Report snapshot

auditoffice OF NEW SOUTH WALES

Internal controls and governance 2025:
Procurement and technology

Internal controls and governance help agencies achieve their outcomes by supporting effective operations, reliable financial reporting, and legal compliance. This report provides Parliament with insights from financial audits of 26 major NSW public sector agencies, focusing on the effectiveness of their internal controls and governance. It presents observations across key elements of these frameworks.

Key findings

Internal control findings have decreased
Audit findings on internal controls and governance were reported across all 26 agencies. While the total number of findings decreased in 2024–25 compared to the 2023–24 interim audits, repeat findings rose and now account for 33% of all reported issues.

IT controls need to improve
Five high-risk findings were reported, all related to ineffective IT controls, including those designed to prevent cyber security incidents. Approximately half of all findings involved IT controls over key financial systems.

Deficiencies in procurement practices
Agency procurement practices show deficiencies in policy alignment, capability, and oversight. Many do not fully incorporate mandatory requirements of the NSW Procurement Policy Framework, and procurement training is either lacking or not mandatory. Around half lack formal policies for best and final offer processes, and supplier relationship management is inconsistently applied, limiting value-for-money assurance.

While all agencies have conflict of interest policies, some are outdated and lack mechanisms for managing complaints, with over half failing to review centralised registers before awarding contracts.

Agencies can better integrate AI into their existing governance and strategy arrangements
Agencies are beginning to adopt AI but have yet to fully integrate it into governance and strategic planning. Fewer than half have formal AI policies or have embedded AI into existing frameworks to guide responsible use. Only a quarter have developed strategies to maximise AI's benefits, and AI is not yet widely used as a strategic or operational tool across the sector.

Cyber security control deficiencies expose supply chains to vulnerabilities and undermine investment effectiveness
Control deficiencies make agencies vulnerable to supply chain cyber security threats and reduce investment effectiveness.

Three agencies lack formal policies addressing supply chain cyber risks, and eight do not have strategies to maintain complete IT asset registers, limiting visibility of systems. Weak third-party oversight was observed, including unclear contractual roles and limited post-termination planning. Additionally, not all agencies conduct cost–benefit analyses or align cyber security spending with threat landscapes, and only seven actively manage underutilised or outdated cyber security tools.

Recommendations

The report recommends that agencies strengthen controls and processes across three key areas: procurement frameworks, adoption of artificial intelligence, and cyber security controls.

Chapter 3 provides key areas of improvement and practical lessons for NSW government agencies in considering the effectiveness of their internal controls and governance.

Fast facts

5
high-risk audit findings relating to IT controls

33%
of reported audit issues were repeat findings

12
of 17 sampled agencies do not check centralised conflict of interest registers before awarding contracts

4
of 17 sampled agencies do not require their staff to undertake mandatory procurement training

29%
of agencies that have implemented AI have a supporting strategy in place

7
of 20 sampled agencies identify and manage underutilised or outdated cyber security tools and services

Tabled in NSW Parliament 29 October 2025