

Cyber security insights 2025

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