SPECIAL REPORT 28 OCTOBER 2021

Compliance with the NSW Cyber Security Policy

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 Government Act 1993*.

AUDITOR-GENERAL NEW SOUTH WALES

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 38E of the *Government Sector Audit Act 1983,* I present a report titled **'Compliance with the NSW Cyber Security Policy'.**

Margaret Crawford
Auditor-General for New South Wales
28 October 2021

contents

Compliance with the NSW Cyber Security Policy

Auditor-General's foreword

This report assesses whether state government agencies are complying with the NSW Cyber Security Policy. The audit was based on the level of compliance reported at 30 June 2020.

Our audit identified non-compliance and significant weaknesses against the government's policy.

Audited agencies have requested that we not report the findings of this audit to the Parliament of New South Wales, even though the findings are more than 12 months old, believing that the audit report would expose their weaknesses to threat actors.

I have reluctantly agreed to modify my report to anonymise agencies and their specific failings because the vulnerabilities identified have not yet been remedied. Time, leadership and prioritised action should have been sufficient for agencies to improve their cyber safeguards. I am of the view that transparency and accountability to the Parliament is part of the solution, not the problem.

The poor levels of cyber security maturity are a significant concern. Improvement requires dedicated leadership and resourcing. To comply with some elements of the government's policy agencies will have to invest in technical uplift and some measures may take time to implement. However, other elements of the policy do not require any investment in technology. They simply require leadership and management commitment to improve cyber literacy and culture. And they require accountability and transparency. Transparent reporting of performance is a key means to improve performance.

Section one

Compliance with the NSW Cyber Security Policy

Executive summary

Cyber security is increasingly a focus of governments around Australia. The Australian Cyber Security Centre (ACSC) is the Australian Government's lead agency for cyber security and is part of the Australian Signals Directorate, a statutory authority within the Australian Government's Defence portfolio. The ACSC has advised that government agencies at all levels, as well as individuals and other organisations were increasingly targeted over the 2021 financial year[1]. The ACSC received over 67,500 cybercrime reports, a 13 per cent increase on the previous year. This equates to one reported cyber attack every eight minutes. They also noted that attacks by cyber criminals and state actors are becoming increasingly sophisticated and complex and that the attacks are increasingly likely to be categorised as 'substantial' in impact.

High profile attacks in Australia and overseas have included a sustained malware campaign targeted at the health sector,[2,] a phishing campaign deploying emotet malware, spear phishing campaigns targeting people with administrator or other high-level access, and denial of service attacks. The continuing trend towards digital delivery of government services has increased the vulnerability of organisations to cyber threats.

The COVID-19 pandemic has increased these risks. It has increased Australian dependence on the internet – to work remotely, to access services and information, and to communicate and continue our daily lives. Traditional security policies within an organisation's perimeter are harder to enforce in networks made up of home and other private networks, and assets the organisation does not manage. This has increased the cyber risks for NSW Government agencies.

In March 2020, Service NSW suffered two cyber security incidents in short succession. Technical analysis undertaken by the Department of Customer Service (DCS) concluded that these cyber breaches resulted from a phishing exercise through which external threat actors gained access to the email accounts of 47 staff members. These attacks resulted in the breach of a large amount of personal customer information contained in these email accounts. These attacks were the subject of the Auditor-General's report on Service NSW's handling of personal information tabled on 18 December 2020.

This audit also follows two significant performance audits. Managing cyber risks, tabled on 13 July 2021 found Transport for NSW and Sydney Trains were not effectively managing their cyber security risks. Integrity of data in the Births, Deaths and Marriages Register, tabled 7 April 2020 found that although there are controls in place to prevent and detect unauthorised access to, and activity in the register, there were significant gaps in these controls.

The NSW Cyber Security Policy (CSP) was issued by Cyber Security NSW, a business unit within the Department of Customer Service, and took effect from 1 February 2019. It applies to all NSW Government departments and public service agencies, including statutory authorities. Of the 104 agencies in the NSW public sector that self-assessed their maturity implementing the mandatory requirements, only five assessed their maturity at level three or above (on the five point maturity scale). This means that, according to their own self-assessments, 99 agencies practiced requirements within the framework in what the CSP's maturity model describes as an ad hoc manner, or they did not practice the requirement at all. Cyber Security NSW and NSW Government agencies need to prioritise improvements to their cybersecurity and resilience as a matter of priority.

This audit looks specifically at the compliance of nine key agencies with the CSP. It looks at their achievement implementing the requirements of the policy, the accuracy of their self-assessments and the attestations they made as to their compliance with the CSP.

[1] ACSC Annual Cyber Threat Report 2020-21 | Cyber.gov.au
[2] Sustained targeting of the health sector | Cyber.gov.au

The CSP outlines the mandatory requirements to which all NSW Government departments and public service agencies must adhere. It seeks to ensure cyber security risks to agencies' information and systems are appropriately managed. The key areas of responsibility for agencies are:

- Lead - Agencies must implement cyber security planning and governance and report against the requirements outlined in the CSP and other cyber security measures.
- Prepare - Agencies must build and support a cyber security culture across their agency and NSW Government more broadly.
- Prevent - Agencies must manage cyber security risks to safeguard and secure their information and systems.
- Detect/Respond/Recover - Agencies must improve their resilience including their ability to rapidly detect cyber incidents and respond appropriately.
- Report - Agencies must report against the requirements outlined in the CSP and other cyber security measures.

DCS has only recommended, but not mandated the CSP for state owned corporations, local councils and universities.

NSW Government agencies must include an attestation on cyber security in their annual report and provide a copy to Cyber Security NSW by 31 August each year stating whether, for the preceding financial year, the agency has:

- assessed its cyber security risks
- appropriately addressed cyber security at agency governance forums
- a cyber incident response plan that is integrated with the security components of business continuity arrangements, and the response plan has been tested during the previous 12 months (involving senior business executives)
- certified the agency's Information Security Management System (ISMS) or confirmed the agency's Cyber Security Framework (CSF)
- a plan to continuously improve the management of cyber security governance and resilience.

The purpose of the attestation is to focus the agency's attention on its cyber risks and the mitigation of those risks.

Agencies assess their level of compliance in accordance with a maturity model. The CSP does not mandate a minimum maturity threshold for any requirement, including implementation of the Australian Cyber Security Centre's (ACSC) Essential 8 Strategies to Mitigate Cyber Security Incidents (Essential 8).

Agencies are required to set a target maturity level based on their risk appetite for each requirement, seek continual improvement in their maturity, and annually assess their maturity on an ascending scale of one to five for all requirements (refer to Appendix two for the maturity model). Each control within the Essential 8 is assessed on an ascending scale of zero to three reflecting the agency's level of alignment with the strategy (refer to Appendix three for the maturity model).

Scope of this audit

We assessed whether agencies had provided accurate reporting on their level of maturity implementing the requirements of the CSP in a documented way and covering all their systems.

The scope of this audit covered nine agencies (the participating agencies). These agencies were selected because they are the lead agency in their cluster, or have a significant digital presence within their respective cluster. The list of participating agencies is in section 1.2. The audit aimed to determine whether, during the year to 30th June 2020, the participating agencies:

- met their reporting obligations under the CSP
- provided accurate reporting in self-assessments against the CSP's mandatory requirements, including their implementation of the Australian Cyber Security Centre's (ACSC) Essential 8
- achieved implementation of mandatory requirements at maturity levels which meet or exceed the 'level three - defined' threshold (i.e. are documented and practiced on a regular and consistent basis).

While the audit does assess the accuracy of agency self-assessed ratings, the audit did not assess the appropriateness of the maturity ratings.

Conclusion

Key elements to strengthen cyber security governance, controls and culture are not sufficiently robust and not consistently applied. There has been insufficient progress to improve cyber security safeguards across NSW Government agencies.

The NSW CSP replaced the NSW Digital Information Security Policy from 1 February 2019. New requirements of the CSP were, inter alia, to strengthen cyber security governance, strengthen cyber security controls and improve cyber security culture.

The CSP is not achieving the objective of improved cyber governance, controls and culture because:

- The CSP does not specify a minimum level for agencies to achieve in implementing the 'mandatory requirements' or the Essential 8 Strategies to Mitigate Cyber Security Incidents.
- The CSP does not require agencies to report their target levels, nor does it require risk acceptance decisions to be documented or formally endorsed.
- All of the participating agencies had implemented one or more of the mandatory requirements in an ad hoc or inconsistent basis.
- None of the participating agencies had implemented all of the Essential 8 controls to at least level one.
- Agencies tended to over-assess their cyber security maturity, with all nine participating agencies unable to support some of their self-assessments of compliance with one or more mandatory criteria. Optimistic assessment of the current state of cyber resilience undermines effective decision making and risk management in responding to cyber risks.
- There is no systematised and formal monitoring, by either Cyber Security NSW or another agency, of the adequacy or accuracy of agencies' cyber self-assessment processes.

1. Key findings

The CSP allows agencies to determine their own level of maturity to implement the 'mandatory requirements', which can include not practicing a policy requirement or implementing a policy requirement on an ad hoc basis. These determinations do not need to be justified

Agencies can decide not to implement requirements of the CSP, or they can decide to implement them only in an informal or ad-hoc manner. The CSP allows agencies to determine their desired level of maturity in implementing the requirements on a scale of one to five - level one being 'initial – not practiced' and level five being 'optimised'. The desired level of maturity is determined by the agency based on their own assessment of the risk of the services they provide and the information they hold.

The reporting template for the 2019 version of the CSP stated that level three maturity - where a policy requirement is practiced on a regular and consistent basis and its processes are documented - was required for compliance with the CSP. This requirement was removed in the 2020 revision of the reporting template.

This CSP does not require the decisions on risk tolerance, or the timeframes agencies have set to implement requirements to be documented or formally endorsed by the agency head. There is no requirement to report these decisions to Cyber Security NSW.

Some comparable jurisdictions require formal risk acceptance decisions where requirements are not implemented. The NSW CSP does not have a similar formal requirement

Some jurisdictions, with a similar policy framework to NSW, require agencies to demonstrate reasons for not implementing requirements, and require agency heads to formally acknowledge the residual risk. The NSW CSP does not require these considerations to be documented, nor does it require an explicit acknowledgement and acceptance of the residual risk by the agency head or Cyber Security NSW. The NSW CSP does not require that the records of how agencies considered and decided which measures to adopt to be documented and auditable, limiting transparency and accountability of decisions made.

All of the participating agencies had implemented one or more of the mandatory requirements in an ad hoc or inconsistent basis

All of the participating agencies had implemented one or more of the mandatory requirements at level one or two. Maturity below level three typically means not all elements of the requirement have been implemented, or the requirements have been implemented on an ad-hoc or inconsistent basis.

None of the participating agencies has implemented all of the Essential 8 controls at level one – that is, only partly aligned with the intent of the mitigation strategy

Eight of the nine agencies we audited had not implemented any of the Essential 8 strategies to level three – that is, fully aligned with the intent of the mitigation strategy. At the time of this audit the ACSC advised that:

> as a baseline organisations should aim to reach to reach Maturity Level Three for each mitigation strategy[3].

The Australian Signals Directorate[4] currently advises that, with respect to the Essential 8:

> [even] level three maturity will not stop adversaries willing and able to invest enough time, money and effort to compromise a target. As such, organisations still need to consider the remainder of the mitigation strategies from the Strategies to Mitigate Cyber Security Incidents and the Australian Government Information Security Manual.

All agencies failed to reach even level one maturity for at least three of the Essential 8.

Cyber Security NSW modified the ACSC model for implementation of the Essential 8

The NSW maturity model used for the Essential 8 does not fully align with the ACSC's model. At the time of this audit the major difference was the inclusion of level zero in the NSW CSP maturity scale. Level zero broadly means that the relevant cyber mitigation strategy is not implemented or is not applied consistently. Level zero had been removed by the ACSC in February 2019 and was not part of the framework at the time of this audit. It was re-introduced in July 2021 when the ACSC revised the detailed criteria for each element of the essential 8 maturity model. The indicators to reach level one on the new ACSC model are more detailed, specific and rigorous than those currently prescribed for NSW Government agencies. Cyber Security NSW asserted the level zero on the CSP maturity scale:

> is not identical to the level zero of the ACSC's previous Essential 8 maturity model, but is a NSW-specific inclusion designed to prevent agencies incorrectly assessing as level one when they have not achieved that level.

[3] ACSC Essential Eight Maturity Model (June 2020)
[4] Australian Signals Directorate

Attestations did not accurately reflect whether agencies implemented the requirements

Of the nine participating agencies, seven did not modify the proforma wording in their attestation to reflect their actual situation. Despite known gaps in their implementation of mandatory requirements, these agencies stated that they had 'managed cyber security risks in a manner consistent with the Mandatory Requirements set out in the NSW Government Cyber Security Policy'. Only two agencies modified the wording of the attestation to reflect their actual situation.

Attestations should be accurate so that agencies' and the government's response to the risk of cyber attack is properly informed by an understanding of the gaps in agency implementation of the policy requirements and the Essential 8. Without accurate information about these gaps, subsequent decisions as to prioritisation of effort and deployment of resources are unlikely to effectively mitigate the risks faced by NSW Government agencies.

Participating agencies were not able to support all of their self-assessments with evidence and had overstated their maturity assessments, limiting the effectiveness of agency risk management approaches

Seven of the nine participating agencies reported levels of maturity against both the mandatory requirements and the Essential 8 that were not supported by evidence.

Each of the nine participating agencies for this audit had overstated their level of maturity against at least one of the 20 mandatory requirements. Seven agencies were not able to provide evidence to support their self-assessed ratings for the Essential 8 controls.

Where agency staff over-assess the current state of their cyber resilience, it can undermine the effectiveness of subsequent decision making by Agency Heads and those charged with governance. It means that actions taken in mitigating cyber risks are less likely to be appropriate and that gaps in implementing cyber security measures will remain, exposing them to cyber attack.

Agencies' self-assessments across government exposed poor levels of maturity in implementing the mandatory requirements and the Essential 8 controls

We reviewed the data 104 NSW agencies provided to Cyber Security NSW. The 104 agencies includes nine audited agencies referred to in more detail in this report. Our review of the 104 agency self-assessment returns submitted to Cyber Security NSW highlighted that, consistent with previous years, there remains reported poor levels of cyber security maturity. We reported the previous years' self-assessments in the Central Agencies 2019 Report to Parliament and the Central Agencies 2020 Report to Parliament.

Only five out of the 104 agencies self-assessed that they had implemented all of the mandatory requirements at level three or above (against the five point scale). Fourteen agencies self-assessed that they had implemented each of the Essential 8 controls at level one maturity or higher (using Cyber NSW's four point scale). The remainder reported at level zero for implementation of one or more of the Essential 8 controls, meaning that for the majority of agencies the cyber mitigation strategy has not been implemented, or is applied inconsistently.

Where agencies had reported in both 2019 and 2020, agencies' self-assessments showed little improvement over the previous year's self-assessments:

- 14 agencies reported improvement across both the Essential 8 and the mandatory requirements
- 8 agencies reported a net decline in both the Essential 8 and the mandatory requirements.

The poor levels of maturity in implementing the Essential 8 over the last couple of years is an area of significant concern that requires better leadership and resourcing to prioritise the required significant improvement in agency cyber security measures.

2. Recommendations

Cyber Security NSW should:

1. monitor and report compliance with the CSP by:
    - obtaining objective assurance over the accuracy of self-assessments
    - requiring agencies to resolve inaccurate or anomalous self-assessments where these are apparent
2. require agencies to report:
    - the target level of maturity for each mandatory requirement they have determined appropriate for their agency
    - the agency head's acceptance of the residual risk where the target levels are low
3. identify and challenge discrepancies between agencies' target maturity levels and the risks of the information they hold and services they provide
4. more closely align their policy with the most current version of the ACSC model.

Participating agencies should:

5. resolve the discrepancies between their reported level of maturity and the level they are able to demonstrate with evidence, and:
    - compile and retain in accessible form the artefacts that demonstrate the basis of their self-assessments
    - refer to the CSP guidance when determining their current level of maturity
    - ensure the attestations they make refer to departures from the CSP
    - have processes whereby the agency head and those charged with governance formally accept the residual cyber risks.

Repeat recommendation from the 2019 Central Agencies report and the 2020 Central Agencies report

6. Cyber Security NSW and NSW Government agencies need to prioritise improvements to their cyber security and resilience as a matter of urgency.

1. Introduction

1.1 Background to the Policy

The NSW Cyber Security Policy (CSP) took effect from 1 February 2019, replacing the NSW Digital Information Security Policy following the Audit Office's 2018 performance audit Detecting and responding to cyber security incidents.

The CSP is owned by Cyber Security NSW, which is a function within the Department of Customer Service. It is subject to annual review including agency feedback. The current version of the CSP was issued in April 2020.

Cyber Security NSW is responsible for providing policy and guidance on cyber security, coordination and communication on whole-of-government security threats and incidents, liaison with security functions in other branches of government and conducting whole-of-government cyber security exercises. Cyber Security NSW was established in May 2019 taking over the responsibilities of the former government Chief Information Security Officer. Its responsibilities are to enhance whole-of-government cyber security capabilities and standards, improve cyber incident response coordination and the development of cyber policies.

The CSP requires that agencies submit a report covering the following:

- Assessment against their implementation of 20 mandatory requirements, which address cyber security governance, culture and awareness, security over third party IT providers, and information sharing across government.
- Assessment of implementation of the Essential 8 controls. The Essential 8 are the highest priority mitigation strategies identified by the Australian Cyber Security Centre as the most effective measures to defend against cyber attacks.
- Their cyber security risks with high or extreme residual ratings.
- A list of their most valuable systems and information known as their 'crown jewels'.

Agencies are required to include an attestation on cyber security in their annual report and provide a copy to Cyber Security NSW by 31 August each year.

1.2 About this audit

We designed our audit procedures to conclude whether agencies were complying with the CSP during the year to 30th June 2020, including the reporting in August 2020.

The audit evaluated implementation of the CSP at nine participating agencies. The names of the agencies have been anonymised in respect of detailed information contained in this report, but were:

- the Department of Premier and Cabinet
- the Department of Communities and Justice
- the Department of Customer Service
- the Department of Education
- the Department of Planning, Industry and Environment
- the Department of Regional NSW
- the Ministry of Health
- the Treasury
- Transport for NSW (specifically the former functions of Roads and Maritime Services).

It addressed whether participating agencies:

- met their reporting obligations under the CSP
- provided accurate reporting in self-assessments against the CSP's mandatory requirements, including their implementation of the Australian Cyber Security Centre's (ACSC) Essential 8 strategies to mitigate cyber security incidents
- achieved implementation of mandatory requirements at maturity levels which meet or exceed the 'level three - Defined' threshold (i.e. are documented and practiced on a regular and consistent basis).

1.3 The maturity model

Implementation of the requirements is measured on a maturity scale

Agencies must assess the level to which they have implemented risk mitigation requirements each year. There are 25 elements to the CSP, five of which relate to reporting. The CSP requires agencies to assess their maturity in implementing the 20 elements with active requirements using a five point maturity model (refer to Appendix two for details of the CSP mandatory requirements maturity model).

Element 3.2 of the CSP relates to implementation of the Essential 8. The CSP requires agencies to assess their maturity against the Essential 8 using a four point maturity model (refer to Appendix three for details of the Essential 8 maturity model).

The CSP requires agencies to determine their level of maturity implementing the requirements using the scale outlined below.

Maturity Model for the mandatory requirements of the CSP

Maturity Model for the mandatory requirements of the CSP*

All requirements are defined on a scale of one to five categorised as:

1. Initial - the policy requirement is not practiced
2. Managed (Developing) - the requirement of the policy may only be performed on an ad-hoc basis and/or is not completely covering the scope of the requirement
3. Defined - the requirement is practiced on a consistent and regular basis and the relevant processes are documented
4. Quantitatively Managed - the requirement is reviewed/audited/governed on a regular basis to ensure that it is being performed as per the documented process/requirement and address any potential blockers
5. Optimised - the requirement is delivered with improved effectiveness such as through increased coverage/stakeholder involvement, automation of processes, continuous improvement, compliance requirements, etc.

Note: Some requirements will have slight variation in the maturity levels to these principles and so it is important to reference the maturity model for specific details of each mandatory requirement.

Source: Cyber Security Policy Maturity Model Guidance, updated April 2020.

Maturity Model for the Essential 8

The CSP requires agencies to report maturity against the Essential 8 using a four point scale based on the ACSC maturity model. The ACSC maturity model for the Essential 8 has changed a number of times since the inception of the CSP, including a revision in July 2021. The ACSC's broad definition of the maturity levels that were in force at the time of this audit[5] were:

- Level One: Partly aligned with the intent of the mitigation strategy
- Level Two: Mostly aligned with the intent of the mitigation strategy
- Level Three: Fully aligned with the intent of the mitigation strategy.

Cyber NSW adopted this model, but added a level zero for those agencies that were unable to attest to even level one on the ACSC maturity model. This meant NSW agencies used a four point maturity model whereas Commonwealth agencies were using a three point maturity model for the Essential 8. The specific maturity levels for each of the Essential 8 used by Cyber Security NSW and applicable in NSW at the time of the audit for reporting are detailed at Appendix three.

Agencies must make a self-assessment of their own cyber maturity

By 31 August each year, agencies must submit a report covering their self-assessment of the following:

- their maturity against all mandatory requirements in the CSP for the previous financial year
- their level of implementation of the Australian Cyber Security Centre (ACSC) Essential 8
- cyber security risks with a residual rating of high or extreme
- a list of the agency's 'crown jewels'.

Cyber Security NSW provides a template for this reporting, which agencies must use.

[5] ACSC Essential Eight Maturity Model (June 2020 version)

2. Implementation of the CSP

The objective of the CSP is to ensure cyber security risks are appropriately managed. However, meeting this objective depends on the requirements being implemented at all agencies to a level of maturity that addresses their specific cyber security risks. Agency systems and data are increasingly interconnected. If an agency does not implement the requirements, or implements them only in an ad-hoc or informal way, an agency is more susceptible to their systems and data being compromised, which may affect the confidentiality of citizens' data and the reliability of services, including critical infrastructure services.

Agencies determine their own target level of maturity, which may mean the requirement is not addressed, or is addressed in an ad hoc or inconsistent way

While the CSP is mandatory for all agencies, it does not set a minimum maturity threshold for agencies to meet.

The reporting template issued in 2019 stated that agencies were required to reach level three maturity in order to comply with the CSP. The 2020 revision[6] of the CSP and guidance indicates that level three maturity may not be sufficient to mitigate risks. It advises the agency may determine the level to which it believes it is suitable to implement the requirements, and allows for an agency to aim for a target level of maturity less than level three. The agency can set its optimal maturity level with reference to its risk tolerance with the objective that that aim ‘to be as high as possible’. However, ‘as high as possible’ does not necessarily mean ‘fully implemented’. The CSP contemplates that a lower level of maturity is sufficient if it aligns with the agency's risk tolerance.

2019 reporting template	**2020 reporting template**
‘A Mandatory Requirement is considered met if a maturity level of three is achieved. The Agency may choose to pursue a higher maturity level if required. There is no mandated level for the Essential 8 Maturity reporting’.	‘There is no mandated maturity level for either the Mandatory Requirement reporting or Essential 8 reporting. Agencies need to risk-assess their optimal maturity and aim to be 'as high as possible’.
Source: Maturity Reporting Template v4.0, February 2019.	Source: CSP Reporting Template 2020, May 2020.

The Department of Customer Service asserts that while the quotes above were part of their annual templates and policy documents, their documents were incorrect. They assert that the policy has never required a minimum level of maturity to be reached. They have responded to our enquiries that:

> …a level three maturity was not a requirement of the Policy or Maturity Model’ and ‘it is misleading to suggest it was a requirement of the Policy.

This audit found that, based on the 2020 reporting template there is no established minimum baseline. Consequently, because the Department of Customer Service had not established a minimum baseline agencies are able to target lower levels (providing they were within the agency’s own risk appetite), which includes targeting to not practice a CSP policy requirement, or to practice a CSP policy requirement on an ad hoc basis.

[6] The reporting template issued in 2019 required agencies to reach level three, but that guidance was removed in the 2020 revision.

Where requirements are not implemented, documentation of formal acceptance of the residual risks by the agency head is not required

The New Zealand Government has an approach that is not dissimilar to NSW, in that it also identifies 20 mandatory requirements and allows for a risk based approach to implementation. However, the New Zealand approach puts more rigor around risk acceptance decisions.

The New Zealand Government requires that agencies that do not implement the requirements must demonstrate that a measure is not relevant for them. It requires agencies to document the rationale for not implementing the measure, including explicit acknowledgement of the residual risk by the agency head. They require these records to be auditable.

> A security measure with a 'must' or 'must not' compliance requirement is mandatory. You must implement or follow mandatory security measures unless you can demonstrate that a measure is not relevant in your context.
>
> Not using a security measure without due consideration may increase residual risk for your organisation. This residual risk needs to be agreed and acknowledged by your organisation head.
>
> A formal auditable record of how you considered and decided which measures to adopt is required as part of the governance and assurance processes within your organisation.

Source: Overview of Protective Security Requirements, New Zealand Government (PSR-Overview-booklet.pdf (protectivesecurity.govt.nz).

The NSW CSP does not require these considerations to be documented or auditable and does not require an explicit acknowledgement or acceptance of the residual risk by the agency head.

None of the participating agencies achieved level three implementation for all mandatory risk prevention and mitigation requirements

Maturity level three is the minimum level whereby an agency has implemented documented processes that are practiced on a regular basis across their environment. An agency has not reached level three if the requirement is implemented on an ad-hoc or inconsistent basis, or if not all elements of the requirement have been implemented.

None of the participating agencies achieved level three implementation for all mandatory requirements.

The requirements of the CSP are organised into five sections. Agency implementation of these requirements is discussed in the next five sections of this report.

- Lead: Planning and governance requirements. Section 2.1
- Prepare: Cyber security culture requirements. Section 2.2
- Prevent: Managing cyber incident prevention requirements. Section 2.3
- Detect/Respond/Recover: Resilience requirements. Section 2.4
- Report: Reporting requirements. Section 2.5.

2.1 Planning and governance requirements

The first of the set of five mandatory requirements in the NSW CSP address leadership in the planning and governance for managing cyber risks. These requirements are:

- 1.1 Allocate roles and responsibilities.
- 1.2 A governance committee at the executive level to be accountable for cyber security including risks, plans and meeting the requirements of this policy.
- 1.3 An approved cyber security plan to manage the agency's cyber security risks, integrated with business continuity arrangements.
- 1.4 Cyber security threats are considered when performing risk assessments, which includes high and critical risks in the agency's overall risk management framework.
- 1.5 The agency is accountable for the cyber risks of their ICT service providers and ensuring their providers comply with the applicable parts of this policy and any other relevant agency security policies.

Our assessment of the level of maturity at each participating agency in implementing the five planning and governance requirements is summarised in the table below:

Audit assessment of agency maturity against planning and governance requirements

	Requirement				
Agency	**1.1**	**1.2**	**1.3**	**1.4**	**1.5**
Agency A	◔	○	○	◕	◔
Agency B	◐	◕	○	◔	◔
Agency C	◐	◐	○	◐	◐
Agency D	◐	◐	◔	◔	◔
Agency E	◐	◐	◐	◔	◔
Agency F	●	●	●	●	◕
Agency G	◔	◕	◐	◔	◔
Agency H	●	●	●	◔	◕
Agency I	◐	◐	◔	◔	◔

○ Level one maturity

◔ Level two maturity

◐ Level three maturity

◕ Level four maturity

● Level five maturity

Ratings surrounded by a box indicate that the agency reported a higher rating than we found to be supported by evidence. The accuracy of agency assessments of maturity is addressed below and at section 2.7 of this report.

Source: Audit Office analysis.

Some agency self-assessments were not accurate

Agency B over assessed their maturity at level two and Agency C over assessed at level three for requirement 1.3 (having an approved cyber security plan to manage the agency's cyber security risks). Neither agency had an approved cyber security plan at the time. Under the Maturity Model (see Appendix two) we assessed both of these agencies at level 1, which is defined as 'there is no approved cyber security plan'.

Eight of the nine participating agencies had not implemented all the planning and governance mandatory requirements at maturity level three or higher

These requirements are intended to ensure that responsibilities are defined for managing cyber risks, including those managed by third parties, and that cyber security risks are considered and planned for through integration with other strategic plans.

The level of maturity obtained by agencies indicates gaps exist in meeting these objectives, with the majority of audited agencies not reaching a 'defined' level of implementation of the requirements to:

- have an approved cyber security plan to manage the agency's cyber security risks, integrated with business continuity arrangements. This must include consideration of threats, risks and vulnerabilities that impact the protection of the agency's information and ICT assets and services
- consider cyber security threats when performing risk assessments and include high and critical risks in the agency's overall risk management framework
- be accountable for the cyber risks of their ICT service providers and ensure the providers comply with the applicable parts of this policy and any other relevant agency security policies.

Planning and governance are foundational steps in establishing a cyber resilient organisation. Failure to more fully implement these requirements can increase the risk that cyber security is not adequately considered in strategic planning and the management of third parties.

2.2 Cyber security culture requirements

The second of the set of five mandatory requirements address how agencies prepare themselves to build and support a cyber security aware culture. Requirements in this section address cyber security culture at agencies and across government. These requirements are:

- 2.1 Implement regular cyber security education for all employees and contractors, and ensure that outsourced ICT service providers implement similar cyber security requirements.
- 2.2 Increase awareness of cyber security risk across all staff including the need to report cyber security risks.
- 2.3 Foster a culture where cyber security risk management is an important and valued aspect of decision-making and where cyber security risk management processes are understood and applied.
- 2.4 Ensure that people who have access to sensitive or classified information or systems and those with privileged system access have appropriate security screening, and that access is removed when no longer appropriate.
- 2.5 Agencies share information on security threats and intelligence with Cyber Security NSW and cooperate across NSW Government to enable management of government-wide cyber risk.

Our assessment of the level of maturity at each participating agency in implementing the five cyber security culture requirements is summarised in the table below:

Audit assessment of agency maturity against cyber security culture requirements

	Requirement				
Agency	**2.1**	**2.2**	**2.3**	**2.4**	**2.5**
Agency A	◔	◔	◔	◔	◐
Agency B	◔	◐	◔	◐	◕
Agency C	◔	◐	◐	◔	◐
Agency D	◔	◐	◔	◔	◐
Agency E	◐	◐	◐	◔	◐
Agency F	◐	◕	●	◔	◔
Agency G	◔	◔	◔	◔	◕
Agency H	◔	◔	◔	◔	●
Agency I	◔	◐	◔	◔	◐

○ Level one maturity

◔ Level two maturity

◐ Level three maturity

◕ Level four maturity

● Level five maturity

□ Ratings surrounded by a box indicate that the agency reported a higher rating than we found to be supported by evidence. The accuracy of agency assessments of their maturity is addressed below and at section 2.7 of this report.

Source: Audit Office analysis.

Some agency self-assessments were not accurate

Agency A, Agency B, and Agency C each over assessed their maturity for requirement 2.1 (implementing regular cyber security education for all employees and contractors, and ensuring outsourced ICT service providers understand and implement the cyber security requirements of their contracts). Each of these agencies self-assessed at level three but achieved only level two maturity because they did not ensure education is available for contractors and ICT service providers.

Agency D and Agency I assessed their maturity for requirement 2.3 (fostering a culture where cyber security risk management is an important and valued aspect of decision-making and where cyber security risk management processes are understood and applied) at level four. We assessed them at level two because their enterprise risk management framework had not been finalised or rolled out within the reporting period.

Agency F and Agency G over assessed their maturity for requirement 2.4 (ensuring people who have access to sensitive or classified information or systems and those with privileged system access have appropriate security screening, and that access is removed when they no longer need to have access, or their employment is terminated) at level three. We assessed them at level two because controls over the removal and auditing of access privileges were not performed on a regular basis.

Agency F over assessed their maturity for requirement 2.5 (sharing information on security threats and intelligence with Cyber Security NSW and cooperating across the NSW Government to enable management of government-wide cyber risk) at level 4. We assessed them at level two because an assessment of maturity above that level requires a defined workflow for information sharing as part of the procedures for incident management. This did not exist at this agency.

No participating agency had implemented all the cyber security culture mandatory requirements at maturity level three or higher

These requirements are intended to establish behaviours and attitudes across the organisation that adequately reflect the importance of cyber security risks.

The level of maturity attained by agencies indicates that these objectives are not being met, with the majority of audited agencies not reaching a 'defined' level of implementation of the requirements to:

- Conduct regular cyber security education for all employees and contractors, and ensure that outsourced ICT service providers understand and implement the cyber security requirements under their contracts.
- Foster a culture where cyber security risk management is an important and valued aspect of decision-making and where cyber security risk management processes are understood and applied.
- Ensure that people who have access to sensitive or classified information or systems and those with privileged system access have appropriate security screening, and that access is removed when they no longer need to have access, or their employment is terminated.

Agencies without cyber secure awareness and behaviours are more susceptible to cyber attacks.

2.3 Managing cyber incident prevention requirements

The third of the set of five mandatory requirements address the prevention of cyber security incidents. These requirements are:

- 3.1 Implement an Information Security Management System (ISMS) or Cyber Security Framework (CSF), with scope at least covering systems identified as an agency's 'crown jewels'. The ISMS or CSF should be compliant with, or modelled on, one or more recognised ICT/OT standard.
- 3.2 Implement the ACSC Essential 8 - (for further details on the implementation of the Essential 8 refer to sections 2.6 and 2.8 of this report).
- 3.3 Classify information and systems according to their importance (i.e. the impact of loss of confidentiality, integrity or availability), adhere to the requirements of the NSW Government Information Classification Labelling and Handling Guidelines and:
  - assign ownership
  - implement controls according to their classification and relevant laws and regulations
  - identify the agency's 'crown jewels' and report them to Cyber Security NSW as per mandatory requirement 5.4.
- 3.4 Ensure cyber security requirements are built into procurements and into the early stages of projects and the system development life cycle (SDLC), including agile projects.
- 3.5 Ensure new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data including processes for internal fraud detection.

Our assessment of the level of maturity at each participating agency in implementing the five cyber incident prevention requirements is summarised in the table below:

Audit assessment of agency maturity against cyber incident prevention requirements

	Requirement				
Agency	**3.1**	**3.2**	**3.3**	**3.4**	**3.5**
Agency A	○	○	◐	○	○
Agency B	◔	◔	◐	◔	◔
Agency C	○	◐	○	◐	○
Agency D	◐	◔	○	◔	◔
Agency E	◐	◔	○	◔	◔
Agency F	◐	◔	◐	◐	◔
Agency G	○	◔	◕	◔	◔
Agency H	○	◔	◔	◐	◔
Agency I	◐	◔	◐	◔	◔

○ Level one maturity

◔ Level two maturity

◐ Level three maturity

◕ Level four maturity

● Level five maturity

Ratings surrounded by a box indicate that the agency reported a higher rating than we found to be supported by evidence. The accuracy of agency assessments of their maturity is addressed below and at section 2.7 of this report.

Source: Audit Office analysis.

Requirement 3.2 mandates that agencies implement the Essential 8. The self-assessments against Requirement 3.2 measure the state of maturity in terms of the extent an agency has commenced implementing all the Essential 8 requirements (refer Appendix two). The actual implementation of each of the Essential 8 mitigation strategies is measured against the detailed criteria set out in the maturity model at Appendix three. The table above shows the agency aggregate assessment of Essential 8 implementation. Agencies must then make a detailed assessment of maturity against each of the Essential 8 mitigation strategies. We cover the results and accuracy of agencies' assessment of their maturity in implementing mitigation strategies for the individual components of the Essential 8 at section 2.6 of this report.

Only one agency had achieved level three maturity against the aggregate maturity model at Appendix two, being 'Implementation of the Essential 8 has commenced for all mitigation strategies and maturity is projected to improve year-on-year'. Notably, this does not mean all of the mitigation strategies have been implemented.

Seven agencies achieved level two maturity – 'Implementation of the Essential 8 has not commenced for all mitigation strategies but there is a plan to begin implementation with CIO approval'.

One agency attained only level one maturity – 'Implementation of the Essential 8 has not commenced for all mitigation strategies or implementation of the Essential 8 has not been approved by the CIO.'

The Essential 8 are the frontline of cyber attack prevention and are a series of practical controls to specifically address system vulnerabilities that leave agencies open to cyber-attacks. The low level of maturity agencies reported in regards to agencies' overall maturity and the level to which they have progressed implementing each of the Essential 8 strategies should be of significant concern.

Some agency self-assessments were not accurate

Agency C and Agency G over assessed their maturity for requirement 3.1 (implementing an Information Security Management System (ISMS) or Cyber Security Framework (CSF), with scope at least covering systems identified as an agency's 'crown jewels' that is compliant with, or modelled on, one or more recognised ICT/OT standard) at level three. We assessed them at level one because there were 'crown jewels' not covered by an ISMS, which is required for assessments at level two or higher. Each agency is required to nominate their crown jewels and register them with Cyber NSW.

Agency C and Agency E over assessed their maturity for requirement 3.3 (classifying information and systems according to their importance and applying the NSW Government Information Classification Labelling and Handling Guidelines) at level two. We assessed them at level one because an assessment at a maturity level above level one requires dedicated owners to be assigned to systems. This had not occurred at these agencies.

Agency A over assessed their maturity for requirement 3.4 (ensuring cyber security requirements are built into procurements and into the early stages of projects and the system development life cycle) at level two. We assessed them at level one because their project management process did not incorporate security considerations in the early stages. Agency H over assessed their maturity for this requirement at level four. We assessed the agency at level three because there was a lack of documentation of required formal procedures.

Agency A over assessed their level of maturity for requirement 3.5 (ensuring new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data including processes for internal fraud detection) at level two. We assessed them at level one because the policy and procedures were not documented as required. Agency D, Agency F and Agency I over assessed their maturity at level three. We assessed them at level one because an assessment above this level requires the agency to have processes to ensure audit and activity logging is in place. This was not in place for these agencies.

We have previously reported in the Central Agencies 2019 Report to Parliament and the Central Agencies 2020 Report to Parliament that poor levels of maturity in implementing the Essential 8 is an area of significant concern that requires better leadership and resourcing to remediate to a minimum standard.

We deal with agency performance against this criteria in more detail at section 2.6.

No participating agency has implemented all the cyber security prevention mandatory requirements at maturity level three or higher

These requirements are intended to reduce the likelihood of a successful cyber-attack.

The level of maturity obtained by agencies indicates that these objectives are not being met, with the majority of audited agencies not reaching a 'defined' level of implementation of the requirements to:

- implement an Information Security Management System (ISMS) or Cyber Security Framework (CSF), with scope at least covering systems identified as an agency's 'crown jewels'. The ISMS or CSF should be compliant with, or modelled on, one or more recognised ICT/OT standard
- implement the ACSC Essential 8
- ensure cyber security requirements are built into procurements and into the early stages of projects and the system development life cycle (SDLC), including agile projects
- ensure new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data, including processes for internal fraud detection.

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

2.4 Resilience requirements

The fourth of the set of five mandatory requirements address resilience. These requirements are:

- 4.1 Have a current cyber incident response plan that integrates with the agency incident management process and the NSW Government Cyber Incident Response Plan.
- 4.2 Test their cyber incident response plan at least every year, and involve their senior business and IT executives, functional area coordinators (if applicable), as well as media and communication teams.
- 4.3 Deploy monitoring processes and tools to allow for adequate incident identification and response.
- 4.4 Report cyber security incidents to Cyber Security NSW according to the NSW Cyber Security Response Plan.
- 4.5 Participate in whole-of-government cyber security exercises as required.

Our assessment of the level of maturity at each participating agency in implementing the five cyber resilience requirements is summarised in the table below:

Audit assessment of agency maturity against resilience requirements

	Requirement			
Agency	**4.1**	**4.2**	**4.3**	**4.4**
Agency A				
Agency B				
Agency C				
Agency D				
Agency E				
Agency F				
Agency G				
Agency H				
Agency I				

 Level one maturity

 Level two maturity

 Level three maturity

 Level four maturity

 Level five maturity

 Ratings surrounded by a box indicate that the agency reported a higher rating than we found to be supported by evidence.

Source: Audit Office analysis.

Some agency self-assessments were not accurate

Agency A over assessed their maturity for requirement 4.1 (having a current cyber incident response plan that is integrated with the agency's incident management process and the NSW Government Cyber Incident Response Plan) at level three. We assessed them at level two because their disaster recovery plan did not cater for cyber security incidents, which is a requirement of the maturity model. Agency F assessed their maturity at level four. We assessed them at level two because their incident management plan had not been updated since 2016, and was not current.

Agency A and Agency F over assessed their maturity for requirement 4.2 (testing cyber incident response plans at least every year, and involving senior business and IT executives, functional area coordinators and media and communication teams). The maturity model requires a test to have been conducted, either in the current year or at any time previously, to reach level two or above. Agency A self-assessed at level two but had never conducted testing. We assessed them at level one. Agency F self-assessed at level four, but had not tested their incident response plan within the current reporting period. We assessed them at level two.

Requirement 4.5 mandates that agencies take part in whole-of-government security exercises. This was the only requirement for which any agencies' self-assessed rating was lower than what was supported by the available evidence.

All agencies were represented at a whole-of-government exercise conducted in August 2019 (within the period covered by the self-assessments), and therefore should have assessed at level three or four. There was a planned whole-of-government exercise later in the year, which was cancelled due to restrictions arising from the pandemic. Because of this cancellation, some agencies reported at level one where they believed no exercise had taken place in the year.

Eight of the nine agencies had not implemented all the cyber security resilience mandatory requirements at maturity level three or higher.

These requirements are intended to ensure agencies can detect and respond to cyber incidents. The level of maturity attained by agencies indicates that these objectives are not being met, with the majority of audited agencies not reaching a ‘defined’ level of implementation of the requirements to:

- Test their cyber incident response plan at least every year, and involve their senior business and IT executives, functional area coordinators (if applicable), as well as media and communication teams.
- Deploy monitoring processes and tools to allow for adequate incident identification and response.

Inadequate identification and response to cyber incidents can increase the likely impact and duration of cyber attacks.

2.5 Reporting requirements

The last of the set of five mandatory requirements set out the reporting obligations, which are due by 31 August each year. These are not measured on a maturity model.

Agencies are required to:

- report their maturity against the mandatory requirements in the format provided
- report their maturity against the Essential 8 in the format provided
- report cyber security risks with a residual rating of high or extreme
- report their crown jewels
- provide an attestation of their compliance signed by the agency head.

Attestations do not reflect the actual realities in levels of implementing the requirements

The CSP provides a proforma for agency heads to make the required annual attestations but encourages modification to suit the situation. The attestation should address the following:

- the agency has assessed its cyber security risks
- cyber security is appropriately addressed at agency governance forums
- the agency has a cyber incident response plan, it is integrated with the security components of business continuity arrangements, and has been tested over the previous 12 months (involving senior business executives)
- confirmation of the agency's Information Security Management System (ISMS), Cyber Security Management Framework/s (CSF) and/or Cyber Security Framework (CSF) including certifications or independent assessment where available
- what the agency is doing to continuously improve the management of cyber security governance and resilience.

The proforma contains the following draft attestation:

> I, [name of Department Head or Governing Board of the Statutory Body], am of the opinion that [name of Department or Statutory Body] has managed cyber security risks in a manner consistent with the Mandatory Requirements set out in the NSW Government Cyber Security Policy.

Source: Cyber Security Policy, updated May 2020.

Of the nine participating agencies, seven did not modify the proforma wording in their attestation to acknowledge known gaps in their implementation of mandatory requirements and low maturity in some areas. Two agencies modified the wording to reflect their situation.

The Department of Customer Service responded to this finding by stating that it is incorrect because:

> the example attestation is a suggested only and can be adapted to accurately reflect the circumstances of the agency or cluster, but not that it **must** be adapted.

It is our view that any attestation should reflect the facts and substance of the subject matter, and not simply replicate the wording in a proforma.

Attestations should be accurate and demonstrate that management's response to the risk of cyber attack is informed by an understanding of the gaps in their implementation of the policy requirements and the Essential 8. Without an acknowledgement of these gaps, risk management decisions may not be appropriate to the actual level of risk faced by the agency.

Alignment between attestations and implementation of the mandatory requirements

Agency	Number of the 20 mandatory requirements self-assessed at level three or above	Modified wording of attestation to reflect incomplete implementation
Agency A	7	No
Agency B	10	No
Agency C	14	Yes
Agency D	11	No
Agency E	12	No
Agency F	19	No
Agency G	9	Yes
Agency H	10	No
Agency I	11	No

Source: Audit Office analysis.

2.6 Implementing the Essential 8

Requirement 3.2 of the CSP mandates that agencies implement the Essential 8.

The ACSC recommends the Essential 8 as important controls in preventing cyber attacks

The Australian Cyber Security Centre (ACSC) was established in 2014 to lead the Australian Government's work to improve cyber security. ACSC is part of the Australian Signals Directorate within the Defence portfolio. The ACSC has defined 37 cyber security strategies, prioritising eight of these as a baseline for all organisations in mitigating cyber-attacks. These eight highest priority strategies are called the 'Essential 8'.

The guidance from ACSC[7] states that:

> As a baseline, organisations should aim to reach maturity level three for each mitigation strategy.

The CSP requires agencies to report maturity against the Essential 8 using a four point scale based on the ACSC maturity model. The ACSC maturity model for the Essential 8 has been revised a number of times, including a significant revision in July 2021. At the time of the audit, the broad definitions in the CSP for each maturity level[8] were:

- Level Zero: Not meeting the criteria for Level One
- Level One: Partly aligned with the intent of the mitigation strategy
- Level Two: Mostly aligned with the intent of the mitigation strategy
- Level Three: Fully aligned with the intent of the mitigation strategy.

The specific maturity levels used by Cyber Security NSW for reporting and that were applicable at the time of the audit are detailed at Appendix three.

[7] ACSC Essential Eight Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
[8] PROTECT - Essential Eight Maturity Model (April 2020).pdf (cyber.gov.au)

The Essential 8 are key IT controls aimed at protecting against cyber attack

	Requirement	Importance
	Mitigation strategies to prevent malware delivery and execution	
1.	***Application control** (whitelisting) to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.	Non-approved applications (including malicious code) are prevented from executing. It is more effective than traditional anti-virus or anti-malware programs and can stop attacks that are not blocked by these tools.
2.	***Patch applications** e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.	Security vulnerabilities in applications can be used to execute malicious code on systems.
3.	**Configure Microsoft Office macro settings** to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.	Microsoft Office macros can be used to deliver and execute malicious code on systems.
4.	**User application hardening**. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.	Flash, ads and Java are popular ways to deliver and execute malicious code on systems.
	Mitigation strategies to limit the extent of cyber security incidents	
5.	***Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.	Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.
6.	***Patch operating systems**. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.	Security vulnerabilities in operating systems can be used to further the compromise of systems.
7.	**Multi-factor authentication** including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.	Stronger user authentication makes it harder for adversaries to access sensitive information and systems.
	Mitigation strategies to recover data and maintain system availability	
8.	**Daily backups** of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.	To ensure information can be accessed following a cyber security incident (e.g. a ransomware incident) limiting the loss of data to no more than one day.

* Denotes this strategy is part of the 'top four'. Refer to Appendix three.

Source: The requirements are from the ACSC Essential Eight Explained June 2020.

Cyber Security NSW modified the ACSC model for implementation of the Essential 8

The NSW maturity model used for the Essential 8 does not fully align with the ACSC's model. At the time of this audit the major difference was the inclusion of level zero on the CSP maturity scale, broadly meaning that the relevant cyber mitigation strategy is not implemented, or is not applied consistently. Level zero had been removed by the ACSC in February 2019 and was not part of the framework at the time of this audit. It was re-introduced in July 2021 when the ACSC revised the detailed criteria for each element of the essential 8 maturity model. The indicators to reach level one on the new ACSC model are more detailed, specific and rigorous than those currently prescribed for NSW Government agencies. Cyber Security NSW asserted the level zero on the CSP maturity scale:

> is not identical to the level zero of the ACSC's previous Essential 8 maturity model, but is a NSW-specific inclusion designed to prevent agencies incorrectly assessing as level one when they have not achieved that level.

No participating agency has implemented all of the Essential 8 controls at level one or above

Number of participating agencies achieving each maturity level against the Essential 8

Essential 8 mitigation strategies	Maturity level zero	Maturity level one	Maturity level two	Maturity level three
Application control (whitelisting)*	9	--	--	--
Patch applications*	6	1	2	--
Configure Microsoft office macro settings	7	1	--	1
User application hardening	8	--	--	1
Restrict administrative privileges*	4	5	--	--
Patch operating systems*	8	--	1	--
Multi-factor authentication	3	6	--	--
Daily backups	1	5	3	--

* The asterisk denotes that this strategy is part of the 'top four' (Appendix three).

Note: Maturity levels for the Essential 8 are described in section 1.3 of this report.

Source: Audit Office analysis.

Few controls were implemented in a way that could be considered fully or mostly aligned with the cyber security strategy. Some strategies have been implemented by very few or none of the agencies. The most common level of implementation of Essential 8 controls was level zero - that is, the control had not been implemented, or is not applied consistently. Other controls were only partially implemented by agencies.

The ACSC advises that the baseline all organisations should aim to reach is maturity level three for each of these 8 highest priority strategies to mitigate cyber security incidents[9].

Agency B had implemented two of the Essential 8 strategies to level three - fully aligned with the strategy. No other participating agency had implemented any of the Essential 8 to this level.

[9] ASD Essential Eight Maturity Model June 2020

The two least implemented controls were application whitelisting and user application hardening. Whitelisting prevents malicious code from executing, protecting against many types of attack such as trojans and phishing attacks. It is more effective than traditional anti-virus or anti-malware programs and can stop attacks that are not blocked by these tools. Implementing application whitelisting can be costly, and some of our participating agencies reported cost as an impediment to implementing sufficient measures in the short term. Application hardening removes insecure or non-essential elements which might be used by attackers.

The lack of multifactor authentication contributed to the cyber attacks on Service NSW in March 2020, in which staff members had their email accounts accessed without authorisation, and documents containing personal information on NSW residents were compromised. This was reported in the Auditor-General's report on the Service NSW's handling of personal information tabled on 18 December 2020.

We reported the status of implementing the Essential 8 in the Central Agencies 2019 Report to Parliament and the Central Agencies 2020 Report to Parliament. We recommended in those reports that Cyber Security NSW and NSW Government agencies need to prioritise improvements to their cyber security resilience as a matter of urgency. The poor levels of maturity in implementing the Essential 8 is an area of significant concern that requires better leadership and resourcing.

Agencies' implementation of the 'top four' cyber controls is poor

Four of the Essential 8 strategies (the 'top four') have previously been assessed by the Australian Signals Directorate as mitigating:

> Over 85 per cent of adversary techniques used in targeted cyber intrusions which ASD has visibility of.[10]

The top four controls[11] are:

- Application whitelisting
- Patching applications
- Patching operating systems
- Restricting administrative privileges.

There is currently no requirement in NSW for any agency to implement the 'top four' to any designated level of maturity.

[10] Source: ACSC Essential Eight Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

[11] Information security | Protective Security Policy Framework

2.7 Accuracy of self-assessments

Participating agencies were not able to support all of their ratings with evidence

Seven of the nine participating agencies had reported levels of maturity against both the mandatory requirements and the Essential 8 that were not supported by evidence.

Each of the nine participating agencies for this audit had overstated their level of maturity against at least one of the 20 mandatory requirements. Seven agencies were not able to show evidence to support their self-assessed rating across all of the Essential 8 controls.

Accuracy of self-reported maturity against the mandatory requirements

Agency	Number of requirements for which evidence did not support the stated level of maturity
Agency A	5
Agency B	2
Agency C	4
Agency D	2
Agency E	1
Agency F	5
Agency G	2
Agency H	1
Agency I	2
Total	**24**

Source: Audit Office analysis.

Inaccurate self-assessments limit the effectiveness of risk management strategies as the level of risk exposure is not properly considered or understood

For all except one requirement the inaccuracy overstated the level of implementation. Most inaccuracies arose from a misunderstanding of the maturity model or applying the model without fully considering all aspects of the environment. The reasons for inaccuracy in the self-assessments against the mandatory requirements included are detailed in the relevant sections of this report.

Inaccuracies in self-assessments against the Essential 8 were generally that some but not all aspects of the strategy had been implemented, or that the strategy was being implemented but had not been completed by the reporting date.

Agency ratings for these were either level one or level two, and in every case we assessed the level of maturity at zero:

- Two agencies over-assessed their implementation of application whitelisting. One agency relied on mitigating controls but had not implemented the specified control - i.e. to run only executables which are defined in an approved whitelist. The other agency had not completed their implementation at the time of reporting.
- Two agencies over-assessed their patching of applications, and four agencies over-assessed patching of operating systems. These agencies had applications or operating systems that were no longer supported by the vendor with patches.
- Four agencies over-assessed their configuration of macros and three agencies over-assessed their application hardening, either because they had not implemented all elements of the strategy, or because implementation was still underway at the time of reporting.
- Three agencies over-assessed their restriction of privileged access. In one case access levels for privileged accounts did not prevent reading emails and web browsing. Two other agencies' assessments were inaccurate because of ineffective operation of controls to approve new privileged user accounts and review existing privileged accounts.
- One agency over-assessed daily backups as they could not evidence that backups were stored for the period required or tested periodically.
- One agency over-assessed their multifactor authentication as it was not applied to all privileged accounts.

2.8 Self-reported levels of implementation across government

Agencies are required by the CSP to report their self-assessed levels of cyber maturity to Cyber Security NSW. 2020 was the second year of reporting, and this section reports observations from the self-assessed ratings submitted by 104 agencies, nine of which were audited and their results reflected in the earlier sections of this report. One hundred and three of these agencies submitted self-assessed ratings against the Essential 8. The analysis below indicates the need for prioritised and urgent improvement to agencies' cyber security and resilience across the sector.

Agencies across government self-assessed low levels of maturity in implementing the mandatory requirements

Only five out of the 104 agencies self-assessed that they have implemented all of the mandatory requirements at level three or above (on the five point maturity scale, refer Appendix two). This means that, according to their own self-assessments, 99 agencies practiced the requirements in the framework in a way that can be described as either ad hoc, or not practiced at all. Two agencies self-assessed that they have not reached this level for any of the mandatory requirements, and a further three agencies have reached this level for only one requirement. One of these agencies lists critical infrastructure systems among systems it identified as being one of its crown jewels. Forty-seven agencies reported not having reached level three for more than half of the 20 mandatory requirements.

The requirements which were most commonly reported to be below level three include:

- 43 agencies self-reported below level three for requirement 1.3 (an approved cyber security plan to manage the agency's cyber security risks, integrated with business continuity arrangements)
- 34 agencies self-reported below level three for requirement 3.5 (ensure new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data including processes for internal fraud detection)
- 42 agencies self-reported below level three for requirement 4.1 (have a current cyber incident response plan that integrates with the agency incident management process and the NSW Government Cyber Incident Response Plan).

Some agencies have reported improvement since 2019, others have declined

Forty-nine agencies self-assessed and reported their maturity ratings against the mandatory requirements in both 2019 and 2020. Since 2019, most agencies had improved their rating against one or more requirements, and also reported a lower rating in one or more other requirements.

Of those 49 agencies reporting in both years:

- 25 agencies reported a net improvement (reporting improvements against more requirements than those where they declined)
- 21 agencies reported a net decline (reporting they declined against more requirements than those where they improved)
- 3 agencies improved and declined against the same number of requirements.

The Department of Customer Services, whilst acknowledging the above information is correct, contended that:

> it does not account for modifications to the policy between 2019 and 2020 and further clarifications and guidance which were designed to help agencies with more accurate understanding and assessment.

Our findings, based on this audit, would indicate that accuracy in the self-assessment process still has some way to go.

Most agencies had not implemented all of the Essential 8 controls at level one or above

Fourteen agencies have reported that they implemented the Essential 8 controls at level one maturity or higher. The remainder of agencies (89 of the 103 agencies) have not reached this level against one or more of the Essential 8 controls. A further agency reported on other aspects of its cyber security implementation but did not report on its implementation of the Essential 8.Failing to implement these strategies to mitigate cyber incidents increases the exposure to intrusions and ransomware, and as reported in the Central Agencies 2019 Report to Parliament and the Central Agencies 2020 Report to Parliament, there is an urgent need to uplift cyber security resilience.

Maturity in some Essential 8 controls has reduced since 2019

Patching operating systems, multifactor authentication, performing daily backups and application whitelisting all require improvement.

Of those 48 agencies that reported their maturity against the Essential 8 in both 2019 and 2020:

- 25 agencies reported a net improvement (they improved against more requirements than they declined)
- 14 agencies reported a net decline (they declined against more requirements than they improved)
- 9 agencies improved and declined against the same number of requirements.

Across the Essential 8 and the mandatory requirements:

- 14 agencies improved across both the Essential 8 and the mandatory requirements
- 8 agencies declined in both the Essential 8 and the mandatory requirements.

Twenty-three agencies did not meet the reporting and attestation requirements

Of the 104 agencies required to report:

- 15 agencies did not submit their reports by the 31 August deadline
- 1 agency reported on time but did not use the required format
- 8 agencies had not had their attestations signed by the Agency Head at the time of reporting to Cyber Security NSW.

Section two

Appendices

Appendix one – Response from agencies

Response from the Department of Premier and Cabinet

Ref: A3908166

Ms Margaret Crawford
Auditor-General for New South Wales
Level 19
Darling Park Tower 2
201 Sussex Street
Sydney NSW 2000

RE: Special Audit – Compliance with the NSW Cyber Security Policy

Dear Ms Crawford

Thank you for the opportunity to provide a response to your draft report on the Special Audit – Compliance with NSW Cyber Security Policy (the **Report**).

I acknowledge your key findings and recommendations; my Department is implementing a Cyber Security Uplift Program which will address recommendations 4 and 5 for participating agencies.

I have major concerns about the Report being published in the public domain. The Report contains aggregated data on the current state of nine NSW Government Departments' cyber security maturity, including individual agencies' maturity against the Australian Cyber Security Centre's Essential 8.

Making this information available in the public domain would increase the risk of a successful cyber-attack against the nine NSW Government Departments covered by the Report.

I am also concerned that the Report has assessed that, to be compliant, an agency must reach level 3 maturity. This goes against the risk-based intent of the policy, which encourages agencies to identify the level of maturity that is appropriate for their organisation, given their risk profile.

In these circumstances, I respectfully request that the Audit Office consider options to allow:

- a public, summary version of the Report to be prepared for tabling in Parliament (containing, for example, only the Executive Summary of the Report); and
- a private, detailed version of the Report being made available for inspection by Members of Parliament on a confidential basis and to relevant agencies.

Yours sincerely

Tim Reardon
Secretary

14 July 2021

52 Martin Place, Sydney NSW 2000 ■ GPO Box 5341, SYDNEY NSW 2001
Tel: (02) 9228 5555 ■ www.dpc.nsw.gov.au

Response from the Department of Communities and Justice

NSW GOVERNMENT | Communities & Justice

Margaret Crawford
Auditor-General for New South Wales
Audit Office of NSW
201 Sussex Street
SYDNEY NSW 2000

8 July 2021

Ref: EAP21/9556

Dear Ms Crawford

Special Audit – Compliance with the NSW Cyber Security Policy

Thank your letter dated 17 June 2021 and for the opportunity to respond to the recently completed audit.

DCJ considers the information in the report to be valuable for internal use.

Please find attached a table responding to each recommendation in the report. As you will see, we have outlined the action we will take in response to your recommendations about NSW Cyber Security policy.

The DCJ Chief Information Security Officer (CISO) recent met with the other departmental CISOs at the Cyber Security Senior Officers Group (CSSOG) meeting. There was consensus that the report provides an inappropriate amount of detail regarding the security maturity of departments.

Whilst it is appropriate to identify poor practice and behaviour, from a cyber-security perspective we ask that the Audit Office not be identify control weaknesses and publish them which may support a successful cyber-attack.

The approach taken by the Audit Office to publicly release this detailed information is out of step with industry standards and will assist attackers in better targeting agencies. Whilst other organisations undertake invasive audits and share their reporting with customers these reports are shared under a non-disclosure agreement and not released into the public domain.

An amended report focused on identifying over-inflated scoring (but not identifying the score) for departments should be developed. The report could identify non-compliance to the policy, but specific control references need to be removed.

I look forward to continuing our progress in relation to cyber security and compliance with the NSW Cyber Security policy including our response to the report's recommendations.

Should you require any further information please contact Thomas Thornton, Director, Audit, Risk and Compliance on 0475 985 672 or Thomas.Thornton@dcj.nsw.gov.au.

Yours sincerely

Michael Coutts-Trotter
Secretary

Department of Communities and Justice
Postal address: Locked Bag 10, Strawberry Hills NSW 2012
W www.dcj.nsw.gov.au
T (02) 9377 6000 | **TTY** (02) 8270 2167
ABN 36 433 875 185

Response from the Department of Customer Service

NSW GOVERNMENT | Customer Service

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

Office of the Secretary

Our reference: COR-06791-2021

Ms Margaret Crawford
Auditor-General
Audit Office of NSW
By email: mail@audit.nsw.gov.au

Dear Ms Crawford

Thank you for your letter dated 28 September 2021, and for the opportunity to respond to the *Compliance with the NSW Cyber Security Policy* final report (the Report). I would like to express gratitude to the Audit Office of New South Wales (NSW Audit Office) for its genuine engagement and consideration of concerns raised by the Department of Customer Service (the Department) regarding the sensitivity of information contained in previous iterations of the Report.

The Report raises important issues regarding the implementation of the NSW Cyber Security Policy (the Policy). As in previous NSW Audit Office reports, the analysis and recommendations play a critical role in improving cyber security resilience and the accountability of NSW Government entities.

I note that the Report examined the 2020 iteration of the Policy. The Policy has been updated since that time with version 4.0 released in April 2021. The Policy continues to undergo regular review and update. Cyber Security NSW has recently commissioned an independent external review of the Policy and is also consulting closely with State and Federal government agencies to identify potential changes. The Policy review will consider findings and recommendations from the NSW Audit Office and the Parliamentary Inquiry into Cybersecurity. This review and the feedback from ongoing consultation will enable the Policy to continue to evolve to address the changing technological and threat landscape as well as address lessons learnt.

The Department notes the recommendation to increase monitoring and compliance of maturity reporting to ensure greater accuracy. Cyber Security NSW's Governance, Risk and Compliance (GRC) team will be commencing a Maturity Assurance Review program with selected Policy mandatory requirements being reviewed across all Clusters. This program will assess the accuracy of maturity reporting, provide guidance for cyber security uplift requirements, and report uplift outcomes to Secretaries Board.

The Department notes the recommendations for agencies to report target maturity levels for each mandatory requirement and provide acceptance of residual risk for low target levels, and to better identify discrepancies in target maturity levels, risks associated with information held and services provided. These recommendations will be addressed in the review of the Policy.

The Department notes the recommendation to align the Policy closely to the Australian Cyber Security Centre's (ACSC) Essential Eight. Relevant sections of the 2022 NSW Cyber Security Policy will align with the recent updates to the Essential Eight framework.

The Department notes the concerns of the NSW Audit Office about the presence of a level 0 maturity for Essential Eight in the 2020 iteration of the Policy. However, the Department stands by its inclusion as part of supporting accurate assessment of maturity. This approach is supported by the re-introduction by the ACSC of level 0 in the July 2021 version of the

Essential Eight. This iteration of the Policy was made in consultation with the ACSC and industry partners. Cyber Security NSW would be happy to facilitate deeper engagement between the NSW Audit Office and the ACSC to ensure enhanced understanding of this framework and its implementation.

The Department notes the recommendation to prioritise improvements to cyber security and resilience across NSW Government agencies. The net decline in agency scores across the Policy in the 2020 reporting reflected a growing understanding by agencies on how to report maturity and Cyber Security NSW in analysing it. NSW Government is unique in its strategic view of uplift in cyber security and the Policy is a key element in achieving this. Agency uplift will be an ongoing journey that builds on learnings from all parties. A strong understanding of areas that require uplift help focus new iterations of the Policy and the engagement and assistance provided by Cyber Security NSW.

NSW Government is currently leading the nation by requiring its entities to assess and report on cyber maturity. To the best of our knowledge, no other State, Territory or Federal Government Department has the same strategic view of cyber security maturity which includes not only technical controls, but also people and process controls – or a detailed view of the status of whole-of-government cyber uplift.

The Department would like to highlight that this work is being supported through unprecedented levels of investment in cyber security. The NSW Government leads the nation with a $240m investment dedicated to uplifting cyber maturity, with all clusters having started this process. This investment is part of $1.6 billion over three years to ensure comprehensive digital transformation. This investment has been further supported by an additional $500m injection to the Digital Restart Fund, which includes $75m for cyber uplift in small agencies.

The NSW Government's dedication to the state's digital transformation journey, including in cyber security, has been reflected in recent benchmarks and indexing. This includes the NSW Government being ranked first (9.8/10) in the 2021 Intermedium Digital Government Readiness Indicator, and second (9.3/10) in the 2021 Intermedium Cyber Security Readiness Indicator. Whilst these indicators are a positive reflection of the existing journey, cyber security is not "set and forget". The Department and NSW Government will remain focused on building cyber resiliency and on continuous improvement.

The Department seeks to continually improve the Policy and other processes used to assist reporting entities, including through supporting documentation and guidance. The NSW Audit Office's reports this year continue to be a reminder that there is still much work to be done. With the assistance of agencies like the NSW Audit Office, the Department will continue to engage with reporting entities to assist in uplifting their cyber security culture.

Emma Hogan
Secretary

Date: 21/10/21

Response from the Department of Education

DGL21/282

Ms Margaret Crawford
Auditor-General for New South Wales
Audit Office NSW
PO Box 12
SYDNEY NSW 2001

mail@audit.nsw.gov.au

Dear Ms Crawford

Thank you for your letter of 17 June 2021, providing a copy of the *Special Audit – Compliance with the NSW Cyber Security Policy,* and requesting a response from the Department of Education.

The Department is dedicated to the safety, integrity, confidentiality, and availability of our data, and has prioritised the ongoing maturity of our Cyber Security capability with its progress regularly reported to the Executive. We welcome the feedback provided by the Audit Report and I am advised the issues identified are being addressed.

We are, however, concerned that publicly tabling the report would provide potential attackers with a roadmap of how and where to attack NSW Government departments and agencies, and in our case, increase the risk profile to students and staff, which is inconsistent with our strategy.

As you are aware, the Department is currently responding to a significant ongoing cyber incident. Whilst we support the report's findings in principle and are addressing the comments regarding the Department, we would strongly recommend that the full Audit Report not be publicly tabled. This would compromise our current recovery efforts and the inevitable risk of increasing cyber activity exceeds the benefit of placing this information on the public record.

Yours sincerely

Georgina Harrisson
SECRETARY
DEPARTMENT OF EDUCATION
15 July 2021

NSW Department of Education
105 Phillip Street Parramatta NSW 2150 GPO Box 33 Sydney NSW 2001 1300 679 332 education.nsw.gov.au

Response from the Department of Planning, Industry and Environment

Planning, Industry & Environment

Office of the Secretary

15 July 2021

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

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

Dear Ms Crawford,

Special Audit: Compliance with the NSW Cyber Security Policy

Thank you for the opportunity to provide a formal response for inclusion in the final report to be tabled in Parliament.

I acknowledge this audit incorporates findings related to nine agencies including the Department of Planning, Industry and Environment (DPIE) and their respective compliance with relevant requirements for the NSW Department of Customer Service Policy 'DCS-2020-02 NSW Cyber Security Policy'.

The Digital Information Office (DIO) of Corporate Services of DPIE has several comments in relation to the report that we request are considered prior to finalisation.

With respect to the reported levels of maturity for DPIE, these were determined through interviews and evidence collection by an independent external Auditor rather than through an internal self-assessment, which was not recognised in the audit report. Notwithstanding DIO acknowledges the identified discrepancies between the reported level of maturity and the level DIO was able to demonstrate with evidence sufficient for the Audit office team for two CSP mandatory controls. It is pertinent to note that these discrepancies were identified in only two out of twenty CSP mandatory controls while all ratings for the Essential 8 strategies were consistent.

DIO was directed by both the independent auditor and Audit office audit teams and supplied all evidence requested. The conclusions of both teams were reached based on this evidence. Although justification for the maturity rating established by the Audit Office for two CSP mandatory controls was provided, the criteria used to determine maturity levels was not shared with DIO. As such, DIO is not in a position to determine the basis on which of the two independently assessed maturity ratings more readily reflect current state. Nonetheless, DIO will adopt the more conservative rating provided by the Audit office for the FY19/20 reporting as final. DIO will continue engaging an external vendor to evaluate annual levels of maturity and will enhance

4 Parramatta Square, 12 Darcy Street, Parramatta NSW 2150 | Locked Bag 5022 Parramatta NSW 2124 | planning.nsw.gov.au

the compilation and retention of artefacts necessary to determine levels of CSP maturity utilising CSP guidance.

DIO opposes the potential publication of sensitive information about maturity levels including the Essential 8 strategies and requests that these remain confidential and not be publicly released by the NSW Audit Office on security grounds. Advice from the Australian Cyber Security Centre confirms that adversaries use publicly available information about cyber vulnerabilities to more effectively target their malicious activities. Publication of CSP and Essential 8 maturity levels and specific mitigations will unnecessarily expose DPIE and equip adversaries with the core information to compromise agency systems. If reporting is required to be published then we request this is done in an aggregated and deidentified manner to reduce, although not eliminate, potential security risks.

Furthermore, a mandatory minimum maturity level of '3' as outlined in the Audit Office report is not a requirement in the Circular, Policy or Guidance. The policy is consciously risk-based requiring agencies to develop practical and realistic security goals and spend their resources in the most effective way depending on key risk areas as opposed to having a minimum standard required to be met by all participants.

DIO management acknowledges that ongoing enhancement of the maturity of CSP controls is required, especially in relation to the ACSC Essential 8 strategies. Since the establishment of the DPIE cluster in July 2019, DIO has embarked on the simplification and modernisation of its ICT environment with security and privacy by default as its priorities. In addition to this, with the initial $5m DRF cyber security funding granted in March 2021, DIO has commenced a 12-month journey to further uplift DPIE's/DRNSW's cyber security maturity through the delivery of 20 initiatives. One of the initiatives is to develop a Treasury business case for the remaining funds, to cover Phase 2 of the Program, which would take potentially another 2-3 years. In this way, DPIE is prioritising improvements to its cyber security resilience as a matter of urgency.

I would like to acknowledge the important work undertaken by your team and the professionalism they demonstrated throughout this process.

Yours sincerely,

Jim Betts
Secretary

4 Parramatta Square, 12 Darcy Street, Parramatta NSW 2150 | Locked Bag 5022 Parramatta NSW 2124 | planning.nsw.gov.au

Response from the Department of Regional NSW

Regional NSW

Your Ref# D2111088

Ms Margaret Crawford
Auditor-General
Audit Office of NSW
GPO Box 12
SYDNEY NSW 2001

21 July 2021

Dear Ms Crawford

RE: Compliance with the NSW Cyber Security Policy

Thank you for your letter of 17 June 2021 and the opportunity to respond to your audit report *Compliance with the NSW Cyber Security Policy*. The audit provides valuable insight for the ongoing improvement of cyber security resilience across the Sector.

As you would be aware, Regional NSW was created on 2 April 2020 and while fully accepting its accountability and responsibility for managing cyber security relied (as it still does) on the Department of Planning, Industry and Environment for much of its IT infrastructure and security.

Having said that, Regional NSW has continued to address and strengthen its cyber security controls in line with the *NSW Cyber Security Policy* and believe the current level of maturity to be appropriately higher than at the time of the audit.

Regional NSW note and accept the two specific audit findings attributed to Regional NSW and have taken steps to address these issues as part of the overall maturity process.

Lastly, it is our strong preference for the findings of this report to not be available publicly. We are committed to increasing our cyber security maturity and believe that the findings of your report should be handled internally, so to not flag any potential weaknesses to adverse actors.

Yours sincerely,

Gary Barnes
Secretary

Response from the Ministry of Health

Ms Margaret Crawford
Auditor General of NSW
NSW Audit Office
GPO Box 12
SYDNEY NSW 2001

Your ref D2111091
Our ref H20/112992

Dear Ms Crawford

SPECIAL REPORT – COMPLIANCE WITH NSW CYBER SECURITY POLICY

I refer to your letter of 17 June 2021 seeking comment from NSW Health on the special audit report *Compliance with the NSW Cyber Security Policy*.

As you are aware the NSW Government's Cyber Security Policy and its application is evolving. NSW Health has worked diligently on the implementation of the requirements of the policy and will continue to work closely with Cyber Security NSW in its ongoing development.

I would like to highlight the leadership of eHealth NSW in the application of policy requirements and in the work undertaken to seek independent assurance on the integrity of NSW Health's cyber security frameworks. The information presented in your report will be considered as part of the ongoing efforts in this area.

I note that this report has been provided for review as a final version, which is a departure from the established process of distributing a draft report first and seeking agency feedback on any areas of disagreement. In context of this, I wish to highlight two key areas of concern.

First, I highlight the sensitivity of the report content and request your discretion in publishing detailed findings which may put the integrity of agency cyber security frameworks at risk. I am aware that this concern has been raised during the conduct of the audit by representatives of NSW Health and other participating agencies.

Second, I also wish to highlight NSW Health's position regarding its performance in the report. Based on the extensive evidence that was provided in the course of this audit, the discrepancies regarding the Audit Office's assessment of compliance with the Cyber Security Policy have not been sufficiently identified or explained. As such, it remains unclear as to what evidence was found to be insufficient and how the assessments made in the report were determined.

Despite this, NSW Health is committed to prioritising work to enhance our cyber security maturity and will continue to work closely with Cyber Security NSW and our colleagues in other NSW Government agencies to achieve this.

NSW Ministry of Health
ABN 92 697 899 630
1 Reserve Road, St Leonards NSW 2065
Locked Mail Bag 2030, St Leonards NSW 1590
Tel (02) 9391 9000 Fax (02) 9391 9101
Website: www.health.nsw.gov.au

Please find attached to this letter further comments in response to the audit recommendations.

Yours sincerely

Elizabeth Koff
Secretary, NSW Health

Encl. 20/7/21

No.	Recommendation	Response	Comment
Cyber Security NSW should:			
1.	Monitor and report compliance with the CSP by: • obtaining assurance over the accuracy of self-assessments • requiring agencies to resolve inaccurate or anomalous self-assessments where these are apparent.	-	Currently assurance is provided to Cyber Security NSW through the Attestation Statements which were strengthened by NSW Health during the reporting period to reflect the accuracy of the status on self-assessment. NSW Health will work closely with Cyber Security NSW in relation to any perceived deficiencies in complying with the Cyber Security Policy.
2.	Require agencies to report: • the level of maturity for each mandatory requirement they have determined appropriate for their agency • the agency head's acceptance of the residual risk where the target levels are low	-	NSW Health will address this issue in consultation with Cyber Security NSW.
3.	Identify and challenge discrepancies between agencies' target maturity levels and the risks of the information they hold and services they provide.	-	NSW Health has recognised the value in improving its maturity level consistent with the Cyber Security Policy and will work closely with Cyber Security NSW. NSW Health has prioritised activities aimed at increasing its maturity levels consistent with the Cyber Security Policy and has set appropriate targets for its Cyber Security Uplift Program, which will be progressed in collaboration with Cyber Security NSW.
Participating agencies should:			
4.	Resolve the discrepancies between their reported level of maturity and the level they are able to demonstrate with evidence: • compiling and retaining in accessible form the artefacts that demonstrate the basis of their self-assessments • referring to the CSP guidance when determining their current level of maturity.	Disagree	NSW Health has reported their level of maturity based on evidence held and has appropriately attested to this as required under the Cyber Security Policy. Based on the extensive evidence that was provided by NSW Health in the course of this audit, the discrepancies regarding the assessment of compliance with the policy have not been sufficiently addressed nor identified to come to this conclusion.

No.	Recommendation	Response	Comment
5.	Cyber Security NSW and NSW Government agencies need to prioritise improvements to their cyber security resilience as a matter of urgency	Agree	This will be addressed by activities being undertaken as part of the new Essential 8 uplift program.

Response from the Treasury

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

Dear Ms Crawford

Special Audit – Compliance with the NSW Cyber Security Policy

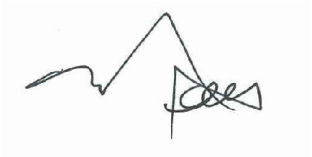
Thank you for the opportunity to provide a response to your Report, *Special Audit – Compliance with NSW Cyber Security Policy*.

I acknowledge your key findings and recommendations. NSW Treasury has addressed the agency specific issues identified in the Report and has an approved uplift plan in place to raise cyber security maturity.

I share the concerns raised by Cyber Security NSW and other NSW Government agencies regarding the external publication of your Report in its current form. I am advised that the detail it contains would provide an advantage to adversaries seeking to target the NSW Government and increase the risk of a successful cyber-attack.

I trust the Audit Office is exploring options with Cyber Security NSW to reduce this risk while enabling transparent and accountable reporting to Parliament, such as creating a public summary version of the Report and making the full version available to Members of Parliament on a confidential basis.

Yours sincerely



Michael Pratt AM
Secretary

14 July 2021

GPO Box 5469, Sydney NSW 2001 ■ Telephone: (02) 9228 4567 ■ www.treasury.nsw.gov.au

Response from Transport for NSW (TfNSW)

Your ref: D2110328
Our Ref: OTS20/07456

Ms Margaret Crawford
Auditor-General
Audit Office of NSW
GPO Box 12
SYDNEY NSW 2000

Response to Special Audit – Compliance with the NSW Cyber Security Policy – Final Report

Dear Ms Crawford

Thank you for the opportunity to respond to the Special Audit Report (the Report) on compliance with the NSW Cyber Security Policy (the Policy). Transport for NSW (TfNSW) welcomes the findings of the Report and the confirmation that the evidence we provided substantially supports our assessed cyber security maturity ratings.

Since the release of the Policy in February 2019, TfNSW has been working closely with Cyber Security NSW to implement the Policy and strengthen our cyber defence capabilities. We will continue to work with them in accordance with the Policy to further improve our organisational and operational cyber security maturity to protect our customers, our staff and our critical infrastructure.

In the current cyber security environment of forever changing threats and high-profile cyberattacks on all types of organisations in Australia and overseas, TfNSW recognises the need to continuously improve our cyber defence capabilities to protect our staff, the NSW Government, and the people of NSW.

While further uplift is still required, TfNSW's cyber security controls already effectively prevent a significant number of intrusion attempts and our teams constantly monitor our cyber security environment and respond rapidly to cyber security threats.

We are pleased to advise that we are aware of the shortcoming of the self-assessment and reporting processes under the Policy and have already made improvements. Evidence is now retained to support our self-assessed maturity ratings. Independent sample reviews of critical self-assessments are conducted to ensure maturity ratings are assessed in accordance with the Policy's guidance and are based on adequate evidence.

We have been, and will continue improving, our cyber security resilience. From July 2020 through to June 2023, Transport will have invested an additional $60 million to support the ongoing uplift of our Cyber Defence Portfolio. In addition, $20 million will be allocated to the Cyber Defence Program from the Digital Restart Fund to further uplift Cyber security.

Transport for NSW
231 Elizabeth Street, Sydney NSW 2000 | PO Box K659, Haymarket NSW 1240
T 02 8202 2200 | **F** 02 8202 2209 | **W** transport.nsw.gov.au | ABN 18 804 239 602

Cyber security training is mandated for all staff. In addition to formal training, we frequently communicate with staff across the Transport cluster about cyber security risks. Furthermore, we have also improved our threat intelligence and response capabilities to proactively detect and prevent potential threats. We are also instigating further uplift in our organisational structure to embed cyber security culture across our organisation by having divisional IT security teams working closely with our business to improve their cyber security maturity.

This journey of continuous improvement and maturity uplift across one of Australia's largest and most complex government entities demonstrates our focus and commitment to cyber security resilience. Our current and future investments will continuously reduce our cyber security risks.

If you have any further questions, Fiona Trussell, Deputy Secretary Corporate Services, would be pleased to take your call. I hope this response has been of assistance.

Yours sincerely,

Rob Sharp
Secretary
10 July 2021

Appendix two – The maturity model for the mandatory requirements

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
1	**Planning and governance**					
1.1	Allocate roles and responsibilities as detailed in this policy.	The Agency Head, CIO, CISO and Audit and Risk are not aware of their cyber security responsibilities as outlined in the policy or are not performing these responsibilities.	The Agency Head, CIO, CISO and Audit and Risk are aware of their cyber security responsibilities as outlined in this policy but are not yet performing all of them.	The CISO or equivalent is appointed responsibilities in this policy and these are assigned and undertaken. The CISO is supported by internal audit, risk and compliance teams. The Agency Head, CIO and CISO (or equivalent) are aware of their responsibilities as outlined in the policy and are performing them. The CISO (or equivalent executive) is a member or advisor of the agency's risk committee.	Maturity level 3 requirements, and in addition: • The CIO (or equivalent) is aware of who is responsible for cyber security for all information and systems including building management systems, IoT and IACS. • The agency's internal audit, risk and compliance teams are actively involved in addressing cyber risks.	Maturity level 4 requirements, and in addition: • The role of the CISO is highly visible and central to delivering on strategic business priorities and objectives. • The CISO is empowered to make security decisions for the agency/cluster.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
1.2	Ensure there is a governance committee at the executive level (dedicated or shared) to be accountable for cyber security including risks, plans and meeting the requirements of this policy. Agencies need to consider governance of ICT systems and OT (Operational Technology) to ensure no gaps in cyber security related to items such as video surveillance, alarms, life safety and building management systems that use automated or remotely controlled or monitored assets including industrial Internet of Things (IoT) devices.	There is no governance committee with a charter to cover cyber security risks, plans and policy requirements.	A governance committee is being established at the executive level but does not meet regularly, or a governance committee exists but with no executive representation or a governance committee exists but does not cover IACS/OT and IoT (if applicable).	There is a governance committee with executive level representation and agreed terms of reference that covers cyber security risks, plans, initiatives and policy requirements. The committee has governance over (or has delegated to another committee) information security as well as cyber security of OT. The governance committee meets at least quarterly to discuss cyber security.	Maturity level 3 requirements, and in addition: • Cyber security is a regular item on the agenda at the agency or cluster Risk and Audit Committees.	Maturity level 4 requirements, and in addition: • Cyber security is fully integrated into entity operations, actively managed, monitored and drives improvements. • The Agency Head understands cyber security risks to their agency.
1.3	Have an approved cyber security plan to manage the agency's cyber security risks, integrated with business continuity arrangements. This must include consideration of threats, risks and vulnerabilities that impact the protection of the agency's information and ICT assets and services.	There is no approved cyber security plan in place for the agency/cluster.	The security plan has been developed and is partially implemented but may not be current or comprehensive. The cyber security plan has been approved by the Agency Head.	A security plan is endorsed by the appropriate governance committee, captures key threats, risks, vulnerabilities and actions/initiatives to make improvements and address any gaps. The plan is linked to the agency's risk management framework and cyber security is considered in business continuity arrangements.	Maturity level 3 requirements, and in addition: • The progress of initiatives and new requirements are reviewed at least quarterly.	Maturity level 4 requirements, and in addition: • The security plan is reviewed by the governance committee at least quarterly and kept current.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
1.4	Consider cyber security threats when performing risk assessments and include high and critical risks in the agency's overall risk management framework.	Risk assessments do not consider cyber security risks.	Cyber security risk assessments are conducted on an ad-hoc basis and risks identified and managed across the IT department but are not identified across the agency.	Cyber security is included in the agency's risk management framework and cyber security risk is considered in all areas across the agency/cluster, including cyber security risks to OT. Actions are identified to mitigate cyber security risks.	Maturity level 3 requirements, and in addition: • Unmitigated cyber risks are escalated from across the agency and are visible to the Risk Committee through the agency's enterprise risk register.	Maturity level 4 requirements, and in addition: • Security risk management is a significant priority for the agency and is identified and aligned to business objectives. • Formal risk management processes to connect security risk management and operations are in place.
1.5	Be accountable for the cyber risks of their ICT service providers and ensure the providers comply with the applicable parts of this policy and any other relevant agency security policies. This must include providers notifying the agency quickly of any suspected or actual security incidents and following reasonable direction from the agency arising from incident investigations.	No consideration for cyber security in procurement processes and contracted arrangements in the agency.	Consideration for cyber security is given in all new contractual arrangements. The agency partially monitors service provider's adherence to contract provisions.	All new third party technology contracts clearly define the cyber security requirements and the responsibilities of the provider. The agency monitors compliance to security requirements in technology contracts with a security provider. There is a process for service providers to notify the agency of suspected or actual security incidents.	Maturity level 3 requirements, and in addition: • All current third party technology contracts define the cyber security requirements and responsibilities of the provider. • Service provider service delivery agreements are periodically reviewed and updated at allowable contract review/ extension periods to ensure they address any changes in business or security requirements. Standard templates for service provider agreements in contracts include clauses dealing with cyber	Maturity level 4 requirements, and in addition: • The agency actively monitors and audits technology service provider capability to fully comply with contractual arrangements.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
					security requirements.	
2	**Cyber security culture**					
2.1	Implement regular cyber security education for all employees, contractors and outsourced ICT service providers.	Cyber security education is not available to employees, contractors and outsourced ICT service providers.	Cyber security education is available for all employees but not for contractors and/or outsourced ICT service providers.	Cyber security education is available for employees, contractors and ICT service providers and completion is encouraged in all areas of the agency.	Maturity level 3 requirements, and in addition: • Cyber security education is available for employees, contractors and ICT service providers and completion is mandatory but not enforced. • Induction programs include ensuring that employees are aware of and acknowledge their security responsibilities and the agency's cyber security policies or guidelines.	Maturity level 4 requirements, and in addition: • Cyber security education is available for employees, contractors and ICT service providers and completion is mandatory and is enforced. • Completion rates are monitored to ensure they are above a defined threshold (minimum 90 per cent).
2.2	Increase awareness of cyber security risk across all staff including the need to report security risks.	Only staff within the cyber security-related teams have awareness of cyber security issues in the workplace. Responsibilities regarding cyber security are not being communicated to all staff.	All staff have been provided information regarding their responsibilities in ensuring the confidentiality, integrity and availability of data e.g. a link to the agencies Information Security Policy prior to logging in or a copy of the policy as part of onboarding. Regular communications relating to cyber security have not been sent to all staff.	Regular cyber security communications are sent to all staff including covering awareness items such as how to identify and report phishing attacks or malicious links. Phishing simulation exercises and incident response exercises (functional or discussion) have been run during the reporting period.	Maturity level 3 requirements, and in addition: • Staff in high risk roles have been identified and are appropriately trained in cyber security.	Maturity level 4 requirements, and in addition: • All staff have been made aware of cyber security threats and what they can do to detect them. • There is evidence that reports of potential malicious emails are increasing and/or improvements in results of simulations.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
2.3	Foster a culture where cyber security risk management is an important and valued aspect of decision-making and where security risk management processes are understood and applied.	Only the IT department play an active role in managing cyber security risks.	Non-IT department employees have been made aware of cyber security. Cyber security risk management is still seen as the responsibility of the IT department.	The importance of cyber security and developing a strong cyber security culture is recognised by agency executives. Cyber security risk management processes are documented, understood and followed by the relevant people across the agency.	Cyber security risk management processes are actively applied and followed by the relevant people across the agency. Leadership is aware of good cyber security practices and factor these into relevant decision-making. Residual cyber security risks are periodically reviewed and reassessed.	Maturity level 4 requirements, and in addition: • Cyber security is integral to the agency's business and clearly informs decision-making. • Secretary is briefed on cyber security risk management as part of cluster risk management reporting.
2.4	Ensure that people who have access to sensitive or classified information or systems and those with privileged system access have appropriate security screening, and that access is removed when they no longer need to have access, or their employment is terminated.	The agency has not classified their information or systems to enable suitable personnel to access the information.	Access controls are in place but removal and auditing of privileges does not occur or takes place on an ad hoc basis.	The agency has classified information or systems and has access controls and security procedures in place to enable sharing with relevant stakeholders who have a need-to-know and are appropriately security cleared. Access controls are implemented and documented to prevent unauthorised access. Access is removed within a defined period of an employee's termination or the employee no longer needing access to the information or system.	Maturity level 3 requirements, and in addition: • Routine auditing takes place to ensure that access is being removed for staff on employment termination / staff that have moved roles have not retained higher privileges (privilege creep). • A documented process is in place to ensure efficient and consistent implementation of access controls in managing all user access, which includes: – Clear identification of privileged users, which means users with access to sensitive or classified information	Maturity level 4 requirements, and in addition: • The agency has automated processes to remove access on role changes and termination of employment.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
					and users with privileged system access. – Clear identification of steps to be taken when 'Privileged Users' leave employment. In some cases, some system password needs to be reset as on any shared accounts.	
2.5	Share information and intelligence on security threats and vulnerabilities with Cyber Security NSW, as well as cooperate across NSW Government to enable management of government-wide cyber risk.	Agency does not provide any information or intelligence on security threats or vulnerabilities outside the Agency.	Agency shares information and intelligence on security threats and vulnerabilities on an ad hoc basis or only shares within its own cluster.	Agency routinely works with Cyber Security NSW to receive and/or provide information and intelligence on security threats and vulnerabilities across NSW Government. In the agency's incident management procedures, there is a defined workflow that indicates when and where information and intelligence should be shared. There is a process for receiving and acting on information and intelligence received from Cyber Security NSW.	Maturity level 3 requirements and in addition: • Agency routinely receives and/or provides information and intelligence on security threats and vulnerabilities across their cluster and with other agencies/ clusters.	Maturity level 4 requirements and in addition: • Agency receives a feed of verified Indicators of Compromise (IoCs) that can be ingested by a Security Information and Event Management (SIEM) system and actions against these IoCs are automated.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
3	**Safeguarding information and systems**					
3.1	Implement an Information Security Management System (ISMS) or Cyber Security Framework (CSF), with scope at least covering systems identified as an agency's 'crown jewels'. The ISMS or CSF should be compliant with, or modelled on, one or more recognised ICT/OT standard (see guideline for more information).	An ISMS or CSF is not in place or scope does not cover all 'crown jewels' as a minimum.	An ISMS or CSF is in place with scope covering only the 'crown jewels'. Controls are implemented to address some agency requirements.	Maturity level 3 requirements, and in addition: • The scope of the ISMS or CSF covers more than just the 'crown jewels'. • Controls are implemented based on agency requirements and current risk appetite. Control effectiveness is assessed and documented.	Maturity level 3 requirements, and in addition: • Agency risk appetite is well defined, gaps have been documented and controls have been implemented. All outstanding risks are within the current risk appetite and reviewed at least every six months. • Control effectiveness is reviewed at least every six months.	Maturity level 4 requirements, and in addition: • An ISMS or CSF is in place and scope covers all ICT and/or OT systems. • Agency executives and finance personnel are engaged by complementing cyber security risk assessment with Factor analysis of information risk (FAIR) or Value at risk (VaR) calculations.
3.2	Implement the ACSC Essential 8.	Implementation of the Essential 8 has not commenced for all mitigation strategies or implementation of the Essential 8 has not been approved by the CIO.	Implementation of the Essential 8 has not commenced for all mitigation strategies but there is a plan to begin implementation with CIO approval.	Implementation of the Essential 8 has commenced for all mitigation strategies and maturity is projected to improve year-on-year.	Priority has been given to Essential 8 implementation and uplift and the CIO is actively engaged in directing other areas of IT to prioritise this work. No mitigation strategies have a maturity level below level 1 as of August 31.	The agencies target level has been achieved and there is continuous monitoring of alignment to this maturity level.
3.3	Classify information and systems according to their importance (i.e. the impact of loss of confidentiality, integrity or availability), adhere to the requirements of the NSW Government Information Classification Labelling and	Information and systems are not classified according to the agency classification guidelines. No asset register exists for identifying agency's 'crown jewels'.	Information and systems are documented and dedicated owners with responsibilities are assigned to them. No asset register exists for identifying agency's 'crown jewels'.	Information and systems are documented and dedicated owners with responsibilities are assigned to them. 'Crown jewels' have been identified.	Information and systems are classified according to agency classification guidelines and systems are assigned business and/or IT owners. Agency has identified their 'crown jewels' and they have been approved by the	Information and systems are classified according to agency classification guidelines and systems are assigned business and/or IT owners. Appropriate controls are in place for the

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
	Handling Guidelines and: • assign ownership • implement controls according to their classification and relevant laws and regulation • identify the agency's 'crown jewels' and report them to Cyber Security NSW as per mandatory requirement 5.4.				Governance Committee.	information and systems. Agency has identified their 'crown jewels' and they have been approved by the Governance Committee.
3.4	Ensure cyber security requirements are built into procurements and early stages of projects and the system development life cycle (SDLC), including agile projects.	There are no cyber security requirements built into the agency SDLC or project assurance.	There are cyber security checks performed before a new system is implemented but not in the early stages of development. Agile projects do not have a method for verifying that cyber security requirements are being designed and built into new systems.	Security requirements are addressed in the requirements and pre-implementation procedures or checks of new projects including agile projects. The agency includes cyber security requirements in the procedures and assurance checks of the purchase/ development of new systems.	Maturity level 3 requirements, and in addition: • System acceptance includes confirmation that appropriate security controls have been applied to the system. • Internet facing applications are penetration tested before implementation. • Functional regression testing includes regression testing of security functions.	Maturity level 4 requirements, and in addition: • Access restrictions and segregation/ isolation of systems have been implemented into all infrastructure, business and user developed applications. Role based controls are implemented to ensure segregation of duties and user access privileges are revalidated at least quarterly. • Vulnerability Assessments occur on a routine basis.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
3.5	Ensure that new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data including internal fraud detection.	No process exists to ensure new system or enhancements have acceptable audit and activity logging in place before implementation.	There are policies in place around auditing and logging covering log retention and alerting. Logging is enhanced for security devices such as firewalls and Intrusion Detection System (IDS) devices.	Processes (including data validity checks, audit trails and activity logging) have been established in 'crown jewels' systems to ensure development and support processes do not compromise the security of applications, systems or infrastructure. New 'crown jewel' systems or major enhancements to them have appropriate audit trails and audit logging to assess the accuracy and integrity of data. The agency has processes to confirm that these are implemented before a new system or major enhancement is implemented into production. Audit and activity logs are regularly reviewed to ensure that there are no anomalies.	Maturity level 3 requirements, and in addition: • System owners follow a process for checking logs at defined intervals to identify irregularities. A procedure is in place to act on identified anomalies. • System health checks are performed frequently to ensure that audit logs are being successfully collected as per design.	Maturity level 4 requirements, and in addition: • Logging is incorporated into a tool/system to generate automatic alerts.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
4	**Cyber incident management**					
4.1	Have a current cyber incident response plan that integrates with the agency incident management process and the NSW Cyber Incident Response Plan.	Cyber security incident management is largely manual and ad-hoc. No analysis of cyber security events or incidents.	Cyber security incident response is integrated with the agency's incident management processes but cyber security incidents cannot easily be extracted and reported.	Cyber security incident management is integrated with the agency incident management process. The agency's incident management process references the NSW Cyber Incident Response Plan. The agency's disaster recovery plan caters for cyber security incidents.	Maturity level 3 requirements, and in addition: • Analysis of cyber security events and incidents take place e.g. post incident root cause analysis, post incident review actions.	Maturity level 4 requirements, and in addition: • Cyber security incidents are reported regularly to a governance committee and are used to identify new initiatives for the agency Cyber Security Plan.
4.2	Test their cyber incident response plan at least every year, and involve their senior business and IT executives, functional area coordinators (if applicable), as well as media and communication teams.	No test of the incident response plan has ever been conducted.	No test of the incident response plan was conducted in the last reporting period, or a test was conducted involving IT only.	The agency has performed a desktop exercise in the reporting period involving the agency's senior executives and media and communications teams.	In the last reporting period, the agency tested the cyber incident response plan via a business continuity exercise (simulation) involving the senior executives, media and communications teams and any other personnel who have a role in the Business Continuity Plan (BCP). Results of the business continuity exercise have been used to update existing processes and templates including those of the media and communications teams.	Maturity level 4 requirements and in addition: • A red team assessment was held during the reporting period, covering at least the agency's 'crown jewels' and improvements have been identified from the results.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
4.3	Deploy monitoring processes and tools to allow for adequate incident identification and response.	The agency does not monitor for threats.	Manual or ad hoc monitoring occurs.	Automated monitoring and alerting is in place e.g. Endpoint protection and Host or Network based Intrusion Detection Systems / Intrusion Prevention Systems (IDS/IPS). IT staff receive automated alerts from monitoring solutions. Ad hoc searching in the public domain is occurring to detect data being dumped, traded or sold.	Maturity level 3 requirements and in addition: • Events are consolidated from various sensors and correlated to actions via a SIEM. • Tools and processes exist for ongoing detection and alerting of data being dumped, traded or sold in the public domain.	Maturity level 4 requirements and in addition: • SIEM correlation events are reviewed / tuned on a regular basis to minimise false positives. • Escalation of high priority incidents is automated.
4.4	Report cyber security incidents to Cyber Security NSW according to the NSW Cyber Incident Response Plan.	The agency did not report cyber security incidents to Cyber Security NSW during the reporting period.	A percentage of cyber security incidents were reported to Cyber Security NSW during the reporting period.	All cyber security incidents and crises have been reported to Cyber Security NSW in line with the NSW Cyber Incident Response Plan during the reporting period.	Maturity level 3 requirements, and in addition: • Continual updates are provided to Cyber Security NSW on what remediation is taking place.	Automated reporting of incidents to Cyber Security NSW is in place, which includes known indicators of attack (IOAs) and/or indicators of compromise (IOCs).
4.5	Participate in whole-of-government cyber security exercises as required.	Did not send a representative to exercises held during the reporting period, or no whole-of-government cyber security exercises were held.	Representatives attended exercises but were are not part of an appropriate team.	Appropriate representatives were sent to whole-of-government cyber security exercises during the reporting period.	CIO and CISO or equivalent attended the exercises.	Maturity level 4 requirements, and in addition: • The cluster's Minister(s) and Secretary attended the exercises.

Source: Cyber Security Policy – Maturity Model Guidance (April 2020).

Appendix three – Essential 8 maturity model

Maturity level zero	Maturity level one	Maturity level two	Maturity level three
Application control (whitelisting)			
Application control is not fully implemented on workstations, or running in audit mode. Application control is not occurring on servers.	Application control is implemented on all workstations to restrict the execution of executables to an approved set. Application control is implemented on all servers to restrict the execution of executables to an approved set.	Application control is implemented on all workstations to restrict the execution of executables and software libraries scripts and installers to an approved set. Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.	Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set. Microsoft's latest recommended block rules are implemented to prevent application control bypasses.
Patch applications			
Patches to security vulnerabilities in applications and drivers assessed as extreme risk are not applied consistently or applied on a greater than monthly basis. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are still being used.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

Maturity level zero	Maturity level one	Maturity level two	Maturity level three
Configure Microsoft Office macro settings			
Microsoft Office macros can execute without prompting users for approval. Microsoft Office macro settings can be configured by users.	Microsoft Office macros are allowed to execute, but only after prompting users for approval. Microsoft Office macro security settings cannot be changed by users.	Only signed Microsoft Office macros are allowed to execute. Microsoft Office macros in documents originating from the internet are blocked. Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros. Microsoft Office macros in documents originating from the internet are blocked. Microsoft Office macro security settings cannot be changed by users.
User application hardening			
Web browsers allow Adobe Flash, web advertisements and Java from the Internet. Unneeded features in Microsoft Office, web browsers and PDF viewers aren't disabled.	Web browsers are configured to block or disable support for Flash content.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements. Web browsers are configured to block Java from the internet.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements. Web browsers are configured to block Java from the internet. Microsoft Office is configured to disable support for Flash content. Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.
Restricting administrative privileges			
Requirements for privileged accounts are not consistently validated. No duties-based restrictions on privileged accounts are applied. Privileged accounts are capable of reading emails and web browsing.	Privileged access to systems, applications and information is validated when first requested. Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.	Privileged access to systems, applications and information is validated when first requested and revalidated on an annual or more frequent basis. Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.	Privileged access to systems, applications and information is validated when first requested and revalidated on an annual or more frequent basis. Privileged access to systems, applications and information is limited to that required for personnel to undertake their duties. Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.

Maturity level zero	Maturity level one	Maturity level two	Maturity level three
Patching operating systems			
Patching for extreme risk security vulnerabilities in operating systems are not consistently applied or applied on a greater than monthly basis. A non-vendor supported operating system is used.	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor supported versions.
Multi-factor authentication			
Multi-factor authentication is not implemented for remote access or when accessing sensitive data repositories or when performing privileged actions.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication uses at least two of the following authentication factors: passwords with six or more characters, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards, mobile app one-time password tokens, SMS messages, emails, voice calls or software certificates.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication uses at least two of the following authentication factors: passwords with six or more characters, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards or mobile app one-time password tokens.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication is used to authenticate all users when accessing important data repositories. Multi-factor authentication uses at least two of the following authentication factors: passwords with six or more characters, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smartcards.

Maturity level zero	Maturity level one	Maturity level two	Maturity level three
Daily backups			
Backups of important new/changed data, software and configuration settings are not performed consistently or are performed less often than monthly, or Full recovery has not been tested for backups of important information, software and configuration settings.	Backups of important information, software and configuration settings are performed monthly. Backups are stored for between one to three months. Partial restoration of backups is tested on an annual or more frequent basis.	Backups of important information, software and configuration settings are performed weekly. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for between one to three months. Full restoration of backups is tested at least once. Partial restoration of backups is tested on a bi-annual or more frequent basis.	Backups of important information, software and configuration settings are performed at least daily. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for three months or greater. Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur. Partial restoration of backups is tested on a quarterly or more frequent basis.

Source: CSP Reporting Template (May 2020).

Appendix four – About the audit

Audit objective

This audit assessed agencies' compliance with the NSW Department of Customer Service's Policy 'DCS-2020-02 NSW Cyber Security Policy'.

Audit criteria

We addressed the audit objective by:

1. verifying that the CSP's mandatory requirements for reporting and attestation have been performed
2. verifying the accuracy of agency self-assessments against the CSP's mandatory requirements, including their implementation of the Australian Cyber Security Centre's (ACSC) Essential 8
3. assessing the extent to which maturity levels meet or exceed the 'level three - Defined' threshold (i.e. are documented and practiced on a regular and consistent basis)
4. assessing progress towards target maturity levels across government since the CSP was introduced.

Audit procedures

Our audit procedures included:

1. interviewing:
    a) information security and risk management staff at each case study agency
    b) cluster Information Security staff where they are involved in self-assessments for the case study agencies
    c) agency staff responsible for managing IT Service Providers
    d) agency staff responsible for management of cyber security training to staff
    e) agency staff responsible for security screening of people who have access to sensitive or classified information or systems and those with privileged system access
    f) agency staff responsible for the operation of ACSC Essential 8 controls (patching, whitelisting, hardening, backups, Multifactor authentication, etc.)
    g) Cyber Security NSW staff.

3. examining:
    a) self-assessments and attestations produced by agencies
    b) materials produced by agencies to complete and support their self-assessments
    c) policies and procedures addressing the mandatory requirements of the CSP
    d) technical configurations and settings relevant to the CSP's requirements or the ACSC Essential 8
    e) agency risk registers, risk assessments, risk tolerance or appetite statements, and supporting documents
    f) agency information and asset registers relevant to classification of information and systems
    g) agency uplift plans and proposals for measures to increase cyber security
    h) budgets and expenditure details for such measures or projects.
4. analysing data:
    a) data collected by Cyber Security NSW on agency self-assessments since the launch of the CSP.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Audit Standard ASAE 3100 Compliance Engagements and 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 *Public Finance and Audit Act 1983*.

Acknowledgements

We gratefully acknowledge the co-operation and assistance provided by the participating agencies and by Cyber Security NSW, as well as those stakeholders who participated in the discussions held during the audit.

Audit cost

Including staff costs and overheads, the estimated cost of the audit is $237,000.

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.

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au