



PERFORMANCE AUDIT

26 MARCH 2024

Cyber security in local government

NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

THE ROLE OF THE AUDITOR-GENERAL

The roles and responsibilities of the Auditor-General, and hence the Audit Office, are set out in the *Government Sector Audit Act 1983* and the *Local Government Act 1993*.

We conduct financial or 'attest' audits of state public sector and local government entities' financial statements. We also audit the Consolidated State Financial Statements, a consolidation of all state public sector agencies' financial statements.

Financial audits are designed to add credibility to financial statements, enhancing their value to end-users. Also, the existence of such audits provides a constant stimulus to entities to ensure sound financial management.

Following a financial audit the Audit Office issues a variety of reports to entities and reports periodically to Parliament. In combination, these reports give opinions on the truth and fairness of financial statements, and comment on entity internal controls and governance, and compliance with certain laws, regulations and government directives. They may comment on financial prudence, probity and waste, and recommend operational improvements.

We also conduct performance audits. These examine whether an entity is carrying out its activities effectively and doing so economically and efficiently and in compliance with relevant laws. Audits may cover all or parts of an entity's operations, or consider particular issues across a number of entities.

As well as financial and performance audits, the Auditor-General carries out special reviews, compliance engagements and audits requested under section 27B(3) of the *Government Sector Audit Act 1983*, and section 421E of the *Local Government Act 1993*.

© Copyright reserved by the Audit Office of New South Wales. All rights reserved. No part of this publication may be reproduced without prior consent of the Audit Office of New South Wales. The Audit Office does not accept responsibility for loss or damage suffered by any person acting on or refraining from action as a result of any of this material.



GPO Box 12
Sydney NSW 2001

The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 421D of the *Local Government Act 1993*, I present a report titled '**Cyber security in Local Government**'.

A handwritten signature in black ink, appearing to read 'Margaret Crawford'.

Margaret Crawford PSM
Auditor-General for New South Wales
26 March 2024



RECONCILIATION COMMITMENT STATEMENT

The Audit Office of New South Wales pay our respect and recognise Aboriginal people as the traditional custodians of the land in NSW.

We recognise that Aboriginal people, as custodians, have a spiritual, social and cultural connection with their lands and waters, and have made and continue to make a rich, unique and lasting contribution to the State. We are committed to continue learning about Aboriginal and Torres Strait Islander peoples' history and culture.

We honour and thank the traditional owners of the land on which our office is located, the Gadigal people of the Eora nation, and the traditional owners of the lands on which our staff live and work. We pay our respects to their Elders past and present, and to the next generation of leaders.

contents

Cyber security in local government

Section one – Cyber security in local government

Executive summary	1
Introduction	6
Council findings	13
Guidance and support for cyber security management in local government	22

Section two – Appendices

Appendix one – Response from entities	27
Appendix two – Glossary	36
Appendix three – Overview of Audit Office of New South Wales reports that consider cyber security	37
Appendix four – Cyber Security Guidelines – Local Government foundational requirements	38
Appendix five – About the audit	40
Appendix six – Performance auditing	42

Section one

Cyber security in local
government

Executive summary

Local councils in New South Wales (NSW) provide a wide range of essential services and infrastructure to their communities and are increasingly reliant on digital technologies for this.

Councils use various information systems and software to manage significant amounts of information and data relevant to their corporate functions, infrastructure and service delivery. This may include sensitive information about residents, customers and staff.

Audit Office of New South Wales reports to Parliament have highlighted gaps in councils' cyber security risk management approaches since 2020. The Local Government 2023 report, tabled in March 2024, found that 50 councils were yet to implement cyber security governance frameworks and related internal controls.

The threat from cyber security incidents continues to rise. Such incidents can harm local government service delivery and may include the theft of information, denial of access to critical technology, or even the hijacking of systems for profit or malicious intent.

It is important that councils are effectively identifying and managing cyber security risks to:

- protect their information, data and systems
- be prepared to detect, respond to and recover from cyber security incidents
- ensure confidence in the services they are providing for their communities.

This report outlines important findings and recommendations from a performance audit of three councils: City of Parramatta Council, Singleton Council and Warrumbungle Shire Council. This audit report has deidentified findings for each council, but the specific findings have been directly shared with each council to enable them to remediate and improve cyber safeguards. The findings and recommendations in this report are likely to be relevant to most local councils in NSW and councils are encouraged to ensure they have sufficient cyber safeguards.

This audit assessed how effectively the selected councils identified and managed cyber security risks. The audit considered whether the councils:

- effectively identify and plan for cyber security risks
- have controls in place to effectively manage identified cyber security risks
- have processes in place to detect, respond to, and recover from cyber security incidents.

This audit also included the Department of Customer Service and the Office of Local Government (OLG) within the Department of Planning and Environment (DPE) due to their roles in providing guidance and support to local government.¹

Cyber Security NSW, part of the Department of Customer Service, supports local councils to improve their cyber resilience through a range of services and guidance, including the Cyber Security Guidelines – Local Government issued in December 2022.

The OLG is responsible for strengthening the sustainability, performance, integrity, transparency and accountability of the local government sector.

¹ The OLG was part of DPE up to 1 January 2024, when DPE was abolished and the OLG became part of the Department of Planning, Housing and Infrastructure (DPHI).

Conclusion

The three councils are not effectively identifying and managing cyber security risks. As a result, councils' information and systems are exposed to significant risks, which could have consequences for their communities and infrastructure.

Ineffective cyber security risk management can result in unmitigated risks to the security of information and assets which, if compromised, could impact the councils' local communities, service delivery and public infrastructure.

Poor management of cyber security can lead to consequences including theft of information or money, service interruptions, costs of repairing affected systems, and reputational damage.

Each council undertook activities to improve their cyber security during the audit period, but there were significant gaps in the councils' risk management processes and controls meaning the councils are not effectively identifying and managing cyber security risks.

Key findings include:

- None of the councils are effectively using risk management processes to identify and manage cyber security risks.
- None of the councils have assessed the business value of their information and systems to inform cyber security risk identification and management, nor have they assigned cyber security responsibilities for all core systems.
- Two of the three councils do not have a formal plan to improve their cyber security, resulting in an uncoordinated approach to cyber security activities and related expenditure. The council that does have a plan has not formally considered the resourcing required to fully implement the plan.
- None of the councils have implemented effective governance arrangements to ensure accountability for managing cyber security risks, and their reporting to ARICs did not link activities to risk mitigation.
- None of the councils have effective cyber security policies and procedures for managing cyber security risks and to support consistent cyber security practices.
- None of the councils have a clear and consistent approach to monitoring the effectiveness of controls to mitigate identified cyber security risks.
- All three councils are not effectively identifying or managing third party cyber security risks.

None of the councils have up to date plans and processes to support effective detection, response and recovery from cyber security incidents.

Councils need to be prepared to identify when a cyber incident occurs, and be able to respond to cyber incidents to contain any compromises and minimise the impact. This is even more important for councils with low levels of maturity in their preventative cyber security controls.

Key findings include:

- None of the councils have a cyber incident response plan to ensure an effective response to and prompt recovery from cyber incidents, and their business continuity and disaster recovery planning documentation is not up to date.
- None of the councils have clearly defined roles and responsibilities for detecting, responding to (including through appropriate reporting) and recovering from cyber incidents.
- None of the councils maintain a register of cyber incidents to record information about the sources and types of incidents experienced and relevant responses, to support post-incident evaluation.

Cyber Security NSW and the OLG recommend that councils adopt requirements set out in the Cyber Security Guidelines for Local Government, but could do more to monitor whether the Guidelines are enabling better cyber security risk management in the sector.

Cyber Security NSW and the OLG recommend that local councils implement the Cyber Security Guidelines for Local Government. However, while the roles of both Cyber Security NSW and the OLG involve identifying and responding to specific sector risks, neither is monitoring the uptake of the Guidelines by local councils to identify whether they are enabling better cyber security risk management.

Cyber Security NSW and the OLG did not ensure that their roles, responsibilities and actions relevant to cyber security management were coordinated and complementary during the audit period. Cyber Security NSW's Local Government Engagement Plan was updated in November 2023 to include information about its approach to stakeholder collaboration to support a cyber secure NSW Government, including through engagement with the OLG.

1. Recommendations

As a matter of priority, the councils should:

1. integrate the assessment and monitoring of cyber security risks into corporate governance processes by:
 - a) implementing clear governance arrangements for cyber security, including a mechanism for regular reporting to management, ARIC and councillors
 - b) ensuring the Council's enterprise risk management framework is being applied to cyber security risks, including through maintaining risk registers
2. complete a self-assessment against the foundational requirements in the Cyber Security Guidelines – Local Government and:
 - ensure that the outcomes of the self-assessment are reflected in other relevant documentation including risk registers and insurance documentation
 - report the results to management, ARIC and councillors
3. implement a plan and structured program of activities to improve the Council's cyber security that considers and addresses current cyber security maturity, a comprehensive assessment of cyber security risks, and gaps identified in this report and by the Council through implementation of recommendations 1 and 2 above.

At a minimum, the plan and program of activities should:

 - a) define the Council's cyber security objectives
 - b) set out roles and responsibilities for oversight and implementation
 - c) establish implementation timeframes, and processes for regular review and reporting on how cyber security activities and controls are supporting risk management
 - d) establish a plan to re-assess the Council's cyber security maturity in the future
 - e) establish a regular schedule of testing of the cyber security of systems and the network
4. ensure that the plan and program of activities (recommendation 3) are underpinned by:
 - a) a catalogue of all information and systems held by the Council
 - b) an assessment of cyber security risks informed by the business value of the information and systems, including for systems used to support important infrastructure services
 - c) consideration of required resources and capability
 - d) a structured program of regular training and awareness activities
 - e) policies and procedures that support staff and third party providers to understand their roles and responsibilities for cyber security
 - f) clearly defined roles and responsibilities and documented risk assessments for third party arrangements
5. develop, implement and test a cyber incident response plan.

By June 2024, the Department of Planning, Housing and Infrastructure (Office of Local Government) and Department of Customer Service (Cyber Security NSW) should:

6. implement and maintain a schedule of regular consultation between the agencies to share information on cyber security risks facing the local government sector and identify opportunities for collaboration to:
 - a) highlight the importance of cyber security risk management, including through sharing case studies that demonstrate good practice within local councils
 - b) promote guidance and support available from the NSW Government and other sources that may assist councils to improve their cyber security risk management.

By September 2024, the Department of Planning, Housing and Infrastructure (Office of Local Government) should:

7. update the draft procurement guidelines for local councils to include relevant guidance on identifying and managing cyber security risks in procurement processes and third party arrangements.

By September 2024, Department of Customer Service (Cyber Security NSW) should:

8. implement an annual review of the Cyber Security Guidelines – Local Government (the Guidelines) and related resources. The review should include consideration of:
 - a) updates made to the NSW Cyber Security Policy
 - b) the usefulness, relevance and effectiveness of the Guidelines and related resources based on local councils' feedback.

Key takeaways for all NSW local councils

All NSW local government entities should consider the findings and recommendations in this report, as well as other Audit Office reports that include findings relevant to cyber security (see [Appendix three](#)), to consider whether they are effectively identifying and managing cyber security risks.

At a minimum, all NSW local councils should:

1. implement clear governance arrangements and leadership for cyber security risk management, plans and reporting
2. ensure they are identifying and managing cyber security risks consistent with an up-to-date and approved enterprise risk management framework
3. ensure that cyber security risk assessments and implementation of controls are informed by clear evidence, set within the council's risk management framework and integrated with broader planning and financial reporting processes
4. complete a self-assessment against the foundational requirements within the Cyber Security Guidelines – Local Government and report the results to its management, ARIC and councillors
5. use the outcome of that assessment to inform a detailed plan to achieve a level of cyber security capability accepted by management.

1. Introduction

Local councils in New South Wales (NSW) provide a wide range of essential services and infrastructure to their communities. In doing so, councils use a range of information technology (IT) systems, assets, and digital services.

This audit follows several audit reports by the Audit Office of New South Wales that have considered how effectively NSW Government entities, including local councils have managed cyber security risks (see [Appendix three](#)).

The Audit Office of New South Wales has reported on how councils have managed cyber security risks since 2020. In the Local Government 2023 report, tabled in March 2024, gaps in cyber security frameworks and related internal controls were reported in 50 councils.

1.1 The importance of cyber security risk management

Cyber security risk management is an increasingly important consideration for governments, entities, regulators and the public. Cyber security comprises measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them.

The threat from cyber attacks continues to rise. The Australian Cyber Security Centre (ACSC) in its [Annual Cyber Threat Report 2022–23](#) noted 94,000 cybercrime reports, an increase of 23% on 2021–22. The average cost of each reported cybercrime has increased by 14% from 2021–22. That report noted that 12.9% of incidents reported to the ACSC related to State, Territory and Local Government agencies.

Exhibit 1: Definition of cyber security risk

An effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organisational operations (i.e. mission, functions, image, or reputation) and assets, individuals, other organisations, and the nation.

Source: US National Institute of Standards and Technology Glossary.

Common cyber security risks identified by NSW Government agencies in 2021–22 included:

- data breaches relating to unauthorised access to financial reporting applications, data and electronic assets
- failures in preventive and detective controls to safeguard digital assets
- misappropriation of digital assets
- unauthorised access to the IT network
- potential loss of data or inability to access data as required
- IT system failure affecting the agency's primary business
- risks arising from lack of policies and procedures in place related to cyber security.





Inadequate oversight of third parties has been a contributing cause to some major Australian cyber incidents in the past year, with malicious actors exploiting control deficiencies at service providers, and using that to gain access to systems and data. The ACSC [Annual Cyber Threat Report \(2022–23\)](#) states the increasingly complex ICT supply chains and advances in fields like artificial intelligence require a positive cyber security culture across business and the community. The ACSC recommends a focus on cyber supply chain risk management:

Cyber supply chain risk management can be achieved by identifying the cyber supply chain, understanding cyber supply chain risk, setting cyber security expectations, auditing for compliance, and monitoring and improving cyber supply chain security practices.

Source: [ACSC Cyber Supply Chain Risk Management, May 2023](#).

A range of consequences to councils' strategic objectives and operations may stem from a cyber security incident (Exhibit 2).

Exhibit 2: Examples of potential consequences for councils from a cyber security incident

	Financial losses, including recovery and remediation expenses
	Legal and regulatory, including potential liability for harm or loss suffered by customers or stakeholders
	Business continuity risks, such as service disruption to important infrastructure services
	Reputational damage, including loss of community trust and confidence

Source: Audit Office of New South Wales.

NSW Government guidance and industry standards outline approaches to managing cyber security risks (see 1.4 below). Such guidance outlines that implementing a cyber security framework assists entities to effectively identify and manage cyber security risks. A cyber security framework consists of threat identification, protection, detection, response and recovery of IT systems.

Risk management in councils

In New South Wales, the *Local Government Act 1993* (LG Act) and the Local Government (General) Regulation 2021 (the 2021 Regulation) provide the legal framework for the system of local government, including local councils.

Chapter 3 of the LG Act sets out relevant risk management principles:

- Councils should manage risks to the local community or area or to the council effectively and proactively when developing and applying the integrated planning and reporting framework.
- Councils should have effective financial and asset management, including sound policies and processes for risk management practices.

Under section 428A of the LG Act, councils are required to have an Audit, Risk and Improvement Committee (ARIC). The responsibilities of the ARIC include reviewing risk management relevant to the council's operations, including in relation to cyber security risks.

The Local Government (General) Amendment (Audit, Risk and Improvement Committees) Regulation 2023 amends the 2021 Regulation to include additional requirements, including that a council must adopt and implement a system for managing risk with regard to relevant guidelines issued by the Office of Local Government (OLG). It also requires a council's annual report to include an attestation from the general manager about whether the risk management requirements have been complied with. These amendments come into effect on 1 July 2024.

The OLG finalised *Guidelines for Risk Management and Internal Audit for local government in NSW* under section 23A of the LG Act in December 2023.² The guidelines set out three core principles for risk management – councils and joint organisations must:

- have an ARIC that reviews aspects of the council's operations as prescribed under section 428A of the LG Act, including compliance, governance, and risk management
- implement a risk management framework that is consistent with current Australian standards for risk management (AS ISO 31000:2018 Risk Management – Guidelines at the time the draft guidelines were issued)
- have an independent internal audit function that reports to the ARIC and is consistent with current international standards for internal audit.

1.2 Cyber security incidents in local government

Councils use various systems and software to manage significant amounts of information and data relevant to corporate and service delivery functions, including sensitive and valuable data about their community and staff.

Increasing use of digital services in local government, including following the COVID-19 pandemic, has resulted in greater volumes and types of information and data being held by councils and an increased dependence on IT systems for council operations and service delivery. The need for local government to be able to effectively identify and manage cyber security risks is therefore more important than ever.

Cyber security incidents can directly impact governments, organisations and the public through compromise and distribution of sensitive personal information, identity theft, denial of service, and data loss. Governments and businesses that experience a cyber security incident may face financial and reputational damage.

In recent years, high profile cyber security incidents have increased community awareness and expectations that information and data is appropriately protected from cyber security incidents.

Exhibit 3: Recent examples of cyber security incidents impacting NSW Government and local councils

Date	Cyber security incidents
March-April 2020	Service NSW experienced a targeted phishing attack which resulted in 3.8 million documents being stolen, compromising the personal information of 104,000 people. Ineffective business email processes and a lack of multi-factor authentication were identified as key contributing factors to the data breach. The costs associated with the agency response were estimated to be more than \$30 million.
February 2021	Transport for NSW reported being impacted by a data breach on a third party file transfer system used by the agency to share and store files, resulting in information being taken. Sensitive customer and employee data was compromised by the incident.
November 2021	A human resources and payroll solutions provider used by government entities suffered a data breach. An unauthorised third party gained access to the provider's corporate network and removed data on that network including the personal information of employees. This incident caused reputational damage, and potential harm to individuals who may become subject to identity theft and other cybercrime.

² A Council must take any relevant guidelines issued under section 23A of the LG Act into consideration before exercising any of its functions.

Date	Cyber security incidents
April 2022	A council in New South Wales suffered a ransomware attack which impacted a wide range of business operations, including council records, employee financial data, and systems responsible for monitoring water quality.
April 2023	A commercial law firm that provides advice to Australian Government entities, NSW Government entities and local governments became aware in April 2023 of a data breach. Following this breach, sensitive information was published on the dark web.
May 2023	A company that provides enterprise technology services to local councils and other entities was subject to illegal access to its Microsoft 365 back-office system by an unauthorised third party.
August 2023	A council in New South Wales reported that their social media account was hacked, resulting in the account being compromised and taken offline.

Source: Audit Office of New South Wales based on publicly available information.

1.3 Relevant agencies

The following NSW Government and the Australian Government agencies provide guidance and support to local councils for cyber security risk management.

NSW Office of Local Government

The Office of Local Government (OLG) is responsible for strengthening the sustainability, performance, integrity, transparency and accountability of the local government sector. It does this through a range of activities including monitoring sector-wide and council-specific risks, issuing guidance, engaging with councils to build capacity and supporting the Minister for Local Government's discretionary intervention powers under the LG Act.

The OLG was part of the Department of Planning and Environment during this audit. On 1 January 2024, DPE was abolished and the OLG became part of the Department of Planning, Housing and Infrastructure.

Cyber Security NSW

Cyber Security NSW, part of the Department of Customer Service, aims to support NSW Government departments, agencies and local councils in continually improving their cyber resilience, and provide strategic cyber security leadership.

Cyber Security NSW's Local Government Engagement Plan (2023) states that it is focused on delivering services to support the vision of a cyber-secure NSW Government by:

- delivering products, services and best practice advice and guidance to NSW Government entities, including those in the local government sector
- coordinating whole-of-government cyber security strategies
- leading the NSW Government response to significant cyber security incidents and crises.

Australian Government agencies

The Australian Department of Home Affairs supports the Minister for Cyber Security's development of cyber security policy and implementing the Australian Government cyber security strategy. The National Office of Cyber Security within the Department of Home Affairs was established on 1 May 2023 to support the National Cyber Security Coordinator to lead this work.

The Australian Cyber Security Centre (ACSC), within the Australian Signals Directorate (ASD), leads the Australian Government's cyber security activities. The ACSC's services include cyber threat monitoring and publishing alerts, technical advice, advisories and notifications on significant threats. This audit did not examine operations performed by Australian Government agencies.

1.4 Legislative and policy framework for cyber security in local councils

The NSW Government has not set mandatory cyber security requirements for local councils in legislation or other policy.

However, there is a range of guidance available to councils, including recommended standards set out in the Cyber Security Guidelines – Local Government and the NSW Cyber Security Policy, developed and managed by Cyber Security NSW.

Cyber Security Guidelines – Local Government

In December 2022, the OLG issued the Cyber Security Guidelines – Local Government (the Guidelines). The Guidelines were developed by Cyber Security NSW in consultation with the OLG, following recommendations from the Audit Office of New South Wales that the OLG develop a cyber security policy to ensure cyber security risks over key data and IT assets are appropriately managed across councils, and key data is safeguarded.

Exhibit 4: Cyber Security Guidelines – Local Government on risk management

Extract from the Introduction to the Cyber Security Guidelines – Local Government

Councils should establish effective cyber security policies and procedures and embed cyber security into risk management practices and assurance processes. When cyber security risk management is done well, it reinforces organisational resilience, making entities aware of their risks and helps them make informed decisions in managing those risks. This should be complemented with meaningful training, communications and support across all levels of the Council.

Source: Cyber Security Guidelines – Local Government 2022 (December 2022), Introduction.

The Guidelines set out 'foundational requirements' for councils based on the NSW Cyber Security Policy (see [Appendix four](#)). This includes implementation of the ACSC Essential Eight Strategies to Mitigate Cyber Security Incidents (Essential Eight).

The ACSC developed the Essential Eight controls to serve as a baseline set of protections for organisations to make it more difficult for adversaries to compromise a system. The ACSC's Essential Eight Maturity Model uses a four-point scale (levels zero to three) to assist organisations to implement the controls in a graduated manner.³ The ACSC periodically updates the model in response to the observed techniques in use by malicious actors.

The Guidelines establish that compliance is 'strongly encouraged' but voluntary. Councils are not required to complete or report on self-assessments of their maturity against the Guidelines. Cyber Security NSW has advised that the Guidelines will be updated in 2024 in accordance with the recent review of the NSW Cyber Security Policy (see below).

NSW Cyber Security Policy

The NSW Cyber Security Policy sets out mandatory requirements for NSW Government agencies.

Each year, NSW Government agencies are required to self-assess against the NSW Cyber Security Policy and report that assessment to Cyber Security NSW.

The NSW Cyber Security Policy is not mandatory for local councils, but Cyber Security NSW recommends its adoption by councils as a foundation of strong cyber security practice.

Cyber Security NSW issued the latest version of the NSW Cyber Security Policy on 19 February 2024 which updates the minimum baseline requirements expected of agencies, and the way in which agencies are required to report to Cyber Security NSW.

³ ACSC webpage on the Essential Eight: [Essential Eight | Cyber.gov.au](https://www.cyber.gov.au/essential-eight).

Relevant legislative requirements

Privacy legislation

Under New South Wales privacy laws, Councils have legal obligations relating to the security of personal and health information.

Exhibit 5: Summary of information security requirements under NSW privacy laws

A council that holds personal and/or health information must ensure that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised use, modification or disclosure, and against all other misuse.

Source: Section 12 of the *Privacy and Personal Information Protection Act 1998* and clause 5 of Schedule 1 of the *Health Records and Information Privacy Act 2002*.

Privacy legislation in New South Wales is overseen by the NSW Privacy Commissioner, supported by the NSW Information and Privacy Commission (IPC). The IPC issues resources and guidance to support councils and other relevant entities to understand their privacy obligations, including guidance relevant to cyber security risk management such as data breach guidance and a fact sheet on compliance obligations relevant to Microsoft 365 platforms.

Mandatory data breach notification scheme

From 28 November 2023, local councils are required under the *Privacy and Personal Information Protection Act 1998* to notify the NSW Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm.

Prior to 28 November 2023, a voluntary data breach notification scheme was in place.

Australian Security of Critical Infrastructure Act 2018

The Australian Government's *Security of Critical Infrastructure Act 2018* (the SOCI Act) regulates critical infrastructure nationally and provides for mandatory cyber security incident reporting to the ACSC for critical infrastructure assets in certain circumstances. The SOCI Act defines what constitutes a critical infrastructure asset for the purposes of the Act, which includes assets that may be relevant to councils.

The SOCI Act is overseen by the Australian Government's Cyber and Infrastructure Security Centre, part of the Department of Home Affairs.

Other cyber security risk management guidance and frameworks

Other sources of good practice may inform councils' approaches to identifying and managing cyber security risks. These include:

- ACSC resources, including guidance on implementing the Essential Eight mitigation strategies from the ACSC's *Strategies to Mitigate Cyber Security Incidents* and an *Information Security Manual* which outlines a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and data from cyber threats.
- US National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*.
- Relevant Australian and International Organization for Standardization standards, including ISO 27001 'Information security, cybersecurity and privacy protection— Information security management systems – Requirements'.

In addition to the NSW Cyber Security Policy, these sources were available to local councils to inform their cyber security risk management practices prior to the release of the Guidelines. The Audit Office of New South Wales *Local Government 2022* report, published in May 2023, found that some councils had started developing their cyber security plans based on these sources in 2021–22.

1.5 Audited councils

The councils selected for this audit were City of Parramatta Council, Singleton Council and Warrumbungle Shire Council.

Exhibit 6: Overview of selected councils 2022–23

	City of Parramatta Council	Singleton Council	Warrumbungle Shire Council
Audit Office grouping	Metropolitan	Regional	Rural
Area (km ²)	84	4,893	12,380
LGA population	256,729	24,719	9,225
Number of staff	821	237	182

Source: Audit Office of New South Wales based on internal and publicly available information.

These councils were selected to provide coverage of cyber security risks across different council sizes, characteristics, location, demographics and kinds of services provided – including whether the council manages important infrastructure services.

This audit report has deidentified findings for each council, but the specific findings have been directly shared with each council to enable them to remediate and improve cyber safeguards. The findings and recommendations in this report are likely relevant to most local councils in NSW and they are encouraged to ensure they have sufficient cyber safeguards.

1.6 About the audit

This audit assessed how effectively the selected councils identified and managed cyber security risks from 1 July 2021 to 31 October 2023. The audit assessed this with the following questions:

- Does the council effectively identify and plan for cyber security risks?
- Does the council have controls in place to effectively manage identified cyber security risks?
- Does the council have processes in place to detect, respond to, and recover from cyber security incidents?

The audit focused on council risk management frameworks, processes and practices. Sound risk management processes and practices can assist councils to identify potential system vulnerabilities, reduce the likelihood of an incident occurring, and mitigate the severity of consequences where an incident occurs. These processes do not prevent an incident from occurring.

The audit did not conduct simulated cyber security exercises on the selected councils, or undertake detailed assessment or testing of the effectiveness of specific cyber security controls.

This audit did not assess the effectiveness of responses to cyber security incidents experienced by the selected councils, or the support provided to them during an incident response.

This audit also included Cyber Security NSW within the Department of Customer Service and the OLG within the Department of Planning and Environment (DPE) due to their roles in providing guidance and support to local government. The OLG was part of DPE up to 1 January 2024, when DPE was abolished and the OLG became part of the Department of Planning, Housing and Infrastructure.

2. Council findings

This chapter includes a summary of thematic key findings for the selected councils.

2.1 Identifying cyber security risks

Ineffective identification of cyber security risks can leave councils exposed to unmanaged risks which can lead to unnecessary costs, disruptions to services and reputational risk.

Two of the three councils identify cyber security as a strategic risk, but gaps in risk management processes across all three councils limit effective risk management

Obtaining an effective understanding of strategic and operational risks requires robust and documented risk assessments, determining a risk appetite, identifying mitigating actions, and clear timeframes and accountabilities for addressing the risks.

Council A has not undertaken a risk assessment to identify and assess cyber security risks to the Council and has significant gaps in its risk management approach. Council A did not have an enterprise risk management policy and framework until April 2023. The Council has not ensured that important elements of the risk management framework have been implemented in a timely way, including developing and finalising its enterprise risk register, and maintaining operational risk registers to apply the Council's risk appetite to strategic and operational risks.

Council B identifies cyber security as a risk in its strategic risk register, but listed controls refer to activities that are not being implemented in practice. The Council did not have an approved risk appetite statement throughout the audit period and therefore could not demonstrate whether risks were being managed within its risk appetite. Council B adopted a new enterprise risk management policy and risk appetite in December 2023. The Council did not effectively maintain operational risk registers to identify and manage cyber security risks (see [Chapter 2.3](#)).

Council C's strategic risk register identifies cyber security as a risk to its information and systems. The Council reviewed its risk appetite in February 2023 and defined its risk appetite in relation to technology and systems. Although Council C identifies a cyber-attack as a potential cause of risk in operational risk registers for most business units across the Council, some relevant risk registers have gaps such as controls not identified, risk ownership not defined, and some 'existing' controls are not in place.

None of the councils have assessed the business value of their information and systems to inform cyber security risk identification and management

To effectively identify and manage cyber security risks, councils need to understand the information and systems being used across their corporate and service delivery functions. This should include an assessment of the business value of the information and systems by considering how their availability, integrity, confidentiality, and reliability may be affected during or after a cyber security incident.

None of the councils have compiled a comprehensive list of the types of information and data they collect and store, or the systems and applications they use to collect and store information and data to inform cyber security risk assessments. Nor have they classified the business value or operational importance of their information and systems. This limits their ability to prioritise their activities to ensure that their most valuable information and systems are adequately safeguarded and secure.

None of the councils have identified and assigned responsibility for cyber security risks in relation to all core systems

The three councils use various IT systems and assets, including some supplied and managed by third party providers, to support their corporate and service delivery functions.

None of the councils have ensured that they have identified cyber security risks and assigned relevant risk management responsibilities for all core systems relevant to their corporate and service delivery functions, including systems used to manage important infrastructure services.

This has resulted in gaps in the coverage of the councils' cyber security activities and controls, and unclear cyber security risk management roles and responsibilities between council staff and third party IT providers which manage some of these systems. This may expose the councils to unknown or unmanaged vulnerabilities. See [Chapter 2.3](#) for further findings on managing third party risks.

2.2 Planning to improve cyber security

Councils should develop, implement and maintain a cyber security plan to ensure cyber security risks to their information systems and IT assets are appropriately managed and key data is safeguarded.

Building effective cyber resilience requires leadership and committed executive management, along with dedicated resourcing to build improvements in cyber security and culture.

Two of the three councils do not have a formal plan to improve their cyber security

Having a formal cyber security plan or strategy can support an entity to clearly understand and monitor its priorities and apply a systematic and strategic approach to the identification and management of cyber security risks.

Council A has not reviewed or assessed its cyber security capabilities to inform its approach to cyber security risk management. Council A started developing an IT strategy in 2020, but did not yet have a final and approved strategy by the end of the audit period. The most recent draft strategy (October 2022) referred to data security as a high risk to the Council but did not set out how the Council would address this risk. Council A advised in October 2023 that it intended to self-assess its maturity against the ACSC Essential Eight by December 2023. However, it has no structured plan for the completion of this self-assessment, such as by identifying the resources and expertise it requires to complete the self-assessment.

Council B does not have an approved plan to support improvements in its cyber security maturity. The Council assessed it had a low level of maturity against the ACSC's Essential Eight in July 2021, but the process and evidence behind this assessment were not clearly documented. The Council reported updates on an 'IT Cyber Security Program' in September and October 2022. However, it could not produce evidence of an approved plan or a strategic and structured approach to improving its cyber security maturity during the audit period. The Council advised in October 2023 that it intends to develop a plan to improve its cyber security.

Council C developed an IT strategy in August 2022 which includes 'Information Security' as one of four strategic priorities and set out key improvement initiatives in a cyber security roadmap. The roadmap sets out the Council's plan to address gaps identified and recommendations made by a third party provider and Cyber Security NSW in reviews of the Council's cyber security maturity and controls in 2021 and 2022. The Council's 2022–23 and 2023–24 operational plans include a deliverable of continual review and enhancement of cyber security capabilities linked to implementation of the roadmap.

Two of the three councils have not assessed the adequacy of cyber security resourcing and expertise to support effective cyber security risk management

Each NSW council has a unique resourcing profile in terms of their staffing, as well as their income and expenditure. This was reflected in the resourcing of cyber security activities across the selected councils.

Councils B and C have an IT team with cyber security responsibilities and also use third party systems and services to varying degrees. Council A does not have any staff with IT or cyber security roles and responsibilities and relies on third party arrangements, including a managed service provider arrangement with another NSW council, to manage its IT network and infrastructure.

Councils A and C have not undertaken workforce planning to identify the cyber security expertise, systems, processes or services required (internally and externally) to meet their desired level of cyber security maturity based on an assessment of the council's operating environment, cyber security risks and risk appetite. This creates challenges for the councils to demonstrate that they are effectively planning for and managing cyber security risks. For example:

- Council A has not ensured that cyber security roles and responsibilities for its managed service provider and other third party IT providers are defined and understood to ensure accountability for identifying and managing cyber security risks.
- Council C advised that limited resourcing is a factor in its ability to meet targets under its cyber security roadmap because relevant staff also have broader IT responsibilities. The Council's IT strategy also identifies resourcing gaps within its IT operations. However, the Council has not formally assessed the cyber security expertise and resources it requires to deliver its cyber security roadmap.

Council B dedicates resources and budget to cyber security activities and restructured its IT team in 2023 to reflect an increased use of third party arrangements. However, gaps in its record keeping and planning documentation limit accountability and transparency around how resource allocation is contributing to improved cyber security within the Council. For example, the Council lacked documentation to demonstrate that the engagement of a cyber security expert between March 2021 and November 2022 contributed to improving the Council's cyber security resilience.

None of the councils have implemented effective governance arrangements to ensure accountability for managing cyber security risks

None of the councils have effective governance arrangements to ensure accountability for cyber security risk management, planning and reporting during the audit period. This limits executive oversight of cyber security risks and the measures being taken to manage those risks.

Council A introduced a process for quarterly reporting to its executive leadership team on IT security in around 2021, but this formal reporting only occurred once in 2021. The Council provided updates on cyber security activities at executive leadership team meetings in May and August 2023, but did not have a mechanism for regularly reporting on cyber security risks. The Council advised in October 2023 that cyber security quarterly reports would be provided to its executive leadership team.

Council B regularly reported on IT activities, including cyber security updates and risk reports, to its executive leadership team between September 2021 and November 2022. However, the Council does not maintain records of relevant executive leadership team meetings and therefore cannot demonstrate how these reports were considered and related outcomes.

Council C developed a mechanism to track the progress of actions in the cyber security roadmap under its IT strategy, but has not yet implemented roles and responsibilities to oversee the strategy and roadmap to ensure accountability for its delivery. The Council has not regularly reported progress of the implementation of its roadmap to its executive leadership team. The Council advised in December 2023 that it intends to use its corporate reporting system to improve executive leadership team visibility of actions in the roadmap.

In 2023, Councils B and C each developed terms of reference for committees to improve corporate and executive oversight of their IT and cyber security activities. These committees were yet to be established and commence meetings at the end of the audit period in October 2023. These committees present an opportunity for the councils to improve executive-level accountability for timely and effective cyber security risk management, planning and reporting.

All three councils' reporting on cyber security to their ARICs lacked a consistent and risk-focused approach

The councils' reporting on cyber security activities to their ARIC during the audit period varied in frequency and content. None of the councils have developed a consistent and risk-focused approach to reporting to support their ARIC's role in reviewing risk management relevant to the council's operations.

Council A's ARIC requested in November 2022 that the Council develop a management mechanism for regular reporting on cyber security. Only one instance of such reporting occurred over the audit period. Council A advised in October 2023 that cyber security had been added as a standing item on the ARIC meeting agenda.

Council B included some information on cyber security controls implementation and effectiveness in reports to its ARIC during the audit period. However, these reports did not follow a consistent approach to assessing, monitoring and reporting the effectiveness of cyber security controls, and the Council has not documented how it implemented actions to address identified control weaknesses or gaps. Discussions and requests were recorded in ARIC meeting minutes. However, Council B does not have a process to monitor and report on the implementation of requests made by the ARIC relevant to cyber security. The Council did not provide evidence that ARIC requests from 2022 had been addressed.

Council C provided regular cyber security updates to its ARIC during the audit period, including progress updates on the implementation of its roadmap, but did not link relevant actions to the mitigation of identified cyber security or operational risks. This limits accountability for whether the prioritisation of activities under the roadmap is supporting the Council to manage cyber security risks.

2.3 Managing cyber security risks

Management of cyber security risks should be proportionate to, and situated within the context of, the council's risk appetite, resources and governance arrangements.

Gaps in the framework for managing cyber security, and failures to implement prevention strategies can increase councils' exposure to cyber threats.

None of the councils have effective cyber security policies and procedures

All three councils each have a cyber security policy, but the audit identified gaps and issues with their policies and related procedures that limit their usefulness to support effective cyber security risk management.

Key gaps and issues identified include:

- high level cyber security policy expectations are defined but not supported by procedures and processes to support staff implementation (all three councils)
- lack of clearly assigned responsibilities for core cyber security functions (all three councils) including:
 - managing cyber security risks
 - identifying, implementing and monitoring the effectiveness of cyber security controls
 - information and system backups
 - monitoring systems to detect and respond to cyber security incidents and events
- policies and procedures assign roles and responsibilities, but these are not being implemented in practice (Council A)
- policy had not been recently reviewed (Council B)
- lack of procedures to define expectations for documenting controls implementation and monitoring (all three councils)
- third party roles and responsibilities not defined (all three councils).

Council B was in the process of developing new policies and procedures during the audit period and advised that these were being implemented in October 2023.

None of the councils have a clear and consistent approach to monitoring the effectiveness of controls to mitigate identified cyber security risks

None of the councils were able to demonstrate that they were effectively monitoring the implementation of cyber security controls to manage cyber security risks.

Council A advises that it relies on third parties, including its managed service provider, to implement cyber security controls on its behalf such as multi-factor authentication, endpoint protection, and patching applications and systems. However, the Council has no processes to oversee and obtain evidence of the implementation of cyber security controls on its behalf. Some of the Council's statements about controls or practices in place (for example in insurance documentation) were not supported by evidence. Gaps in a council's self-assessment of the state of their cyber resilience and controls implementation may undermine effective decision making and risk management in responding to cyber risks.⁴

Council B used IT-specific risk registers between September 2021 and May 2022 to report on IT risks and related controls, including some relevant to cyber security. However, without an approved risk appetite statement, or an approved cyber security plan or strategy, it is unclear whether the Council was managing risks within its risk appetite and consistent with the Council's security objectives. Council B has not provided evidence that it has used IT or cyber-specific risk registers to identify, manage and report on cyber security risks since May 2022, and has not implemented an alternative mechanism to ensure it is taking a risk-based approach to prioritising its cyber security controls implementation.

Council C is implementing cyber security controls through its cyber security roadmap. In August 2023, the Council reported that it had completed ten of the 27 actions under the roadmap, including six actions identified as a high priority and actions relevant to Essential Eight mitigation strategies for patching applications, configuring macros, application hardening and patching operating systems. The Council's risk registers identify cyber-attack as a risk to its operations across various business units, but the Council does not clearly link its actions under the roadmap to the mitigation of cyber security risks.

⁴ The Audit Office of NSW's performance audit report on [Compliance with the NSW Cyber Security Policy \(2021\)](#) includes further discussion of risks relating to inaccurate self-assessments.

None of the councils are ensuring timely, risk-based responses to recommendations to address weaknesses and vulnerabilities in their cyber security controls

None of the councils have processes to ensure that recommendations from internal and external reviews that identified weaknesses or vulnerabilities in their cyber security controls are assessed and implemented in a timely, risk-based manner.

Examples of the councils not ensuring a timely and risk-based approach include:

- Council A has not yet developed an IT security risk assessment process, despite a recommendation that this be done in Audit Office financial audit management letters since 2016–17.
- Council B assessed its cyber security maturity as low in 2021 but provided limited evidence of progress to address identified weaknesses. The Council has advised that it has been reviewing and updating cyber security controls to address gaps and improve effectiveness since November 2022, including through external reviews of its network and operating environment. In October 2023, the Council provided a 'remediation action plan' which outlines actions relevant to implementation of recommendations made in cyber-related reviews of the Council's network and operating environment.
- Council C monitors timeframes for implementing cyber security controls recommended in external reviews under its roadmap, but timeframes have been extended without clearly documenting reasons for delay or assessing risks caused by failure to meet target timeframes.

All three councils could improve their record-keeping and reporting on actions taken to address relevant recommendations.

All three councils are not effectively identifying or managing third party cyber security risks

As discussed in [Chapter 2.1](#), the three councils each engage third party providers to varying degrees to provide IT and cyber security systems and services to support their service delivery and corporate functions. None of the councils have processes to ensure that cyber security risks relating to third party engagements are being identified and managed.

All three councils do not include guidance on cyber security risk assessments in their procurement policies and procedures. The procurement policy and guidance in Councils B and C note the importance of identifying and managing risks in procurement, but do not make specific reference to cyber security risks. Council A's procurement policy does not define procurement procedures or provide guidance on managing risks, including cyber security related risks, relevant to third party arrangements. None of the councils have provided evidence of risk assessments being undertaken for third party engagements relevant to cyber security.

All three councils did not ensure the following steps were undertaken and documented for each third party IT provider:

- defining cyber security expectations, roles and responsibilities in contracts and agreements
- checking the cyber security qualifications and certifications of third party providers
- assessing and documenting the risk management and controls of third parties
- seeking assurance to ensure cyber security expectations were being met.

The lack of clearly defined roles and responsibilities relating to cyber security for the councils and their third party providers reduces the likelihood that the councils' cyber security risks are being managed. It also limits the councils' ability to hold third party providers to account if their cyber-related service provision is not consistent with the councils' expectations.

Two of the three councils required all staff to complete cyber security training, but all three councils lacked a plan for regular cyber security training during the audit period

Cyber Security NSW reported in 2022 that people continue to play a large part in cyber security incidents and data breaches, with 82% of all breaches involving the use of stolen credentials, phishing or simply an error. Regular cyber security awareness training can ensure staff remain up-to-date on the types of cyber security attacks they should be alert to, and ensure that staff know what to do if they are involved in an incident.

Councils A and C required all staff to complete mandatory cyber security training during the audit period, but had not implemented a regular schedule of training.

- Council A introduced mandatory cyber security training for staff in May 2023. In October 2023, the Council advised that this training had been included in its staff induction program and that it will implement mandatory, annual cyber security training for all staff from 2024. The Council provided no cyber security training to staff until May 2023.
- Council C introduced mandatory cyber security training for staff in 2022 and for its councillors in 2023. However, the Council has not yet developed a regular or planned schedule of cyber security training.

Council B did not require all staff to complete cyber security training during the audit period, and only a small number of staff completed optional training. Council B implemented a mandatory program of regular cyber security training in October 2023.

2.4 Detecting, responding to and recovering from cyber incidents

The ACSC defines a 'cyber incident' as an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.

Cyber security incidents have the potential to damage the council concerned and spread to and impact other entities.

All three councils use third party tools to monitor for cyber incidents, but have not ensured that relevant roles and responsibilities are well defined and documented

Councils should ensure that their ICT systems and assets are monitored to identify cyber security events and verify the effectiveness of protective measures.

All three councils use third party tools to monitor for cyber incidents and events. However, the councils have not clearly defined the scope of their monitoring and detection activities, or the roles and responsibilities of council staff and third parties in monitoring and detecting incidents. This limits the councils' ability to demonstrate that these activities are effectively mitigating cyber security risks.

Council C's risk registers identified testing and monitoring of systems as partially effective controls against risks relevant to cyber security, but the Council had not documented the relevant testing and monitoring mechanisms, or how they were being used to mitigate risks across its various systems. Councils A and B do not assess the adequacy of monitoring and detection activities in risk management documentation.

All three councils tested their network resilience during the audit period, but do not have processes to ensure vulnerabilities are identified and managed effectively

All three councils do not have processes to ensure a timely and risk-based approach to identifying and managing vulnerabilities in their systems and networks.

All three councils receive vulnerability scanning reports and alerts from Cyber Security NSW, but roles and responsibilities for actioning these are not clearly defined.

All three councils each engaged a third party to test their network resilience during the audit period, which resulted in recommended actions for the councils to take to improve relevant cyber security controls. The three councils advised their ARIC of the outcome of the testing and the steps being taken to address the recommendations, but lacked clear processes to track and record activities to demonstrate the timely mitigation of identified risks. Council C has not considered and actioned a suggestion by its ARIC that further testing may be appropriate.

None of the councils have a formal plan for future testing of their systems or network.

None of the councils have a cyber incident response plan to ensure an effective response to and prompt recovery from cyber incidents

None of the councils have a cyber incident response plan. According to the ACSC:

All organisations should have a cyber incident response plan to ensure an effective response and prompt recovery in the event security controls don't prevent an incident occurring. This plan should be tested and regularly reviewed.

To be effective, a cyber incident response plan should align with the organisation's incident, emergency, crisis and business continuity arrangements, as well as jurisdictional and national cyber and emergency arrangements. It should support personnel to fulfill their roles by outlining their responsibilities and all legal and regulatory obligations.

Source: ACSC Cyber Incident Response Plan Guidance.

Council A advised that it relies on its managed service provider for incident response and recovery, but has not formally established relevant roles and responsibilities for managing and reporting on cyber security incidents in the managed service agreement or other documentation.

Councils B and C advised that their IT or corporate incident management processes apply to cyber security incidents. However, these processes do not define expectations, roles and responsibilities specific to cyber security incidents.

Council B was developing new cyber security policies during the audit period, including a policy specific to cyber security incidents.

Council C advised that it did not intend to develop a specific cyber incident response plan in addition to its business continuity plan and data breach policy. Although these documents are relevant to the Council's cyber incident response processes, they do not serve the same purpose as a cyber incident response plan.

None of the councils have up to date business continuity and disaster recovery planning documentation that includes cyber security

Cyber security should be included in business continuity and disaster recovery planning. The three councils do not have up to date business continuity and disaster recovery planning documentation. Two of the councils include cyber security in relevant documentation.

Council A's business continuity plan was last updated in 2015 and does not set out actions, roles and responsibilities in the event of a cyber security incident. The Council's managed service provider started to draft an IT disaster recovery plan in 2019 but this was not finalised and approved.

Council B's 2022 business continuity plan includes some guidance on responding to a cyber attack, but gaps in the plan limit its utility in guiding an incident response. The plan is under review, and related plans and policies are not in place or up to date. An internal audit found a lack of a disaster recovery plan or testing program was a significant risk for the Council and the Council was updating its IT disaster recovery arrangements in 2023. By the end of the audit period, the Council had not yet addressed all recommendations made in the internal audit, including development of a disaster recovery plan that defines all critical systems, roles and responsibilities.

Council C's business continuity plan and related sub plans include processes for responding to cyber security incidents. However, there were some gaps in these documents, which do not clearly define roles, responsibilities and expectations for responding to and reporting on cyber security incidents. Council C's disaster recovery procedure was last reviewed in May 2021 and does not reflect current disaster recovery arrangements which were being updated in 2023. Council C's roadmap and internal audit plan include items relevant to reviewing, updating and testing its IT disaster recovery and business continuity arrangements in 2023–24 and 2024–25.

None of the councils have clearly defined expectations for reporting cyber security incidents

Knowing who to notify about a cyber security incident is important so the right people can be involved at the right time to mitigate damage, and ensure councils comply with reporting requirements.

All three councils have not clearly defined processes and expectations for reporting cyber security incidents to ensure council staff understand what types of incidents should be reported and to whom, and that the council is effectively managing relevant business and operational risks.

All three councils do not maintain a register of cyber incidents to record information about the sources and types of incidents experienced and relevant responses

All three councils do not implement clear and consistent processes to record information about cyber security incidents that enable the council to track the sources and types of incidents experienced, and demonstrate the remediation actions taken, including whether the incidents were reported (internally or externally) and whether there was any post-incident evaluation to review the effectiveness of controls or the council's response.

Councils A and B did not have a cyber incident register or similar process to record cyber security incidents during the audit period. In December 2023, Council A advised it had developed a cyber incident register.

Council C provided a copy of a cyber security incident register, but the register only recorded one incident which occurred in 2021 and did not include other incidents that the Council advised had occurred since then. Council C advised that cyber security incidents are recorded in its corporate incident management system, but it has not defined what types of incidents should be reported and to whom to ensure a consistent and effective approach.

Two of the three councils developed policies to reflect the requirements of the new mandatory notification of data breach scheme in 2023

On 28 November 2023, amendments to the *Privacy and Personal Information Protection Act 1998* came into effect which require local councils to notify the NSW Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm.

Councils are also required to satisfy other data management requirements, including to maintain an internal data breach incident register, and have a publicly accessible data breach policy.

Councils A and C developed data breach policies in 2023 to reflect the new requirements under the mandatory notification of data breach scheme.

Council B did not ensure it was ready to comply with the new requirements. Council B's Privacy Management Policy and Plan were last updated in December 2022. Council B advised in December 2023 that it intends to develop a data breach policy and consider how it will comply with the mandatory notification of data breach scheme by June 2024.

3. Guidance and support for cyber security management in local government

Cyber Security NSW is responsible for supporting local councils to improve their cyber resilience through a range of services and guidance and published its Local Government Engagement Plan in 2023 (discussed below).

The Office of Local Government (OLG) is responsible for strengthening the sustainability, performance, integrity, transparency and accountability of the local government sector. It does this through a range of activities including monitoring sector-wide and council-specific risks, issuing guidance, engaging with councils to build capacity and supporting the Minister for Local Government's discretionary intervention powers.

3.1 Cyber Security Guidelines – Local Government

The NSW Government issued cyber security guidelines specific to the local government sector in December 2022

Since 2020, Audit Office reports on the results of the local government sector financial statements have identified that councils need to strengthen their cyber security. Gaps identified in councils' basic governance and internal controls to manage cybersecurity include councils not having a cyber security framework.

The Audit Office's [Report on Local Government 2019](#) recommended that the OLG develop a cyber security policy by 30 June 2021 to ensure cyber security risks over key data and IT assets are appropriately managed across councils, and key data is safeguarded.

Up to December 2022, there was no cyber security policy or guidelines specific to local councils. However, since 2019, Cyber Security NSW has recommended that councils adopt the NSW Cyber Security Policy, which sets out mandatory requirements for NSW Government departments and Public Service agencies. It is not mandatory for local councils.

The OLG advised Cyber Security NSW in late 2020 that voluntary guidelines would be more appropriate for the local government sector.

Between early 2021 and December 2022, Cyber Security NSW developed guidelines for the local government sector in consultation with the OLG and the local government sector.

The Cyber Security Guidelines – Local Government (the Guidelines) were issued to the sector via an OLG circular in December 2022.

The NSW Government recommends that councils implement the Guidelines, but could do more to monitor whether the Guidelines are enabling better cyber security risk management in the sector

The Guidelines outline cyber security standards recommended for NSW local government by Cyber Security NSW. Compliance with the Guidelines is voluntary, but strongly encouraged. In summary, the Guidelines:

- are designed to be read by General Managers, Chief Information Officers, Chief Information Security Officers (or equivalent) and Audit and Risk teams
- state that the Guidelines should form the basis of an internally developed cyber security policy for individual councils
- list requirements focused on enhancing planning and governance, developing a cyber security culture, safeguarding information and systems, strengthening resilience against attacks and improved reporting
- recommend that councils implement the ACSC Essential Eight mitigation strategies as a baseline.

The Guidelines also refer to self-assessment templates developed by Cyber Security NSW that councils can use to understand their level of cyber security maturity, and track progress against the foundational requirements and Essential Eight mitigation strategies.

Councils are not required to report their progress in implementing the Guidelines to Cyber Security NSW or the OLG.

The Audit Office's [Local Government 2023](#) report, tabled in March 2024, recommends that all councils should prioritise planning and governing cyber security to ensure cyber security risks over key data and IT assets are appropriately managed and key data is safeguarded. It states councils should refer to the Guidelines in fulfilling this recommendation.

While the roles of Cyber Security NSW and the OLG involve identifying and responding to specific sector risks, neither is monitoring the uptake of the Guidelines by local councils to identify whether they are enabling better cyber security risk management. Cyber Security NSW and the OLG have advised that they are not resourced to undertake such monitoring. This audit has not included detailed assessment of the resourcing of Cyber Security NSW or the OLG.⁵

Cyber Security NSW's Local Government Engagement Plan (November 2023) states that Cyber Security NSW will annually update the Guidelines in line with reviews of the NSW Cyber Security Policy and feedback from the OLG, Local Government NSW and local government entities.

Cyber Security NSW encourages councils to report cyber security incidents to Cyber Security NSW

The Cyber Security Guidelines – Local Government include a foundational requirement for councils to report cyber security incidents to their Chief Information Security Officer and/or Cyber Security NSW.

Cyber Security NSW advised that cyber security incident reporting is important because risks within some incidents may apply to other councils or government agencies, and that they encourage councils to report through existing channels of engagement with councils (see below on Cyber Security NSW's Local Government Engagement Plan).

This audit has found that the selected councils did not have procedures in place to define when cyber security incidents should be reported to Cyber Security NSW, although some councils did report incidents to Cyber Security NSW during the audit period.

⁵ The Audit Office of New South Wales considered the resourcing of Cyber Security NSW and the OLG in performance audits tabled in 2023: [Cyber Security NSW: governance, roles, and responsibilities \(February 2023\)](#) and [Regulation and monitoring of local government \(May 2023\)](#).

3.2 Supporting local councils

Cyber security poses a risk to councils and their communities, and it is a matter for each council to identify relevant business and operational risks and determine how to manage these risks.

Cyber Security NSW and the OLG have a role to engage with the sector to understand the extent and nature of these risks to ensure the support they provide to councils is tailored and proportionate to the risk context.

Cyber Security NSW provides a range of services to support local councils to strengthen their cyber security

Cyber Security NSW has no formal authority to mandate cyber security requirements for local councils but has a remit to assist local government to improve cyber resilience. Cyber Security NSW provides initiatives to strengthen councils' cyber security and assist with uplift.

Cyber Security NSW published a Service Catalogue in February 2023 which sets out the range of products, services and guidance available to NSW Government entities, including local councils. Cyber Security NSW does not charge for these services. Key products and services listed in the Service Catalogue include security assessments, awareness and training, advice and guidance, threat intelligence and incident response through advice and assistance on triage and containment. Each of the selected councils had some engagement with Cyber Security NSW during the audit period, but the scope of engagement varied from council to council, which is consistent with Cyber Security NSW's services being opt-in.

Cyber Security NSW also published its Local Government Engagement Plan in 2023 which outlines its methods of engagement with local government entities and the services that it provides. The Plan states 'Services offered by Cyber Security NSW will be prioritised on an as-needed basis. In consultation with local government entities, the plan states that Cyber Security NSW will assess risk and help determine what entities are most in need of support and which services will be most beneficial'.

NSW Government agencies are planning to do more to coordinate key messages, advice and expected maturity levels for local councils

Cyber Security NSW and the OLG advised that the focus of their engagement in relation to the local government sector during the audit period was to develop the Cyber Security Guidelines – Local Government and implement the DMARC email authentication solution to better protect councils' internet domains.⁶

Cyber Security NSW and the OLG did not have a mechanism for regularly sharing information about cyber security risks within the local government sector or to ensure that their roles and responsibilities and actions relevant to cyber security management were coordinated and complementary to support improved sector awareness and resilience.

Cyber Security NSW's Local Government Engagement Plan was updated in November 2023 to include information about its approach to stakeholder collaboration to support a cyber secure NSW Government, including through engagement with the OLG. The Plan states that Cyber Security NSW has established a schedule of engagement with the OLG to ensure their input into local government sector cyber security uplift. This will include the commencement of quarterly Executive meetings in 2024 and a series of webinars on thematic areas such as risk management and incident response, to complement Cyber Security NSW's Local Councils Forum.⁷

⁶ See Appendix 2 – Glossary for definition of DMARC.

⁷ The Local Councils Forum creates a community for local councils to exchange information relating to cyber security issues, trends and threats encountered in local government (Cyber Security NSW Service Catalogue, 2023).

The OLG is developing procurement guidelines for local councils, but the draft guidelines do not include guidance on managing third party cyber security risks

Managing third party risks is an important element of cyber security management. Councils use third parties to provide systems, software and services to support their IT infrastructure. Councils also use third parties for cyber security management activities such as monitoring vulnerabilities, scanning for unusual activity and endpoint protection.

Third party engagement brings additional risks since councils remain accountable for ensuring that their information and systems are adequately protected even when relying on third parties. Councils should consider such risks during procurement and third party engagement processes.

The OLG has not updated its procurement guidelines for local government since 2009.

An Audit Office [performance audit on procurement management in local government](#) in December 2020 recommended that by June 2022, the OLG⁸ should publish comprehensive and updated guidance on effective procurement. The OLG accepted this recommendation but did not meet the timeframe for implementation. At October 2023, the new guidelines were still in draft. The draft guidelines do not provide specific guidance on managing cyber security risks in the procurement process. However, they include general guidance which may be relevant to councils when engaging with third parties for ICT and cyber security services, such as on risk management, supplier due diligence and unsolicited proposals.

⁸ Part of the former Department of Planning, Industry and Environment at the time the recommendation was made.

Section two

Appendices

Appendix one – Response from entities

Response from City of Parramatta Council



22 March 2024

Ms Margaret Crawford PSM
Auditor General NSW
GPO Box 12
SYDNEY NSW 2001

Your Reference: R009-170534826-22146
Our ref: D09374298S

Dear Ms Crawford,

Performance Audit – Cyber Security in Local Government

Thank you for the opportunity to comment on the recent Performance Audit Report – Cyber Security in Local Government dated 21 February 2024.

Council acknowledges the valuable work of the NSW Audit Office and appreciates the cooperative manner in which the Performance Audit Team conducted this engagement. The audit process and communication between Council officers and the Performance Audit Team was open and transparent throughout the engagement.

Council accepts the formal recommendations contained within the Performance Audit Report and acknowledges the steps that the Audit Office has taken to de-identify the councils in the detailed findings sections of the final report that will be tabled in NSW Parliament.

The recommendations listed in the findings are consistent with the program Council has adopted to improve its Cyber Security position and this should be evident in Council's response to the Audit Office.

In conclusion, Council looks forward to being given the opportunity to update the Audit Office on our continued improvements in the Cyber Security space.

Yours sincerely

A handwritten signature in black ink, appearing to read "G. Connolly".

Gail Connolly PSM
Chief Executive Officer

Contact us:
council@cityofparramatta.nsw.gov.au | 02 9806 5050
@cityofparramatta | PO Box 32, Parramatta, NSW 2124
ABN 49 907 174 773 | cityofparramatta.nsw.gov.au

Response from Singleton Council



Council Reference: 23/00195

21 March 2024

Margaret Crawford
Auditor General
Audit Office of New South Wales

Via e-mail

Dear Ms Crawford,

Re: Performance Audit – Cyber Security in Local Government

Thank you for your letter dated 21 February 2024 and for allowing Singleton Council to respond to your final report of the Performance Audit – Cyber Security in Local Government.

The report outlines current weaknesses with Singleton Council's cyber security posture and no doubt these are common across the NSW Local Government industry. Singleton Council acknowledges and supports the Audit Office findings and recommendations outlined in the report.

Cyber Security is the highest rated risk within Council's Risk Register and has been the subject of several external reviews resulting in a detailed Cyber Security Actions Roadmap which underpins Council's ICT Strategy.

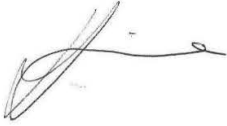
This report from the Audit Office along with an ASD8 review currently being undertaken on Council's cyber posture will be used to refresh Council's ICT Strategy and Council is committed to work with our Internal Audit Committee, IT Team and various external vendors to further strengthen Council's Cyber Security posture.

12 - 14 Queen Street Singleton
PO Box 314 Singleton NSW 2330
ABN 52 877 492 396

T 02 6578 7290
E council@singleton.nsw.gov.au
singleton.nsw.gov.au

Council thanks the NSW Audit Office and its staff for the professional manner in which this audit was undertaken, the communication throughout the process and the opportunity to be part of this Performance Audit. Council is looking forward to implementing the recommendations in the report.

Yours faithfully

A handwritten signature in black ink, appearing to read 'Jason Linnane', with a stylized flourish at the end.

Jason Linnane
General Manager

Response from Warrumbungle Shire Council

Coonabarabran:

14-22 John Street
Coonabarabran NSW 2357

PO Box 191
Coonabarabran NSW 2357

ABN: 63 348 671 239



Calls from within Shire
1300 795 099

Calls from outside Shire area
Coonabarabran:
02 6849 2000

Coolah: 02 6378 5000

Fax: 02 6842 1337

Email:
info@warrumbungle.nsw.gov.au

Coonabarabran - Coolah - Dunedoo - Baradine - Binnaway - Mendooran

Please address all mail to:
The General Manager

Please refer enquiries to:

21 March 2024

Ms Margaret Crawford
Auditor-General for NSW
GPO Box 12
SYDNEY NSW 2001

Dear Ms Crawford

PERFORMANCE AUDIT – CYBER SECURITY IN LOCAL GOVERNMENT

Thank you for your letter dated 21 February 2024 providing a copy of the Performance Audit Report on Cyber Security in Local Government.

Warrumbungle Shire Council appreciates the opportunity to respond to the final report. Council notes the findings and recommendations of the report and acknowledges the valuable contribution that the work of your agency provides to the local government sector in the conduct of such performance audits. Council sees continuous improvement as a key factor in our ability to meet the ever-changing needs of our community, noting that this must be accompanied by stringent standards of corporate governance in the business processes we implement to meet those community needs.

The audit identified many opportunities for improvement to our cyber policies and procedures in relation to cyber security. We note through our conversations with the Audit team that Council has some processes in place but a documented approach would further improve our focus in these areas. Council notes these finding and will consider ways to document our approach for these items. Council agrees with the findings identified in the report. [REDACTED]

Thank you again for undertaking the performance audit and for providing an opportunity to comment on the findings. Should you have any further enquiries regarding this matter please contact Council's Acting Manager Corporate Services, [REDACTED] at email: info@warrumbungle.nsw.gov.au.

Yours faithfully

LINDSAY MASON
ACTING GENERAL MANAGER



Response from Department of Customer Service

Department of Customer Service
Office of the Secretary



Our reference: BN-01374-2024
Your reference: R009-170535826-22147
15/03/24

By email: mail@audit.nsw.gov.au

Ms Margaret Crawford PSM
Auditor-General for New South Wales
Audit Office of NSW
Level 19, Darling Park Tower 2, 201 Sussex St
Sydney NSW 2000

Re: Performance audit – Cyber security in local government

Dear Ms Crawford,

Thank you for your letter conveying the final report of the 'Performance Audit – Cyber security in local government'. The local government sector delivers critical services to NSW communities, and such reports continue to highlight the requirement for enhanced cyber security capabilities and appropriate risk management, and will help inform the uplift of their cyber resilience.

Our approach

To support a cyber-secure NSW Government, Cyber Security NSW develops and implements initiatives to enhance the capability of NSW Government entities to prevent, detect, respond to and recover from cyber attacks. These offerings are outlined in our detailed, complete and accessible Service Catalogue.

In November 2023, Cyber Security NSW released the Local Government Engagement Plan, which outlines the model for engagement between NSW local government entities and Cyber Security NSW.

The Cyber Security NSW Local Government Engagement Plan sets out Cyber Security NSW's strategic approach to local government sector engagement, including: streams of engagement; expectations of local government entities; prioritisation strategy; and challenges to consider.

As noted in the report, Cyber Security NSW provides a vast range of products and services to support local councils in managing their cyber risk. These are detailed in the Cyber Security NSW Service Catalogue, which has been disseminated to local government stakeholders through multiple channels.

Among other cyber security initiatives to support local government in improving cyber resilience, Cyber Security NSW has engaged all 128 councils in the Domain-based Message Authentication,

McKell Building
2-24 Rawson Place, Sydney NSW 2000

Tel 02 9372 8877
TTY 1300 301 181

ABN 81 913 830 179
nsw.gov.au

Reporting and Conformance (DMARC) project. This initiative was centrally funded by Cyber Security NSW, and is one of the most effective methods of combatting email spoofing and phishing attacks.

It is also worth noting that more than half of all councils have been engaged in Cyber Security NSW's Essentials cyber security awareness training, through either live sessions or e-modules. This training improves the cyber security awareness of staff and provides councils with training insights.

Cyber Security NSW has established a dedicated Cyber Security Councils Forum, which creates a community to exchange information relating to issues, trends and threats encountered in the local government sector.

Furthermore, all councils receive Cyber Security NSW's intelligence products and are provided weekly vulnerability scanning reports as well as reports from the Australian Cyber Security Centre, when relevant.

Cyber Security NSW is also centrally funding a vulnerability risk management platform that enables NSW Government entities to monitor their public-facing internet presence and identify associated vulnerabilities using passive detection capabilities. The platform helps prevent and mitigate cyber security risks by monitoring the entity's and their vendors' domains, and can provide cyber security ratings and automatically detect leaked credentials and data exposures.

The platform provides third and fourth-party risk exposure reporting and access to vendor risk assessments, providing visibility of vendors' security profiles. With access to this platform, councils can review timely insights into where resources can be focused to achieve optimal cyber security outcomes for public-facing systems.

Cyber Security NSW provides this platform to all NSW Government entities, and is in the process of providing training and access to councils. This is occurring in staggered phases as not all councils have the technical resources to utilise the platform. Cyber Security NSW continues to provide reporting and technical guidance for uplift opportunities to NSW Government entities without the capacity to manage the platform.

Cyber Security NSW is preparing a paper that examines the Chief Information Security Officer (CISO)-as-a-service model that is currently in place across some councils. This emerging shared resource option is designed to assist small agencies and councils with cyber advisory leadership to ensure investment in cyber resilience is aligned to improving the cyber security of systems, networks and platforms.

This model is effectively operating for several councils where funding does not allow the employment of a dedicated CISO. It enables a cohesive cyber uplift strategy to be developed across several councils with efficiencies delivered through shared procurement of services.

Recommendations

Cyber Security NSW accepts Recommendation 6 and Recommendation 8 of the report.

Consistent with Recommendation 6 of the report, Cyber Security NSW has established a schedule of engagement with the Office of Local Government to ensure their input into local government sector cyber security uplift. This includes quarterly Executive meetings where opportunities for collaboration, including joint events, are discussed. The Office of Local Government advertises all relevant Cyber Security NSW events on its website, including the well-established Councils Forum.

Consistent with Recommendation 8 of the report, Cyber Security NSW is currently reviewing the Cyber Security Guidelines – Local Government to align with the updated NSW Cyber Security Policy. Councils can implement voluntary self-assessment against the guidelines, which sets out foundational cyber security requirements for local government and has been received positively by councils. While it is strongly recommended to follow the guidelines, councils are not required to report against them to Cyber Security NSW.

To foster holistic cyber resilience, it is critical to move beyond a singular focus on maturity levels and compliance and instead consider the unique risk profile of an entity and appropriate risk

mitigation strategies. A rigid understanding of maturity as a linear process does little to support the prioritisation of resources, funding and effort into meaningful and targeted uplift.

Cyber Security NSW is committed to delivering services to support a cyber-secure NSW Government, and will continue to engage with councils to enhance their cyber security.

As the NSW Government's dedicated cyber security agency, Cyber Security NSW leads collaboration and coordination with its state, territory and Commonwealth counterparts. The NSW Government places great importance on cyber security coordination initiatives, and to this end, Cyber Security NSW represents the NSW Government at the National Cyber Security Committee (NCSC). Cyber security uplift across the local government sector is a key priority for the NCSC. In line with this, the NCSC is promoting existing state, territory and Commonwealth service offerings to local government authorities through peak bodies, scalable engagement and direct outreach.

Additionally, the NCSC is working to enhance its understanding of local government agencies' cyber security needs, and continuing to engage with local government authorities through organisations such as the Australian Local Government Association (ALGA) to promote the importance of cyber security uplift.

Sincerely,



Graeme Head AO
Secretary

McKell Building
2-24 Rawson Place, Sydney NSW 2000

Tel 02 9372 8877
TTY 1300 301 181

ABN 81 913 830 179
nsw.gov.au

Response from Department of Planning, Housing and Infrastructure

Department of Planning, Housing and Infrastructure



Ref: A892204

Ms Margaret Crawford PSM
NSW Auditor General
GPO Box 12
SYDNEY NSW 2001

Via email

14 March 2024

Subject: Performance Audit Report – Cyber security in local government

Dear Ms Crawford,

Thank you for your letter of 21 February 2024 and the opportunity to respond to your Performance Audit Report – Cyber Security in Local Government (the Report).

I note you have also made recommendations in the Local Government Report to Parliament 2023 about councils' compliance with Cyber Security Guidelines – Local Government.

Council responsibilities

On 4 December 2023, the Office of Local Government (OLG), released the amended Local Government (General) Regulation 2022 (the Regulation) to give statutory force to key elements of the OLG Guidelines for Risk Management and Internal Audit for Local Government in NSW (the Guidelines). This requires each council in NSW to have an audit, risk and improvement committee (ARIC), a robust risk management framework, and an effective internal audit function effective from 1 July 2024.

ARICs will ensure councils develop a robust risk management framework that accurately identifies and mitigates the risks facing the council and its operations, including the recommendations identified in the Report regarding cyber security risks.

Draft procurement guidelines

OLG is currently updating the draft procurement guidelines and have acknowledged the inclusion of the management of cyber security risks. OLG anticipates these will be released by September 2024.

4 Parramatta Square, 12 Darcy Street, Parramatta NSW 2150
Locked Bag 5022, Parramatta NSW 2124

dphi.nsw.gov.au 1

Review of Cyber Security Guidelines – Local Government

The arrangements around a forward program for webinars and engagements are being finalised by Cyber Security NSW and OLG.

Should you require further assistance in relation to these matters, please do not hesitate to contact Brett Whitworth, Deputy Secretary, Office of Local Government on 0437 868 167 or by email at olg@olg.nsw.gov.au.

Sincerely,

A handwritten signature in black ink, appearing to read 'Kiersten Fishburn', with a small dot at the end.

Kiersten Fishburn
Secretary

4 Parramatta Square, 12 Darcy Street, Parramatta NSW 2150
Locked Bag 5022, Parramatta NSW 2124

dphi.nsw.gov.au 2

Appendix two – Glossary

Item	Definition
Business continuity plan	A plan that outlines how an organisation will respond effectively to disruptions and ensure continuity of service delivery, safety and availability of staff, availability of information technology and other systems, financial management and governance
Classification	The categorisation of systems and information according to the expected impact if it was to be compromised
Cyber attack	A deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity
Cyber incident	An unwanted or unexpected security event, or a series of such events, that have a significant probability of compromising business operations
Cyber incident response plan	A plan for responding to cyber security incidents
Cyber security	Measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them
Cyber security maturity	An assessment of the organisation's preparedness to identify, respond and recover from cyber attacks. This may include consideration of cyber security models such as the ACSC Essential Eight, or policies and guidance such as the Cyber Security NSW Cyber Security Policy and Cyber Security Guidelines – Local Government
Cyber threat	Any circumstance or event with the potential to harm systems or information
Disaster recovery plan	A plan that outlines an organisation's recovery strategy for how they are going to respond to a disaster
DMARC	Domain-based message authentication, reporting and conformance is an email authentication protocol to prevent hostile actors using 'spoofed' or forged email accounts
Essential Eight	The Essential Eight are eight essential mitigation strategies that the ACSC recommends organisations implement as a baseline to reduce the risk of adversaries compromising systems
ICT	Information and Communications Technology, also referred to as Information Technology (IT), includes software, hardware, network, infrastructure, devices and systems that enable the digital use and management of information and the interaction between people in a digital environment
Information security	The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability
Multi-factor authentication	A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are)
Patching	The action of updating, fixing, or improving a computer program
Risk appetite	The amount and type of risk that an organisation is willing to accept

Source: Audit Office of New South Wales based on internal and publicly available information.

Appendix three – Overview of Audit Office of New South Wales reports that consider cyber security

Report title	Year	Audit scope
Security of Critical IT Infrastructure	2015	This audit assessed whether the systems used to operate and manage critical infrastructure are secure and if systems go down, there are sound recovery arrangements.
Detecting and responding to cyber incidents	2018	This audit assessed how well cyber incidents are monitored and remedial advice is communicated in the NSW public sector.
Service NSW's handling of personal information	2020	This audit assessed how effectively Service NSW handles personal customer and business information to ensure its privacy.
Managing cyber risks	2021	This audit assessed how effectively selected agencies – Transport for NSW and Sydney Trains – identify and manage their cyber security risks.
Compliance with the NSW Cyber Security Policy	2021	This audit assessed agencies' compliance with the NSW Department of Customer Service's Policy 'DCS-2020-02 NSW Cyber Security Policy'.
Audit insights 2018–2022	2022	This report describes key findings, trends and lessons learned from audits conducted during 2018–2022. The report found that inadequate cyber security is a serious and increasing risk to agencies and citizens.
Cyber Security NSW: governance, roles and responsibilities	2023	This audit assessed the effectiveness of Cyber Security NSW's arrangements in contributing to the NSW Government's commitments under the NSW Cyber Security Strategy, in particular, increasing the NSW Government's cyber resiliency.
Annual reports on the results of findings of the financial audits of the local government sector since 2018–19 ⁹	2020 to 2023	These reports provide the results and findings of the completed annual financial audits of the local government sector (councils, joint organisations and county councils). The reports include findings relevant to cyber security in the context of the management of key IT risks and controls.
Internal controls and governance reports ¹⁰	2019 to 2023	These reports analyse the internal controls and governance of the largest agencies in the NSW public sector. The reports contain audit observations, conclusions and recommendations arising from review of agencies' information technology and cyber security planning and governance arrangements.

⁹ [Report on Local Government 2019](#); [Report on Local Government 2020](#); [Local Government Report 2021](#); [Report on Local Government 2022](#).

¹⁰ [Internal Controls and Governance 2019](#); [Internal controls and governance 2020](#); [Internal controls and governance 2021](#); [Internal controls and governance 2022](#); [Internal controls and governance 2023](#).

Appendix four – Cyber Security Guidelines – Local Government foundational requirements

This table includes the foundational requirements in the December 2022 version of the Cyber Security NSW Cyber Security Guidelines – Local Government as these were the relevant requirements during the audit period. Cyber Security NSW’s website contains the latest Guidelines and requirements.

Lead

1	Councils should implement cyber security planning and governance. Councils should:
1.1	Allocate roles and responsibilities as detailed in the Guidelines.
1.2	Ensure there is a governance committee at the executive level or equivalent (dedicated or shared) to be accountable for cyber security including risks, plans, reporting and meeting the requirements of the Guidelines.
1.3	Develop, implement and maintain an approved cyber security plan that is integrated with your organisation’s business continuity arrangements.
1.4	Include cyber security in their risk management framework and consider cyber security threats when performing risk assessments.
1.5	Be accountable for the cyber risks of their ICT service providers with access to or holding of government information and systems and ensure these providers understand and comply with the cyber security requirements of the contract, including the applicable parts of the Guidelines and any other relevant organisational security policies.

Prepare

2	Councils should build and support a cyber security culture across their organisation. Councils should:
2.1	Implement regular cyber security awareness training for all employees, contractors and outsourced ICT service providers.
2.2	Increase awareness of cyber security risk across all staff including the need to report cyber security risks.
2.3	Foster a culture where cyber security risk management is an important and valued aspect of decision-making and where cyber security risk management processes are understood and applied.
2.4	Ensure that appropriate access controls and security screening processes are in place for people with privileged access or access to sensitive or classified information.
2.5	Receive and/or provide information on security threats and intelligence with Cyber Security NSW and cooperate with NSW Government to enable management of government-wide cyber risk.

Prevent

3	Councils should manage cyber security risks to safeguard and secure their information and systems. Councils should:
3.1	Implement an Information Security Management System (ISMS), Cyber Security Management System (CSMS) or Cyber Security Framework (CSF).
3.2	Implement the ACSC Essential Eight.
3.3	Classify information and systems according to their business value (i.e. the impact of loss of confidentiality, integrity or availability).
3.4	Ensure cyber security requirements are built into procurements and into the early stages of projects and the system development life cycle (SDLC), including agile projects. Any upgrades to existing systems must comply with your organisation's cyber risk tolerance.
3.5	Audit trail and activity logging records are determined, documented, implemented and reviewed for new ICT systems and enhancements.

Detect, respond, recover

4	Councils should improve their resilience including their ability to rapidly detect cyber incidents and respond appropriately. Councils should:
4.1	Have a current cyber incident response plan that integrates with the agency incident management process and the NSW Government Cyber Incident Response Plan.
4.2	Exercise their cyber incident response plan at least every year.
4.3	Ensure that ICT systems and assets are monitored to identify cyber security events and verify the effectiveness of protective measures.
4.4	Report cyber security incidents to their CISO and/or Cyber Security NSW. If relevant, ensure incident reporting is compliant with Federal reporting requirements.

Source: Cyber Security Guidelines – Local Government, December 2022.

Appendix five – About the audit

Audit objective

This audit assessed how effectively three selected councils (City of Parramatta Council, Singleton Council and Warrumbungle Shire Council) identified and managed cyber security risks.

Audit criteria

We addressed the audit objective by assessing whether:

1. The councils effectively identified and planned for cyber security risks.
 - a) The council identified cyber security as a risk in its risk register.
 - b) The council classified its information and systems by operational importance and identified relevant cyber risks.
 - c) The council had the required cyber expertise, systems, policies, and processes in place to identify and manage cyber security risks.
 - d) The council had a plan in place to ensure it meets an appropriate level of cyber security maturity based on its risk identification and assessment.
2. The councils had controls in place to effectively manage identified cyber security risks.
 - a) The council had controls in place to address identified cyber security risks.
 - b) The council's leadership and governance supported its approach to managing cyber security risks.
 - c) The council effectively built cyber security awareness across the organisation through regular training and awareness raising activities.
 - d) The council effectively managed cyber security risks relating to third party ICT providers.
3. The councils had processes in place to detect, respond to, and recover from cyber security incidents.
 - a) The council undertook regular testing and monitoring of its ICT systems.
 - b) The council had a plan in place to respond to, and recover from, cyber security incidents.
 - c) The council reported cyber security incidents and actions taken in line with relevant legislation and policies.

Audit scope and focus

In assessing the criteria, we checked the following aspects:

1. risk management planning including workforce planning, the classification of information and systems by operational importance, and whether the council has a cyber security plan
2. effective identification and management of cyber security risks through risk assessments and control implementation processes, including in relation to managing third party cyber security risks
3. leadership and governance relevant to cyber security risk management and promoting a cyber security culture through training and awareness activities
4. processes to detect, respond to and recover from cyber security incidents, including monitoring and testing of systems, disaster recovery and business continuity planning, and cyber incident reporting and post-incident evaluation.

This audit focused on the selected councils' cyber security activities from 1 July 2021 to 31 October 2023.

This audit also included the Office of Local Government (part of the Department of Planning and Environment until 1 January 2024, now part of the Department of Planning, Housing and Infrastructure) and Cyber Security NSW (part of the Department of Customer Service) due to their roles in providing guidance and support to local government.

Audit exclusions

The audit did not:

- conduct simulated cyber security exercises on the selected councils, or undertake detailed assessment or testing of the effectiveness of specific cyber security controls
- conclude on whether the selected councils are compliant with the Cyber Security Guidelines – Local Government
- examine how the Department of Planning and Environment or the Department of Customer Service identify and manage cyber security risks, or the effectiveness of the controls these agencies have in place to manage their cyber security risks
- question the merits of Government policy objectives.

Audit approach

Our procedures included:

1. Interviewing:
 - Senior council staff with responsibility for cyber security
 - Other council staff with cyber security responsibilities
 - Council staff with enterprise risk management responsibilities
 - Cyber Security NSW staff
 - Office of Local Government staff.
2. Examining relevant documentation including:
 - Documentation relating to cyber security activities and incidents
 - Risk management frameworks and documentation
 - Minutes and papers from relevant executive and Audit, Risk and Improvement Committee meetings
 - Relevant internal and external audit reports and reviews
 - Staff training information and completion rates
 - A selection of contracts and contract management documentation.

The audit approach was complemented by quality assurance processes within the Audit Office to ensure compliance with professional standards.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Auditing Standard ASAE 3500 Performance Engagements and other professional standards. The standards require the audit team to comply with relevant ethical requirements and plan and perform the audit to obtain reasonable assurance and draw a conclusion on the audit objective. Our processes have also been designed to comply with requirements specified in the *Government Sector Audit Act 1983* and the *Local Government Act 1993*.

Acknowledgements

We gratefully acknowledge the cooperation and assistance provided by City of Parramatta Council, Singleton Council, Warrumbungle Shire Council, the Department of Planning and Environment (Office of Local Government) and the Department of Customer Service (Cyber Security NSW).

Audit cost

The estimated cost of the audit is \$744,000.

Appendix six – Performance auditing

What are performance audits?

Performance audits assess whether the activities of State or local government entities are being carried out effectively, economically, efficiently and in compliance with relevant laws.

The activities examined by a performance audit may include a government program, all or part of an audited entity, or more than one entity. They can also consider particular issues which affect the whole public sector and/or the whole local government sector. They cannot question the merits of government policy objectives.

The Auditor-General's mandate to undertake audits is set out in the *Government Sector Audit Act 1983* for state government entities, and in the *Local Government Act 1993* for local government entities. This mandate includes audit of non-government sector entities where these entities have received money or other resources, (whether directly or indirectly) from or on behalf of a government entity for a particular purpose (follow-the-dollar).

Why do we conduct performance audits?

Performance audits provide independent assurance to the NSW Parliament and the public.

Through their recommendations, performance audits seek to improve the value for money the community receives from government services.

Performance audits are selected at the discretion of the Auditor-General who seeks input from parliamentarians, State and local government entities, other interested stakeholders and Audit Office research.

How are performance audits selected?

When selecting and scoping topics, we aim to choose topics that reflect the interests of parliament in holding the government to account. Performance audits are selected at the discretion of the Auditor-General based on our own research, suggestions from the public, and consultation with parliamentarians, agency heads and key government stakeholders. Our three-year performance audit program is published on the website and is reviewed annually to ensure it continues to address significant issues of interest to parliament, aligns with government priorities, and reflects contemporary thinking on public sector management. Our program is sufficiently flexible to allow us to respond readily to any emerging issues.

What happens during the phases of a performance audit?

Performance audits have three key phases: planning, fieldwork and report writing.

During the planning phase, the audit team develops an understanding of the audit topic and responsible entities and defines the objective and scope of the audit.

The planning phase also identifies the audit criteria. These are standards of performance against which the audited entity, program or activities are assessed. Criteria may be based on relevant legislation, internal policies and procedures, industry standards, best practice, government targets, benchmarks or published guidelines.

During the fieldwork phase, audit teams will require access to books, records, or any documentation that are deemed necessary in the conduct of the audit, including confidential information which is either Cabinet information within the meaning of the *Government Information (Public Access) Act 2009*, or information that could be subject to a claim of privilege by the State or a public official in a court of law. Confidential information will not be disclosed, unless authorised by the Auditor-General.

At the completion of fieldwork, the audit team meets with management representatives to discuss all significant matters arising out of the audit. Following this, a draft performance audit report is prepared.

The audit team then meets with management representatives to check that facts presented in the draft report are accurate and to seek input in developing practical recommendations on areas of improvement.

A final report is then provided to the accountable authority of the audited entity(ies) who will be invited to formally respond to the report. If the audit includes a follow-the-dollar component, the final report will also be provided to the governing body of the relevant entity. The report presented to the NSW Parliament includes any response from the accountable authority of the audited entity. The relevant Minister and the Treasurer are also provided with a copy of the final report for State Government entities. For local government entities, the Secretary of the Department of Planning, Housing and Infrastructure, the Minister for Local Government and other responsible Ministers will also be provided with a copy of the report. In performance audits that involve multiple entities, there may be responses from more than one audited entity or from a nominated coordinating entity.

Who checks to see if recommendations have been implemented?

After the report is presented to the NSW Parliament, it is usual for the entity's Audit and Risk Committee / Audit Risk and Improvement Committee to monitor progress with the implementation of recommendations.

In addition, it is the practice of NSW Parliament's Public Accounts Committee to conduct reviews or hold inquiries into matters raised in performance audit reports. The reviews and inquiries are usually held 12 months after the report received by the NSW Parliament. These reports are available on the NSW Parliament website.

Who audits the auditors?

Our performance audits are subject to internal and external quality reviews against relevant Australian standards.

The Public Accounts Committee appoints an independent reviewer to report on compliance with auditing practices and standards every four years. The reviewer's report is presented to the NSW Parliament and available on its website.

Periodic peer reviews by other Audit Offices test our activities against relevant standards and better practice.

Each audit is subject to internal review prior to its release.

Who pays for performance audits?

No fee is charged to entities for performance audits. Our performance audit services are funded by the NSW Parliament.

Further information and copies of reports

For further information, including copies of performance audit reports and a list of audits currently in-progress, please see our website www.audit.nsw.gov.au or contact us on 9275 7100.

OUR VISION

Our insights inform and challenge government to improve outcomes for citizens.

OUR PURPOSE

To help Parliament hold government accountable for its use of public resources.

OUR VALUES

Pride in purpose
Curious and open-minded
Valuing people
Contagious integrity
Courage (even when it's uncomfortable)

Level 19, Darling Park Tower 2
201 Sussex Street
Sydney NSW 2000 Australia

PHONE +61 2 9275 7100

mail@audit.nsw.gov.au

Office hours: 8.30am-5.00pm
Monday to Friday.