PERFORMANCE AUDIT

8 FEBRUARY 2023

Cyber Security NSW: governance, roles, and responsibilities

NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

audit office
OF NEW SOUTH WALES

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 Goverment Act 1993*.

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 38EC of the *Government Sector Audit Act 1983,* I present a report titled **'Cyber Security NSW: governance, roles, and responsibilities'.**

Margaret Crawford PSM
Auditor-General for New South Wales
8 February 2023

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.

auditoffice
OF NEW SOUTH WALES

Banner image: 'Yarning Circle' by Caitlin Liddle, Audit Office Indigenous Internship Program participant used with permission.

contents

Cyber Security NSW: governance, roles, and responsibilities

Section one

Cyber Security NSW: governance, roles, and responsibilities

Executive summary

The NSW Cyber Security Strategy details a vision for '…NSW to become a world leader in cyber security, protecting, growing, and advancing our digital economy'. Cyber Security NSW, located within the Department of Customer Service, has lead responsibility for one of the four commitments in the strategy: to increase the NSW Government's cyber resilience.

Cyber Security NSW 'aims to provide the NSW Government with an integrated approach to preventing and responding to cyber security threats'. It does not provide broader consumer-focused services.

In August 2020, the NSW Government approved a business case to enhance the funding and remit of Cyber Security NSW to include a broader range of services and functions. As a result, Cyber Security NSW is receiving $60 million in funding from 2020–21 to 2022–23, an increase from its previous funding of around $5 million per year (which had been sourced from contributions from each NSW Government department).

The objective of this performance audit was to assess the effectiveness of Cyber Security NSW's arrangements in contributing to the NSW Government's commitments under the NSW Cyber Security Strategy, in particular, to increase the NSW Government's cyber resilience.

We assessed this objective through two lines of inquiry:

1. Are internal planning and governance processes in place to support Cyber Security NSW meet its objectives?
2. Are Cyber Security NSW roles and responsibilities defined and understood across the public sector?

The Audit Office of New South Wales has reported on the topic of cyber security previously. Most recently, the Internal Controls and Governance 2022 report included findings and recommendations relating to cyber security internal controls and governance at 25 of the largest agencies in the NSW public sector. While that report is multi-agency and sought to assess the level of cyber security attained in selected agencies, this current performance audit report focuses specifically on Cyber Security NSW and how well-equipped it is to meet its whole-of-government cyber security leadership and coordination roles.

Conclusion

Cyber Security NSW has a clear purpose that is aligned with wider government policy and objectives, but it cannot effectively demonstrate its progress toward improving cyber resilience

Cyber Security NSW's high-level purpose is to support the NSW Government's delivery of digitised services that are protected, connected, and trusted. This purpose is consistent with broader NSW Government and Australian Government policy and builds on the purpose of the previous NSW Office of the Government Chief Information Security Officer, which was itself informed by external research and previous Audit Office of New South Wales recommendations.

In delivering its purpose, Cyber Security NSW provides a wide range of services to NSW government agencies and the local government sector. The majority of agencies and councils consulted during this audit reported that the services they received contributed to improving their individual cyber security.

However, Cyber Security NSW does not clearly and consistently communicate its key objectives to ensure that its efforts are effectively and efficiently targeted, prioritised, planned, and reported. This is despite it receiving enhanced funding to expand the scope of services it provides. It currently has many sets of objectives across a range of sources, including the Cyber Security Strategy, business plans, corporate material, and public communications. It has too few reliable and meaningful ways of measuring progress toward its objectives, and no overall workplan or roadmap to show how the objectives will be achieved.

Without a clear and consistent program logic, it is difficult to determine whether the functions and services delivered by Cyber Security NSW are helping to achieve the level of cyber resilience required to meet the increasing cyber threats faced by the NSW public sector.

Cyber Security NSW does not provide assurance of the cyber security maturity self-assessments performed by individual NSW Government agencies

The NSW Government has a devolved model for cyber security assurance. Cyber Security NSW administers the whole-of-government policy settings, and agency heads are responsible for ensuring compliance with policy requirements.

Cyber Security NSW has a remit to carry out audits of agencies' self-assessments, but it has not carried out these audits and does not seek its own assurance of the results of these self-assessments. It is not sufficiently addressing previously identified inconsistencies and inaccuracies in how those self-assessments are performed and reported.

This form of auditing would be an important assurance that self-assessment and reporting is reliable. This is important given that maturity reporting is the main source of knowledge about the cyber security maturity and resilience of NSW Government agencies to cyber threats. If these self-assessments are unreliable, then it creates the risk that knowledge of the potential resilience of the NSW public sector to cyber security incidents is similarly unreliable. There is no other body in NSW with the mandate to routinely provide this form of assurance.

Cyber Security NSW has a remit to assist local government improve cyber resilience, however it cannot mandate action, and does not have a strategic approach guiding its efforts

Consistent with the expectations that accompanied its 2020 funding enhancement, Cyber Security NSW has engaged with the local government sector, albeit with mixed results. While these mixed results are partly a consequence of it not being provided a formal mandate in the sector, it has also been impacted by the fact that Cyber Security NSW has not established an engagement plan or strategy to guide its engagement with the local government sector.

1. Key findings

The high-level purpose and foundational pillars of Cyber Security NSW align with broader NSW Government policy and have an evidence base or rationale

Cyber Security NSW has a high-level purpose to support the NSW Government's delivery of digitised services that are protected, connected, and trusted.

This purpose aligns with broader NSW Government policy, including the NSW Premier's priorities to make it easy to engage with government and to provide a world-class public service. The 2019 NSW Government Beyond Digital Strategy expressly cites the establishment of a whole-of-government cyber security function as an enabler of the strategic direction to deliver better frontline technology. This is reiterated in the 2021 revision to the strategy, which specifically cites Cyber Security NSW.

The work of Cyber Security NSW, and its organisational structure, is based on pillars, which have been substantively carried over from its predecessor body, the Office of the Government Chief Information Security Officer. These pillars were informed by research and are consistent with previous Audit Office of NSW recommendations.

Cyber Security NSW has not effectively communicated its key strategic aims and objectives and is not measuring and reporting on progress against these

While the high-level purpose and core pillars that frame Cyber Security NSW's structure are sound, the structure and communication of its supporting objectives are less clear. Various sources describe a range of different performance standards, including:

- target areas
- priorities
- key areas
- strategic objectives
- aims
- benefits
- objectives.

Cyber Security NSW has not clearly articulated which of these are the key aims and objectives it is working towards. This is also reflected in team-level work planning, where we found evidence of sound planning techniques, though different teams aligned their workplans to different objectives.

Most reporting by Cyber Security NSW on progress toward achieving its purpose is activity-based. Without conceptually sound performance measurement and reporting, it is difficult to determine whether these services and functions are contributing to uplifting cyber maturity and improving resilience at a public sector-wide level.

Stakeholders consulted during this audit reflected positively on the services and functions provided to them by Cyber Security NSW. However, without sound performance measures, it is difficult to objectively determine if these services and functions contribute to meeting outcomes.

While there was consultation and analysis performed to inform original decision-making about the services and functions provided, there has been little systematic review or analysis about whether Cyber Security NSW is meeting agency or council needs.

Cyber Security NSW is developing its organisational capabilities to meet its purpose

Cyber Security NSW is a relatively new entity, having been initially established in 2017 (as the Office of the Government Chief Information Security Officer), then issued an expanded remit (and funding) in 2020. It has been managing a period of substantial growth, while still maintaining its business-as-usual functions of providing the NSW public sector with intelligence, capability-development, and support with the implementation of the NSW Government Cyber Security Policy.

As an evolving organisation, Cyber Security NSW was able to demonstrate a range of initiatives intended to raise its organisational capability. This includes improving how it uses information to drive public sector uplift, building its capability in project management, improving how it reports to the NSW Government and the community on sector maturity, and enhancing the accessibility of its service offerings to agencies and councils.

Individual agencies are responsible for managing their own cyber security risk and Cyber Security NSW has a limited mandate to intervene where risks emerge

While Cyber Security NSW has a whole-of-government leadership, coordination, and assurance role, each agency is responsible for its own cyber security risk. This is clearly established in the NSW Government Cyber Security Policy, as well as the Cyber Security Incident Emergency Sub Plan under the State Emergency Management Plan. Agencies are also responsible for implementing the relevant controls specified in the Cyber Security Policy. At the same time as announcing the enhanced funding for Cyber Security NSW, the NSW Government also announced an additional $180 million (over three years from 2020–21 to 2022–23) from the Digital Restart Fund for departments to directly support their own cyber security maturity uplift.

Moreover, the establishment of the Cyber Security Senior Officers' Group was intended to reflect that cyber security risk is owned by the executive leadership of agencies, and not made the responsibility of information technology (IT) departments. This is reinforced by the Cyber Security Policy.

As individual agencies own their cyber security risk – along with their IT infrastructure - Cyber Security NSW has limited mandate to directly intervene where risks emerge. Cyber Security NSW also has no mandate to ensure that agencies set appropriately challenging targets under the self-assessment model.

Agencies and councils consulted in this audit had a sound understanding of Cyber Security NSW's high-level purpose generally, although limited awareness of its specific services and functions

Among agencies and councils consulted in this audit, there was general acceptance and understanding of the high-level purpose of Cyber Security NSW, although there were mixed views on how robustly it should undertake its compliance and assurance role. While agencies consulted were not receptive to the idea of Cyber Security NSW playing a strong enforcement and regulatory role, there was acknowledgement of the need to ensure that agencies were achieving, assessing, and reporting on their compliance under the Cyber Security Policy in a consistent and reliable manner.

While the high-level purpose of Cyber Security NSW was well understood, there was relatively poor understanding of the services offered by Cyber Security NSW. This highlighted the importance of communicating a clear, accessible, detailed, and comprehensive service catalogue.

Cyber Security has not audited agency self-assessments under the Cyber Security Policy

As a central agency whole-of-government function, Cyber Security NSW's primary form of authority is a mandatory administrative requirements circular issued by the Secretary of the Department of Customer Service. The circular notes that clusters and agencies will be '…subject to audits by Cyber Security NSW commencing 2020–21 to test compliance with the Policy and reporting these outcomes to the Secretaries' Board'.

Cyber Security NSW has not yet performed audits of agencies to test compliance with the Cyber Security Policy. This is despite the Audit Office of NSW (and an external consultant engaged by Cyber Security NSW) previously finding inconsistency in how agencies perform and report these self-assessments.

This form of auditing would be an important assurance that self-assessment and reporting is reliable. This is important given that this maturity reporting is the main source of knowledge about the maturity and resilience of NSW Government agencies to cyber threats. If these self-assessments are unreliable, then it creates the risk that knowledge of the potential resilience of the NSW public sector to cyber security incidents is similarly unreliable.

Cyber Security NSW has some responsibility, although no authority, to improve cyber security resilience in the local government sector

Under its 2020 enhanced funding, Cyber Security NSW was given a range of general responsibilities for extending support to, and raising capability of, cyber security in the local government sector, including to provide:

- proactive monitoring and intelligence
- training and awareness.

However, despite this responsibility, Cyber Security NSW has no formal authority to mandate cyber security requirements on local councils. While it has had some success in engaging with local councils on specific programs or projects, it is unclear whether the services available to councils are well targeted to raise their cyber security resilience, or whether councils have detailed awareness of existing services. Cyber Security NSW relies on relationship building and an opt-in approach to engaging with councils. However, this approach is not supported by a formal or strategic engagement plan. The absence of a formal stakeholder engagement strategy or plan may limit how effectively Cyber Security NSW can improve cyber resilience in the local government sector.

Cyber Security NSW has developed non-binding guidelines for local government in collaboration with the Office of Local Government (OLG). However, implementation of these guidelines was delayed. The guidelines were released on 19 December 2022.

2. Recommendations

By 30 June 2023, the Department of Customer Service should:

1. implement an approach that provides reasonable assurance that NSW Government agencies are assessing and reporting their compliance with the NSW Government Cyber Security Policy in a manner that is consistent and accurate
2. ensure that Cyber Security NSW has a strategic plan that clearly demonstrates how the functions and services provided by Cyber Security NSW contribute to meeting its purpose and achieving NSW Government outcomes
3. ensure that Cyber Security NSW has a detailed, complete, and accessible catalogue of services available to agencies and councils
4. develop a comprehensive engagement strategy and plan for the local government sector, including councils, government bodies, and other relevant stakeholders.

1. Introduction

Cyber security is an evolving landscape where the nature and scale of threats are increasing. The Australian Cyber Security Centre (ACSC), the Australian Government lead agency for cyber security, reported in its in 2020–21 annual report that it received over 67,500 cybercrime reports, equating to one report of a cyber attack every eight minutes, with no sector of the economy or type of government agency immune.

Citizens of NSW are increasingly accessing online government services in this context, providing different types of sensitive personal information. This reliance and transition to digital services has increased in recent times, particularly during the COVID-19 pandemic. The NSW Legislative Council's Portfolio Committee (the Committee) noted in the March 2021 inquiry report into cyber security in NSW that 'a failure to get cyber security right in New South Wales represents a significant risk to the State's economy, business and community, and will affect public trust in government'.

The Committee noted that sound cyber security practices across NSW Government agencies, which Cyber Security NSW was established to drive, will enable the State and community to leverage opportunities from the digital world. Indeed, NSW aims to become a world leader in cyber security by protecting, growing and advancing the digital economy.

Establishment of Cyber Security NSW

Prior to the establishment of Cyber Security NSW, the Office of the Government Chief Information Security Officer was responsible for cyber security across the NSW government sector. This role was announced in March 2017 and was tasked with 'identifying areas of high risk of attack, and working across NSW agencies to share intelligence, facilitate minimum security standards, and ultimately ensure that citizens can trust in the NSW Government's delivery of digital transformation'. At the time of this appointment, the Minister for Customer Service and Digital Government stated that 'cyber security and risk has emerged as one of the most high-profile, borderless and rapidly evolving risks facing government'.

The Office of the Government Chief Information Security Officer was renamed on 20 May 2019 to Cyber Security NSW. Governance updates at the time note that this was undertaken to 'better reflect the leadership and coordination role required to uplift cyber security and decision-making across NSW Government'. The establishment of Cyber Security NSW was also partly in response to the Audit Office of New South Wales 2018 performance audit report on 'Detecting and Responding to Cyber Security Incidents'. That audit found that there was no whole-of-government capability to detect and respond effectively to cyber security incidents. Cyber Security NSW is relatively new and is established as a branch within the Department of Customer Service (DCS).

The Office of the Government Chief Information Security Officer, and subsequently Cyber Security NSW, was initially funded through a levy imposed on clusters. Funding arrangements for Cyber Security NSW changed with the announcement in August 2020 of $240 million over three years for the stated purpose of bolstering the NSW Government's cyber security capability and creating a world leading cyber industry. This funding included direct investment of $60 million from 2020–21 to 2022–23 for Cyber Security NSW to increase its capability and capacity, with the size of the team at the time expected to grow from 25 to 100 staff. In announcing this funding, the Minister for Customer Service and Digital Government stated that '…this is the biggest single cyber security investment in national history and will strengthen the government's capacity to detect and respond to the fast-moving cyber threat landscape'.

Cyber Security NSW is divided into two directorates, with one directorate having a focus on operations, and the other on policy and awareness. In turn, there are seven teams within the two directorates. As at March 2022, Cyber Security NSW had 76 ongoing positions filled, five contractors and 22 vacancies.

Cyber Security NSW states that its aim '…is to provide the NSW Government with an integrated approach to preventing and responding to cyber security threats. By building a stronger cyber resilience across whole-of-government, Cyber Security NSW is able to support the economic growth prosperity and efficiency of NSW'.

NSW Government Cyber Security Strategy

The NSW Government Cyber Security Strategy was released in September 2018 to '…guide and inform the safe management of government's growing cyber footprint'. The 2018 Cyber Security Strategy also set out an action plan with success criteria against each of the six themes of the NSW cyber security framework. Based on a framework from the US National Institute of Standards and Technology (NIST), these themes are:

- lead
- prepare
- prevent
- detect
- respond
- recover.

The Strategy was revised in 2021 and combined with the Cyber Security Industry Development Strategy. The aim of this current strategy is to '…outline the key strategic objectives, guiding principles, and high-level focus areas that the NSW Government will use to align existing and future programs of work'. The strategy includes four NSW Government commitments to:

- increase NSW Government cyber resiliency
- help NSW cyber security businesses grow
- enhance cyber security skills and workforce
- support cyber security research and innovation.

Cyber Security NSW has responsibility as 'lead agency' on the first commitment. This role requires it to set commitment objectives and focus areas for the strategy and provide central leadership and coordination of programs and initiatives.

NSW Government Cyber Security Policy

The NSW Government's Cyber Security Policy was released in February 2019, replacing the former Digital Information Security Policy. All NSW Government agencies must comply with the Cyber Security Policy, and it was recommended for adoption by State Owned Corporations (SOC), local councils, and universities.

The current version of the Cyber Security Policy sets out a range of mandatory requirements for agencies, including:

- annual reporting of their self-assessed levels of maturity against all the mandatory requirements of the Policy and the Australian Cyber Security Centre's 'Essential Eight' requirements
- that agencies must provide a list of their 'crown jewels' and high and extreme risks to their cluster Chief Information Security Officer (CISO).

The Policy sets out that Cyber Security NSW:

- may assist agencies with their implementation of the Policy with an FAQ document and guidelines on several cyber security topics
- will summarise the maturity reports provided by agencies and provide the results to the relevant governance bodies including the Cyber Security Steering Group, Secretaries' Board, relevant committees of Cabinet, Cyber Security Senior Officers' Group, and the ICT and Digital Leadership Group, as well as use these reports to identify common themes and areas for improvement across NSW Government.

As discussed further in Chapter 3, a mandatory guideline issued by the Secretary of the Department of Customer Service in 2020 established that departments and agencies will be subject to audits by Cyber Security NSW. This is to test compliance with the Cyber Security Policy and report these outcomes to the Secretaries' Board.

1.1 National cyber security context

Cyber security threats do not respect jurisdictional boundaries. Efforts to mitigate threat and increase resilience operate in a broader national and international context. Cyber Security NSW formally interacts and shares information with lead cyber security agencies across the Australian Government, states and territories, through national committees which the NSW Government Chief Information Security Officer attends.

Federally, the ACSC is part of the Australian Signals Directorate and leads cyber security efforts nationally. It monitors threats globally, disseminating alerts, providing advice, and working with community, business, government, and academic partners. Cyber Security NSW receives alerts from the ACSC. A formal agreement exists between Cyber Security NSW and the ACSC which facilitates the disclosure of confidential information to support the work undertaken.

Entities responsible for cyber security across other states and territories differ in the scope of their functions and in their organisational arrangements. Most cyber security functions are located within first ministers' departments or equivalent as standalone units.

Critical infrastructure

The Australian Government's *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (Cth)* came into effect on 2 April 2022. This Act amended the *Security of Critical Infrastructure Act 2018* (SOCI Act), which regulates critical infrastructure nationally. It was amended in 2022 to strengthen the security and resilience of critical infrastructure, by expanding the sectors and asset classes the SOCI Act applies to, and to introduce new obligations.

New obligations as a result of amendments include requirements to comply with a new framework for enhanced cyber security obligations required for operators of national significance. This includes mandatory reporting of cyber security incidents.

NSW has eight SOCs. Some of these SOCs may be included within the scope of the SOCI Act and recent amendments. SOCs were excluded from the scope of this performance audit as changes to the legislation were underway during the audit, and the implications for SOCs were uncertain at the time.

1.2 Previous Audit Office of New South Wales findings relevant to Cyber Security NSW

Cyber security and public sector resilience continue to be areas of focus for the work of the Audit Office of New South Wales. Recent Audit Office reports have identified weaknesses in public sector cyber security prevention, capability, and remediation. These findings have been made across performance audits, financial audits, and reviews of internal controls and governance.

Relevant reports include:

- 'Detecting and Responding to Cyber Security Incidents' (2018): Examined cyber security incident detection and response in the NSW public sector, focusing on the then Department of Finance, Services, and Innovation. Findings included recognition of poor and inconsistent detection, as well as response practices and procedures, with limited information sharing and no mandate within the public service for a lead agency to enforce compliance with existing policies.
- 'Compliance with the NSW Cyber Security Policy' (2021): Assessed nine agencies' compliance with the Cyber Security Policy, including whether they met their reporting requirements, and accurately self-assessed their maturity against Cyber Security Policy requirements.
- 'Managing Cyber Risks' (2021): Assessed the effectiveness of Transport for NSW and Sydney Trains in identifying and managing cyber risks. It found that the agencies were not effectively identifying or managing their cyber security risks, with neither agency reaching targets against the NSW Cyber Security Policy.
- 'Internal Controls and Governance 2022': Analysed the internal controls and governance of the 25 largest agencies in the NSW public sector (excluding SOCS and public financial corporations for 2021–22. It found that agencies had low self-assessed cyber security maturity levels, with a lack of consistency across policies, processes, and definitions around security incidents and data breaches.

1.3 Key terms

Under the NSW Government Cyber Security Policy, the term 'cyber security' means 'measures used to protect the confidentiality, integrity and availability of systems and information'.

The term 'resilience' is not defined in the Cyber Security Policy, though a definition is provided on the Digital.NSW website as 'the capacity to withstand or recover quickly from difficulties'.

The Cyber Security Strategy defines 'cyber security resilience' as 'a measure of how well an organisation can manage a cyber security incident while continuing to operate its business effectively'.

The Australian Cyber Security Centre also provides a similar definition of 'cyber resilience' as:

> The ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cyber security incidents.

2. Priorities and planning

This chapter considers whether the Department of Customer Service has a strategic plan for Cyber Security NSW that includes a consistent hierarchy of priorities, which are then reflected in workplans, and inform decisions about specific functions and activities. It also considers whether:

- there was a sound, evidence-based rationale for why Cyber Security NSW was established
- the specific services and functions Cyber Security NSW provides are adequately targeted to agency and council needs
- there is adequate performance assessment of how the services and functions performed by Cyber Security NSW contribute to uplifting cyber maturity and increasing cyber resilience.

2.1 Purpose of Cyber Security NSW

Cyber Security NSW is intended to support connected, protected, and trusted NSW Government digital services

There are various sources that communicate the high-level purpose or objective of Cyber Security NSW. This audit found that the most consistently articulated is that Cyber Security NSW is intended to support economic growth, prosperity, and efficiency by enabling the NSW Government's policy of digitising government services and functions in such a way that they are 'connected, protected and trusted'. This is effectively the need or problem that Cyber Security NSW is intended to address.

To achieve its purpose, Cyber Security NSW is set up as a whole-of-government function that coordinates cyber security and resilience activity across the public sector, including representing the NSW Government interjurisdictionally and being a conduit to the Australian Government.

The high-level purpose of Cyber Security NSW is supported by, and consistent with, broader government policy

The importance of ensuring the security of government digital services is embedded, either expressly or implicitly, across several related policies and strategies, including:

- the NSW Premier's priorities of 'Government made easy' and 'World class public service'
- the Department of Customer Services' intended budget outcomes of 'Excellence in customer service' and 'Digital leadership in government services'
- the NSW Government's December 2019 Beyond Digital Strategy, which expressly cites the establishment of the NSW Cyber Security Officer as an enabler of the strategic direction to 'Deliver better frontline technology' – reference to Cyber Security NSW is expanded upon in the 2021 revision to this strategy
- the NSW State Infrastructure Strategy 2022–2042, which recommends that the State '…uplift cyber security capabilities and practices in infrastructure planning, delivery and operation'
- the Australian Cyber Security Strategy, which notes that 'State and territory and local governments have a role in protecting their systems from cyber attacks'.

Cyber Security NSW's purpose is comparable to bodies in other jurisdictions, both in Australia and overseas.

The purpose and high-level objectives of Cyber Security NSW remain consistent with those that accompanied the establishment of the NSW Government Chief Information Security Officer

The foundations of Cyber Security NSW stem from the appointment of the Government Chief Information Security Officer in March 2017, which served the same high-level purpose of supporting government online service delivery. This role had four high-level 'pillars' to guide activity:

- coordinating the annual cyber security exercise program
- implementing the NSW Cyber Security Policy
- expanding the cyber security intelligence capability of the State
- cultural uplift and awareness raising.

These pillars have substantively been retained and can be seen, along with other actions, among the key focus areas or priorities of Cyber Security NSW. At the time, these pillars were informed by external research into cyber security risks to NSW commissioned by the then Government Chief Information Security Officer. This research was reported in a 2018 NSW Strategic Cyber Risk Assessment and was based on '…data collected from multiple sources on the nature of the threat, impacts and capabilities available to prevent, detect and respond.'

Cyber Security NSW's purpose and high-level functions have been influenced by previous Audit Office of New South Wales recommendations

Cyber Security NSW's current purpose and high-level functions can also be seen in recommendations made by the Auditor-General in the 2018 performance audit, 'Detecting and responding to cyber security incidents'.

Of the seven headline recommendations in the 2018 audit, all have been progressed, with one having been substantially completed.

2.2 Linkages between purpose, objectives, and aims

Cyber Security NSW has not clearly communicated the link between its purpose and the objectives or aims that guide its activity

Cyber Security NSW has had a range of 'pillars', target areas', priorities', 'key areas', 'strategic objectives', 'key focus areas', 'aims', 'benefits', and 'objectives'. These have evolved over time since its inception as the Office of the Government Chief Information Security Officer in March 2017, through to its renaming in May 2019, and its expansion in scope and budget in August 2020

Many of these appear to exist simultaneously, though the relationship between them is not always clear. For example, Cyber Security NSW currently has three 'target areas', though its orientation handbook includes these target areas among a larger set of 12 'key areas'.

Cyber Security NSW also has several objectives that relate to its intended outcome. This audit particularly focused on its role in leading one of the four principles in the NSW Cyber Security Strategy, that is, to improve the NSW Government's cyber resiliency. There are five 'strategic objectives' associated with this role:

1. Provide coordinated leadership for best practice cyber security guidance and advice across government.
2. Promote clear roles and responsibilities across cyber security, privacy, safety and resiliency for NSW Government agencies and external partnerships.
3. Instil a cyber security risk culture across government by educating all staff on importance of cyber security and changing the accountability model that promotes identifying risks, and rewards remediation.
4. Be proactive in managing cyber security risks and threats.

5. lead by example in continual uplift and improvement of NSW Government cyber security maturity against the NSW Cyber Security Policy.

Collectively, this lack of a clear and consistent organisational strategy makes it difficult to assess whether Cyber Security NSW is making progress toward achieving its high-level purpose, and likely hinders clarity in planning and prioritising its resourcing and efforts, as well as accountability.

Cyber Security NSW has received enhanced funding and a broader scope

The development of a 2020 business case was the key process for how Cyber Security NSW established some of its current range of objectives and aims. This business case informed the NSW Government's August 2020 decision to enhance Cyber Security NSW's funding and broaden its scope.

A version of the business case was provided to the Cyber Security Senior Officers' Group in early 2020. This business case describes how a series of options were codesigned in consultation with NSW government clusters and seeks to provide a case for change to underpin the business case. The business case also outlines why additional funding was perceived as being needed in response to heightened cyber security risk, low overall public sector cyber maturity, and increasing digitisation of NSW Government functions and services.

The business case outlined that the need to uplift sector maturity in response to greater cyber risk is core to the high-level purpose of Cyber Security NSW. The business case identified an overall goal for Cyber Security NSW to increase the maturity of the NSW Government sector against the NSW Cyber Security Policy. It refers to increasing overall sector maturity from 2.7 out of five overall to 'at least' three out of five (over three years).

Subsequent advice to government about the business case proposal attempted to detail links between specific activities and overall benefits. However, this was primarily to inform resource planning, rather than to establish how the outputs of various Cyber Security NSW activities would lead to outcomes. For example, it was not clear how specific activities would lead to an increase in security maturity score.

2.3 Prioritising activities and functions

Cyber Security NSW does not have an overall workplan and does not prioritise its activities in line with a clear strategy or plan

Cyber Security NSW performs a range of activities and has multiple workstreams. When asked, staff were able to explain why particular individual tasks or projects had been initiated, such as to address vulnerabilities identified in cyber incidents, or respond to specific enquiries or requests from agencies or councils.

It is unclear what method or process is applied to prioritising functions or activities, particularly longer-term initiatives. Interviews with staff and stakeholders noted that Cyber Security NSW has a service-focused, customer-centric approach to engaging with agencies and councils, including to build its reputation during its period of expansion. In some cases, this has resulted in bespoke, client-specific services being delivered. This may be appropriate during a period where Cyber Security NSW is seeking to establish and build relationships with, as well as display its value proposition to, those agencies and councils with which it has not previously engaged.

However, without appropriate prioritisation and forward work planning, there is a risk that Cyber Security NSW, as one well-informed stakeholder suggested, may be seen as trying '…to be all things, to all people'.

There are sources that could be used as potential inputs to how Cyber Security NSW prioritises its work, such as analysis of cyber security maturity reports submitted by agencies, though we did not source evidence that these potential inputs had been used for that purpose in a systematic way. These self-assessment reports are primarily used as accountability instruments for the submitting agency.

In August 2020, a paper to the Cyber Security Steering Group noted that a forward workplan was being finalised to reflect how the new funding allocation would be used. However, we were not provided with a copy of a finalised plan.

Team-level planning and prioritisation is inconsistent

Across Cyber Security NSW's seven teams, there were examples of comprehensive planning linked to the achievement of specific objectives, and consideration of risks, benefits, resources, and timeframes. However, there was inconsistency across teams in how planning was demonstrated, and the level of detail considered.

Planning documents vary in their strategic alignment, variously referencing business case objectives, NSW Government state objectives, specific policies, as well as objectives that the audit was unable to cross-reference to a source. The inconsistency and complexity in how the objectives and aims of Cyber Security NSW have been constructed and communicated is reflected in these differing approaches to planning.

The 2018 Cyber Security Strategy was accompanied by a roadmap that included a model for the prioritisation of activities

The 2018 Cyber Security Strategy aimed to meet the 'needs of government, business and citizens for connected, protected and trusted services and infrastructure'. A detailed 'roadmap' was developed as part of this to raise sector maturity in each of the six themes embedded in the strategy (lead, prepare, prevent, detect, respond, recover), with specific priorities identified and allocated to each function.

This roadmap also set out a consistent method for how work priorities were determined based on an 'investment mapping' framework that placed projects on a matrix based on their 'business value' and 'delivery risk'. A 'target investment area' was defined as one where business value was high, though delivery risk only low to medium.

Progress against the roadmap was reported to the Cyber Security Senior Officers' Group until at least February 2020. Prior to the additional funding allocation in August 2020, Cyber Security NSW was unable to meet some priorities due to insufficient resourcing.

The revised 2021 Cyber Security Strategy does not appear to be accompanied by a comparable model for prioritisation.

Cyber Security NSW does not rigorously and regularly assess the needs of agencies and councils, so it is unclear whether their needs are being met

For the purpose of developing the January 2020 business case (which would form the basis of the August 2020 funding enhancement), NSW Government departments and a small number of agencies were consulted in late 2019 about their perceived priorities for potential functions or services from Cyber Security NSW. These perceived priorities were compared to each agency's self-assessed level of maturity to determine whether the agency required uplift against each requirement.

However, while there was consultation and analysis to inform the business case, there has not been subsequent review or evaluation, or a planning for such a review. Accordingly, it is unclear whether the services being offered meet the needs of agencies and councils.

The Cyber Security Policy provides that cyber security maturity reports submitted by agencies will be summarised and used to identify common themes and areas for improvement across the NSW Government. We saw evidence that analysis of common issues has been conducted and reported to various governance forums, though it was unclear whether the results of this analysis had been used in developing forward workplans to raise sector maturity and improve resiliency.

Stakeholders from agencies and councils also reported that there have been limited formal opportunities to provide feedback to Cyber Security NSW about whether the services that are available align with their needs.

While there are few formal feedback or review processes about the services provided, some stakeholders did comment positively on the responsiveness of Cyber Security NSW to unsolicited feedback and to requests for advice, information, or services. However, this was generally done on an ad hoc basis and at the agency or council's own initiative, rather than through formal and structured feedback or analysis of agency and council needs.

Agencies and councils identified a range of potential services to raise their cyber maturity and increase resilience

When prompted by the audit team, stakeholders were able to identify a broad range of currently potentially unmet needs, including:

- greater incident management procedural and policy support to local councils
- further guidance on implementing the Essential Eight
- further guidance on determining 'crown jewels'
- access to centralised procurement arrangements and panels
- more proactive outreach, onboarding and induction of new CISOs/CIOs, including for those who are new members of the Cyber Security Steering Group and Cyber Security Senior Officer's Group
- more targeted training to middle executives (Band 1, Band 2)
- providing policy guidance on matters that affect all agencies, such as validating changes in vendor details
- a dedicated whole-of-government security operations centre for cyber security.

Notably, some of these needs repeat those identified in the 2019 consultation process, referred to above, while others are not recorded as having been raised in that process. In some cases, services might have already been available, but the agency or council was not aware of them.

It was beyond the scope of this audit to validate these needs on an agency level. However, it highlights that there is a pool of unmet demand among agencies and councils for services and functions that they believe would assist in uplifting their cyber maturity and improving their cyber resilience.

Cyber Security NSW has a limited understanding of the needs of the local government sector

The January 2020 business case noted that little was known about cyber security in the local government sector and that this was largely a consequence of councils having no obligation to assess and report their cyber security maturity.

One council stakeholder explained that Cyber Security NSW had offered services to the council, though noted that there was '…no real alignment with where they fit within the council's business, why they were important, or how the services line up with the Essential Eight or NIST'.

This is potentially compounded by variations in the degree of cyber security maturity between different councils, and wide variation in IT environments. As one council stakeholder expressed it, '…the problem with local government is every council is running different systems, networks, and programs, with no consistency'.

It should be noted that we found that councils that received Cyber Security NSW services viewed those services favourably, though there does appear to be scope for a more evidence-based approach to meeting council needs. In the absence of evidence, it is not clear what the outcomes of those services are.

Cyber Security NSW has introduced a number of initiatives to raise its organisational capability

Cyber Security NSW proposes to make greater use of agencies' maturity reporting and incident information to inform activity. It was able to outline work that is underway to make better use of the information it collects about cyber maturity and from incidents. This includes:

- an approach to in-depth agency reviews based on the COMPASS review model applied by the NSW Police Force, which may take into account the various reports submitted by agencies under the Cyber Security Policy - this approach will be led by a new Cyber Insights and Performance Team, which will manage an Insights Panel that will review the performance of individual agencies
- enhanced IT-enabled retrospective analysis of incidents, with the results intended to be used to inform service planning.

Cyber Security NSW has also commenced initiatives to support greater rigour in service planning, implementation, and governance. These include:

- process improvement initiatives, such as a project management framework, service catalogue framework, and a project governance committee
- an externally conducted review of its IT strategy, which mapped Cyber Security NSW's services and processes to its objective of increasing cyber resiliency, leading to accepted recommendations around enterprise architecture, better customer relationship management, an improved performance framework, and an enhanced customer front-door service.

Cyber Security NSW performs detailed internal workforce planning

While it was challenging to see how Cyber Security NSW prioritised and planned its work and functions, we saw evidence that Cyber Security NSW developed detailed internal workforce plans as part of its enhanced scope and funding. This included linking specific positions to support high-level functions. It has a considered and deliberate approach to engaging additional staff to meet specific business needs. This includes a detailed approach to business capability management in key operational areas, which maps the level of capability against what is needed to achieve business outcomes and is updated as staff leave or commence with the organisation.

This planning is prudent given the high demand for cyber security skills across the economy and the difficulty that the public sector can face in retaining skilled staff. This is an issue that was raised by several agencies and councils, and which has affected Cyber Security NSW. Onboarding and induction materials have also been developed to provide new starters with detailed information on how Cyber Security NSW functions.

2.4 Measuring and reporting Cyber Security NSW's performance

Cyber Security NSW reports primarily about its activities, not on progress toward meeting measurable objectives

Cyber Security NSW reports on its performance to various audiences, including:

- within DCS, including two measures for the purpose of meeting outcomes-based budgeting requirements, though neither of these measures are conceptually well linked to its purpose, or its objectives around raising maturity and increasing cyber resiliency
- to the Cyber Security Steering Group, ICT and Digital Leadership Group, Cyber Security Seniors Officers' Group, and the Secretaries' Board
- to the NSW community via annual published updates on the Digital.NSW website for 2020 and 2021.

This reporting is primarily activity based, either reporting volumes of activity performed, or providing text descriptions of activities undertaken.

Activity-based performance reporting can be useful where volume, inputs, or effort is of interest (such as when assessing efficiency). However, it is less valuable in measuring the achievement of, or progress toward, desired outcomes. Such measurement requires robust and conceptually valid indicators that reveal the program logic between purpose, input, and outcomes.

One area of activity that is subject to meaningful measurement is awareness and training. In addition to being assessed by survey, many of the agencies we consulted conducted their own phishing simulations to measure changes in behaviour following training. It is unclear whether the results of these assessments are standardised and collated by Cyber Security NSW to sector-wide outcomes.

There is no plan for assessing how Cyber Security NSW's enhanced scope and funding will impact outcomes or be reflected in performance indicators

NSW Treasury's 2020–21 'Budget Guidelines for submitting proposals under Outcomes Budgeting' sets out that budget proposals must '…provide evidence of the connection between proposals and their outcomes and programs'. This document also references Treasury's policy paper on outcome-based budgeting, which notes that the '…allocation of public resources should be based on the outcome achieved for people, not the amount spent, or the volume of services delivered'. The same policy paper also says in regard to measuring these outcomes, that '…the measures should be integrated into agency planning and management processes and should be able to be measured consistently and accurately over time.'

A version of the business case for the expanded scope and funding of Cyber Security NSW was presented to the Cyber Security Senior Officers' Group in early 2020. This document outlined that the goal and 'outcome-based budget key performance indicator (KPI)' of the business case was to uplift aggregate NSW public sector cyber security maturity from level 2.7 to 'at least' level 3 in three years. We found no subsequent plan or roadmap for moving toward the level 3 target, nor any benefits realisation plan illustrating how other intended benefits or outcomes of the business case would be achieved, as well as how they would be monitored to track progress. It is unclear whether changes to the maturity assessment model in 2021–22 have affected how this target would be assessed.

Meaningful performance measurement and reporting in cyber security agencies is a global challenge

Cyber Security NSW does not report on outcomes outside of outcome budget indicators. There is also no overarching outcomes framework that guides investment or service design. However, a review of experience in other jurisdictions found that accurate and meaningful outcomes-based performance measurement is a challenge across similar organisations.

As with Cyber Security NSW, similar organisations in other jurisdictions rely on indicators that are either input or activity focused, or are based on assumptions about causation and attribution that are difficult to validate. By way of example, these performance measures include:

- incident management and operational function - for example, time to respond to incidents and events, time between notification of a major incident and publishing information, or total financial loss reported
- engagement - interaction metrics with social media accounts or attendance at events
- public education - the number of education campaigns run, number of partnerships, or visits to a campaign website
- technical metrics - the number of takedown requests created and actioned, the amount of phishing campaigns and scam sites disrupted through takedowns, or understanding cyber resilience through measuring progress against programs or frameworks such as the Essential Eight
- law enforcement metrics - the number of cases opened and investigations with law enforcement agencies undertaken, warrants serviced, or arrests made.

Cyber Security NSW is actively working to develop sector-level benchmarks and targets

Cyber Security NSW has entered into an agreement with the Cyber Security Cooperative Research Centre to develop a whole-of-government cyber security benchmark. The scope of the benchmark 'would assess a number of metrics to determine the individual roadmaps of the various agencies, mapped against the NSW Cyber Security Strategy'. The benchmark is intended to augment the data provided through regular reporting under the Cyber Security Policy and better understand the capacity of the different types of agencies across the public service, including the types of assets they manage and organisational size.

Of note is that one output of the research is the development of a 'customisable set of KPIs aimed at uplifting cyber security capability development'. While there does not appear to be a target maturity state for the whole of sector, successful development of these KPIs may support a whole-of-sector approach to increasing maturity. The proposal also notes that 'understanding where an entity is placed in terms of cyber benchmarking will help the NSW Government identify areas to improve the cyber security maturity across agencies and support targeted skills mapping and training needs to uplift priority areas'.

While this work may assist in providing more accurate and meaningful measures of sector-wide cyber security maturity, it does not directly address the difficulty of measuring the contribution of Cyber Security NSW to any change in maturity. A conceptually robust program logic is required to ensure that any uplift in cyber maturity, or increase in overall cyber resilience, can reasonably be attributed (whether fully or partially) to Cyber Security NSW's functions and services.

3. Clarity and awareness of roles and responsibilities

This chapter considers the distribution of responsibility for cyber security in the NSW public sector, as well as whether the responsibilities and roles of Cyber Security NSW are clear and understood by agencies and councils. It also considers whether Cyber Security NSW has sufficient authority and mandate to fulfill its responsibilities for both NSW Government agencies and the local government sector.

3.1 Responsibilities for cyber security in the NSW public sector

NSW Government departments are responsible for managing their cyber security risks

While Cyber Security NSW has a central-agency, whole-of-government coordination function, each NSW Government department remains responsible for owning its cyber risk, implementing cyber security measures, and managing incidents. This is recognised in the terms of reference for the Cyber Security Senior Officers' Group. While the Cyber Security Senior Officers' Group is intended to ensure a whole-of-government approach to evolving cyber security risks, its terms of reference make clear that 'each agency remains accountable for its own cyber security arrangements'.

The Cyber Security Senior Officers Group terms of reference shift ownership of cyber security risk management from IT departments to the executive leadership of agencies. This is also reflected in the NSW Cyber Security Policy, which establishes that agency heads, including departmental secretaries, have a range of specific accountabilities in regard to cyber security, including:

- to determine their agency's risk appetite
- to ensure that their agency '…develops, implements and maintains an effective cyber security plan and/or information security plan'.

Secretaries are further accountable for '…ensuring all agencies in their cluster implement and maintain an effective cyber security program'.

Cyber Security NSW complements the cyber security efforts of departments and agencies, which remain responsible for their internal incident response mechanisms and compliance with the mandatory requirements of the Cyber Security Policy.

Moreover, unlike some other jurisdictions in Australia, NSW has a decentralised and fragmented model of public sector IT infrastructure ownership, with departments owning and managing their own systems. Consequently, Cyber Security NSW does not own, nor have direct visibility or control over, the NSW public sector's IT infrastructure. This complicates, though does not preclude, the possibility of developing a whole-of-government security operations centre. Some agencies and councils identified the provision of a state operations centre as a potentially useful future service enhancement. The January 2020 business case also identified that a key initiative that could be provided under enhanced funding would be '24/7 incident response and forensics capability' and 'tactical, operational and strategic intelligence and analysis of security operations'. Any decision to progress the development of a whole-of-government state operations centre would need to be subject to analysis of its feasibility and an assessment of relative priorities.

Cyber Security NSW's key roles and responsibilities are defined in a number of sources

There are a number of sources that formally define roles and responsibilities for Cyber Security NSW. These include:

- **NSW Cyber Security Policy** - sets out obligations on NSW Government agencies to report on various matters to Cyber Security NSW. It also sets out that Cyber Security NSW has the authority to provide assurance about the accuracy of that reporting.
- **NSW Cyber Security Strategy** - sets out that Cyber Security NSW is responsible for the leading the NSW Government's commitment to improve cyber resiliency.
- **Bilateral and interjurisdictional agreements** - including with its cluster department, DCS, to delineate how it will provide services to that department in a manner that is consistent with other clusters, though also agreements setting out mutual responsibilities with bodies such as the NSW Information and Privacy Commission and, interjurisdictionally, the Australian Cyber Security Centre.
- **Terms of reference for related governance bodies** - including the Cyber Security Steering Group, Cyber Security Senior Officers' Group, and the ICT and Digital Leadership Group. While Cyber Security NSW does provide some reporting to these groups, their functions in regard to Cyber Security NSW are primarily limited to endorsing policy. Governance bodies do not have broader responsibilities to give direction to Cyber Security NSW about its work program or functions.

The NSW State Emergency Plan and Cyber Incident Response Arrangements define Cyber Security NSW's operational roles and responsibilities during cyber security related emergencies

The Cyber Security Incident Emergency Sub Plan is a sub plan to the State Emergency Management Plan (EMPLAN) The sub plan details the procedures and coordination arrangements for the NSW Government in prevention of, preparation for, response to, and initial recovery from, an emergency that is the consequence of a significant cyber security incident or a cyber security crisis affecting NSW Government organisations. This sub plan is endorsed by the State Emergency Management Committee in accordance with the provisions of the *State Emergency and Rescue Management Act 1989*.

The current version of the sub plan is dated December 2018, which pre-dates the current nomenclature of Cyber Security NSW. However, the sub plan does reference the predecessor to Cyber Security NSW, the NSW Government Chief Information Security Officer. It is expected that specific reference to the role of Cyber Security NSW will be included in a forthcoming revision of the sub plan.

Under the current sub plan, defined operational roles for the Government Chief Information Security Officer include:

- making classification decisions about cyber incidents under the related Cyber Security Incidents Response Plan, and informing the State Emergency Operations Controller of the plans and action being undertaken
- during the detection stage, providing advice to support agency response teams and sharing information on threats to enable agencies to rapidly take protection measures
- coordinating notifications of cyber security incidents to the cyber security community
- notifying the State Emergency Operations Centre of any cyber security incident that poses a potential threat to NSW, as well as real and credible threats
- during the response stage to a significant incident or crisis, act as the Emergency Cyber Security Operations Coordinator, including to provide actionable threat intelligence and advice or threat detection, control or neutralisation, as well as coordinate, develop and maintain a whole-of-government assessment of the cyber incidence
- during the recovery stage, participating in a recovery committee that '…may be formed for strategic coordination of recovery activities', as well as being responsible for ongoing coordination between the State Emergency Operations Controller and the cyber security community.

The sub plan also describes - though does not mandate - the establishment by the Government Chief Information Security Officer of the Cyber Security Senior Officers' Group and a Cyber Security Advisory Council. Two additional governance groups, established independently of the Government Chief Information Security Officer, are also described in the sub plan: the ICT and Digital Leadership Group, and the Cyber Security Steering Committee.

The independent Cyber Security Advisory Council is not currently operational. A Cyber Insight Series has been convened by Cyber Security NSW as a forum to achieve industry, academic, and government engagement of key thematic issues.

We found that Cyber Security NSW was well regarded for the role it plays during incident management. In particular, agencies consulted as part of this audit valued Cyber Security NSW's external coordination and liaison role, as agencies were not resourced or prepared to fulfil these roles. This was highlighted during the Log4j vulnerability threat over the summer of 2021–22 (discussed below in Exhibit 1).

Exhibit 1: Incident management during a global vulnerability threat - Log4j

In December 2021, a critical internet vulnerability was detected globally in an obscure, but widely-used piece of software called Log4j. This vulnerability allowed threat actors to potentially steal personal information, take over systems, and conduct ransomware and other criminal activities, including espionage. The UK National Cyber Security Centre described the vulnerability as '…potentially the most severe computer vulnerability in years'.

On 10 December 2021, Cyber Security NSW became aware of the Log4j vulnerability and released five alerts within the first week of discovery.

Cyber Security NSW used its cross-agency Technical Officers' Group to provide advice to individual departments on how to respond to the threat. Along with emails and alerts, the Technical Officers' Group was convened on ten occasions during the December - January period. A post-activation review found that the timely and active use of the Technical Officers' Group by Cyber Security NSW facilitated a coordinated whole-of-government response plan, the identification of potential risk areas across the NSW Government, and the dissemination of information from the Australian Government. Cyber Security NSW also held five information sessions for local councils over the same period.

The Vulnerability Management Centre, established by Cyber Security NSW in Bathurst, also offered Log4j scanning services by request, and provided this service to 50 councils, three agencies and one department.

This performance audit found strong support from NSW Government agencies and local councils for the role played by Cyber Security NSW during the Log4j event, with entities acknowledging the 'significant' or 'massive' role played in coordinating efforts across the public sector. One council highlighted that because it had been given detailed and timely information about the threat, it was able to put in place decision making delegations for the end-of-year holiday period, that would allow critical systems to be shut down even if decision makers could not be reached immediately.

Source: Audit Office New South Wales research.

Cyber Security NSW's role with local councils is unclear

Though Cyber Security NSW provided some services to local councils before the announcement, the August 2020 funding announcement was accompanied by an expectation of the NSW Government that Cyber Security NSW's support to councils would be expanded.

While we have not made findings about cyber maturity in local government, which is the topic of a future performance audit, this audit did consider how well-placed Cyber Security NSW is to contribute to uplifting maturity and improving resilience in the local government sector.

A key driver of Cyber Security NSW's increase in funding was the NSW Government's assessment that the improvement of cyber security in local government required additional resources. While there was no empirical evidence to support the case, the NSW Government assumed low levels of cyber security maturity in local government due to the limited resources available to councils to address cyber security. Based on our interviews with staff representing 13 councils this was, and remains, a reasonable conclusion to draw.

Cyber Security NSW has provided a range of services to the local government sector. We found that these services are well regarded. Our survey of members of the Cyber Security NSW community of practice found that members from councils were more likely to describe these services as providing a 'major' contribution to improving cyber security than were members from NSW Government agencies. The strong support for the services provided was also consistent with our interviews with council staff.

However, while councils appreciate the service received from Cyber Security NSW, the exact nature of Cyber Security NSW's responsibilities and role in this sector remain unclear. As discussed further below, Cyber Security NSW has no authority to mandate action from local councils. In NSW, the Office of Local Government (OLG), within the Department of Planning and Environment, has the policy, legislative, and program focus for regulating local councils. Engagement with Cyber Security NSW in any form is at the discretion of individual councils. This is notwithstanding that councils may potentially face the same types of cyber security threats as NSW Government agencies, will often be less well equipped to manage these threats, and increasingly have digital systems that are interconnected with the other councils and the state government sector.

For example, we note that local councils have access to the nsw.gov.au internet domain. While Cyber Security NSW has been successful in working with councils to implement a DMARC solution (an email authentication protocol to prevent hostile actors using 'spoofed' or forged email accounts), participation in this program is on an opt-in basis.

Cyber Security NSW has a role in building capacity for recovery after incidents, but its prioritisation of this work is unclear

The NSW Cyber Security Strategy establishes Cyber Security NSW as the lead for coordinating efforts to increase NSW Government cyber resilience. While resilience is significantly increased by active planning and preparation, specific capabilities to help manage recovery after cyber security incidents is also essential for resilience.

The NSW Cyber Security Policy sets out a six-stage model of cyber security: lead, prepare, prevent, detect, respond, and recover. The policy lists 20 mandatory requirements spread across the six stages (there are a further five mandatory reporting requirements, hence the so-called 'mandatory 25'). None of these mandatory requirements relate to the recovery stage, except arguably for the requirements around regular data backups contained in the Essential Eight (compliance with which is incorporated into the 'prepare' stage of the policy).

Frameworks from other jurisdictions provide insight into potentially useful recovery activities. In particular, the Cyber Security Framework of the US National Institute of Standards and Technology, from which the six stages of the NSW policy were adapted, sets out that the recover stage should include:

- developing and testing recovery plans
- communication activities to manage public relations, repair reputation, and communicate effectively to internal stakeholders, management teams, and executives
- managing lessons learned from the incident and reflecting those lessons in recovery planning.

The majority of Cyber Security NSW's activities, consistent with the structure and content of the Cyber Security Policy, are focused on preparation, detection, and response to cyber threats, rather than recovery after incidents.

Exhibit 2: ID Support NSW and recovery from cyber incidents

One area where DCS has exceeded the recovery activities recommended in the NIST framework is by providing a capability to assist individuals with identity recover through the ID Support NSW service. The establishment of ID Support NSW has uniquely enhanced NSW Government capabilities to assist individuals with identity recovery following cyber-attack or privacy incidents.

ID Support NSW aims to help individuals if their government proof of identity credentials are stolen or fraudulently obtained, including giving advice on how to restore the security of compromised identities. ID Support NSW is established in the same division of DCS as Cyber Security NSW and is designed to work with Cyber Security NSW in the event of NSW Government cyber breaches that affect individuals' personal information. Cyber Security NSW has established a standard operating procedure to manage the handover of a cyber incident involving a data breach to ID Support NSW.

Source: Audit Office of New South Wales research.

Cyber Security NSW does not build sector capability for agencies to manage how they learn from incidents

Agencies are responsible for their own cyber security risk and managing their own responses to cyber security incidents. Activities such as post-incident reviews should be conducted by agencies, which are then best positioned to feed those lessons into recovery planning. While Cyber Security NSW does not have a role to conduct post-incident reviews of individual agencies' incident management, the provision of resources to build agency capability in this area is consistent with Cyber Security NSW's role to provide whole-of-government resources that raise sector maturity.

The NIST framework and UK Cyber Security Strategy 2020 - 30 recognise the importance of learning from experience as a key contributor to resilience. One subject matter expert interviewed for this audit explained their view that resilience was a process of '…learning through lived experiences and adapting and adjusting as a result of those experiences so that we're better prepared and able to withstand that disruption in the future'.

The Cyber Security Incident Emergency Sub Plan specifies that the Government Chief Information Security Officer (as the predecessor to Chief Cyber Security Officer within Cyber Security NSW), should conduct whole-of-government post cyber incident reviews and participate in the After-Action Review process of emergency management operations. The sub plan does not define or explain the distinction between whole-of-government post-incident review and After-Action Review.[1]

Conducting post-incident reviews is an example of 'lessons management', which is itself effectively a sub-discipline of emergency management. The Australian Institute of Disaster Resilience has published a handbook for this sub-discipline, titled 'Lessons Management'. This handbook describes the field of lessons management as '… an overarching term that refers to collecting, analysing, disseminating and applying learning experiences from events, exercises, programs and reviews.' Moreover, the handbook highlights the benefits of a consistent approach to lessons management, in that:

> Interoperability of lessons management processes across agencies, sectors and jurisdictions will facilitate information sharing and analysis.

One cyber security subject matter expert expressed the view that the principles in this handbook form a useful basis for developing cyber security specific principles for managing lessons from cyber security incidents.

[1] A forthcoming revision to the sub plan is expected to draw a distinction between *post-incident reviews* (conducted by an agency as a review of its own incident management response) and *post-activation reviews* (conducted by Cyber Security NSW of the governance arrangements activated under the sub plan and incident response plan).

3.2 Awareness and understanding of Cyber Security NSW's role and functions

Public sector stakeholders are clear on the overall role of Cyber Security NSW, but have inconsistent knowledge of the specific services Cyber Security NSW provides

During the audit, senior staff were consulted from every NSW Government department, as well as a range of key agencies, and a sample of staff representing 13 local councils. We found there was a relatively clear understanding of Cyber Security NSW's high-level purpose and the type of functions it performed, particularly regarding information sharing, providing training and awareness resources, and supporting incident management.

However, while agency and council stakeholders had sound awareness of Cyber Security NSW's purpose, their understanding of the full range of specific services available to their organisations varied. There was almost no awareness of Cyber Security NSW having a service catalogue. A consultant's report commissioned by Cyber Security NSW made similar findings, noting that there has been uncoordinated engagement of Cyber Security NSW's customers, with manual and ad hoc engagement processes and feedback loops. The report specifically notes the absence of, and need for, a service catalogue.

Such a resource is essential to ensuring that stakeholders are fully aware of the services available to them, and to avoid duplication of services between Cyber Security NSW and organisations. We found that in at least one overseas jurisdiction, a service catalogue was deemed so essential that its production was made a legislative requirement of the cyber security body.

Cyber Security NSW has developed a high-level service catalogue. While this document may be adequate for building awareness of Cyber Security NSW, it lacks the sufficient detail for prospective 'client' agencies to fully understand the scope, limitations, and benefits of prospective services. The expression of services in high-level, general terms also potentially hampers how effectively Cyber Security NSW can plan and resource its activities.

There is evidence of active and planned communication focused on awareness campaigns and specific initiatives

Review of Cyber Security NSW documentation has identified communication strategies and stakeholder mapping held at the individual team level. This includes the:

- 2022 Cyber Security Awareness Strategy - this document details planning for social communication related to cyber security awareness across 2022. This includes drafted wording for posts, intended audiences for messaging, and alignment with ACSC campaigns
- councils and clusters stakeholder awareness document - this is the most detailed stakeholder mapping document reviewed by the audit team. It logs all enquiries made to Cyber Security NSW regarding 'Essentials' training, newsletters, and the Community of Practice, provides a collated list of contacts relevant to the 'Essentials' training program, and collates all stakeholder actions relating to training.

The level of detail and planning evidenced across these two examples indicates considered approaches to tailoring communication across the public sector for specific purposes.

Cyber Security NSW does not have an overall engagement plan for the local government sector

We found that, when asked, councils that engaged with Cyber Security NSW valued the services they received. However, many council staff were not aware of other services that they could access. Further, there is little evidence that Cyber Security NSW has conducted an analysis of council needs.

Cyber Security NSW has not developed a substantive stakeholder engagement and communication plan to guide more comprehensive engagement with the local government sector. A progress report to the Cyber Security Steering Committee from March 2020 said that a small agency and council 'uplift toolkit' was under development and was expected to be launched by mid-2022, though this did not occur.

Cyber Security NSW has had some successes in its engagement with local councils, including:

- the work outlined earlier in implementing a DMARC solution to better protect email domains
- approximately 50% take-up by councils of the cyber security awareness 'Essentials' training
- the establishment of the Councils' Technical Officers' Group, which was convened regularly during the Log4j threat over the December 2021–January 2022 period.

However, the lack of a clear service offering (such as through a comprehensive service catalogue), uncertainty regarding the alignment of Cyber Security NSW's service to council needs, and the lack of an overall council stakeholder engagement plan, limit the effectiveness of Cyber Security NSW's engagement with the local government sector.

Cyber Security NSW recognises the important role played by Audit and Risk Committees, but does not have a stakeholder engagement strategy for these bodies

Audit and Risk Committees (ARC) play a key role in monitoring risk and compliance in agencies and councils on an ongoing basis. Building Audit and Risk Committee capability in cyber security governance appears a valuable role for Cyber Security NSW, as these committees can provide ongoing and detailed oversight of agency and council performance in way that Cyber Security NSW could likely not replicate. One subject matter expert suggested that effective cyber security relied on senior management engagement, especially in setting cyber risk tolerance, with vigilant ARC oversight of whether the organisation is working within acceptable tolerance.

Cyber Security NSW has invested resources into supporting the role of ARCs in the NSW public sector, and Cyber Security NSW staff recognise the importance of engaging with them. By early 2019, the former Office of the Government Chief Information Security Officer had developed a document outlining key questions that committee members should ask of agency and council staff. This document remains available on the Cyber Security NSW resources webpage. When invited, Cyber Security NSW staff also attend ARC meetings and conferences.

There are around 300 ARCs across the NSW state and local government sectors, including government businesses. While Cyber Security NSW staff recognise the important role they play, and some efforts have been expended to engage this audience, we did not find an engagement plan or additional resources for Audit and Risk Committees. The NSW Public Service Commission has set out advice for the content of engagement plans in its publication 'A guide to effective stakeholder engagement'.

3.3 Mandate and powers of Cyber Security NSW

A circular issued by the Department of Customer Service mandates NSW Government agencies' compliance with the Cyber Security Policy

A circular issued by the Secretary of the Department of Customer Service (DCS) on 16 October 2020 sets out mandatory directions requiring NSW Government agencies to comply with the Cyber Security Policy. This circular:

- mandates annual cyber security training for all NSW public servants (including contractors)
- details cyber hygiene practices (such as using multifactor authentication where available) all NSW public servants must follow
- assigns responsibilities to agency or department executives (such as assigning overall responsibilities for information asset protection and ownership and approving policies as appropriate)
- assigns responsibilities to agencies and departments more broadly (such as having an incident response plan tested annually).

The Secretary of DCS issued this circular under the NSW Government's Administrative Requirements Framework. This framework outlines how NSW Government administrative requirements are managed. It specifies that DCS is one of the central agencies that may issue, through its Secretary, requirements in relation to government sector administrative policy and operational matters. While requirements issued through DCS circulars do not override any applicable legislation, agencies are required to comply with their terms, unless they are stated to be non-mandatory.

Cyber Security NSW has not audited agency self-assessments under the Cyber Security Policy

The circular issued by the Secretary of DCS notes that departments and agencies will be '…subject to audits by Cyber Security NSW commencing 2020–21 to test compliance with the Policy and reporting these outcomes to the Secretaries' Board'.

Cyber Security NSW has not performed audits of the artifacts that support agency self-assessments. By not conducting targeted audits, Cyber Security NSW is not providing a level of assurance, implicitly expected by the NSW Government in making the policy, that agencies' self-assessments are consistent and sound.

These self-assessments provide the only measure of cyber security maturity of the NSW Government. The Audit Office's 2021 report 'Compliance with the NSW Cyber Security Policy' found that, among other things:

- each participating agency had implemented one or more of the mandatory requirements in an ad hoc or inconsistent basis
- agencies tended to over-assess their cyber security maturity – all nine participating agencies were unable to support all their self-assessments with evidence.

These issues have not only been identified by the Audit Office of New South Wales. A 2021 report by an external consultant engaged by Cyber Security NSW found divergent approaches in how agencies perform their maturity self-assessments. Cyber Security NSW does not obtain reasonable assurance from the public sector that self-assessments are reasonably consistent, evidence-based, and accurate.

In its January 2020 business case, DCS explained that is has '…been focused on compliance with the Cyber Security Policy' and it acknowledged that it has a '…key role to keep clusters accountable for reporting and driving coordinated security maturity uplift'.

While it would be neither reasonable nor feasible for Cyber Security NSW to audit every NSW Government agency's self-assessment, a risk-based approach may have both an educative benefit for agencies, as well as ensuring that agencies are diligent and considered in their assessments. As one senior agency stakeholder suggested, agencies are more likely to comply with the policy if '…someone might be looking over their shoulder'. Another stakeholder expressed concern about the capacity of agencies to conduct their self-assessments uniformly, arguing that this left open the need for 'basic assurance and spot checking' by Cyber Security NSW.

Agencies have responsibility for improving their capability against the requirements of the Cyber Security Policy, though Cyber Security NSW is responsible for leadership, governance, and, importantly, assurance.

Cyber Security NSW has formal information sharing agreements with relevant state and federal bodies to support its functions

Formal agreements are in place with both state and federal government bodies directly relevant to the cyber security infrastructure in NSW. These include:

- Information and Privacy Commission NSW - arrangements for information sharing between Cyber Security NSW and the NSW Privacy Commissioner are set out in a formal information sharing protocol
- Australian Cyber Security Centre (ACSC) - Cyber Security NSW has signed a Confidentiality Deed Poll with the ACSC which allows it to discuss and receive confidential information of the Australian Signals Directorate and other ACSC partners.

Cyber Security NSW has responsibility, though no authority, to improve cyber security resilience in the local government sector

The Audit Office's 'Report on Local Government 2019' found that 80% of councils did not have a cyber security policy or framework. It recommended that the Office of Local Government 'develop a cyber security policy by June 2021 to ensure a consistent response to cyber security risks across councils'. The 'Local Government 2021' report found that while there had been improvement, 50% of councils still did not have cyber security frameworks and related controls in place by June 2021.

Cyber Security NSW understands that it has no formal authority to mandate any requirements on local councils, the regulator of which (as discussed earlier) is OLG, located within the Department of Planning and Environment. OLG has the policy, legislative, investigative and program focus to regulate local councils, and is responsible for '…strengthening the sustainability, performance, integrity, transparency and accountability of the local government sector'. From 2019, Cyber Security NSW consulted with OLG to draft cyber security guidelines for local councils and has subsequently disseminated these guidelines directly to some councils.

Among those councils consulted as part of this audit, there was substantial confusion and uncertainty about the status and progress of these guidelines, as well as the general standing of Cyber Security NSW. In expectation that mandatory measures may be imposed in the future, some councils developed their own cyber security policies which mirrored, as closely as possible, the terms of the NSW Cyber Security Policy. Other councils chose not to adopt this approach, explaining the potential unsuitability of the Cyber Security Policy to the NSW local government sector.

This confusion and uncertainty are likely to have been - and possibly will continue to be - a significant barrier to increasing cyber resilience in local councils.

The guidelines were released on 19 December 2022 and are advisory, rather than mandatory.

Section two

Appendices

Appendix one – Response from agency

NSW GOVERNMENT | Customer Service

McKell Building – 2-24 Rawson Place, Sydney NSW 2000
Tel 02 9372 8877 | TTY 1300 301 181
ABN 81 913 830 179 | www.nsw.gov.au

Office of the Secretary

Our reference: COR-06843-2022
Your reference: D2226449

Ms Margaret Crawford
Auditor-General of New South Wales
Audit Office NSW
By email: [redacted]

Dear Ms Crawford

Thank you for your letter conveying the Performance Audit – "Cyber Security NSW: governance, roles and responsibilities" report.

The audit report accurately details the challenges Cyber Security NSW and other similar organisations face in measuring how its activities contribute to cyber security maturity uplift.

The audit includes recommendations that will enhance the capability of Cyber Security NSW to lead the uplift of NSW Government's cyber security resiliency.

Cyber Security NSW has commenced planning for initiatives that would fulfil the recommendations, including development of a business case for future funding. The $60 million funding provided to Cyber Security NSW in 2020 expires on 30 June 2023, and so initiatives will be finalised once the funding allocation beyond that time is confirmed.

Cyber Security NSW accepts all four recommendations. Comments against each recommendation are provided below:

1. **Implement an approach that provides reasonable assurance that NSW Government agencies are assessing and reporting their compliance with the NSW Government Cyber Security Policy in a manner that is consistent and accurate.**

   Consistent with Recommendation 1 from the NSW Auditor-General's Report 'Special Audit: Compliance with the NSW Cyber Security Policy', Cyber Security NSW is developing an assurance methodology to assist NSW Government agencies to consistently assess and report their compliance with the Policy. This will be included in the 1 July 2023 release of the Policy, for reporting against FY2023-24.

2. **Ensure that Cyber Security NSW has a strategic plan that clearly demonstrates how the functions and services provided by Cyber Security NSW contribute to meeting its purpose and achieving NSW Government outcomes.**

   A Strategic Plan is being developed capturing existing and planned activities associated with:

   - building maturity in line with the 2023 iteration of the NSW Cyber Security Policy;
   - incident response;
   - intelligence sharing; and
   - awareness raising.

3. **Ensure that Cyber Security NSW has a detailed, complete, and accessible catalogue of services available to agencies and councils.**

   The development of a detailed, complete and accessible service catalogue was self-identified by Cyber Security NSW in work commissioned and delivered in June 2022 and is nearing completion.

4. **Develop a comprehensive engagement strategy and plan for the local government sector, including councils, government bodies, and other relevant stakeholders.**

   A comprehensive engagement strategy and plan is being developed, building on successful engagement with *all* local councils and lessons learned, over the past 12 months.

Recommendations 2 and 4 will be finalised following confirmation of the funding allocation for Cyber Security NSW for FY2023-24 and beyond.

Yours sincerely

Emma Hogan
Secretary

Date: 27/01/23

Appendix two – About the audit

Audit objective

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.

Audit criteria

We addressed the audit objective with the following audit criteria:

1. Are internal planning and governance processes in place to support Cyber Security NSW meet its objectives?
2. Are Cyber Security NSW's roles and responsibilities defined and understood across the public sector?

Audit scope and focus

This audit focused on the internal effectiveness of CS NSW processes. CS NSW is a relatively new functional area with a large scope of responsibilities. As such, the audit focused on examining whether it had established the necessary planning and governance processes to enable it to meet its objectives, and whether it had established a clear role in the sector.

Audit exclusions

The audit did not assess:

- specific cyber security threats, or the effectiveness of the response by CS NSW to those threats.
- agency vulnerabilities or the adequacy of existing or planned safeguards (for example through penetration testing).
- the achievement of intended outcomes by Cyber Security NSW. Instead, the focus of the audit was on whether intended outcomes are clearly established, and whether CS NSW has the roles, responsibilities, and governance arrangements (including frameworks and processes for planning, resource allocation, stakeholder engagement, and performance management) reasonably necessary to demonstrate credibly that it will be able to achieve those outcomes.

Audit approach

Our procedures included:

1. interviewing:
    - key staff from the Department of Customer Service and Cyber Security NSW
    - NSW public sector stakeholders, including those who had participated in various committees or other forums led or coordinated by Cyber Security NSW, such as the:
        - Cyber Security Senior Officers' Group
        - Cyber Security Steering Group
    - a sample of local councils across NSW
    - cyber security experts.
2. examining relevant data and documentation, including policies, strategies, plans, meeting minutes, reviews, and activity and performance reports.

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 Audit 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 the Department of Customer Service and Cyber Security NSW.

In particular, we wish to thank our liaison officers, and the staff who participated in audit interviews and provided materials relevant to the audit. We also gratefully acknowledge the range of government and non-government stakeholders who participated in interviews or provided information to the audit.

Audit cost

Including staff costs and overheads, the estimated cost of the audit is $420,000.

Appendix three – Performance auditing

What are performance audits?

Performance audits determine whether state or local government entities carry out their activities effectively and do so economically and efficiently and in compliance with all 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 performance audits is set out in section 38EA of the *Government Sector Audit Act 1983* for state government entities, and in section 421BD of the *Local Government Act 1993* for local government entities.

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.

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 head of the audited entity who is invited to formally respond to the report. The report presented to the NSW Parliament includes any response from the head of the audited entity. The relevant minister and the Treasurer are also provided with a copy of the final 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.

Professional people with purpose

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)

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

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.

audit.nsw.gov.au