Cyber security insights 2025

SPECIAL REPORT | 27 JUNE 2025

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 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 give reasonable assurance that financial statements are true and fair, 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 assess whether the activities of government entities are being carried out effectively, economically, 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. Our performance audits may also extend to activities of non-government entities that receive money or resources, whether directly or indirectly, from or on behalf of government entities for a particular purpose.

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
ORTA RECENS QUAM PURA NITES
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 52B of the *Government Sector Audit Act 1983*, I present a report titled **'Cyber security insights 2025'.**

Bola Oyetunji
Auditor-General for New South Wales
27 June 2025

RECONCILIATION STATEMENT

We pay our respect and recognise Aboriginal peoples as the traditional custodians of the land in NSW who have cared for and protected the environment, waterways, and sacred sites over many millennia. We honour and thank the traditional custodians of the land on which our office is located, the Gadigal people of the Eora Nation, and the traditional custodians of all the lands on which our employees live and work. We pay our respects to their Elders past and present, and to the next generation of leaders.

As we mark our 200th anniversary, and our contribution to fostering accountability and transparency in the government and Parliament, we also acknowledge that our long history is shared with the histories of colonisation in New South Wales. We acknowledge the impacts of colonisation, and the resulting marginalisation and disadvantage of Aboriginal and Torres Strait Islander peoples in this state.

We embrace our role in holding government agencies to account for the delivery of effective services for Aboriginal and Torres Strait Islander peoples. We are committed to ensuring that our audits are culturally responsive, respectful and inclusive, and that we engage with Aboriginal and Torres Strait Islander peoples and communities in a meaningful and collaborative way.

We recognise the ancestral tie of Aboriginal and Torres Strait Islander peoples to this land, and we acknowledge that we have much to learn from their wisdom, rich and diverse culture, languages, knowledge and practices.

Image: 'Yarning Circle' by Caitlin Liddle, Audit Office Indigenous Internship Program participant. Used with permission.

contents

Cyber security insights 2025

Section 1 – Cyber security insights 2025

Section 2 – Appendices

Section 1 –

Cyber security insights 2025

1. Executive Summary

Context

Our focus on cyber security, as outlined in our Annual Work Program 2024–27, aims to provide insights into the NSW Government's handling of cyber security risks and its compliance with relevant cyber security frameworks.

This report presents key insights from the following two sources:

1. analysis of 2024 state agency data returns to Cyber Security NSW to establish the status of their compliance with the NSW Cyber Security Policy (CSP)
2. cyber security findings from relevant reports published by the Audit Office of New South Wales between March 2018 and June 2025.

The reality of cyber threats is evident from monitoring and reporting by the Australian Signals Directorate (ASD) and Cyber Security NSW, and from the case studies included in this report. The ASD highlights in its Annual Threat Report 2023–24 that the top three incident types reported by government entities are:

- compromised user accounts or credentials
- malware infections
- compromised assets, networks or infrastructure.

Agencies should remain vigilant as the ASD and Cyber Security NSW report that the tactics of cyber actors are evolving, with the use of more advanced hacking tools, such as artificial intelligence. Cyber Security NSW also emphasises that the risks associated with third–party systems have significantly increased in the NSW Government. The number of reported incidents involving third-party owned or managed systems has tripled in the last reporting year.

Cyber Security NSW continues to create and implement strategies to strengthen cyber resilience across all entities, enabling a cyber-secure NSW Government. NSW Government entities have responded to these strategies, but more work is needed to achieve the minimum requirements set by Cyber Security NSW and to manage the cyber risks faced by individual agencies. The continued focus by Audit and Risk Committees and the Public Accounts Committee on cyber security risk management is also essential to support the achievement of a cyber-secure NSW Government.

Are NSW agencies equipped to deal with cyber threats?

Cyber Security NSW develops strategies to enhance cyber resilience in the NSW Government. Cyber Security NSW's NSW Cyber Security Policy (CSP), updated in February 2024, sets out Mandatory Requirements across three domains: 'Govern and Identify'; 'Detect, Respond and Recover'; and 'Protect'. These include 31 Mandatory Requirements and 114 Detailed Requirements.

The CSP is mandated for NSW Government departments and public sector agencies. It is not mandatory but recommended for adoption for state-owned corporations, local governments and universities.

By 31 October each year, agencies are required to report their CSP compliance status (as either [non-compliant], [partial compliant], or [compliant]) and high or extreme residual risks. They must also provide a cyber security attestation to Cyber Security NSW.

Our analysis of the 2024 data reported to Cyber Security NSW shows that agencies need to improve further to achieve a cyber-secure NSW government. It also highlighted that aggregated reporting and limited independent assurance processes means there is limited visibility of cyber security and a potential risk in reporting accuracy. These insights may assist Cyber Security NSW in improving the overall cyber security attestation process, ensuring more complete and accurate information is provided that enables Cyber Security NSW to focus its activities where needed.

Key insights

- Across NSW agencies, the biggest gaps in cyber resilience are in the implementation of the minimum 'protect' domain controls. The absence of 'protect' domain controls increases the likelihood of a successful cyber attack.
- Agencies' control compliance is not reported when performed by third parties. Agencies and Cyber Security NSW may not be aware of any non-compliance against the CSP where the cyber security control practice is provided by third parties.
- Planned or ongoing cyber security uplift programs and budget constraints were the most common reasons agencies provided for not meeting the minimum cyber security requirements.
- Aggregated reporting to Cyber Security NSW reduces transparency of issues at individual agencies. This is especially relevant when there are portfolios of agencies with mixed or unclear cyber security responsibilities. Due to aggregated reporting, 66 reports were provided to Cyber Security NSW in 2024 representing 177 state agencies, whereas 110 reports were provided in 2023.
- A total of 152 significant, high and extreme residual cyber security risks were reported by 27 agencies. Of the 152 risks reported, 28 had treatment controls that were either largely or completely ineffective. In addition, 60 risks lacked specified timelines to reduce them to an acceptable level.
- There is a lack of independent assurance over agencies' reported compliance against the CSP. Specifically, 59% of reporting agencies advised they did not have independent assurance. The absence of independent assurance increases the risk of inaccurate data being reported to Cyber Security NSW.

Key cyber security insights from seven years of reports

Key insights in this report are derived from our audits of cyber security management within NSW state agencies, universities and the local government sectors between 2018 and 2025. Key themes were identified and structured according to the Mandatory Requirements categories of 'Govern and Identify', 'Detect, Respond and Recover', and 'Protect', which are commonly used in the cyber security frameworks adopted across NSW Government entities. This chapter includes case studies of cyber security incidents from past published reports.

Key insights

- The adoption and use of cyber security policies and frameworks has improved. Implementing a cyber security policy and framework is a critical foundational step that defines organisation-wide expectations, objectives and accountabilities.
- Many entities reported cyber security risks exceeding their risk appetite, but not all have a formal uplift program. A current cyber security uplift program is vital for managing residual risks. Budget constraints and other challenges reported by NSW agencies may also apply to universities and local government sectors.
- While cyber security roles and responsibilities are established, they may not always be clearly defined and effectively communicated. Incident responses are likely to be less effective where role requirements and responsibilities are unclear.
- Inadequate asset identification and cyber security detection capability can hinder protection prioritisation and incident response. Unidentified and unassessed information assets increase the exposure to cyber attacks.
- Third-party cyber risk management is a significant challenge. When outsourcing, entities retain accountability for managing associated risks. Cyber Security NSW reported that the number of incidents involving systems owned or managed by third parties nearly tripled in 2024, including a rise in data breach occurrences.
- Testing of cyber incident response plans could improve along with the development of more comprehensive playbooks. Playbooks provide step-by-step guidance and are key to effective cyber incident response.
- Many agencies have not met level one Essential Eight cyber protection measures despite this approach being a focus for many years. Some agencies reported zero maturity for critical controls such as application control, patching and administrative privilege restrictions.
- Cyber security awareness training has improved but phishing simulations should be used more. Human error frequently contributes to successful cyber attacks, with email phishing being a method commonly used to exploit individuals.
- Culture and accepted practice can drive non-compliance with protection controls. Situations can arise where there is a conflict between achieving business objectives and adhering to cyber security controls. In practice, operational goals are often prioritised over cyber security. Agencies must align culture with their cyber security environment to ensure controls are fit for purpose and protecting community interests.

Appendix 1 lists the audit reports used to derive the key insights while Appendix 2 presents a table summarising the statistics referenced in the key insights. Appendix 2 displays a progressive timeline of how cyber security controls have been implemented in NSW state agencies, universities and the local government sectors from 2018 to the present.

2. Introduction

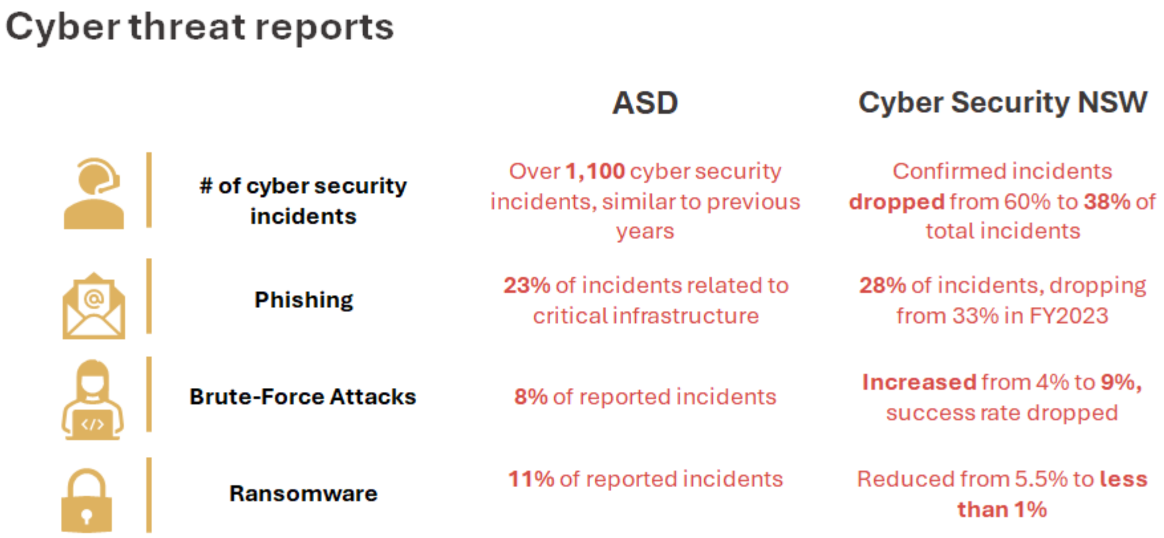
The reliance on information technology in modern government, in addition to the global interconnectivity between computer networks, has dramatically increased the risk of cyber security incidents. Such incidents can harm government service delivery and may include the theft of information, breaches of private information, denial of access to critical technology, or even the hijacking of systems for profit or malicious intent. These outcomes can have adverse impacts on the community and harm trust in government.

2.1. The evolving cyber threat landscape

The Australian Signals Directorate (ASD) noted in its ASD Cyber Threat Report 2023–24 that over 36,700 calls were made to its Australian Cyber Security Hotline – a 12% increase from the previous year. ASD also handled over 1,100 cyber security incidents in 2024. The ASD highlights the top three incident types reported by government entities are:

- compromised user accounts or credentials
- malware infections
- compromised assets, networks or infrastructure.

Ongoing cyber threats are also being reported by Cyber Security NSW. Its reporting highlights that phishing remains one of the most prevalent and effective methods of cyber intrusion.



Cyber threat reports

	ASD	Cyber Security NSW
# of cyber security incidents	Over **1,100** cyber security incidents, similar to previous years	Confirmed incidents **dropped** from 60% to **38%** of total incidents
Phishing	**23%** of incidents related to critical infrastructure	**28%** of incidents, dropping from 33% in FY2023
Brute-Force Attacks	**8%** of reported incidents	**Increased** from 4% to **9%,** success rate dropped
Ransomware	**11%** of reported incidents	Reduced from 5.5% to **less than 1%**

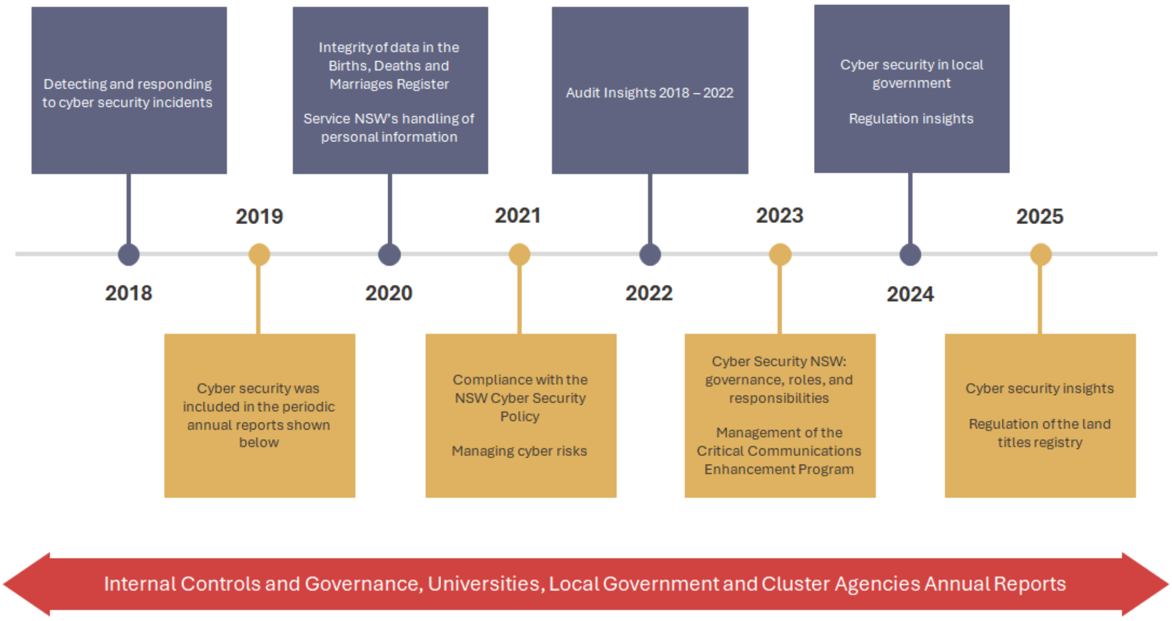
Source: Collated information from the Australian Signals Directorate and Cyber Security NSW.

ASD and Cyber Security NSW both emphasise that cyber actor tactics are evolving, with the use of more advanced hacking tools, including artificial intelligence. Cyber Security NSW informed that the number of incidents related to systems owned or managed by a third party almost tripled this year, including increased instances of data breaches associated with third parties.

2.2. Our ongoing focus on cyber security

Our focus on cyber security as outlined in our Annual Work Program 2024–27 aims to provide insights into how NSW Government departments and agencies handle cyber security risks and comply with certain cyber security frameworks. The infographic below shows our published reports between 2018–25 that address specific cyber security concerns.

Our ongoing focus on cyber security


2018
Detecting and responding to cyber security incidents
2019
Cyber security was included in the periodic annual reports shown below
2020
Integrity of data in the Births, Deaths and Marriages Register
Service NSW's handling of personal information
2021
Compliance with the NSW Cyber Security Policy
Managing cyber risks
2022
Audit Insights 2018 – 2022
2023
Cyber Security NSW: governance, roles, and responsibilities
Management of the Critical Communications Enhancement Program
2024
Cyber security in local government
Regulation insights
2025
Cyber security insights
Regulation of the land titles registry
Internal Controls and Governance, Universities, Local Government and Cluster Agencies Annual Reports

Our performance audits assess whether the activities of government entities are being carried out effectively, economically, efficiently and in compliance with relevant laws. Cyber security has been a key focus of our performance audit program since 2018.

Our annual financial audits consider cyber security planning and governance, and whether cyber security incidents might have a material impact on the financial statements. Identified cyber security gaps are communicated to management and reported in the annual cluster agencies' reports, internal controls and governance reports, universities' reports, and local government reports.

2.3. About this report

This report summarises the key cyber security findings covered in our reports from 2018 to 2025. It also includes an analysis of the latest cyber security status reported by NSW Government departments and public sector agencies to Cyber Security NSW. This report aims to highlight themes and generate insights into the challenges and opportunities the public sector may encounter when responding to cyber security risks.

Findings from the audits referred to in this report were current at the time each respective report was published. In many cases, agencies accepted audit recommendations as reflected in the letters from agency heads included in the appendix of each audit report.

Readers are encouraged to view the full reports for further information. Links to versions published on our website are provided throughout this document and a full list is in Appendix 1.

3. Are NSW agencies equipped to deal with cyber threats?

This chapter presents key insights from analysis of the latest cyber security status reporting to Cyber Security NSW by NSW Government departments and public sector agencies. While equivalent sector analysis is not available for the university and local government sectors, the insights presented here are relevant to those sectors.

> **Chapter highlights**
>
> - Most agencies do not fully meet the requirements of the NSW Cyber Security Policy (CSP) – in particular the 'Protect' domain, for which only 31% of the Mandatory Requirements are met by agencies overall.
> - There is no reporting of control compliance when this is performed by third parties. Agencies and Cyber Security NSW may not be aware of any non-compliance with the CSP by third parties.
> - Planned or in-progress cyber security uplift programs and budget constraints were the most common reasons given for partial or non-compliance with minimum requirements.
> - Aggregated reporting to Cyber Security NSW can mask issues at individual agencies, with 66 reports received across 177 agencies.
> - 27 agencies reported a total of 152 significant, high and extreme residual cyber security risks.
> - There is a lack of independent assurance over agencies' reported compliance with the CSP.

3.1. Background

Cyber Security NSW, part of the Department of Customer Service, creates and implements strategies to strengthen cyber resilience across all entities, ensuring a cyber-secure NSW Government. Cyber Security NSW released the NSW Cyber Security Policy to provide the NSW Government with an integrated approach to preventing and responding to cyber threats and attacks.

The CSP specifies Mandatory Requirements for NSW Government departments and public sector agencies. It is not mandatory but recommended for adoption for state-owned corporations, local governments and universities.

The policy was updated in February 2024 and mandates compliance across three domains: 'Govern and Identify', 'Detect, Respond and Recover', and 'Protect'. These domains include a total of 31 Mandatory Requirements, further divided into 114 Detailed Requirements, setting the minimum expectations for agencies.

The Australian Cyber Security Centre's (ACSC) Essential Eight mitigation strategies are embedded in the CSP Mandatory Requirements. The CSP states that agencies must implement the Essential Eight to applicable information and communication technology (ICT) environments with a minimum requirement of Level 1 maturity.

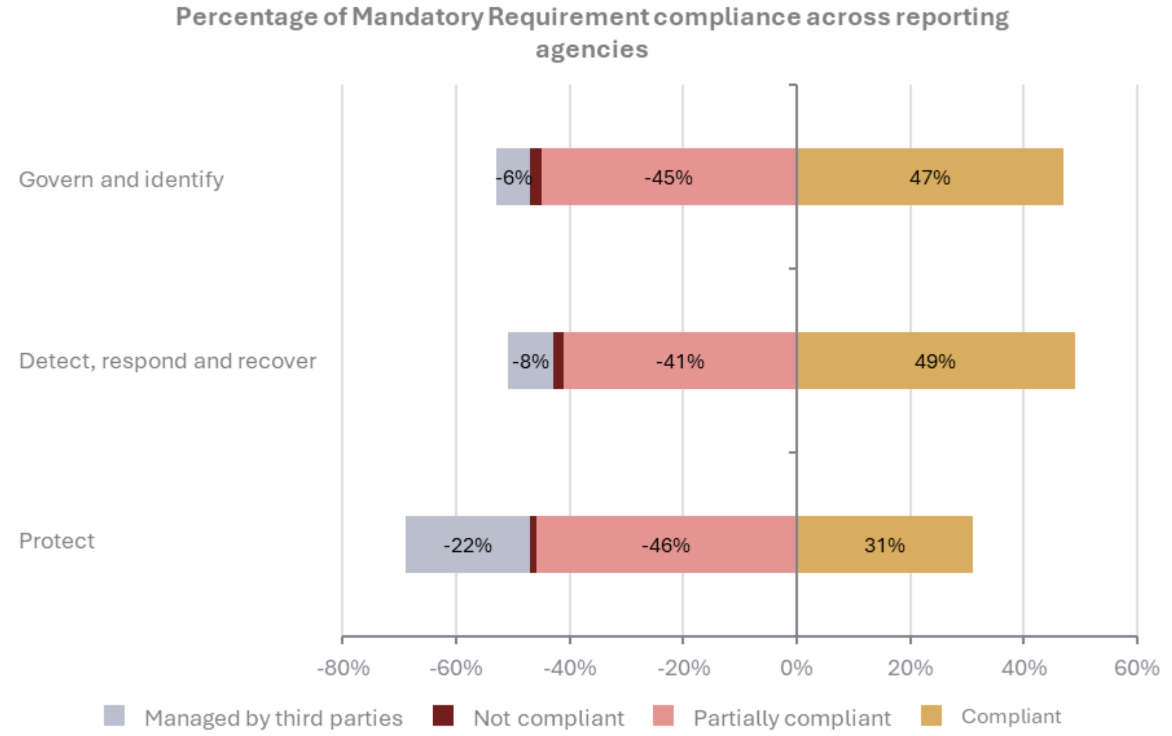
By 31 October each year, Cyber Security NSW must be provided with a report for each agency that covers information about their compliance with the CSP, cyber security risks with a residual rating of high or extreme, and an attestation on cyber security.

3.2. Cyber security requirements compliance status

Most agencies are not fully meeting the requirements of the Cyber Security Policy – particularly, those of the 'Protect' domain, for which only 31% of the Mandatory Requirements are met

Agencies demonstrated the least progress in achieving the minimum 'Protect' requirements, with only 31% of the Mandatory Requirements met, in comparison to the 'Govern and Identify' and 'Detect, Respond and Recover' requirements. Cyber Security NSW noted that agencies are not expected to have fully met all the Mandatory Requirements in the 2023–24 financial year of CSP reporting, as this report year is intended as a baseline only.

The 'Protect' domain includes requirements to implement the ACSC Essential Eight, network security controls and cyber security training programs. Controls within the 'Protect' domain are designed to prevent cyber security incidents, hence a lack of compliance in this domain may increase the likelihood of a cyber security incident and related impacts. The 'Govern and Identify' domain includes understanding information technology (IT) assets and their dependencies, governance of data identification, retention and disposal, and managing third-party relationships. The 'Detect, Respond and Recover' domain includes cyber security event logging, monitoring and response.



Note: The analysis involved summarising Detailed Requirements which form the Mandatory Requirements. Percentage displayed above refers to compliance rate of the Mandatory Requirements across all 66 reporting agencies in FY2024. Reporting agencies did not specify compliance to requirements that were managed by third parties. Therefore, the requirements managed by third parties has been classified separately where it was not assessed. Agencies were not expected to fully meet all Mandatory Requirements of the CSP for FY2024.

Source: Audit Office analysis of agency cyber security compliance returns to Cyber Security NSW for 2024.

Agencies' control compliance is not reported when performed by third parties

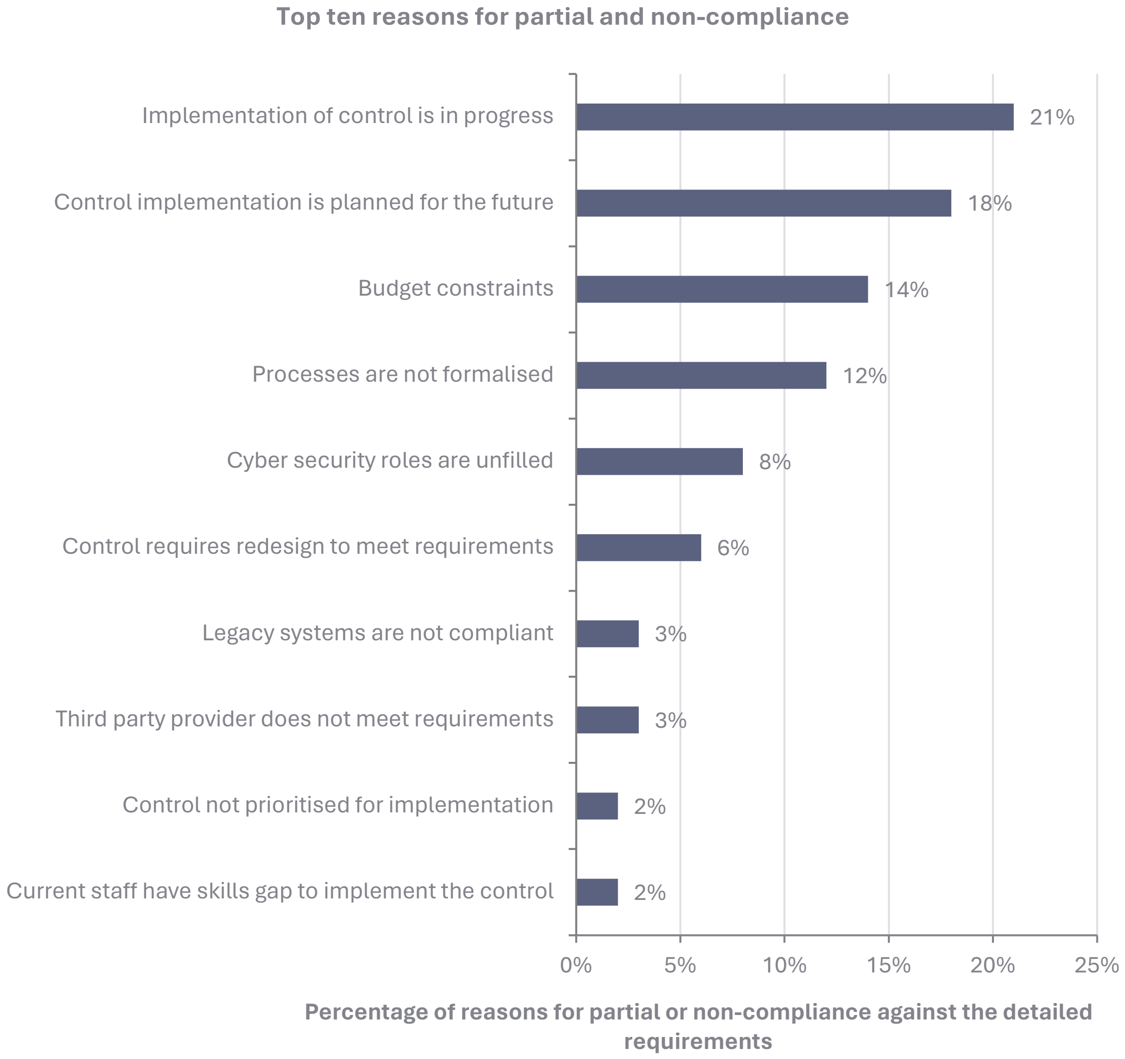
The 2024 CSP compliance graph shown in the previous section highlights that some of the Mandatory Requirements are managed by third parties. CSP specifies guidance and Mandatory Requirements around engagement with third party service providers.

When outsourcing, entities retain accountability for managing associated risks. Third-party compliance with minimum CSP requirements may be known to the agency but is not reported to Cyber Security NSW. An absence of clear reporting risks agencies and Cyber Security NSW not knowing about non-compliance against the CSP where the cyber security control practice is provided by the third parties.

The highest level of third-party reliance that is not reported or assessed against CSP requirements is in the 'Protect' domain. This domain covers all ACSC Essential Eight controls, and controls for access, data, email and network security. When in place and effective, these technical controls provide preventative protection against cyber attacks.

Planned or in-progress cyber uplift programs and budget constraints were the most common reasons for not achieving minimum requirements

Agencies were asked by Cyber Security NSW to provide reasons they could not meet the minimum compliance requirements for each Detailed Requirement in their reporting to Cyber Security NSW. The most common reported reasons for partial and non-compliance includes cyber uplift programs being in progress and or planned, budget constraints, lack of approved or formalised cyber processes and insufficient cyber security resources.



Source: Audit Office analysis of agency cyber security compliance returns to Cyber Security NSW for 2024.

3.3. Compliance reporting structures

Aggregated reporting to Cyber Security NSW could mask issues at individual agencies

The number of agencies that report on their cyber security assessments to Cyber Security NSW does not reflect the actual number of agencies responsible for cyber security or that need to be compliant with the Cyber Security Policy. This is especially relevant where portfolios of agencies exist but responsibility for cyber security and its management is mixed or unclear.

For instance, 66 reports were provided to Cyber Security NSW in 2024 representing 177 agencies, whereas 110 were provided in 2023. This is due to changes in aggregated reporting at a portfolio level instead of at individual agency level. Aggregated reporting can result in less transparency from the individual agencies, with uniquely weak cyber control compliance can be obscured when compared to the rest of the reported group.

The following are the number of agencies reporting their cyber security assessment against the Cyber Security NSW CSP in the last five years:

	FY2020	FY2021	FY2022	FY2023	FY2024
No. of reporting agencies	104	110	112	110	66

Source: Audit Office analysis of agency cyber security data returns to Cyber Security NSW for 2020–2024.

Cyber Security NSW advises agencies in Section 3.1.1 of the Cyber Security Policy Reporting Guidance 2023–24: ‘Agencies required to report under the NSW Cyber Security Policy may report individually, independently or be aggregated into the department report’.

The definitions for each of the reporting methods is as follows:

- individually – the agency submits a separate report, the contents of which may be visible to the lead department, through the Portal (this was previously also known as reporting ‘through cluster CISO’)
- independently – the agency submits a separate report, the contents of which are not visible to the lead department or only limited visibility is available
- aggregated – the agency is included within the lead department report.

3.4. Cyber security risk reporting

As part of the annual attestation, agencies must provide details of significant, high or extreme residual cyber risks to Cyber Security NSW. Agencies do not have to report on cyber risks that have been assessed as significant, high or extreme risks if managed to a lower level of residual risk.

A total of 152 significant, high and extreme residual cyber security risks was reported by 27 reporting agencies

Of 66 reporting agencies, 27 reported a total of 152 cyber security risks with a significant, high and extreme residual risk. Agencies define these significant, high and extreme risk categories differently but generally high risk means there is an impact on a critical agency function, whereas extreme is an impact on the entire agency’s operations.

Insights from this data include:

- 39 risks (25.6%) were not reported by agencies to their respective Audit & Risk Committees
- 30 risks (19.7%) have a mitigation timeframe of more than one year and a further 60 (39.5%) risks have unspecified timing for when agencies plan to reduce the risks to an acceptable level
- 28 risks (18.4%) were reported with treatment controls that are either largely ineffective or totally ineffective.

3.5. Assurance model

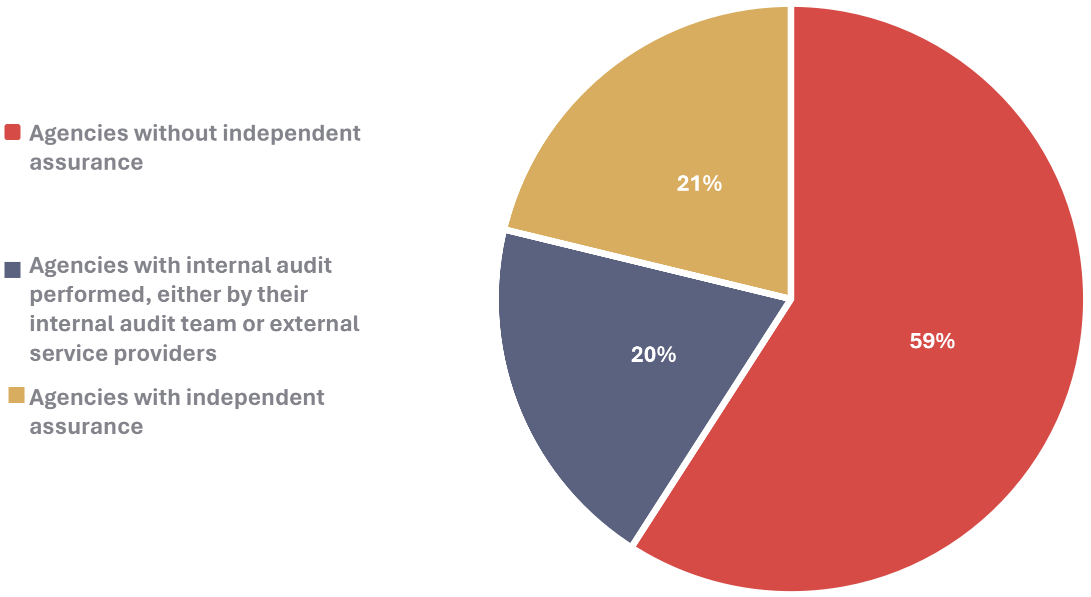
There is a lack of independent assurance over agencies' reported compliance against the Cyber Security Policy

Our Compliance with the NSW Cyber Security Policy report in 2021 highlighted that there was no monitoring of the adequacy or accuracy of agencies' self-assessments. The report suggested that Cyber Security NSW seek independent assurance over agencies' self-assessments. Our performance audit report on Cyber Security NSW: governance, roles, and responsibilities, which was tabled in February 2023, also highlighted the importance of assurance for agency self-assessments.

In 2024, Cyber Security NSW provided assurance guidance in its CSP, which agencies may use to support their attestation and data return. Agencies were required to report the level of assurance that supports their compliance to the CSP submitted to Cyber Security NSW.

The 2024 data submitted to Cyber Security NSW noted the following assurance activities being undertaken by agencies, with 59% of agencies advising they conducted no independent assurance over compliance information.

Level of assurance of agencies' compliance with the CSP



Source: 2024 State Agencies Cyber Security NSW Data Returns.

As we reported in Cyber Security NSW: governance, roles, and responsibilities, if agency self-assessments are unreliable, there is a risk that knowledge of the potential resilience of the NSW public sector to cyber security incidents is similarly incomplete.

We also noted various examples of inconsistencies in the agencies' risk reporting to Cyber Security NSW, which may indicate inaccurate assessment:

- ten risks had a 'substantially effective' control treatment and resulted in the risk decreasing from extreme/high to moderate, while a further 12 risks with 'substantially effective' control treatment did not reduce the risk rating
- two risks were accepted by management, but the risk was reduced from extreme to high, while another risk was also accepted but management assessed the treatment plan as fully effective.

4. Key cyber security insights from seven years of reports

This chapter focuses on thematic insights from audits of the cyber security environments within NSW state agencies, universities and the local government sectors between 2018 and the present. Key themes were identified and structured according to the Mandatory Requirements categories of 'Govern and Identify' 'Detect, Respond and Recover' and 'Protect', which are commonly used in the cyber security frameworks adopted across NSW Government entities.

Chapter highlights

- The adoption and use of cyber security policies and frameworks has improved, but not consistently across the sectors.
- Many entities reported cyber security risks exceeding their risk appetite, but not all have a formal uplift program.
- While cyber security roles and responsibilities are established, they may not always be clearly defined and effectively communicated.
- Inadequate asset identification can hinder protection prioritisation and incident response.
- Third-party cyber risk management is a significant challenge given the prevalence of cases of cyber security incidents involving third parties.
- Cyber security detection capability is improving but coverage is incomplete.
- Testing of cyber incident response plans could improve along with the development of more comprehensive playbooks.
- Many agencies have not met level one Essential Eight cyber protection measures despite these being a focus for many years.
- Cyber security awareness training has improved but phishing simulations should be more commonly used.
- Culture and accepted practice can drive non-compliance with protection controls.

4.1. Background

Cyber Security NSW released the NSW Cyber Security Policy (CSP) in February 2019 for NSW Government departments and public sector agencies, with the latest version published in February 2024.

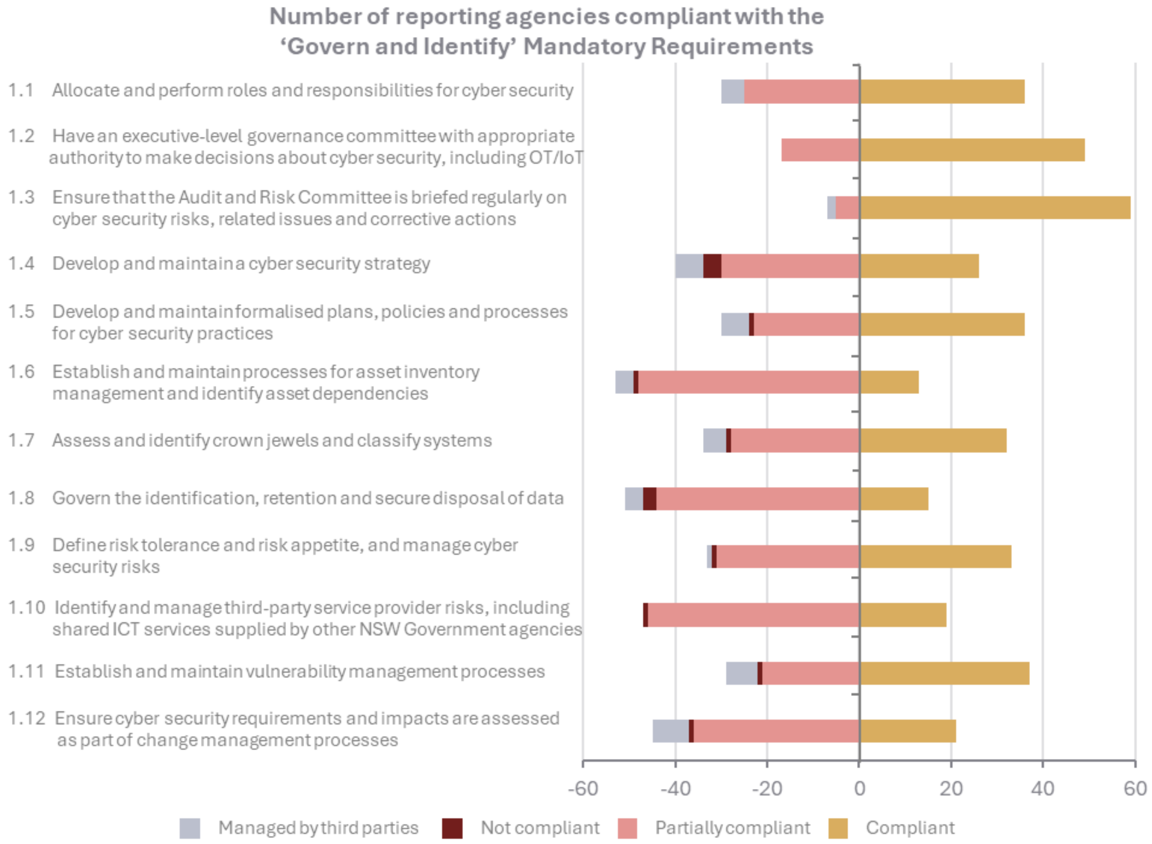
While the CSP does not set mandatory requirements for local government, the Office of Local Government (OLG) issued guidelines in December 2022, following a recommendation by the Audit Office. In January 2025, the OLG issued an update, reflecting the 2024 revision of the CSP. NSW universities have mostly adopted the National Institute of Standards and Technology – Cybersecurity Framework (NIST CSF) as highlighted in our Universities 2023 report.

Snapshots of agencies' compliance with the most recent CSP are presented in this section. Although this section does not include data for the local government and university sectors, it offers insight into areas that may also need improvement in those sectors.

4.2. Govern and Identify

Establishing effective cyber security governance and risk management requires defining several key responsibilities and practices. The NSW Cyber Security Policy's 'Govern and Identify' section within its Mandatory Requirements provides a structured approach to managing these aspects. It covers specific measures for establishing clear governance, strategic planning and policy development, risk management, data protection, and continuous improvement and accountability.

The following graphs show 2024 reporting by state agencies to Cyber Security NSW, outlining their progress in meeting the minimum requirements of the most recent CSP for the 'Govern and Identify' domain.



Note: Reporting agencies did not specify compliance for requirements that were managed by third parties. Therefore, the requirements managed by third parties has been classified separately where it was not assessed.

Source: Audit Office analysis of agency cyber security compliance returns to Cyber Security NSW for 2024.

The least progress was made in achieving compliance with the Mandatory Requirements in the following areas:

- asset inventory management process (Mandatory Requirement 1.6), the purpose of which is to help enable effective asset protection and swift threat response
- identification, retention and secure disposal of data (Mandatory Requirement 1.8,) which ensures data is properly managed throughout its lifecycle, protecting sensitive information and reducing the risk of data breaches
- third-party service provider risks management (Mandatory Requirement 1.10), which ensures third-party service provider risks are identified and managed to protect agency systems and data from potential cyber threats.

Cyber security policy implementation has improved, but not consistently across the sectors

Implementing a cyber security policy is important and a foundational step as it sets organisation-wide expectations, objectives and accountabilities in relation to cyber security.

Our reports indicate improvement over time across NSW state agencies, universities and local government sectors in implementing a formal cyber security policy. We are still identifying agencies that do not have a cyber security policy established.

The Internal controls and governance 2021 report highlighted that some agencies still had only a draft cyber security policy. This has since improved, as reported in the Internal controls and governance 2022 report, where it was noted that all agencies under review had formalised their policy.

In the university sector, the Universities 2021 report highlighted that cyber security policy implementation reached 100% in 2021, up from 90% as reported in Universities 2018.

Cyber security policy implementation for the local government sector is increasing over time. The Local government 2019 report identified a lower base, with only 20% of councils having a cyber security policy, growing to 66% as reported in the Local government 2023 report and up to 74% in the Local government 2024 report.

While these statistics show improvement over the past few years, the Cyber security in local government report from March 2024 highlighted risks relevant to policy implementation. Based on a review of three selected councils, the report found that while they had cyber security policies, there were gaps within their policies and related procedures that limited their effectiveness in supporting cyber security risk management. These included gaps in clearly assigning accountability for core cyber security functions.

The use and adoption of cyber security frameworks is improving, but not consistently across sectors

The use and adoption of cyber security frameworks is essential as they provide structured guidelines and best practice examples to protect an organisation's information systems from cyber threats. These frameworks help to identify and manage risks, ensuring compliance with regulatory requirements and establishing a robust security position. By implementing a cyber security framework, organisations can systematically address vulnerabilities, enhance their incident response capabilities and foster a culture of security awareness among employees. This ultimately leads to improved resilience against cyber attacks and safeguards critical data and assets.

The NSW Cyber Security Policy (CSP) is a mandatory cyber security framework for all NSW Government departments and public sector agencies. As highlighted in the Internal controls and governance 2024 report, other frameworks are also being used by NSW Government departments and state agencies. The most commonly used are the International Standard ISO/IEC 27001 and the NIST CSF.

As the CSP is not mandated for local government and universities, the Universities 2023 report highlighted that in 2021, NIST CSF and Australian Cyber Security Centre (ACSC) Essential Eight mitigation strategies (ACSC Essential Eight) are the two most common frameworks being used, but one university had not adopted any framework. This has improved as of 2023. The University 2023 report highlighted that all ten universities had adopted at least one framework, with the NIST framework (90% of universities) and ACSC Essential Eight framework (80% of universities) being the most commonly used frameworks, individually or in combination.

For the local government sector, the Local government 2019 report highlighted that only 20% of councils had adopted a formal cyber security framework. This grew to 91% by the release of the Local government 2024 report, which outlined that one framework, or a combination of frameworks, had been adopted. The ACSC Essential Eight was the framework most commonly adopted by councils (71%), followed by the OLG Guidelines (26%) and NIST CSF (18%). The low percentage of councils adopting the OLG Guidelines (26%) may be because compliance with the framework is not mandatory.

Many entities reported cyber security risks exceeding their risk appetite, but not all have a formal uplift program

Since the introduction of the CSP in 2019, all NSW Government departments and public sector agencies are required to conduct a cyber security risk assessment and to have an approved cyber security plan, also referred to as a cyber uplift program. Systemically identifying and evaluating potential vulnerabilities and threats through risk assessments is crucial for supporting and targeting cyber uplift programs.

According to our Internal controls and governance 2021 report, 96% of the agencies reviewed had conducted cyber risk assessments, reaching 100% by 2024, as highlighted in the Internal controls and governance 2024 report. However, only 77% had assessed their cyber risks against their cyber risk appetite, with 90% of these noting risks above their appetite. The Internal controls and governance 2024 report also explained that only 65% of agencies covered in the report had a current cyber security uplift program. Additionally, two agencies stated that they do not have funded plans to improve cyber security.

In the university sector, the Universities 2022 report indicated that all universities had performed a risk assessment related to their information technology (IT) assets and identified their 'crown jewels' or 'mission critical' assets. The University 2023 report highlighted that 70% of universities had cyber security risks above their risk appetite, but only 20% of these universities had formally accepted this situation. In addition, the report also noted that only 60% of universities had formal cyber uplift programs, with one university reporting that it did not have a specific budget allocated for improving its cyber security.

In the local government sector, the Local government 2019 report showed that only 54% of councils had included cyber risk in their risk registers, indicating that at least 46% had not performed a cyber security risk assessment. This statistic improved over the years, with 72% of councils including cyber risk in their risk registers by 2021 (Local government 2021), 82% by 2023 (Local government 2023) and 87% in 2024 (Local government 2024).

In the Local government 2024 report, 37% of councils evaluating their cyber security risks rated their residual risk as being above their risk appetite. Additionally, 30% were unable to determine if their residual risk was above or below their tolerable or acceptable risk. The Cyber security in local government report in 2024 audited three selected councils, noting that while two of three audited councils had identified cyber security as a strategic risk, none of the councils were effectively using risk management processes to identify and manage the cyber security risks.

The Local government 2024 report also highlighted that only 59% of councils had a cyber security uplift program and, of these, 14% advised that their spending on cyber security was insufficient to adequately resource their uplift programs.

While cyber security roles and responsibilities are established, they may not always be clearly defined and communicated

Clearly defined roles and responsibilities for cyber security are essential in ensuring effective governance and protection of digital assets. Incident responses are likely to be less effective where role requirements and responsibilities are unclear. As required by the NSW Cyber Security Policy (CSP), agencies have defined and allocated roles and responsibilities in relation to cyber security. In 2021, 96% of the agencies covered in the Internal controls and governance 2021 report had established cyber security roles and responsibilities. In the same year, the Local government 2021 report noted that only 61% of councils had established cyber security roles and responsibilities, which increased to 70% by 2024 per the Local government 2024 report.

The Detecting and responding to cyber security incidents report in 2018, which examined ten selected agencies, found that these agencies could only provide limited information to demonstrate that the role requirements and responsibilities of their staff are clear and well communicated. The 2024 Cyber security in local government audit, which assessed three selected councils, reported a similar finding, where these councils had not clearly defined roles and responsibilities for detecting, responding to (including through appropriate reporting) and recovering from cyber security incidents.

Inadequate asset identification can hinder protection prioritisation and incident response

Asset identification is a key element in effective cyber security management. Maintaining a comprehensive inventory of assets can help better manage cyber security risks, prioritise protection efforts and improve incident response. In 2022, the Internal controls and governance 2022 report highlighted the following:

- 84% of the agencies had comprehensive cyber security plans covering all IT systems, while 16% focused only on their most critical assets or ‘crown jewels’
- 68% of the agencies had not undertaken a process to identify digital or electronic intellectual property assets, such as patents, copyrighted material or trade secrets
- 24% of the agencies had not undertaken a process to identify highly sensitive digital or electronic assets, such as Cabinet-in-confidence information or data requiring security clearance like classified information.

The university sector identified its ‘crown jewels’, as reported in the Universities 2021 report. The Universities 2023 report highlighted that, while universities work with critical infrastructure entities such as defence, health, transport, utilities and telecommunications, all ten universities advised that no critical assets had been identified as defined in the *Security of Critical Infrastructure Act 2018* (SOCI). The SOCI legislation regulates critical infrastructure nationally and mandates cyber security incident reporting to the ACSC for critical infrastructure assets under certain circumstances.

Within the local government sector, only 36% of councils identified all their information assets requiring protection as per the Local government 2024 report. This was further supported by the 2024 Cyber security in local government report, which highlighted that the three councils selected for the audit had not assessed the business value of their information and systems to inform cyber security risk identification and management. This limited the councils’ ability to prioritise their activities and ensure that their most valuable information and systems are adequately safeguarded and secure.

Third-party cyber security risk management is a significant challenge, with some cases of cyber security incidents involving third parties

The NSW Cyber Security Policy's (CSP) Mandatory Requirement 1.10 outlines expectations for third-party security risk management, including contract clauses, monitoring and enforcement. Being unaware of weaknesses in the third-party cyber security controls may lead to slow or inadequate responses to vulnerabilities, allowing threat actors to exploit agency systems, data and assets. Even when a service is outsourced, the agency retains accountability for managing associated risks.

The 2018 Detecting and responding to cyber security incidents audit found that, although agencies advised that IT service providers reported cyber security incidents, only two of ten selected agencies had contractual arrangements requiring providers to report incidents in a timely manner.

In 2022, 96% of agencies covered in the Internal controls and governance 2022 report ensured that their cyber security policies or plans specified the application to third-party service providers. However, only 80% of them detailed how they monitored or ensured compliance with the relevant parts of the CSP.

In the university sector, as per the Universities 2021 report, 60% of universities extended their cyber security policies to third parties, reaching 100% by 2022 as reported in the Universities 2022 report. Additionally, the Universities 2021 report also highlights that 50% of universities required their IT vendors to confirm compliance with their cyber security policies through attestations or certifications, increasing to 70% by 2022 as per the Universities 2022 report. Similar gaps were also highlighted in the following audits:

- The 2021 Managing cyber risks audit found that the two selected agencies were not routinely conducting audits of third-party suppliers to ensure compliance with contractual obligations.
- The 2024 Cyber security in local government audit found that none of the three councils reviewed were effectively identifying or managing third-party risks. The audited councils lacked guidance on cyber security risk assessments in their procurement policies and procedures.

- The 2025 Regulation of the Land Titles Registry audit found that for the land titles registry IT system that was identified as one of the Department of Customer Service's crown jewel, there is a lack of clarity in the assignment of roles and responsibilities between the Office of the Registrar General and the Department of Customer Service for ensuring compliance with the NSW Government CSP, as well as the obligations of the private operator and its third-party contract service providers.

The following are examples from past published reports of cyber security incidents involving third parties that had an impact on NSW state agencies, universities and councils.

Case studies – Cyber security incidents involving third parties

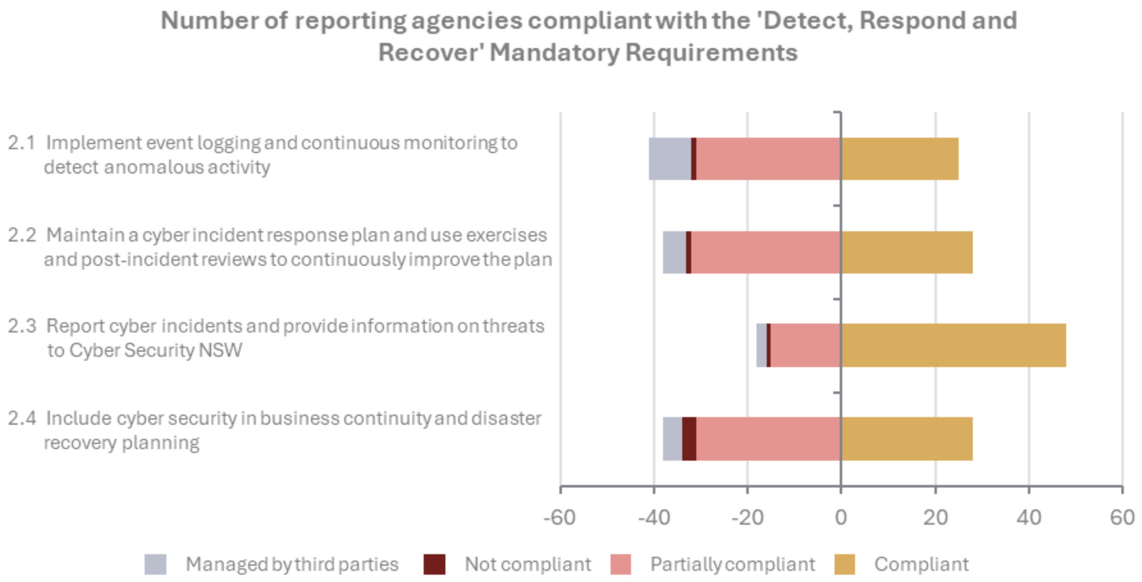
Year	Details
2021	A human resources and payroll solutions provider used by government entities suffered a data breach. An unauthorised third party gained access to the provider's corporate network and removed data on that network, including the personal information of employees. This incident caused reputational damage and potential harm to individuals who may become subject to identity theft and other cybercrime.
2023	A company that provides enterprise technology services to councils and other entities was subject to illegal access to its Microsoft 365 back-office system by an unauthorised third party.
2023	A third-party library system used by many NSW councils and universities was compromised and may have resulted in unauthorised access to customers' personal information. The vendor was aware of the system vulnerability but had not fixed it or informed the council in time.
2024	A council experienced a 'carding' attack on a vendor-hosted payment system, where small transactions were used to verify stolen or randomly generated credit card numbers. Business operations continued through alternative processes until the attack's nature and source were identified and resolved. This incident caused reputational damage and potential future fraudulent transactions elsewhere.

Source: Cyber security in local government, Local government 2024.

4.3. Detect, Respond and Recover

Effective cyber security requires robust measures to detect, respond to and recover from threats. Implementing event logging and continuous monitoring, maintaining a cyber incident response plan, reporting incidents to Cyber Security NSW, and integrating cyber security into business continuity and disaster recovery planning are essential steps to ensure resilience and swift recovery.

The following graph shows the 2024 reporting by state agencies to Cyber Security NSW, outlining their progress in meeting the minimum requirements of the most recent CSP for the 'Detect, Respond and Recover' domain.



Note: Reporting agencies did not specify compliance for requirements that were managed by third parties. Therefore, the requirements managed by third parties has been classified separately where it was not assessed.

Source: Audit Office analysis of agency cyber security compliance returns to Cyber Security NSW for 2024.

The highest compliance is for Mandatory Requirement 2.3, which ensures cyber security incidents are reported and threat information is shared with Cyber Security NSW, enabling coordinated responses, better threat intelligence and improved overall security positioning across all agencies.

The lowest compliance is for Mandatory Requirement 2.1, which ensures continuous monitoring and event logging to detect anomalous activities, enabling early threat detection and timely responses.

Cyber security detection capabilities are improving but coverage is incomplete

Cyber security detection monitoring is critical to ensure the early identification of potential threats and to trigger swift responses that can significantly reduce the impact of cyber security incidents.

The 2018 Detecting and responding to cyber security incidents audit noted that only two of ten selected agencies demonstrated high cyber security incident detection capabilities, while the rest had medium to low capabilities, with some lacking automated monitoring tools. Additionally, many agencies had incomplete response procedures and most had never tested them. Although all agencies had documentation requiring post-incident analysis, only one agency could provide a detailed post-incident review example.

Since then, state agencies have shown improvements as reflected in the Internal controls and governance 2023 report. This report highlights that automated monitoring systems to detect cyber security events were deployed across all agencies under review; however, the scope and sophistication of these systems varied. Automation and artificial intelligence played a crucial role in ensuring efficient and accurate event logging.

For the university sector, the Universities 2023 audit reported that all universities had implemented systems to detect cyber security incidents, recording and logging security events across their networks. However, the extent of cyber security monitoring varied, with 70% of universities noting that their processes did not cover all systems. This was primarily due to challenges with integrating legacy systems and the decentralised management of systems.

The 2024 Cyber security in local government report highlighted that the three audited councils used third-party tools to monitor for cyber security incidents and events. However, the councils had not clearly defined the scope of their monitoring and detection activities, nor the roles and responsibilities of council staff and third parties in these processes.

Regular testing of cyber incident response plans should improve

Regular testing of cyber incident response plans is crucial for validating the effectiveness of response strategies to minimise the impact of cyber security incidents.

The Internal controls and governance 2023 report highlighted that 92% of agencies covered in the review tested their cyber incident response plans. Most of these tests were conducted through tabletop exercises, which involve discussing scenarios and talking through plans and responses.

In the university sector, the Universities 2019 audit highlighted that only 60% of universities tested their incident response plans, reaching 100% by 2023, as highlighted in the Universities 2023 report. Of the tests performed in 2023, only ten per cent were functional, while the rest were tabletop exercises.

In the local government sector, only 57% of councils had a cyber incident response plan, as highlighted in the Local government 2024 report. Additionally, the 2024 Cyber security in local government report noted that none of the three selected councils for review had a cyber incident response plan.

Comprehensive playbooks support cyber incident response preparedness

Developing comprehensive playbooks is essential for ensuring that organisations are prepared to respond effectively to various cyber security incidents. Playbooks are documented incident responses tailored to address plausible cyber security incidents and support cyber incident response plans. Playbooks could cover scenarios such as (but not limited to) denial of service attacks, website defacement, compromise by an external attack, phishing and data breaches.

Our audit reports have highlighted how state agencies, universities and councils have established their playbooks.

- The Internal controls and governance 2023 audit noted that 88% of agencies covered in the review have detailed incident procedures and responses for multiple scenarios, while the rest only have ransomware scenarios in their playbooks.
- The Universities 2023 audit found that 30% of the universities having cyber incident response plans had not developed and finalised playbooks to support it.
- The Local government 2024 audit noted that only 56% of councils having cyber incident response plans have playbooks supporting their response plans.

Playbooks help agencies respond better to cyber security incidents by providing step-by-step procedures that guide response teams. Responses to incidents differ according to type, supporting agencies having multiple playbooks developed.

Below are examples of different types of incidents from past published reports that have had an impact on NSW Government agencies and councils, excluding those involving third parties that have been listed previously in this report.

Case studies – Cyber security incidents indicating importance of playbooks

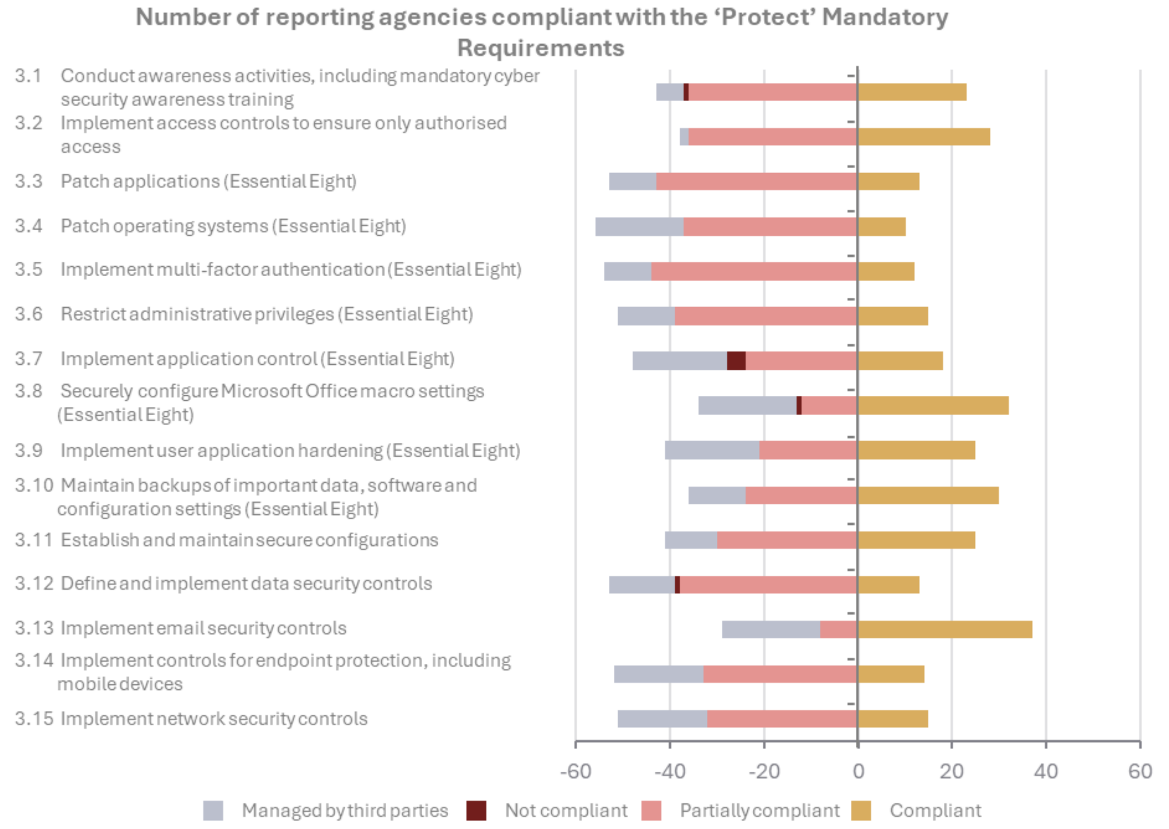
Year	Details
2017	A cyber security incident affected Agency Y and Agency X, which provides IT systems for Agency Y. The attack began with compromised email accounts in Agency Y, leading to phishing emails being sent to other NSW public sector agencies. The attackers aimed to gather financial staff credentials to create fraudulent payments. It took 49 days to fully resolve the incident, during which the payments gateway was closed to prevent fraudulent transactions, and compromised accounts were eventually secured.
2020	Service NSW experienced a targeted phishing attack which resulted in 3.8 million documents being stolen, compromising the personal information of 104,000 people. Ineffective business email processes and a lack of multi-factor authentication were identified as key contributing factors to the data breach. The costs associated with the agency response were estimated to be more than $30 million.
2022	A council in New South Wales suffered a ransomware attack that impacted a wide range of business operations, including council records, employee financial data and systems responsible for monitoring water quality.
2023	A council in New South Wales reported its social media account had been hacked, resulting in the account being compromised and taken offline.

Source: Detecting and responding to cyber security incidents, Cyber security in local government.

4.4. Protect

Protection of systems and information against common threats is becoming increasingly critical as cyber risks continue to evolve with rapid technological changes. The NSW Cyber Security Policy's (CSP) 'Protect' section within its Mandatory Requirements outlines specific measures, such as training, patching applications and operating systems, implementing multi-factor authentication, and restricting administrative privileges, among others. These measures help mitigate the risks associated with cyber threats, ensuring data integrity and confidentiality are maintained, systems are resilient, compliance is enforced, emerging technologies are supported and public trust is upheld.

The following graph shows the 2024 reporting by state agencies to Cyber Security NSW, outlining their progress in meeting the minimum requirements of the most recent CSP for the 'Protect' domain.



Note: Reporting agencies did not specify compliance for requirements that were managed by third parties. Therefore, the requirements managed by third parties has been classified separately where it was not assessed.

Source: Audit Office analysis of agency cyber security compliance returns to Cyber Security NSW for 2024.

The least progress was made in achieving compliance with the Mandatory Requirements in the below areas:

- patching applications (Mandatory Requirement 3.3) and patching operating systems (Mandatory Requirement 3.4), which ensures that applications are regularly updated to fix vulnerabilities, preventing cyber attackers from exploiting these weaknesses
- implementing multi-factor authentication (Mandatory Requirement 3.5), which enhances security by requiring multiple forms of verification, making unauthorised access much more difficult, even if one credential is compromised.

Many agencies have not met level one Essential Eight cyber protection measures despite these being a focus for many years

The Essential Eight, outlined by the ACSC, are strategies designed to mitigate cyber security incidents. Cyber Security NSW has adopted the Essential Eight strategies and included them in the NSW Cyber Security Policy (CSP). The Essential Eight maturity model uses a four-point scale. The definitions for each maturity level are:

Essential Eight Maturity Model

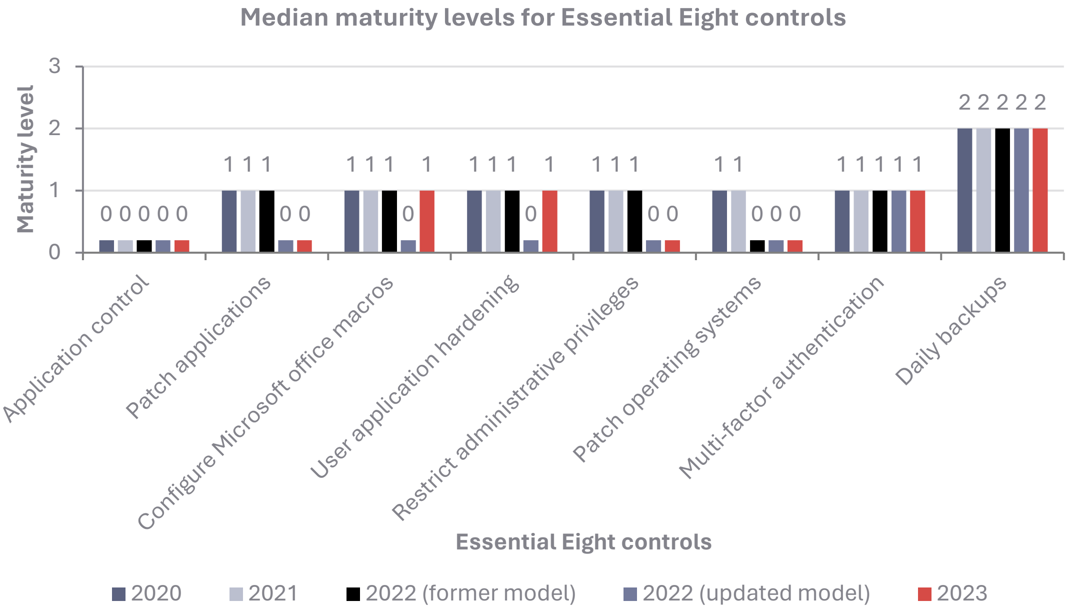
- Level Zero – there are weaknesses in an organisation's overall cyber security posture
- Level One – focused on adversaries who use common tactics that are widely available and opportunistically seek common weaknesses in many targets
- Level Two – focused on adversaries that are more selective in targeting and invest in more effective tools than Level One
- Level Three – focused on adversaries who are more adaptive and less reliant on public tools and techniques, and able to invest some effort in circumventing particular targets.

Source: Essential Eight maturity model.

The current 2024 CSP requires agencies to report their Essential Eight strategies to a baseline maturity level of one, and report each of the Essential Eight strategies as part of their annual CSP reporting. However, based on the number of agencies compliant to the Essential Eight strategies in the 'Protect' section of the Mandatory Requirements (3.3 to 3.10), there remains significant challenges in patching applications and operating systems, implementing multi-factor authentication, restricting administrative privileges and implementing application controls.

The previous versions of CSP require agencies to implement the Essential Eight strategies in applicable information and communication technology (ICT) environments using full maturity scale. There were revisions and additional requirements to meet the level one maturity under the Essential Eight over time. This could explain why the maturity level for some controls have dropped from 2022.

The graph below shows the median maturity levels for the Essential Eight cyber security controls from 2020 to 2023, when agencies reported under the former CSP and Essential Eight models. The table tracks the progress of these controls, highlighting improvements and areas needing attention in cyber security practices over time.



Note: The median represents the level at which half of the maturity assessments are reported as having been met.

Source: Individual self-assessed Essential Eight maturity returns (unaudited).

However, based on the above graph, between 2020 and 2023, some reported controls did not meet this minimum requirement. Specifically, some agencies reported a maturity level of zero for critical controls such as application control, patch applications, restricting administrative privileges and patching operating systems. This suggests that these controls are either not implemented or are implemented in a manner that is ineffective against common cyber threats.

Further, the graph shows that there are controls with a maturity level of zero. Some of the findings from past audit reports reveal potential contributing factors limiting the effective implementation of the Essential Eight controls, leading to low maturity assessments reported by agencies.

- The Internal controls and governance 2021 audit highlighted 82% of agencies had high numbers of deficiencies related to IT general controls, particularly around user access administration and privileged user access.
- The Internal controls and governance 2022 audit revealed that 20% of agencies do not patch or mitigate applications or operating systems for 'high-risk' vulnerabilities within 48 hours, as recommended by the Essential Eight. Further, over 72% of agencies run applications and operating systems that are no longer supported by the IT service provider and are unpatched. The Internal controls and governance 2023 audit highlighted that many agencies operated on legacy systems that were not compatible with modern security controls.
- The Internal controls and governance 2024 audit highlighted agencies’ reliance on third-party IT service providers without adequate oversight, and assurance of their compliance with cyber security policies was a recurring issue. Ineffective controls operating at third parties may reduce the agencies’ Essential Eight maturity level.

Cyber security awareness training has improved but phishing simulations should be more commonly used

Implementing regular cyber security awareness training and exercises is essential for building and maintaining a resilient cyber security culture. It is a cost-effective and quick method to enhance cyber resilience, addressing the human element often targeted by cyber criminals. Human errors are often a common cause of cyber attack, as cyber criminals frequently target individuals through phishing and other methods to infiltrate networks. Cyber security awareness training is covered in Mandatory Requirement 3.1 of the NSW Cyber Security Policy.

Between 2019 and 2024, there was a notable increase in cyber security training and awareness exercises among agencies covered in the internal controls and governance reports.

- 2021: The Internal controls and governance 2021 report showed 92% of agencies conducted cyber security training compared with 70% reported in Internal controls and governance 2019. Additionally, 56% of agencies conducted awareness exercises to test staff knowledge of responding to cyber threats, such as sending a simulated phishing email.
- 2022: Over 90% of agencies conducted awareness exercises, including simulated phishing tests as reported in the Internal controls and governance 2022 report.
- 2024: Only 12% of agencies reviewed had not defined their cyber security training requirements or mandated annual cyber security training as reported in the Internal controls and governance 2024 report. Additionally, 96% had performed phishing simulations.

In the university sector, all entities provided cyber security training and awareness programs in 2021. However, only half had tested staff knowledge through awareness exercises such as sending fake phishing emails (Universities 2021).

In contrast, in the local government sector, only 24% of councils had trained staff in cyber awareness in 2019 (Local government 2019). This figure grew to 74%, as reported in the Local government 2023 report, but dropped slightly to 69% in 2024 (Local government 2024). Additionally in 2024, 45% of councils did not conduct phishing simulations. Among the 55% that did, five councils failed to provide feedback to staff who reacted inappropriately to the phishing exercise.

Past audits that have also identified gaps in awareness training are as follows:

- The 2018 Detecting and responding to cyber security incidents audit found that training was limited and role requirements and responsibilities within the case study agencies (ten in total) were unclear. These agencies could provide only limited evidence of the cyber security training provided to their staff.
- The 2024 Cyber security in local government audit noted that while two of three selected councils had mandated cyber security training, they lacked a regular training schedule. The third council did not mandate the training, resulting in only a small number of staff completing optional training.

Culture and accepted practice can drive non-compliance with protection controls

Human error is often a contributing factor in successful cyber attacks. Situations can arise when there is a conflict between achieving day to day business requirements and adhering to cyber security controls. In practice, preference is often given to the achievement of business goals. For instance, individuals may bypass cyber security procedures during emergencies or time-sensitive work. Another example relates to meeting budget objectives, where an entity might reduce software license costs by sharing accounts and passwords among multiple users, thereby violating cyber security protocols.

Cultural drivers and accepted practices that threaten cyber security can be mitigated through comprehensive cyber security training that enhances employee awareness of cyber risks. However, training may not be enough to address the risk that arises from conflicting priorities between business requirements and cyber security controls. The above highlight the need for agencies to consider how their culture interacts with their cyber security control environment, and to make sure their cyber security controls are fit for purpose. Ultimately, the common purpose of protecting community interests remains paramount – in how government agencies achieve outcomes while protecting their digital environments. These objectives are not at odds.

Section 2 –

Appendices

Appendix 1 – Included reports 2018–2025

This report brings together a summary of key cyber security findings covered in our reports published between March 2018 and present. A total of 52 reports with cyber security coverage were analysed, however only 31 listed below have greater cyber security coverage and were analysed further for this report.

#	Published Year	Report Name
1	2018	Detecting and responding to cyber security incidents
2	2018	Internal controls and governance 2018
3	2019	Universities 2018
4	2019	Internal controls and governance 2019
5	2020	Local Government 2019
6	2020	Integrity of data in the births, deaths and marriages register
7	2020	Universities 2019
8	2020	Internal controls and governance 2020
9	2020	Service NSW's handling of personal information
10	2021	Local Government 2020
11	2021	Universities 2020
12	2021	Managing cyber risks
13	2021	Compliance with NSW Cyber Security Policy
14	2021	Internal controls and governance 2021
15	2022	Local Government 2021
16	2022	Universities 2021
17	2022	Audit Insights 2018-2022
18	2022	Internal controls and governance 2022
19	2023	Cyber Security NSW - governance, roles, and responsibilities
20	2023	Universities 2022
21	2023	Local Government 2022
22	2023	Management of the Critical Communications Enhancement Program
23	2023	Internal controls and governance 2023
24	2024	Regulation insights
25	2024	Cyber security in local government
26	2024	Local Government 2023
27	2024	Universities 2023
28	2024	Internal controls and governance 2024
29	2025	Regulation of the land titles registry
30	2025	Local Government 2024
31	2025	Universities 2024

Appendix 2 – Timeline of cyber security controls implementation across sectors

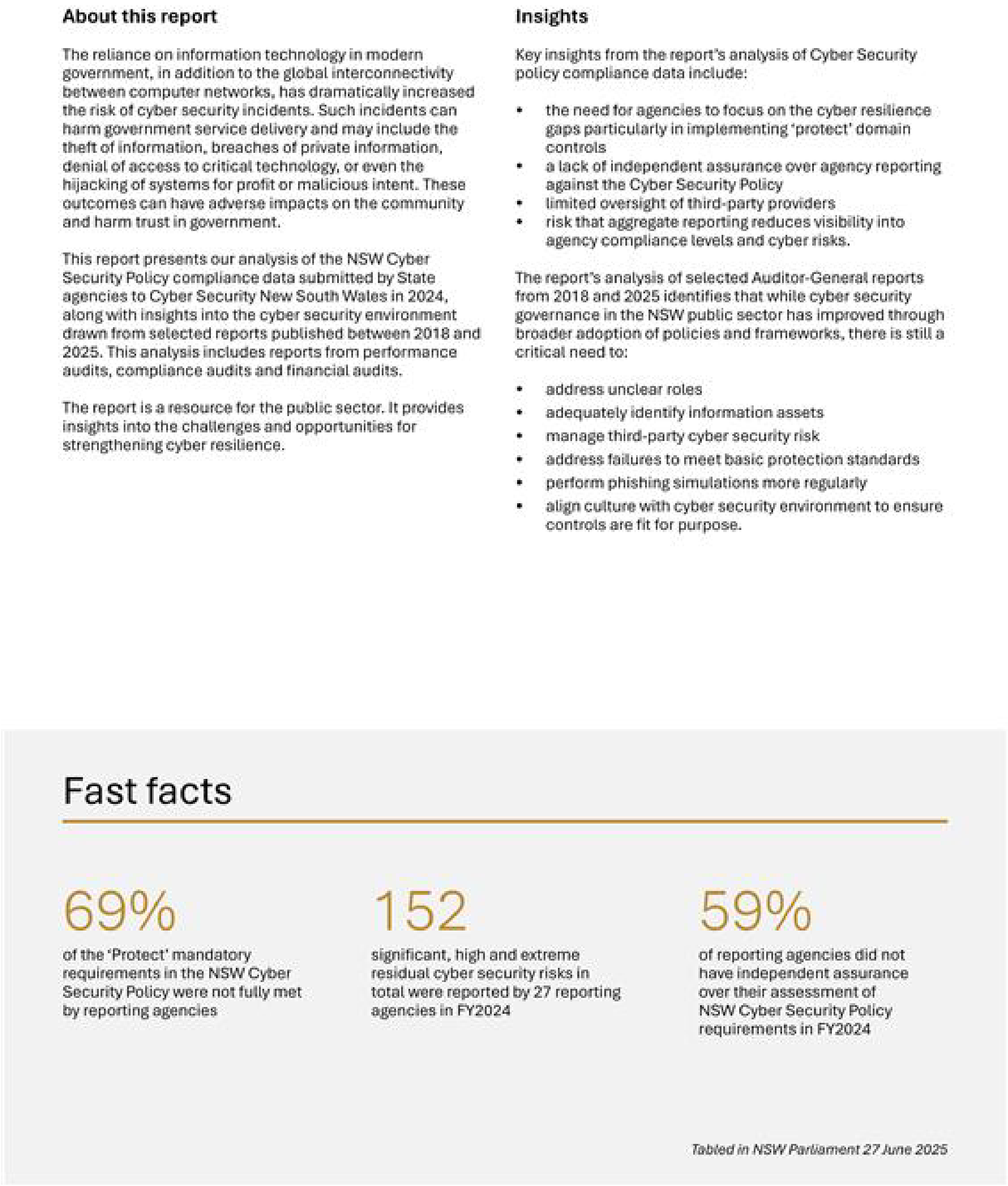
The table below provides a timeline of how cyber security controls have been implemented in NSW state agencies, universities and the local government sectors from 2018 to the present based on our published reports. The percentages indicate the proportion of entities that have implemented the highlighted controls, based on our published internal controls and governance reports (IC&G), university reports (Uni) and local government reports (LG). Each sector report may focus on different aspects of cyber security across various publication years, resulting in some information being unavailable for certain years.

- Internal controls and governance report: reviews cover the largest state-sector agencies in the NSW public sector.
- University report: reflects control implementation in ten universities.
- Local government report: covers majority of councils in the local government sector.

Controls	Sector	Percentage of control implementation						
		2018	2019	2020	2021	2022	2023	2024
Policy implementation	IC&G					100%		
	Uni	90%			100%			
	LG		20%					74%
Framework adoption	IC&G							100%
	Uni						100%	
	LG		20%					91%
Conducting risk assessments	IC&G				96%			100%
	Uni					100%		
	LG		54%					87%
Uplift program implementation	IC&G							65%
	Uni						60%	
	LG							59%
Definition of roles and responsibilities	IC&G				96%			
	Uni							
	LG				61%			70%
Completion of asset identification	IC&G					84%		
	Uni				100%			
	LG							36%
Extension of policy to third parties	IC&G					96%		
	Uni				60%	100%		
	LG							

Controls	Sector	Percentage of control implementation						
		2018	2019	2020	2021	2022	2023	2024
Automated systems for monitoring	IC&G						100%	
	Uni						100%	
	LG							
Cyber incident response plan testing	IC&G						92%	
	Uni		60%				100%	
	LG							
Playbooks implementation	IC&G						88%	
	Uni						70%	
	LG							56%
Conducting cyber awareness programs	IC&G		70%		92%			
	Uni				100%			
	LG		24%					69%

Appendix 3 – Report snapshot



About this report

The reliance on information technology in modern government, in addition to the global interconnectivity between computer networks, has dramatically increased the risk of cyber security incidents. Such incidents can harm government service delivery and may include the theft of information, breaches of private information, denial of access to critical technology, or even the hijacking of systems for profit or malicious intent. These outcomes can have adverse impacts on the community and harm trust in government.

This report presents our analysis of the NSW Cyber Security Policy compliance data submitted by State agencies to Cyber Security New South Wales in 2024, along with insights into the cyber security environment drawn from selected reports published between 2018 and 2025. This analysis includes reports from performance audits, compliance audits and financial audits.

The report is a resource for the public sector. It provides insights into the challenges and opportunities for strengthening cyber resilience.

Insights

Key insights from the report's analysis of Cyber Security policy compliance data include:

- the need for agencies to focus on the cyber resilience gaps particularly in implementing 'protect' domain controls
- a lack of independent assurance over agency reporting against the Cyber Security Policy
- limited oversight of third-party providers
- risk that aggregate reporting reduces visibility into agency compliance levels and cyber risks.

The report's analysis of selected Auditor-General reports from 2018 and 2025 identifies that while cyber security governance in the NSW public sector has improved through broader adoption of policies and frameworks, there is still a critical need to:

- address unclear roles
- adequately identify information assets
- manage third-party cyber security risk
- address failures to meet basic protection standards
- perform phishing simulations more regularly
- align culture with cyber security environment to ensure controls are fit for purpose.

Fast facts

69%

of the 'Protect' mandatory requirements in the NSW Cyber Security Policy were not fully met by reporting agencies

152

significant, high and extreme residual cyber security risks in total were reported by 27 reporting agencies in FY2024

59%

of reporting agencies did not have independent assurance over their assessment of NSW Cyber Security Policy requirements in FY2024

Tabled in NSW Parliament 27 June 2025

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 Office of New South Wales

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

t +61 2 9275 7100

mail@audit.nsw.gov.au

Office hours: 8.30 am–5.00 pm

audit.nsw.gov.au