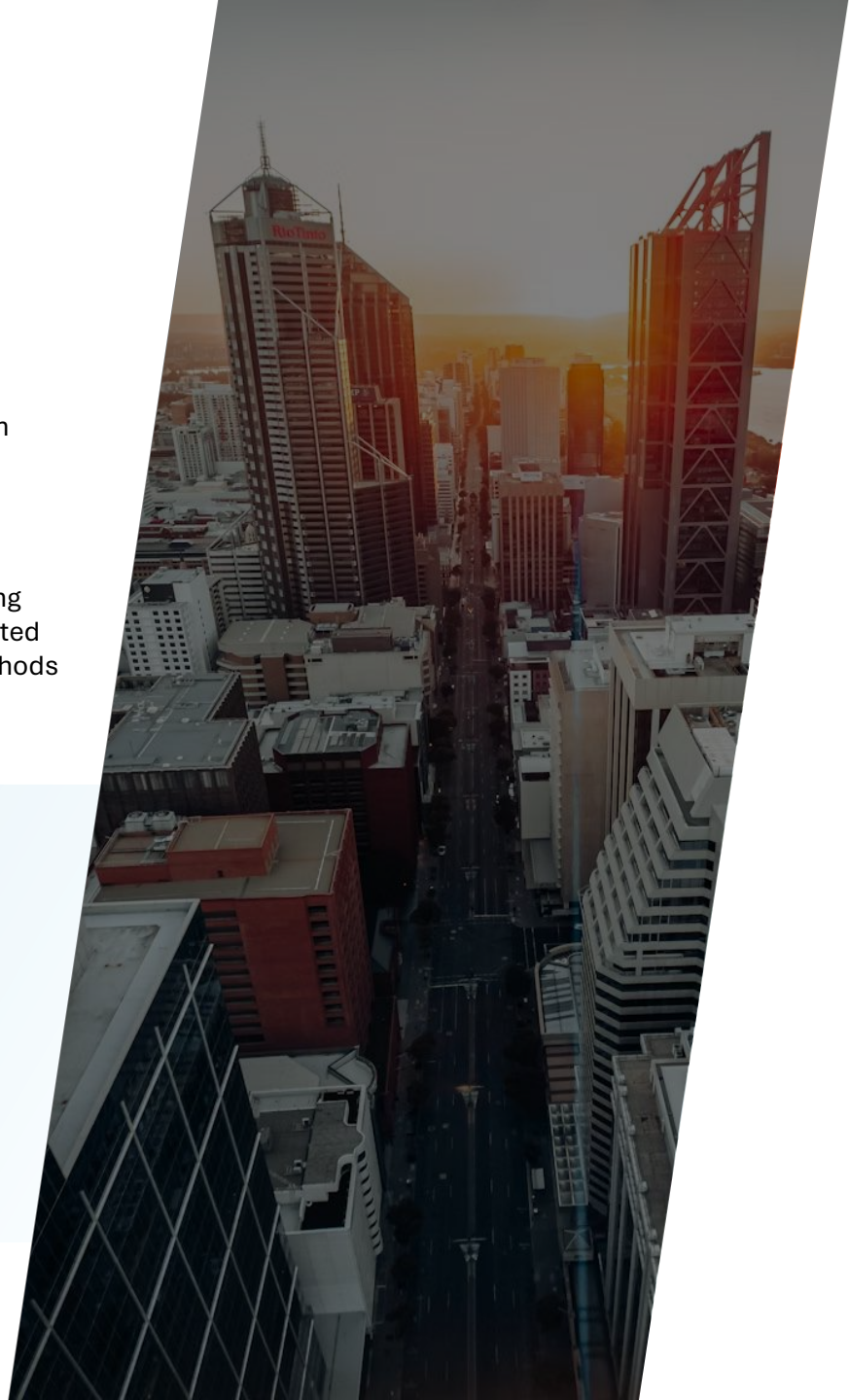
The rapid advancement of AI technologies, coupled with increasing community expectations for digital services and mounting resource pressures, makes understanding and supporting the Sector's AI readiness essential. This research project, conducted in partnership between WALGA, The Strategy Group, and Cygence, employed both quantitative and qualitative research methods to capture the full spectrum of AI Readiness across the Sector. This report shares the project outcomes.

Purpose

- Assess the current state of AI readiness across WA Local Governments
- Identify common risks, threats and preparedness gaps
- Understand support needs to enable safe and effective AI adoption

Objectives

1. Create a baseline understanding of Sector-wide AI readiness
2. Identify priority areas for capability development and support



THE STRATEGY GROUP | WALGA

Sector AI Readiness

108 Local Government WALGA members engaged in the Sector-wide AI readiness assessment to gauge AI readiness, understand AI perceptions and barriers, and identify valuable AI use cases and opportunities.

Overview

108 WA Local Governments participated in a survey to evaluate their current AI implementation status across **six AI readiness dimensions**. Scored responses across **43 readiness indicators** were analysed to inform the Sector readiness profile.

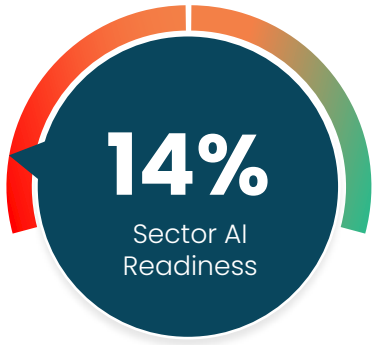
The remainder of the AI Readiness Assessment was focused on uncovering current-state perceptions and future state needs for AI adoption. More specifically, the assessment explored:

- Current perceptions of AI technologies and their potential
- Identified barriers preventing or slowing AI adoption
- Desirability of specific AI use cases
- Opportunities and support needs

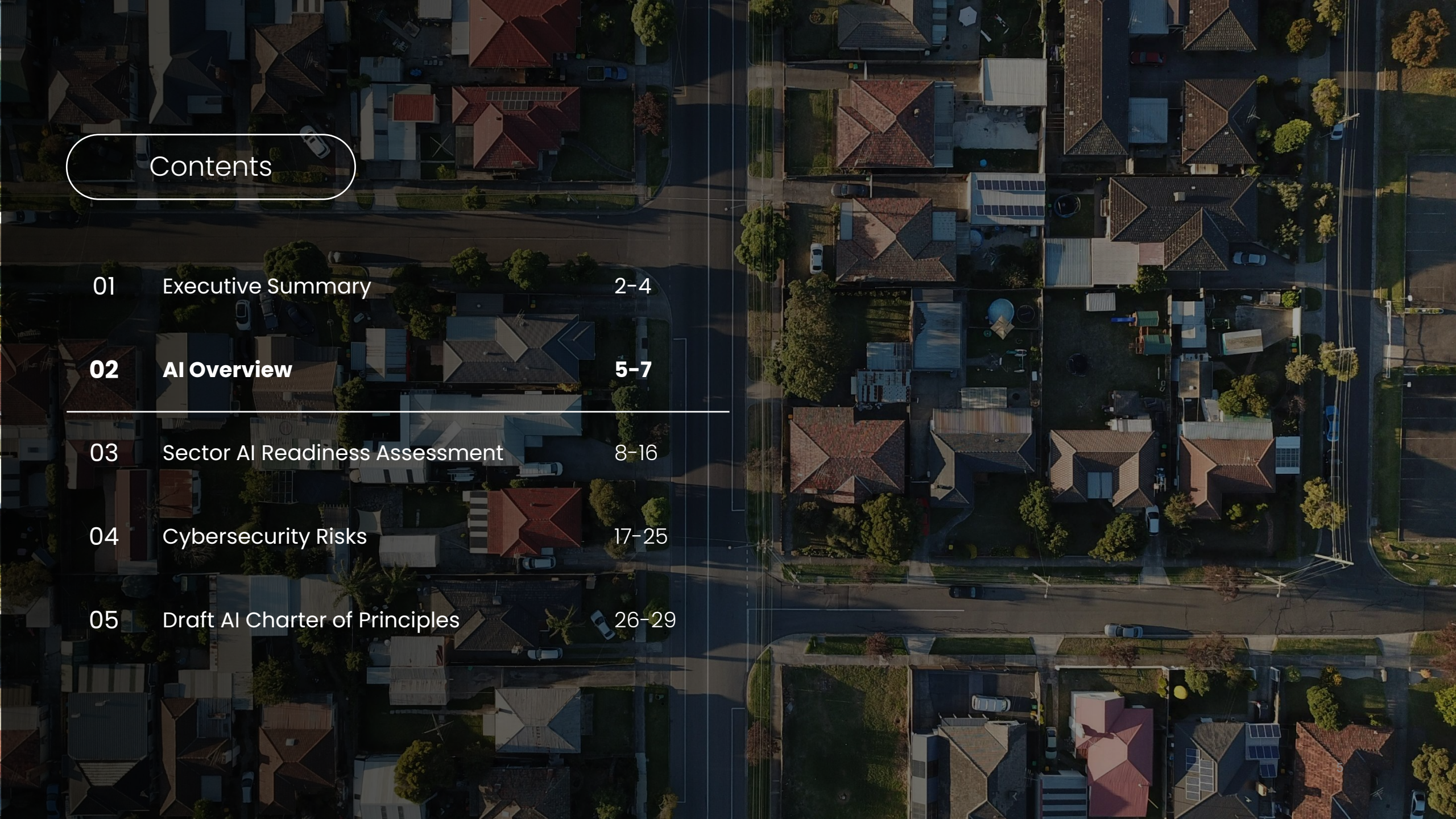
Key Findings

The Sector is poised for AI adoption with several descriptive variables showing optimism and intention to advance AI initiatives. However, with an overall AI readiness score of 14%, AI adoption progress is hampered by several barriers across all six readiness dimensions. The primary readiness drivers sit with Local Government staff and leaders who are beginning to educate themselves and others on the applications of AI. The primary barriers and gaps exist in the underlying infrastructure and technical capability to make AI a reality in Local Government's operations and service delivery.

It is important to note that the analysis was based on information directly provided by the participating Local Governments.



Contents



What is Artificial Intelligence (AI)?

Overview

AI can be thought of as a way of using computers that does not rely on humans manually writing software code to perform tasks. It is designed to mimic human intelligence through problem-solving, learning, and decision-making. Within AI, there are several subsets, including Machine Learning (ML), Generative AI (GenAI), and Agentic AI. ML uses neural networks to process complex patterns based on training data, while GenAI uses these patterns to generate new content. Agentic AI goes further by enabling systems to take autonomous action, combining reasoning, planning, and execution to complete tasks with minimal human input.

Generative AI

AI is evolving at a rapid pace, particularly in the Generative (GenAI) space. Since 2018, it has progressed from simply understanding and generating text to now developing agentic capabilities. For local governments, this creates opportunities to deliver services faster, reduce manual work, and respond more effectively to community needs.

Large Language Models (LLMs)

Understands and generates text.

- **Examples:** ChatGPT 3, Google Gemini, Meta AI
- **Focus:** Reading, writing, summarising, answering questions.
- **Key Impact:** Automating information handling.

Since 2018-2020: Here and mature

Multimodal LLMs (MLLMs)

Understands and generates across text, images, video, and sound.

- **Examples:** GPT-4o, Gemini Veo 3, Google NotebookLM
- **Focus:** Seeing, reading, listening, and speaking.
- **Key Impact:** Broader, richer interactions with information.

Since 2022-2023: Here but still improving

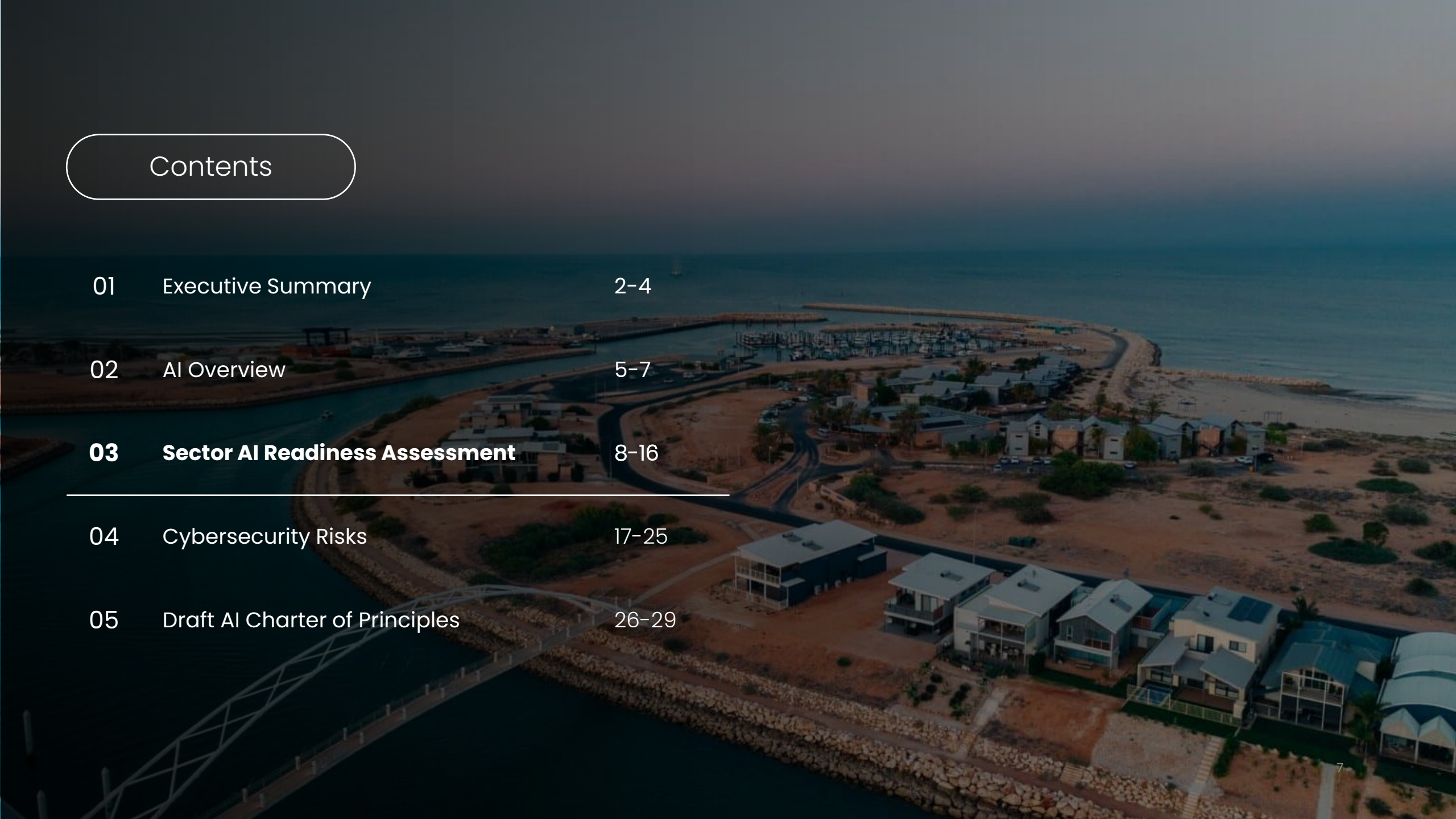
Large Action Models (LAMs)

Understands and can act on your behalf as an agent.

- **Examples:** Microsoft Copilot Agent, Lovable, Cursor
- **Focus:** Completing tasks like writing reports, booking meetings, analysing data.
- **Key Impact:** Moving from advice to execution inside familiar tools.

Since 2023-2025: Emerging quickly

Contents



The Sector AI Readiness Assessment provides comprehensive analysis of current capabilities and future needs

AI Readiness

We surveyed participating Local Governments to evaluate their current AI implementation status across six key readiness dimensions. Responses were scored using the AI Readiness Status Scale (to the right) across 43 readiness indicators were analysed to inform Sector readiness profile. The results were converted to a percentage to reflect an AI readiness score out of 100%

AI Perceptions & Needs

The remainder of the AI Readiness Assessment was focused on uncovering current-state perceptions and future state needs for AI adoption. More specifically, the assessment explored:

- Current perceptions of AI technologies and their potential
- Identified barriers preventing or slowing AI adoption
- Desirability of specific AI use cases
- Opportunities and support needs

Thematic analysis of perception-based questions was used to identify common challenges and opportunities. The current-state assessment was then compared to desired future state to develop clear insights.

AI Readiness Status Scale

Yes (Implemented) = 3

Partially (started or implementing) = 2

Planned (planning to implement) = 1

No (not planned or implemented) = 0

Strategic Readiness

7x indicators

Organisational Readiness

8x indicators

Skills and Capabilities Readiness

6x indicators

Risk and Governance Readiness

7x indicators

Cybersecurity Readiness*

8x indicators

Technical Readiness*

7x indicators

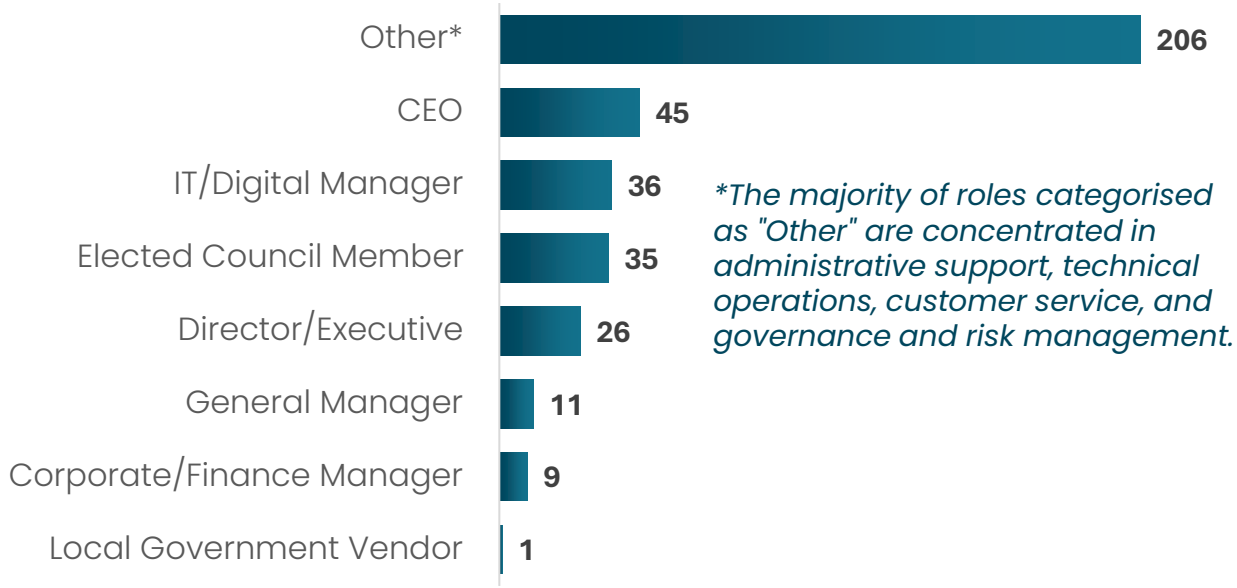
* Technical and Cybersecurity sections were optional and designed for completion by subject matter experts, resulting in lower response rates. Findings in these areas may not fully represent the entire Sector, particularly smaller Local Governments without dedicated technical resources.

370 Local Government representatives engaged in the AI Readiness Assessment

Sample Overview

Overall, 370 representatives from WA's 139 Local Governments participated in the online AI Readiness Assessment survey. While all responses were included in the analysis of perception-based questions, we applied role-based weighting when evaluating AI readiness across the six dimensions. This weighting approach ensured that responses were appropriately aggregated to create a single, representative score for each Local Government, preventing larger councils with multiple respondents from skewing the results.

Participant responses and their roles (Total = 370)

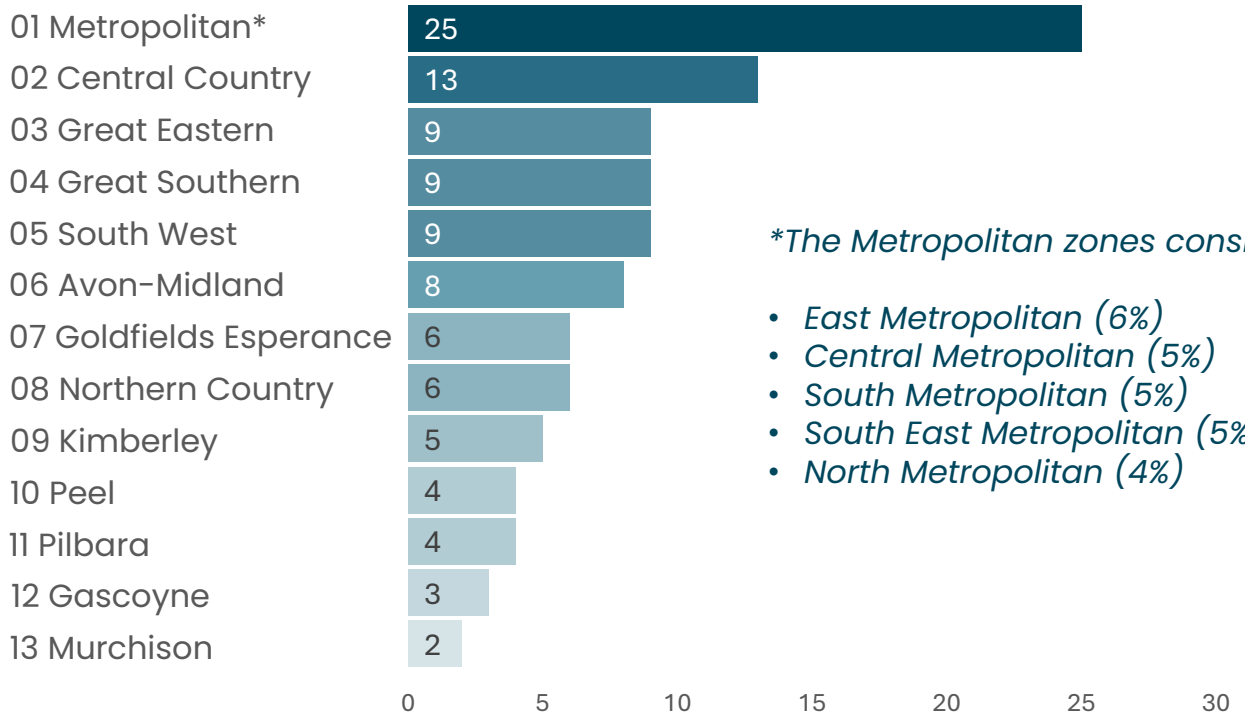


**The majority of roles categorised as "Other" are concentrated in administrative support, technical operations, customer service, and governance and risk management.*

108 Local Government WALGA members engaged in the Sector-wide AI readiness assessment

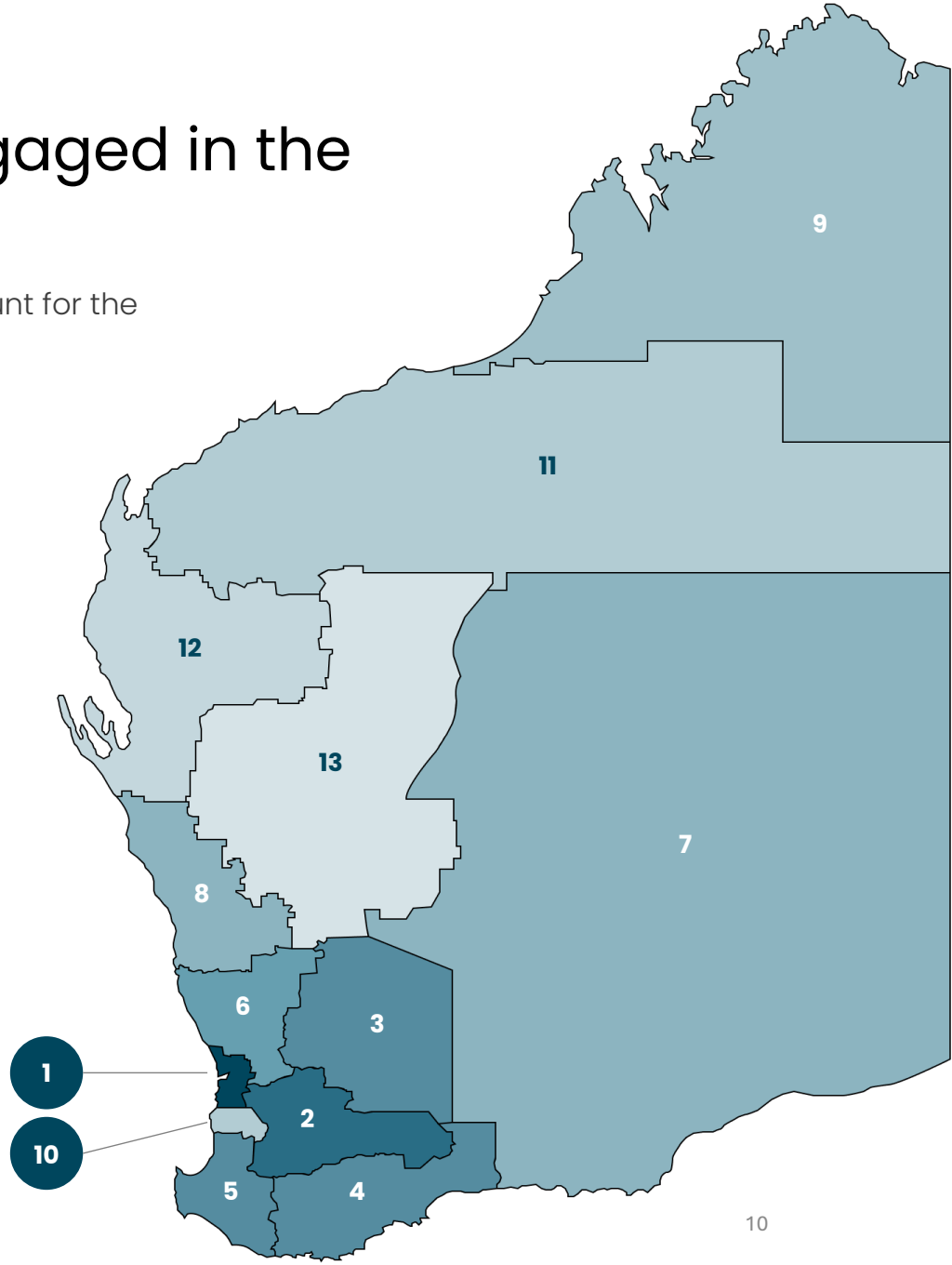
A quarter of Local Governments are from metropolitan areas, while regional zones account for the remainder, with Central Country contributing 13%.

Geographical distribution of 108 Local Governments across WALGA Zones (%)



The Metropolitan zones consist of:

- *East Metropolitan (6%)*
- *Central Metropolitan (5%)*
- *South Metropolitan (5%)*
- *South East Metropolitan (5%)*
- *North Metropolitan (4%)*

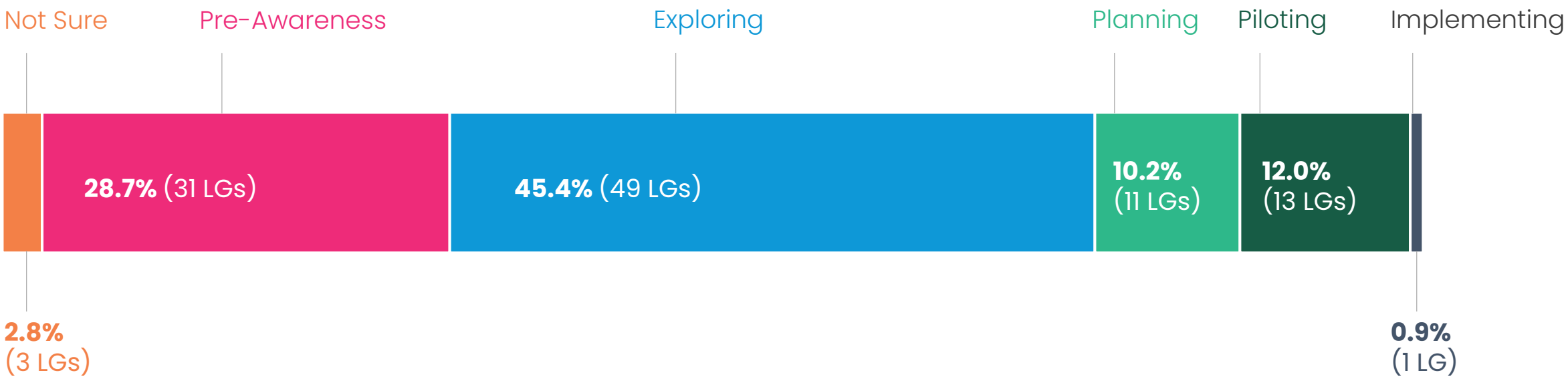


THE STRATEGY GROUP | WALGA

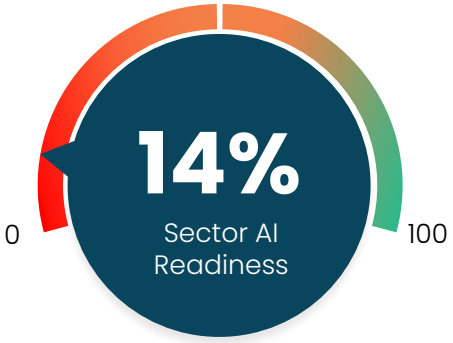
74% of Local Governments are in the early stages of AI adoption

The AI readiness survey results were analysed by counting one aggregated response per Local Government and categorising the Local Governments (LGs) according to their selected AI adoption stages. Nearly half are in the Exploring stage, followed by those in the Pre-awareness stage. 23% are in the planning, piloting or implementing phase.

What is the current stage of AI adoption in your Local Government? (%) (n=108)

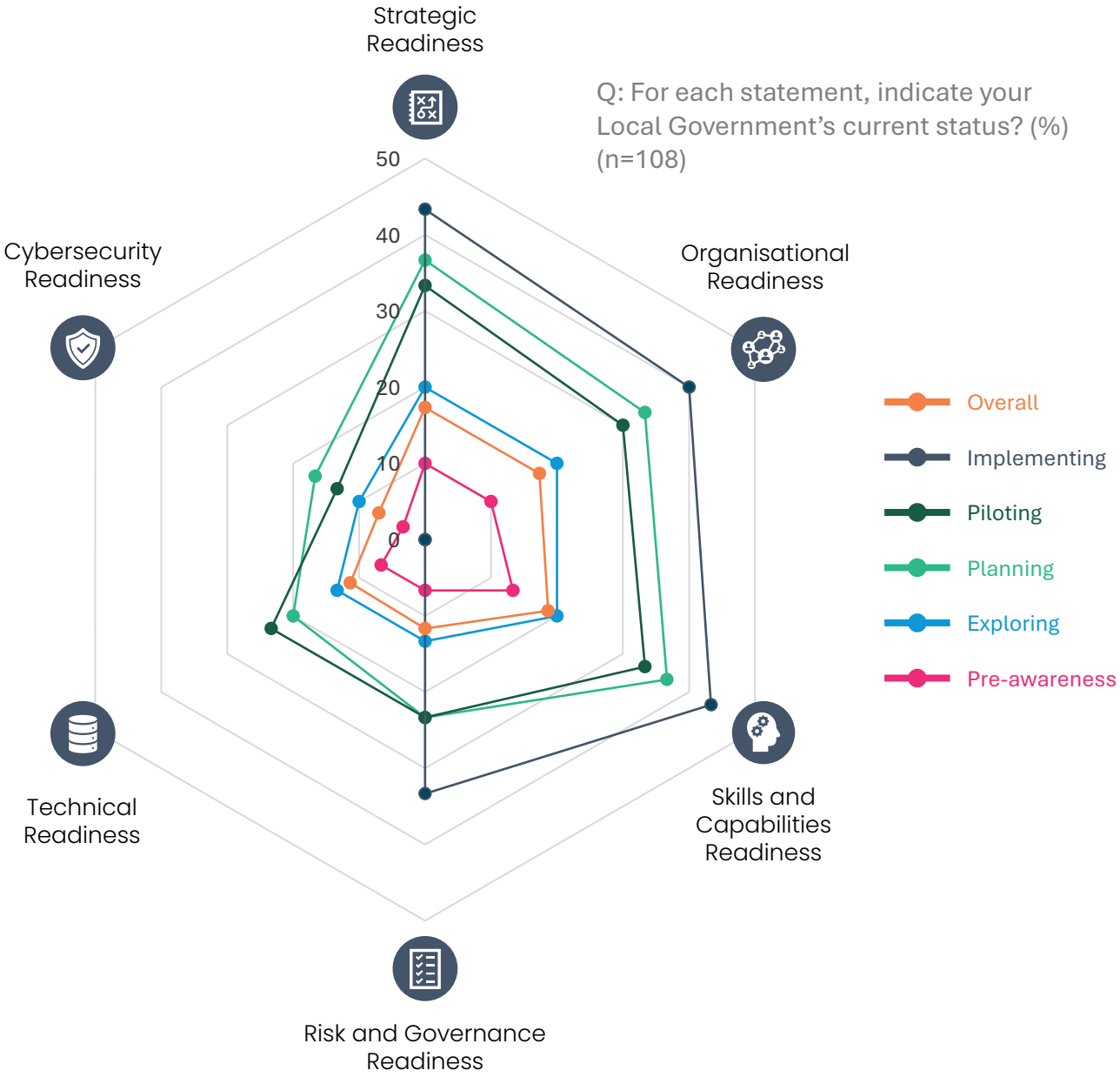


03 Sector AI Readiness Assessment



Higher AI readiness scores are linked to more advanced dimensions, particularly in Skills and Capability, as well as Strategic readiness

While the overall Sector AI readiness score is 14%, Local Governments in the Planning, Piloting, and Implementing stages have a significantly higher average readiness score of 27%, particularly around skills and strategic readiness.



Improved Sector AI Readiness requires Local Governments to focus on risks, governance and further develop digital infrastructure

AI Readiness Findings by Dimension

Strategic Readiness

AI has been discussed at the leadership level in most Local Governments, however its consideration in Local Government's strategic planning and initiatives must be improved to support improved readiness and advance adoption.

Risk & Governance Readiness

Several Local Governments in the Planning and Piloting adoption stages have gone through the process of assessing AI-related risks and putting policies in place for Responsible AI use. The primary development area for Local Governments is in assembling working groups to help manage AI governance.

Organisational Readiness

While many staff are aware of AI's impact on their work, Local Governments should focus on increasing forums to discuss AI applications and plans while also dedicating resources to better understanding AI technologies.

Technical Readiness*

Local Governments in the Exploring, Planning and Piloting adoption stages indicated stronger technical readiness in capabilities like digitised and accessible operational and service data as well as having the ability to share data between systems. Overall the Sector needs to improve its data hygiene and quality and data classification systems

Skills & Capabilities Readiness

The most developed capabilities for this readiness dimensions were having staff with AI knowledge, who could evaluate AI solutions and vendors effectively. The primary development areas were in Local Governments providing AI awareness training to their staff and accompanying AI adoption with robust change management processes.

Cybersecurity Readiness*

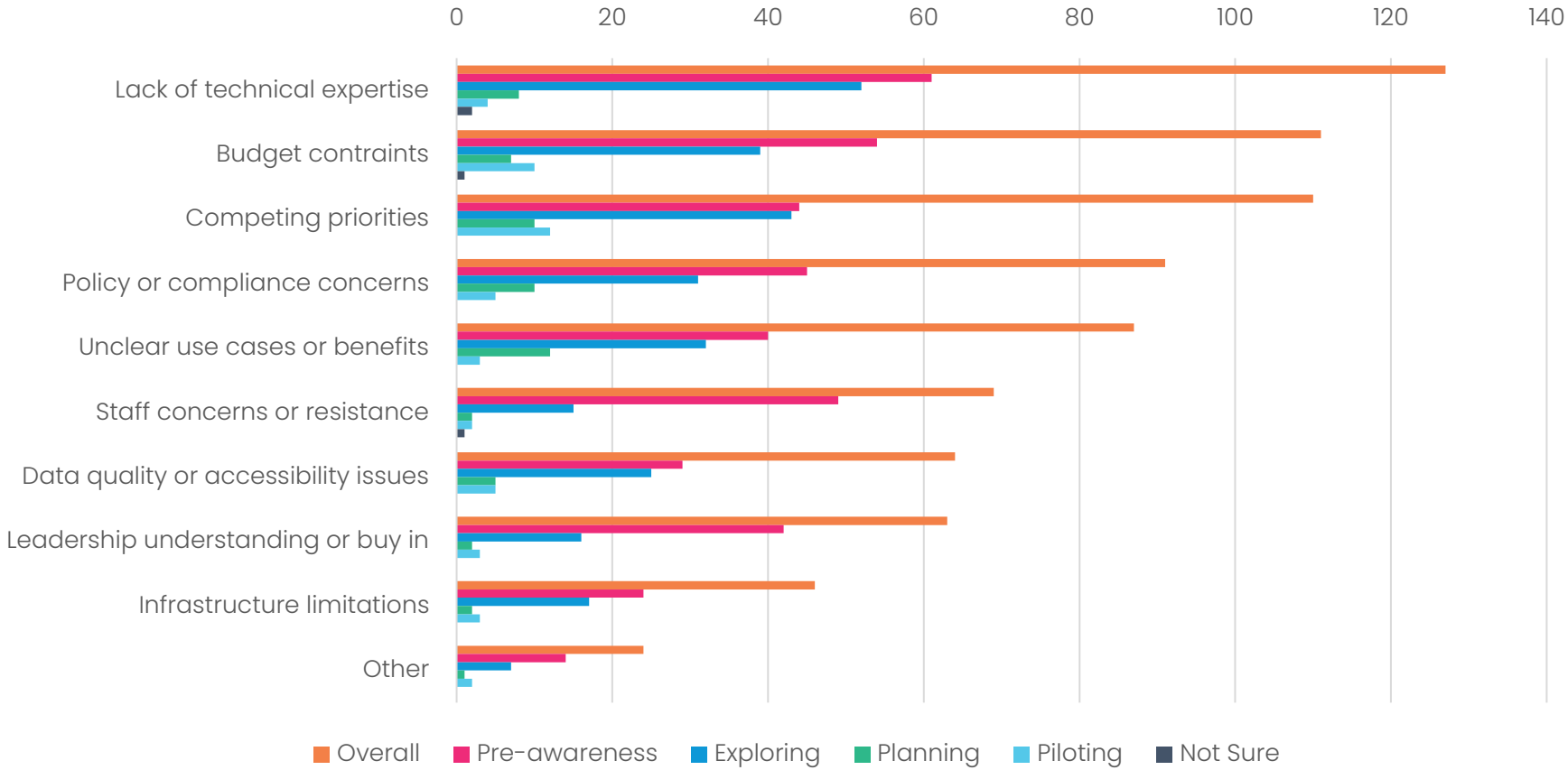
The most advanced capability in this Readiness dimension was Local Governments having cybersecurity practices aligned with State-issued standards. However, there is room for improvement in relation to risk management and response planning and training.

THE STRATEGY GROUP | WALGA

* Technical and Cybersecurity sections were optional and designed for completion by subject matter experts, resulting in lower response rates. Findings in these areas may not fully represent the entire Sector, particularly smaller Local Governments without dedicated technical resources.

The most significant barriers to AI Adoption in Local Government include limited expertise, budget constraints, and competing priorities

Which of the following are the most significant barriers to AI adoption in your Local Government? (n=221)



Key Findings

- The data reveals that while technical and resource constrains are universal challenges, other barriers like
- ‘Lack of technical expertise’ is consistently the most significant barrier, mostly affecting Local Governments in the Pre-awareness and Exploring adoption stages suggesting a general skills gaps preventing progression.
- ‘Competing priorities’ is the most significant barrier for Local Governments in the Piloting adoption stages while ‘Unclear use cases or benefits’ is the most significant challenges for Local Governments in the Planning adoption stage

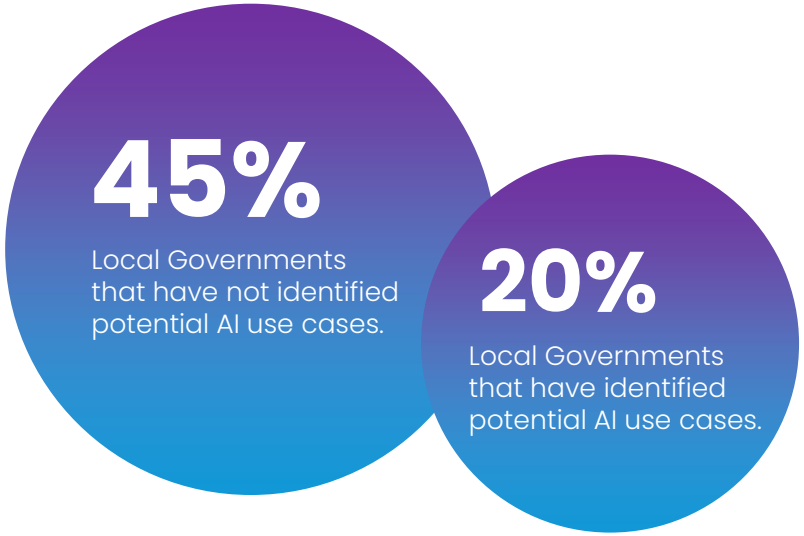
THE STRATEGY GROUP | WALGA

AI adoption starts with identifying use cases and opportunities, but most Local Governments have yet to formalise them

While only 20% of Local Governments have identified potential AI use cases, the most common opportunities relate to content creation, customer service, and operations. A significant portion (45%) have yet to formally identify opportunities and AI use cases, highlighting the need for further awareness and capability-building.

Top Three Prioritised AI Use Cases

The survey identified the top three prioritised uses cases by exploring common patterns in the responses. This was complemented by discussions and brainstorming activities that occurred during the co-design workshop and executive interviews with the selected 12 Local Governments.



1. Improving internal efficiency and staff productivity
   Content creation, meeting transcriptions, templates, etc.
2. Streamlining customer service and request automation
   CRM enhancements, chatbots, self-help automation, etc.
3. Operational intelligence and decision support
   Resourcing, smart surveillance, data analytics, etc.

THE STRATEGY GROUP | WALGA

Contents

Cybersecurity's role in AI Adoption is critical

What is Cybersecurity?

The National Institute of Standards and Technology (NIST) defines cybersecurity as "**the process of protecting information by preventing, detecting, and responding to attacks**"[1]. Cybersecurity risks are created through the execution of Local Government business, as information systems enable underlying functions and communication. Addressing these risks requires risk management. Effective risk management provides an ongoing understanding of threats, vulnerabilities, and the likelihood and potential impact of vulnerability exploitation and system or data compromise [2]. Decision making is better informed and more effective and efficient when supported by strong risk management.

[1] NIST SP 800-160, Vol 2, Rev 1. [2] NIST SP 800-53r5.

How is cybersecurity relevant to AI adoption?

Information systems are protected from cybersecurity risks and vulnerabilities by **ensuring the availability, integrity, authentication, confidentiality, and nonrepudiation of the underlying systems and data**. AI increases the attack surface and provides new opportunities for threat actors by introducing new vulnerabilities and risks. It is the job of system designers, developers, architects, administrators and management to ensure that the new opportunities provided to attackers are addressed and reduced, balancing the available resources and cost of protecting the system with the potential impact for Local Government and its stakeholders.

What is the threat?

Adversaries and threat actors will seek to utilise the vulnerabilities across Local Government technologies, processes, and people to achieve their objectives. These objectives can vary from ransomware attacks, which can cripple information systems and lead to extortion, through to trusted insiders selling intellectual property. The threat is real, with vast numbers of governments and organisations around the world falling victim to cyberattacks.

Local Government should be prepared for threats that possess the intent and capabilities to target vulnerabilities in systems that utilise AI, and those that do not.

Five AI Cybersecurity risks are key to AI adoption in Local Government

1 Trust boundary expansion & exploitation

Local Government trust boundaries will need to be changed to allow long term AI optimisation. High levels of system access, across a multitude of systems, is likely to significantly complicate governance, reduce risk awareness and increase the attack surface.

2 Cybersecurity supply chain opacity

The indirect relationships between data sets, development, deployment and consumption reduces the transparency of the cybersecurity supply chain. There is often a strong reliance on complex underlying systems, from which Local Government will inherit risks and vulnerabilities.

3 Access control & privileges

AI systems introduce new complexities into traditional access control and authorisation models. If an AI agent is given overly broad or unclear permissions, it may access sensitive systems or data in ways that exceed its intended scope. Users may also use AI models to bypass traditional access controls.

4 Integrity manipulation & impersonation

Attackers can alter goals, instructions, or internal memory to change AI agent behaviour. Training data can be manipulated. Spoofing, deepfakes and other specific tactics, techniques and procedures may be employed to facilitate impersonation using, or against, AI agents.

5 Dependency poisoning

Third-party software libraries, APIs, or model updates can become entry points to compromise AI systems. If a poisoned dependency is loaded into an agentic AI system, it can alter decision logic, leak sensitive data, or silently sabotage system integrity.

1 Local Government Risk: Trust boundary expansion & exploitation

/ Summary

AI systems are adopted to streamline operations, make use of seemingly unstructured or disconnected data, and optimise limited resources. Local Government systems and data will need to become increasingly interconnected to take full advantage of the capabilities of Agentic AI systems. The myriad of connections and resulting complexity is likely to reduce the situational awareness of system owners, data owners and security teams. This will have a direct impact on the effectiveness of governance systems employed by Local Government.

Trust boundaries will need to be changed to allow AI optimisation, providing high levels of system access, across a multitude of systems that may otherwise be segmented or siloed. The compromise of an AI system may then allow trust boundaries to be exploited and undermined. The binding that AI creates between systems reduces the resilience of the total system if a compromise occurs, making root cause analysis more difficult and the potential impact of malicious compromise more damaging. Agent Impact Chains and Blast Radius are terms used to refer to the cascading effects when a compromise in one AI system leads to other interconnected agents and systems being compromised. Agent orchestration may also be targeted, using the interaction of agents to facilitate an attack on a system.

/ Risk Scenarios

#1
Autonomy undermining access controls. AI agents can chain together or can trigger downstream actions that are not immediately visible to the user or those planning the system.

#2
Excessive Chaining Depth. Agents can plan too far ahead and create emergent behaviours and unintended consequences through their actions.

#3
Inability to undertake effective Incident Response. Either through malicious action or error, it is likely that AI systems will cause an incident. Lack of preparation can make a simple problem become a critical issue.

/ Potential Mitigations

Apply the principle of least privilege and add agents to access control plans. Restrict agents to specific bounded use cases. Ensure human approvals are built into systems based on risk tolerance.

Limit recursion and chain depth of agents. Apply time to live policies to requests. Ensure human in the loop is applied to either review or confirm tasks where there are multiple agents or they are for an extended period.

In the event of an incident, it is critical that Local Government has implemented centralised logging with sufficient data to enable an investigation. The ability to reverse AI actions and restore systems is very important for overall resilience, and trust in the system.

2

Local Government Risk: Cybersecurity supply chain opacity

/ Summary

The complexity of AI systems and the indirect relationships between data sets, development, deployment and consumption reduces the transparency of the cybersecurity supply chain. There is often a strong reliance on complex underlying systems, from which Local Government will inherit risks and vulnerabilities. Many AI solutions incorporate pre-trained models, third party libraries, and a variety of Application Programming Interfaces (APIs), making it difficult to fully trace the AI and its design origin, assess the security posture of the AI and its developers, or evaluate the integrity of third-party components. The limited transparency increases exposure to hidden vulnerabilities, compromised updates, or embedded malicious code that can propagate across systems undetected. For Local Government adopting AI, the opacity associated with some AI systems can impact trust, complicate compliance, and demands a rigorous governance framework supported by effective risk management and a process to review all elements of the AI supply chain.

/ Risk Scenarios

#1
Data Exploitation. Some AI systems utilise APIs that are delivered by third-parties, bypassing the agreed terms and enabling the third-party to on-sell data or expose it to other parties.

#2
Nested Dependencies. AI systems may rely on a multitude of third-party systems that can introduce vulnerabilities and provide initial access to an attacker.

#3
Compromised Model. Backdoors providing remote access, rogue updates, and misconfigurations can all expose the AI model to attack and expose connected systems and data.

/ Potential Mitigations

Include strict data usage clauses in vendor contracts. Deploy API gateways to monitor outbound data flows and detect policy violations in real time. Conduct detailed cybersecurity supply chain risk assessments that incorporate known AI risks.

Integrate automated vulnerability scanning. Request and review Software Bill of Materials (SBOM) for AI components to identify and track nested third-party dependencies.

Deploy in sandbox environments to test prior to deployment. Conduct continuous monitoring and detection with current cyber threat intelligence to identify anomalous behaviours. Enforce integrity verification through signing and validation prior to updates.

3

Local Government Risk: Access control & privileges

/ Summary

AI systems introduce new complexities into traditional access control and privileged access management. AI systems may operate across multiple environments, assume dynamic roles, or issue commands on behalf of users or other agents. If an agent is given overly broad or unrestricted permissions, it may access sensitive systems or data in ways that exceed its intended scope. Attackers may exploit misconfigurations or vulnerabilities within the AI response to prompts, to deliver malicious responses from the AI, escalate privileges, or trigger unauthorised actions.

The persistent and autonomous nature of some AIs may escalate the impact of the compromise. Inadequate logging, poor AI detection models, and weak boundary enforcement can prevent system administrators from detecting when or how an agent has acted maliciously or prevent a compromise from spreading. Although having programs and systems that access specific privileges is not unusual, the potential extent of access needed for an AI system to provide the efficiency dividends promised by many models would see a significant increase in access and corresponding increase in risk.

/ Risk Scenarios

#1
Excessive privileges. AI agents may be more effective with unrestricted access to other systems. However, broad privileges introduce significant risk if compromised.

#2
Privilege Escalation. The dynamic nature of some AI systems and the complexity of Agentic AI systems provides a variety of ways to bypass authentication controls and escalate privileges.

#3
Inadequate situational awareness. AI systems may make decisions without adequate situational awareness, the traceability of these actions may not allow review or amendment.

/ Potential Mitigations

Apply the principle of least privilege and utilise Just in Time (JIT) access controls. Segment systems and apply isolation and boundary controls to restrict AI system reach. Conduct red team and penetration assessments to support risk management decisions.

Apply input sanitisation and deploy prompt injection review tools. Apply controls that are specifically designed to reduce AI risk, particularly where high privileges are assigned to an AI system.

Deploy logging through a logging plan which includes a centralised logging capability. Review AI systems for their explainability and capacity for logging prior to deployment. Review traceability against risk tolerance and desired situational awareness of governance roles.

4 Local Government Risk: Integrity manipulation & impersonation

/ Summary

Agentic AI systems rely heavily on large datasets, algorithms, models, and software components to make autonomous decisions. This dependency on multiple inputs creates a wide surface area for integrity manipulation, allowing attackers to change an AI agent behaviour. Variations to input data and prompts can cause agents to take unintended actions. As agents often chain decisions based on prior context, a manipulated instruction can cascade into broader errors, particularly when crafted to achieve malicious intent.

Spoofing, deepfakes and other tactics may be employed to facilitate impersonation using, or against, AI agents. Jailbreaking of AI agents may also expose vulnerabilities. These tactics can enable attackers to manipulate AI behaviour, bypass authentication controls, or extract sensitive information. Without robust identity verification and model hardening, AI agents may be exploited to impersonate trusted users or systems, increasing the risk of fraud and disinformation.

/ Risk Scenarios

#1
Poisoned Training. AI agents can favour specific outcomes or suffer from bias as a result of poisoned or biased training data.

#2
Spoofed Prompt Injection. An AI system may be subjected to spoofed prompt injection, which the AI believes is legitimate.

#3
Deepfakes. Although not a direct implication of Local Government AI adoption, the risks related to deepfakes and identify spoofing present a real risk to many traditional security controls.

/ Potential Mitigations

Implement rigorous data provenance checks and validation pipelines, including anomaly detection and adversarial testing of datasets before model training. Use robust version control and change auditing for all training data and model checkpoints.

Deploy strict input validation and verification layers to authenticate the source and intent of all prompts. Apply access controls and inspect prompt context to prevent unauthorised command execution.

Undertake a risk assessment for spoofing and AI supported identity attacks. Review financial controls, procedures for response, and provide training to all staff to identify AI-delivered deepfakes and other identity spoofing attacks.

5

Local Government Risk: Dependency poisoning

/ Summary

Dependency poisoning relates to malicious code, tampered data, or training data that is misaligned to the operating environment. The poisoning can be introduced through datasets, third-party software libraries, APIs, or model updates that the AI system depends upon. If a poisoned dependency is loaded into an agentic AI system, it can alter decision logic, leak sensitive data, or silently sabotage system integrity.

Dependency poisoning attacks exploit the implicit trust AI systems place in upstream components, often bypassing traditional perimeter defenses. Datasets can be extremely difficult to identify for a consumer to assess for drift and overfitting. Poisoned dependencies can be deeply embedded making detection difficult without dedicated tooling and behavioral monitoring. Governance regimes should be capable of determining the trust associated with AI systems compared to risk tolerance levels, employing risk assessments that incorporate the risk from the data, training, APIs, software dependencies and developer pipelines.

/ Risk Scenarios

#1
Malicious Open-Source Library. Most software systems, including AI systems, rely on open-source libraries which can be subjected to attack to introduce vulnerabilities and backdoors into systems.

#2
Drift and Overfitting. When an AI is operating differently to the original training environment, events can be misclassified. Patterns can be too specific to the training data.

#3
Malicious modification of training inputs. Some AI agents can be trained through interactions with live data sources. In some cases, these can be manipulated to change an AI behaviour.

/ Potential Mitigations

Deploy a third party open-source software security tool. Conduct risk assessments of specific solutions. Conduct code reviews.

Develop use cases that match less common scenarios during trials. Review data sources to understand appropriateness and efficacy of training. Identify noise in training data, if accessible.

In the event of an incident, it is critical that Local Government has implemented centralised logging with sufficient data to enable an investigation. The ability to reverse AI actions and restore systems is important for overall resilience, and trust in the system.

Deep dive: Secure AI Adoption

/ Summary

Secure AI adoption involves the minimisation of cybersecurity risk and the promotion of resilience, balanced with the operational demands and resource restrictions faced by Local Governments.

Secure AI adoption manages the risks that can arise from AI and ensures the impacts are positive through the application of effective cybersecurity controls, culture and governance.

Like a building should have solid foundations before looking to expand its footprint, the foundation of Local Government cybersecurity needs to be sound before AI is deployed extensively. The broad range of applicable controls and mitigations to reduce the risk of AI adoption requires a planned and well-led program of work. This should include the creation of a culture of security, supported with effective governance and a review of the maturity of the existing Information Security Management System (ISMS), as described in ISO27001.

Governance and leadership alone do not result in secure systems. Technical delivery of a strong cybersecurity posture that is designed to work against real-world threats is critical to ensuring the core systems, data, and services that will be utilised by an AI are secure. This technical hygiene forms the baseline that AI cybersecurity specialists can build upon to provide secure AI. Finally, resilient design is important to ensure incident response and recovery if timely and effective.

Secure AI adoption should be a critical focus for Local Governments.

The Six Enablers of Secure AI Adoption

There are six critical enablers to secure AI adoption.

1. A culture of security, grounded in available resources with strong governance and genuine cybersecurity leadership.
2. An ever-evolving Information Security Management System that is regularly reviewed for maturity and functionality.
3. Effective technical cybersecurity hygiene, delivering a strong security posture and implementing controls to identify, protect, detect, respond and recover from threats across systems within the Local Government.
4. Focused cybersecurity on AI systems, featuring specialist risk, vulnerability, red team, and supply chain assessments.
5. Robust and resilient design of systems and processes, with planned redundancy and tested incident response capabilities.
6. Adequate funding and resourcing to enable core cybersecurity capabilities.

THE STRATEGY GROUP | WALGA

Contents

Eight AI principles were developed for the Sector

The eight AI principles for WALGA were co-designed with 12 selected Local Governments and informed by AI policies from both the Western Australian and Federal Government bodies. These principles serve as a foundation for Local Governments to consider, adapt, and adopt as part of this draft charter.

How the principles were selected and developed:

11

Brainstormed Principles

The Co-design workshop participants brainstormed 11 principles relevant to Local Governments.

8

Prioritised Principles

Participants voted on key principles, resulting in eight prioritised principles.

8

Finalised Principles

The eight prioritised principles were benchmarked against the AI Ethics Principles by the Australian Government and principles-based policy by the Western Australian Government.

- **Human-centred Values**
- **Fairness, Equity and Ethical Use**
- **Social and Environmental Wellbeing**
- **Privacy, Security and Safety**
- **Reliability and Accuracy**
- **Transparency and Integrity**
- **Governance and Risk Management**
- **Collaboration and Knowledge Sharing**

THE STRATEGY GROUP | WALGA

The Draft AI Charter of Principles is a foundational step in the Sectors broader AI journey

This draft charter acknowledges that one size does not fit all. Local Governments are encouraged to use these principles in a way that best suits their context, whether that means adopting them directly, customising them to fit existing frameworks and structures, or using them to guide future planning.

Human-centred Values

AI should prioritise human rights, dignity, and autonomy, ensuring it serves diverse needs while promoting fairness and respect for human values.

Fairness, Equity and Ethical Use

Design and deployment of AI must focus on fairness, inclusivity, and ethical practices, ensuring equal access and treatment for all individuals and communities.

Social and Environmental Wellbeing

The use of AI must contribute positively to society and the environment, driving outcomes that benefit communities and support sustainable practices.

Privacy, Security and Safety

Strict privacy, security, and safety measures must be embedded within AI solutions to safeguard personal data and protect against potential risks.

Reliability and Accuracy

AI must deliver reliable and accurate outputs, consistently meeting its intended purpose and ensuring trustworthy results in all applications.

Transparency and Integrity

AI must ensure transparency in decision-making processes, with clear explainability of outcomes and mechanisms for contestability throughout its lifecycle.

Governance and Risk Management

Effective governance and robust risk management frameworks are essential to ensure ethical AI deployment, with ongoing accountability and oversight.

Collaboration and Knowledge Sharing

Fostering collaboration and knowledge sharing across Sectors and stakeholders will promote innovation, best practices, and collective benefits in AI adoption.

Suggestions for how smaller and larger Local Governments may want to adapt the Draft Charter to their unique context and capabilities

Principle	Larger Local Government (Class 1 and 2)	Smaller Local Government (Class 3 and 4)
Human-centred Values	• Actively identify and consider potential use cases • Run co-design sessions with diverse groups, using journey maps to assess AI impact • Embed human-centred design frameworks in digital transformation programs • Prioritise accessibility and inclusive language in AI use	• Actively identify and consider potential use cases • Use simple surveys with residents/staff to assess AI awareness and their needs • Leverage existing community groups and networks for feedback or pilot testing • Partner with neighbouring Local Governments to develop shared resources
Fairness, Equity and Ethical Use	• Develop internal AI ethics review processes and escalation pathways • Train leadership teams to identify systemic bias and equity risks in algorithms • Implement bias testing protocols with internal or contracted expertise	• Establish simple checklists to assess potential bias in AI tools before procurement • Provide basic training to staff on ethical use of AI and how to mitigate bias • Focus on ensuring AI tools don't disadvantage staff or residents
Social and Environmental Wellbeing	• Use AI to identify or monitor social or environmental risks • Integrate ESG or sustainability goals into AI project outcomes • Develop metrics and KPIs for measuring community wellbeing outcomes	• Rely on vendor-provided AI solutions to monitor social or environmental risks • Align AI projects with existing community plans and environmental priorities • Focus on 2-3 indicators that demonstrate AI's community benefit
Privacy, Security and Safety	• Implement robust cybersecurity infrastructure and monitoring systems • Develop comprehensive data governance frameworks with dedicated privacy staff • Conduct regular AI-related risk assessments	• Rely on vendor security certifications and government approved platforms • Implement basic data governance policies with external legal support • Provide essential privacy training for staff and share incident response procedure
Reliability and Accuracy	• Develop internal testing and quality assurance processes for AI • Use data analytics and benchmarking to track and improve AI accuracy over time • Create comprehensive backup procedures	• Start with low-risk AI applications, like Microsoft Copilot, to build confidence • Focus on AI tools with proven track records in similar-sized Local Governments • Create basic fallback procedures when AI systems fail
Transparency and Integrity	• Establish regular reporting on AI performance and impacts with staff and/or public • Develop comprehensive AI transparency frameworks and public reporting processes • Allow formal review or appeals processes for AI-supported decisions	• Use townhalls or staff meetings to communicate your AI journey • Focus on transparency about AI limitations and human oversight • Create basic complaint mechanism for AI-related concerns
Governance and Risk Management	• Establish centres of excellence and internal AI expertise • Apply structured risk frameworks to evaluate AI use, applications and opportunities • Lead development of regional AI governance and mentor smaller Local Governments	• Form AI working groups to explore use cases, and formulate risks and limitations • Align internal governance with state or federal-level AI policies and guidance • Partner with other Local Governments for shared governance resources
Collaboration and Knowledge Sharing	• Host inter-Local Government AI forums, webinars or events to share knowledge • Establish formal partnerships with universities and research institutions • Open-source learnings, templates or frameworks for Sector use	• Join inter-Local Government forums, webinars or events to build network • Participate in government-led pilots related to AI or cybersecurity • Provide staff with access to key AI resources from Microsoft or OpenAI

Thank you

Pierre Schaupp
0410 753 715
pierre@thestrategygroup.com.au

Amy Ormrod
0438 200 916
amy@cygence.com.au

Liam Hoffman
0420 722 851
liam@thestrategygroup.com.au

David Ormrod
0401 399 284
dave@cygence.com.au

Jana Plumm
0448 939 879
jana@thestrategygroup.com.au

For more information, contact WALGA Manager Commercial Services, Sam McLeod
SMcleod@walga.asn.au

THE STRATEGY GROUP | WALGA