NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

Internal Controls and Governance 2026: grants, consultants, purchasing cards and technology

FINANCIAL AUDIT | 12 AUGUST 2026

auditoffice
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*.

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 **'Internal Controls and Governance 2026: grants, consultants, purchasing cards and technology'**.

Bola Oyetunji
Auditor-General for New South Wales
12 August 2026

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.

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

Internal controls and governance 2026: grants, consultants, purchasing cards and technology

1. Report snapshot 1
2. Executive summary 2
   - 2.1. Key findings 2
   - 2.2. Recommendations 6
3. Key areas of improvement and practical lessons 7
4. Internal controls and governance – trends in audit findings 10
5. Grants administration 13
   - 5.1. Context 13
   - 5.2. Agency wide monitoring and oversight 14
   - 5.3. Grant administration frameworks 15
6. Consultants 20
   - 6.1. Context 20
   - 6.2. Engaging consultants 23
   - 6.3. Reporting of consultancy expenditure 25
   - 6.4. Internal controls and governance over consultants 26
7. Purchasing cards 28
   - 7.1. Context 28
   - 7.2. Expenditure 28
   - 7.3. Acquittals 30
   - 7.4. Internal controls and governance over purchasing cards 31
8. Technology - Cyber security 33
   - 8.1. Context 33
   - 8.2. Cyber security attestation results 34
   - 8.3. Actions to address deficiencies in controls 38
9. Technology - Artificial intelligence 40
   - 9.1. Context 40
   - 9.2. Adoption of AI 41
   - 9.3. Governance for the responsible use of AI 43

Appendix 1 – Agencies included in this report 45

1. Report snapshot

Overview

Internal controls and governance support operations, compliance with legal obligations and reliable financial statements. This report analyses the internal controls and governance arrangements of 26 of the NSW Government's largest agencies.

Key findings

Repeat findings continue to increase

Interim audits found weaknesses in internal controls and governance at 15 agencies. More findings now relate to high-risk, high-spend areas such as procurement and grants. Repeat findings increased from 33% to 42% of total findings.

Oversight of grant programs by agencies is weak

Most agencies have limited central oversight and monitoring of grants administration, including how they monitor delivery, reporting and financial management.

Some agencies have deficiencies in frameworks for due diligence checks, acquittal controls, evaluations and reconciliations between program records and grant disbursements. This weakens the level of assurance over financial accountability of public funds and limits agencies' ability to demonstrate that grants were used for their intended purpose.

Agencies are not effectively engaging and reporting on consultants

Agencies did not always document the justification for hiring consultants, assess their performance or obtain conflict of interest declarations. Thirteen percent of sampled engagements did not include clauses relating to confidentiality to protect government information.

Mandatory annual reporting captures only a small share of payments to firms that provide consulting services, as payments for other professional service types are excluded. Agencies omitted at least $18.3 million in consultancy expenditure from their annual report disclosures since 2023–24.

High-risk purchasing card transactions require more scrutiny

Purchasing card transactions included vendors that sell gift cards, entertainment, alcohol and tobacco products.

Personal, non-compliant and split purchases were made on purchasing cards. This points to weaknesses in acquittal controls. One in 5 transactions were not acquitted and approved within 30 days, limiting oversight.

Significant gaps remain in compliance with Cyber Security Policy requirements limiting effective oversight

Less than half of agencies reported compliance with requirements to protect and govern their risk exposure. Some agencies did not assess risks from legacy systems that cannot be patched, increasing their exposure to cyber-attack.

Strategic use and assurance of AI is limited

Agencies have limited visibility over AI use as they did not consistently register all AI use cases or centrally track costs. Governance is not keeping pace with the speed at which agencies are adopting AI.

Recommendations

The report makes 4 recommendations for stronger internal controls and governance for grants administration, purchasing cards, cyber security and AI oversight.

Fast facts

$2.3 billion	128	27%
spent on purchasing cards by 26 agencies (1 July 2023 to 28 February 2026)	significant, high and extreme cyber security risks reported by agencies in 2025	of sampled consultancies did not have conflict of interest declarations

2. Executive summary

Good governance strengthens public confidence in the integrity and effectiveness of an organisation's systems and operations.

This report analyses internal controls and governance at 26 of the NSW Government's largest agencies, accounting for 91% of budgeted expenditure for 2025–26. It includes:

- an overview of interim financial audits for 2025–26
- analysis of the effectiveness of internal controls and governance in a selection of important areas of public administration
- key areas of improvement and practical lessons for agencies.

Different areas of internal controls and governance are selected each year for focus. These areas align to the Auditor-General's Audit Work Plan. In 2025–26, we selected:

- grants administration
- consultants
- purchasing cards
- technology, including cyber security and artificial intelligence.

This is the first of 4 financial audit reports on NSW Government agencies for 2025–26. The other reports are:

- **State agencies:** final results and insights from audits of all agencies' financial statements
- **State finances:** findings and insights from the audit of the consolidated financial statements of the general government and total state sectors
- **Infrastructure:** an assessment of significant capital and infrastructure projects.

2.1. Key findings

Internal controls and governance – trends in audit findings

Audit findings are increasing in high-risk, high-expenditure areas

Interim audits found deficiencies in internal controls and governance at 15 agencies. There is an increase in audit findings related to deficiencies in finance operational controls. These include findings in areas of high expenditure and risk such as procurement and grants. Forty-two per cent of audit findings are repeat, up from the 33% in 2024–25. This indicates that vulnerabilities, including IT control weaknesses, such as those which increase the risk of cyber-attack, are going unaddressed.

Deficiencies in procurement controls could limit agencies achieving value for money

Procurement processes and controls which did not meet mandatory requirements were identified, including deficiencies in tendering, supplier evaluation and compliance, putting at risk the achievement of value for money.

Grants administration

The internal controls and governance of 9 selected agencies with expenditure on grants of greater than $300 million were analysed as part of interim audits.

Centralised oversight of grants is limited

Most agencies do not have a centralised framework to oversight, and report on grant programs. In these agencies, grants administration and controls were primarily at the business unit or program level but there were no agency wide monitoring processes of these activities. This has resulted in fragmented oversight, including limited visibility of grant performance, risks and compliance.

Weaknesses observed included limited evidence of reconciliation of grants records to actual expenditure, monitoring acquittals, non-compliant expenditure and recoveries of overpayments or unspent funds at an agency level. This limits assurance over the completeness and accuracy of grant information and reduces visibility over the status and performance of grant programs.

Insufficient governance frameworks, policies and procedures increase the risk of waste or misuse of public funds

The Grants Administration Guide (the Guide), the NSW Government's mandatory framework for grants administration, requires agencies to establish policies and procedures for grants administration. Limitations in agency policies and procedures across the grant lifecycle, including planning, due diligence, monitoring, acquittal and evaluation weaken accountability, increase the risk of waste or misuse of public funds, and limit agencies' ability to demonstrate effective grant administration.

Agencies assess value for money inconsistently

Six agencies policies do not set out the level of analysis required at initial planning stages to demonstrate that a grant will achieve value for money. Four agencies do not specify or enforce requirements for cost–benefit analyses in business cases.

Analysis of a selection of grant programs identified 4 agencies that did not prepare a business case, including Transport for NSW allocating approximately $30 million over 3 successive funding rounds for a program (see page 16).

Deficient due diligence checks and monitoring controls reduce the effectiveness of oversight of the use of grants

Analysis indicates that 5 agencies do not require criminal history checks on funding applicants, 4 do not require financial capacity checks and 3 do not consider recipients' past performance when assessing applications. This increases the likelihood that high-risk applicants are not identified at the outset.

Weak monitoring limits oversight and delivery of grants. The depth and consistency of ongoing monitoring and reporting on performance differs across agencies, limiting assurance over outcomes and risk management. Two agencies did not outline the use of milestones or performance measures in monitoring selected programs as recommended by the Guide. Further, 4 agencies have not embedded a benefits realisation approach in their frameworks.

In one case, limited monitoring at the Department of Planning, Housing and Infrastructure led to inadequate oversight of a grant of $4.1 million made for a project. As of April 2026, the project is incomplete after approximately 5 years with $2.4 million in funding unspent. The funding agreement did not require regular reporting and the department had limited oversight of the recipient's progress and expenditure from 2022 to 2025 (see page 18).

Oversight of grants is ineffective when acquittals are not requested, monitored or evaluated

The policies of 2 agencies do not specify the extent of acquittal requirements for funding recipients, as required by the Guide. Delays in provision of acquittals by funding recipients and review of acquittals by agencies were observed in a sample of grant programs, including instances where unused public funds are yet to be recovered. These deficiencies reduce assurance that recipients have used public funds for their approved purpose or achieved intended outcomes.

Not all agencies require process, outcome and economic program evaluations at the completion of a program, as recommended by the Guide. In practice, evaluation assessments for a selection of grants reviewed were incomplete against the requirements of the Guide.

Consultants

Expenditure across all 26 agencies was analysed, and the internal controls and governance of 6 selected agencies with higher expenditure were examined in detail as part of interim audits.

Reporting on consultancy expenses is not complete

The NSW Procurement Board requires agencies to disclose consulting engagements greater than $50,000 in their annual reports. The Auditor-General's previous performance audit *NSW Government agencies' use of consultants* found that agencies inconsistently applied the definition of consulting engagements. Analysis identified at least $18.3 million in expenditure was for consultancy engagements but not reported as such by agencies in their 2024 and 2025 annual reports.

Some agencies did not comply with mandatory requirements when engaging consultants

Forty-eight contracts were selected for analysis, and 27% were found to have no conflict-of-interest disclosures completed by the consultants. Further, 13% of contracts did not include enforceable confidentiality provisions, increasing the risks around the use of sensitive government data. Agencies did not demonstrate that they considered alternatives, including using internal capability, for 17% of engagements sampled. For 40% of contracts, agencies did not monitor or evaluate the performance of the consultant.

Consultants are often engaged in direct source procurements. This included some instances where agencies applied exemptions from their policy requirements or where consultants were directly approached without a procurement process.

Taken together, these deficiencies heighten the risk of unnecessary costs and reduced value for money.

Purchasing cards

At the 26 agencies, there were 5.7 million transactions on purchasing cards (as credit cards are known in the NSW public sector) with a value of $2.3 billion for the period 1 July 2023 to 28 February 2026. Analysis indicates that purchasing cards are typically used for low-value purchases (such as office supplies, food and travel) and rely on cardholders exercising judgement to ensure expenditure is appropriate.

Expenditure across all 26 agencies was analysed, and the internal controls and governance of 6 selected agencies were examined in more detail as part of interim audits.

Purchasing card transactions include higher-risk expenditure that require scrutiny

Approximately $18 million in transactions were identified that may indicate purchasing card misuse or raise questions about their business purpose. These included purchases from vendors that retail in gift cards, entertainment, alcohol and tobacco products.

Personal purchases incurred and approved on agency purchasing cards

NSW Treasury policy mandates that cardholders are responsible for the proper use of their purchasing cards. Our data analytics identified potential personal (for a non-official purpose) and non-compliant expenditure being incurred on agency purchasing cards. In some cases, an official's line manager approved these transactions as consistent with cardholders' roles and for official purposes as part of acquittals, indicating deficiencies in controls designed to identify and prevent inappropriate expenditure.

Oversight is weak, with 1 in 5 transactions not acquitted within the required 30 days

Almost 21% of acquittals and approvals (to a value of approximately $350 million) took place a month or more after the expenditure was incurred, exceeding NSW Treasury's recommended timeframe. Around 7.4% took place after more than 60 days. Delays in acquittals reduce the assurance that agencies have over the appropriate use of public funds.

Purchasing cards used for high-value purchases contrary to requirements

NSW Treasury policy indicates that purchasing cards should only be used for low-value, high- volume payments less than $10,000. There were approximately 9,350 transactions totalling $137 million that exceeded the $10,000 threshold. Purchases above this threshold increase the risk that expenditure bypasses or circumvents established procurement and payment controls. Analysis of some agencies' policies indicate that card limits are not subject to regular review.

Technology – Cyber security

Agencies have not consistently implemented the mandatory requirements of the Cyber Security Policy

Analysis of 2024–25 annual agency reporting by the 71 agencies that report to Cyber Security NSW shows most did not comply with the policy. Over half of agencies have not implemented the 'govern and identify' and 'protect' mandatory requirements.

Some agencies have remediation strategies in place to meet requirements, though some are at least 4 years from achieving compliance. Reported cyber risks remain elevated across the sector, with 33 agencies reporting 128 significant, high and extreme residual cyber security risks.

Gaps in reporting on the implementation of policy requirements continue to reduce the reliability of the data

Aggregated attestation reporting arrangements, where 71 reports cover 189 agencies, limits visibility of entity-specific issues. Agencies are not required to report compliance with policy requirements where services are delivered by third parties, increasing the risk that deficiencies in third-party controls are not identified.

Management of legacy systems is inconsistent

Of the 10 agencies examined, 3 had not formally assessed the risks associated with each legacy system, and 2 had not implemented compensating controls to mitigate risks from legacy systems that can no longer be updated or patched.

Technology – Artificial intelligence

Internal controls and governance of 10 agencies with more significant use or potential from AI were analysed as part of interim audits.

Visibility of the use of AI and tracking of costs is limited

All 10 selected agencies have AI registers, though 4 only capture AI use that is assessed under the NSW AI Assurance Framework, increasing the risk of unmanaged and unidentified AI use.

Most agencies did not centrally track the costs of AI initiatives, limiting transparency and effective resource management. AI cost models tend to be more volatile than traditional software licencing costs.

Governance is not keeping pace with the speed at which agencies are adopting AI

AI is not consistently embedded as a strategic capability. Only half of the selected agencies have a formal AI strategy to guide adoption and maximise benefits. Agencies' governance arrangements for AI are immature and inconsistent and half have not fully embedded AI-specific risks into their existing governance frameworks.

A focused approach to the strategic use of AI could maximise benefits so that AI use better aligns with agencies' objectives.

Assurance of AI is inconsistent

We identified instances where agencies had not completed NSW Government AI Assurance Framework assessments or cyber security risk assessments, particularly for projects established before the framework's introduction.

While retrospective application is not required, current guidance requires agencies to apply the framework across the solution lifecycle. Agencies need to assess existing AI solutions against the current guidance.

2.2. Recommendations

By 30 June 2027, agencies should strengthen their stewardship of public funds for their grant programs by:

1. putting in place policies, procedures and quality assurance processes to ensure that grants are administered consistently with the Grants Administration Guide, which includes:
    a) a process for demonstrating at the planning and design stage how grant opportunities will deliver value for money by identifying benefits and costs
    b) developing a monitoring and evaluation framework for grant opportunities, including defined performance measures and financial acquittal requirements
    c) a framework to identify and manage risks for all grants
    d) establishing centralised oversight and reporting arrangements to enable timely and effective monitoring of all grants across the entire grant life cycle.

By 30 June 2027, agencies should strengthen monitoring and oversight of the use of purchasing cards by:

2. applying data analytics to identify and investigate high-risk, potentially inappropriate, and non-compliant transactions.

By 30 June 2027, agencies should improve cyber security by:

3. formally assessing the risks associated with legacy systems and implementing appropriate compensating controls.

By 30 June 2027, agencies should strengthen the governance of Artificial Intelligence by:

4. assessing all required AI solutions against the NSW AI Assurance Framework and use that framework to assist in the lifecycle management of AI.

3. Key areas of improvement and practical lessons

This chapter identifies key areas of improvements and practical lessons that all agencies can apply in designing and maturing internal controls and governance.

Grants administration

Agency wide governance and administration
Agency wide governance and oversight arrangements support stewardship of public funds, oversight and assurance over program controls, reporting and acquittals. Such controls could include:

- centralised monitoring and reporting frameworks on finances, progress, acquittals and outcomes
- regular reporting to executive management, exception reporting and analytics to identify higher-risk transactions or programs
- formalised processes to identify, escalate and remediate control deficiencies, including tracking of outstanding issues and follow-up actions
- embedding grant-related risks into enterprise risk management frameworks.

People and culture
Building capability for grants administration promotes achieving value-for-money outcomes. Mandating grants administration training for all relevant staff ensures consistent capability and culture is developed across an agency.

Due diligence
Recipient performance risk can be mitigated from the outset by:

- considering a recipient's previous performance
- undertaking financial assessments to avoid the risk of waste or loss.

Safeguarding public funds
Grants are made to a range of organisations, including those with less sophisticated controls and governance. Achieving benefits and safeguarding funds can be achieved by:

- clearly stating the intended outcomes, performance requirements and accountability measures such as acquittal requirements in funding agreements
- requiring regular reporting on performance measures in milestone reports
- timely follow up, analysis of and closure of acquittals.

Consultants

Building a business case
Without clear policies, procedures or guidance, officials may not address all mandatory requirements, particularly those which are not common to other types of procurement they usually undertake. Including guidance, case studies or examples on the following will enhance procurement outcomes:

- determining whether an engagement is a consultancy
- demonstrating the need for consultants and identifying internal capability
- restricting engagements to the minimum scope and duration required.

Identifying conflicts from the outset
Requesting conflicts of interest to be identified at the time of proposal ensures that where conflicts exist, they are managed before any work is undertaken.

Transparently reporting on consultants
To support complete and transparent disclosures, procedures to review and scrutinise all payments made to known suppliers of consultancy services, as well as transactions recorded in professional services accounts, should be established. This can help identify consultant engagements that have not been disclosed in annual reports.

Purchasing cards

Acquitting expenditure
Timely acquittals and approvals are fundamental to the integrity of purchasing card programs. Monitoring and reporting on outstanding acquittals, including escalation to executive management for long overdue items, provides a framework to ensure that the use of public funds is not at risk.

Using data analytics to enhance assurance and prevent fraud and loss
Data analytics can be used by agencies to identify and detect at risk transactions. Proportionate to risks assessed by agencies, analytics should go beyond compliance checks to address risks of misuse that are specific to that agency.

Cyber security

Extend oversight of third-party cyber security controls
Agencies retain accountability for the effective management of associated risks for services and IT systems delivered by third parties. Seeking assurance and reporting on the effectiveness of cyber controls and processes will enable agencies to be informed about the spectrum of risks, and the control response, for services delivered by third parties. Seeking this assurance and reporting will improve understanding of compliance gaps and reduce risks arising from these services.

Remediation plans
Remediation plans identify the priority areas to be addressed in uplifting the effectiveness of an agency's cyber security controls and should provide a basis for an agency to make informed decisions about future investments and technology. Adopting a project approach to remediation, including regular monitoring and reporting of progress against actions will support informed decisions about risk, priorities and mitigations. Involvement of executive management or relevant governance bodies, such as Audit and Risk Committees, in reviewing reporting and progress will ensure a shared understanding of risk and establish accountability for implementation and delivery.

Managing legacy systems
Cyber security risks may be more pronounced for legacy systems, particularly where they are no longer supported by a vendor. Maintaining an inventory of legacy systems, which is subject to regular review, supports visibility of the operation of these systems and the criticality of their cyber resilience. An inventory should include:

- risks associated with each system, including criticality and priority
- how risks are being mitigated by compensating controls, particularly where systems cannot be updated.

Artificial intelligence

Enterprise level governance
Agencies are increasingly adopting AI across their operations, driven in part by vendors integrating AI capabilities into existing off the shelf platforms and cloud services. Establishing clear enterprise accountability and governance structures will provide assurance that this technology transition is being delivered in a manner which maximises benefits and minimises risks. Enhancing controls could include:

- embedding AI-related risks into enterprise risk management frameworks
- embedding AI into agency's strategies and plans
- incorporating AI-specific considerations into IT procurement processes, including due diligence and contract provisions
- revising policies and procedures to reflect the specific risks and requirements of AI including testing to identify issues such as bias and vulnerabilities
- maintaining a central inventory of AI tools
- enhancing financial management controls, including monitoring of AI costs, particularly solutions involving consumption-based pricing models.

People and culture
As agencies adopt more AI tools, culture and capability must change to meet the challenges. Providing targeted training to staff on the responsible use of AI, including ethical considerations and appropriate use within established guardrails, will provide capability required.

4. Internal controls and governance – trends in audit findings

This chapter highlights findings relating from 2025–26 interim audits at the 26 agencies.

A strong system of internal controls and governance enables agencies to:

- operate effectively and efficiently
- produce reliable financial statements
- comply with laws and regulations
- support ethical and transparent decision-making.

Financial audits include:

- understanding the design, implementation and operating effectiveness of internal controls and governance relevant to the preparation of financial statements
- considering the extent to which an agency has complied with applicable laws, regulatory and policy requirements relevant to financial management and reporting.

Deficiencies identified during interim financial audits were reported to the relevant agency's accountable authority, management and the audit and risk committee.

Results of 2025–26 interim audits

Trends in audit findings

Audit findings are increasing in high-risk, high-expenditure areas such as procurement and grants

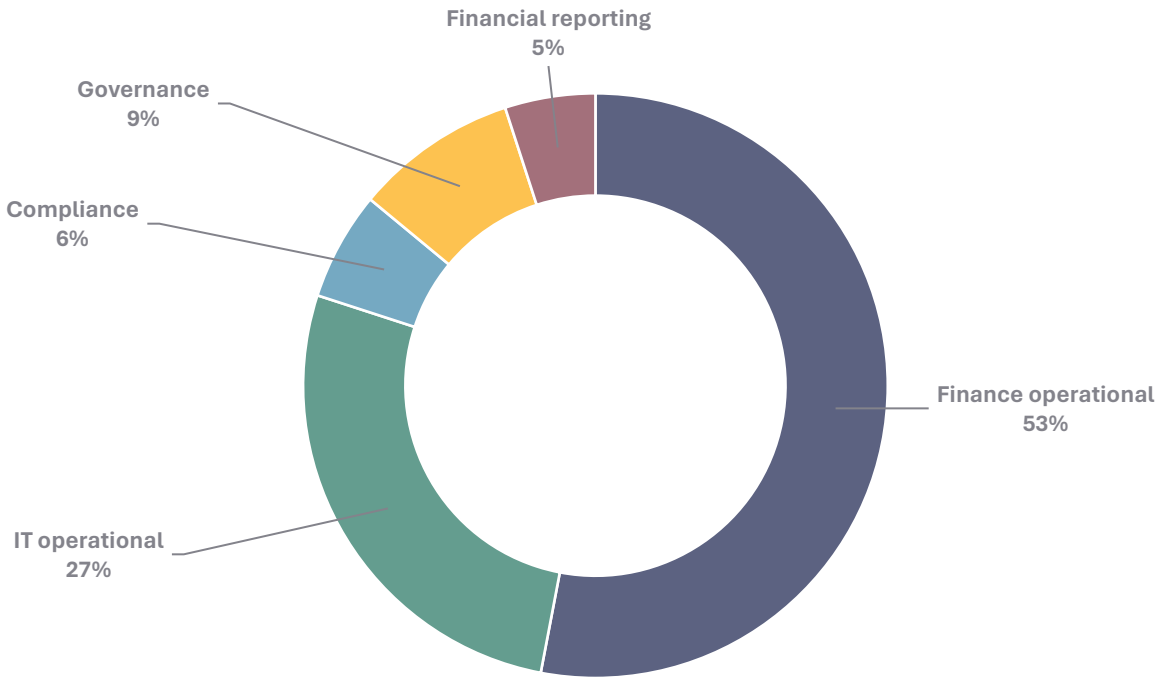
There were 66 new or repeat audit findings identified at 15 of the agencies in 2025–26 interim audits. Of the audit findings identified:

- 53% relate to deficiencies in finance operational controls, an increase from 2024–25, including in high risk, high expenditure areas such as procurement and grants (refer to chapter 5).
- There was 1 new high-risk audit finding which relates to financial reporting controls, relating to the omission by one agency of a payroll provision for financial reporting purposes for staff back payments arising from legal action.

High risk findings are significant because they can affect an agency's ability to achieve its objectives or impact the reliability of its financial statements.

Figure 1 provides an overview of the types of findings identified in 2025–26 interim audits.

Figure 1: Types of findings reported in 2025–26 interim audits



Note: The figure above does not include 138 unresolved audit findings, including 6 high risk findings, from prior periods which have not yet reached their due date.

Source: Audit Office of NSW 2025–26 interim management letters.

Deficiencies in procurement controls limit agencies achieving value for money

The Auditor-General's *Internal Controls and Governance 2025: Procurement and Technology* report identified deficiencies in end-to-end procurement by agencies that could limit value-for-money. The report recommended that all agencies enhance their procurement processes by adopting all mandatory and relevant recommended requirements of the NSW Procurement Policy Framework.

Similar deficiencies identified in interim audits included:

- procurement policies, procedures and frameworks which are insufficient to meet mandatory requirements or support value for money, including a lack of risk-based compliance monitoring, training for procurement staff, and post-completion reviews of major procurements
- an absence of centralised evaluation, tracking, monitoring and reporting of supplier performance
- no consideration of supplier performance information to inform future procurement decisions
- requests for quotation, sourcing or tenders not conducted in line with mandatory policy requirements
- purchase orders authorised after services or goods were received, indicating that procurement controls, including proper approach to market and approval, could be being circumvented.

Repeat audit findings

Increase in the proportion of repeat findings indicates vulnerabilities remain unaddressed

Repeat audit findings account for 42% of all findings identified, up from 33% in 2024–25. These mainly relate to:

- IT general controls
- outdated policies and procedures
- payroll and workforce management.

Weaknesses in the management of user access expose 1 in 4 agencies to a heightened risk of cyber-attacks or fraud

Most audit findings on IT general controls relate to deficiencies in managing and monitoring user access to key IT systems, including privileged user accounts. Deficiencies were identified at 7 agencies, relating to:

- insufficient monitoring of privileged user activities
- weaknesses in access restriction and monitoring of employee master data changes
- limited reviews of user access to key systems
- instances where system access was assigned without appropriate approval documentation
- no formal or documented procedures to guide user access reviews.

IT access management ensures only authorised individuals perform transactions and data changes in the normal course of business. Agencies should:

- appropriately approve access for new and modified access requests
- remove access when no longer required
- ensure highly privileged accounts are restricted and monitored.

Deficiencies in controls over shared services limit accountability and effectiveness

The Auditor-General's *State Agencies 2024* report recommended service level agreements are in place and authorised before agencies provide or receive shared services. Agreements should define the services, roles, responsibilities and rights of each party.

Deficiencies identified in interim audits include instances where finalised agreements are not in place despite services being provided or received and expired or outdated agreements.

The absence of formalised and agreed arrangements erodes the purpose of shared services and increases the risk of disputes, operational inefficiencies due to unclear responsibilities and higher costs of service.

5. Grants administration

The NSW Government Grants Administration Guide (the Guide) defines a grant, for the purposes of the Guide, as an arrangement for the provision of financial assistance by the NSW Government whereby money:

- is paid to a grantee other than the NSW Government
- is intended to help address one or more of the NSW Government's policy outcomes
- is intended to assist the grantee to achieve its objectives
- does not result in the return of goods or services by the grantee of an equivalent value.

This chapter analyses whether 9 selected agencies grant administration policies and procedures:

- allow them to monitor and demonstrate that programs achieve intended outcomes
- align with the NSW Government policies and guidance, including the Guide.

The chapter also analyses the extent to which these policies and procedures were followed in the administration of a selection of 16 grant programs administered by the agencies.

The 9 agencies were selected based on the value of their grant expenditure (greater than $300 million) and the scale and risks associated with the programs administered.

5.1. Context

The NSW Government reported $18 billion in grants and subsidy expenses in 2024–25

The $18 billion in grants and subsidy expenses recorded in 2024–25 accounts for 13% of total NSW Government expenses.

This chapter analyses expenditure that meets the definition of a grant as set out in the Guide. For accounting purposes other types of transactions are also recognised as grants expenses in agency financial statements, including:

- payments to non-government organisations for service delivery
- gifts of government property
- third-party asset transfers
- ex gratia and compensation payments
- transfers between agencies
- scholarships
- transfers to local government, such as Financial Assistance Grants.

These types of transactions are not analysed in this chapter.

Grants administration must comply with requirements as set out in the Guide

The Guide provides the framework for administering grants, setting out principle-based guidance and mandatory requirements. All ministers, ministerial staff and government employees must comply with its mandatory provisions, which have been a requirement under the *Government Sector Finance Act 2018* (GSF Act) since 1 July 2022. The Guide is issued by Premier's Memorandum.

The term 'grants administration' covers all activities across the grant lifecycle, from initial planning through to final evaluation and reporting. Grants must deliver value for money in achieving stated objectives and adhere to the principles of transparency, accountability and probity.

The Guide sets out requirements across all stages of grants administration, including program planning and design, funding decisions, monitoring and acquittals, and the evaluation of outcomes.

The Guide also provides non-mandatory guidance on areas such as funding agreements, monitoring and acquittals, and evaluation. While this guidance is not mandatory, Premier's Memoranda are binding on NSW Government agencies and compliance is expected.

Agency staff responsible for administering grants must also comply with relevant legislative requirements, including the *Government Sector Employment Act 2013*, which establishes core public sector values such as fiscal responsibility, efficient and prudent use of resources, and transparency.

5.2. Agency wide monitoring and oversight

Agency wide oversight and monitoring of grants is limited, weakening assurance over performance and compliance

Not all agencies are routinely reconciling grant program reports or listings and records to payments made, acquittal outcomes, or general ledger reported expenditure. Most of the 26 agencies could not readily provide grant program listings that reconcile to reported expenditure nor key information such as grant recipients, acquittal status, non-compliant expenditure or amounts to be returned. Information provided often required manual effort and coordination with individual business units.

Without regular reconciliation between grant registers, financial systems and program reporting, agencies may not readily identify discrepancies, incomplete acquittals, overpayments, unrecovered funds, or omissions in reporting. This limits assurance over the completeness and accuracy of grant information and reduces visibility over the status and performance of grant programs.

Most of the 9 selected agencies have established policies, procedures and guidance for grants administration, however, have not established organisation wide controls or reporting to monitor grants administration, delivery, performance and acquittals status. Grants administration in these agencies is largely decentralised and performed at the business unit level, covering specific grant programs. As a result, few agencies have a consistent, organisation-wide system or framework to monitor performance and from which to draw observations and assurance around performance, risk and compliance.

Organisation wide oversight and monitoring:

- improves decision-making
- makes it easier to identify and manage grant program risks and take corrective action
- improves the reliability and completeness of information reported to executive management
- means grant funds are more likely to accord with funding agreements and deliver intended outcomes.

Gaps in monitoring limits assurance over expenditure on grants

As required by TPG24-08 'Policy and Guidelines: CFO Certification on the Internal Control Framework over Financial Systems and Information', chief financial officers (CFOs) design, implement and regularly monitor a risk-based internal control framework, supported by reliable data and monitoring processes.

In the context of grants administration, weak centralised oversight and monitoring limit the ability of agencies to demonstrate that these assurance requirements have been met. A consolidated view of organisational-wide grant program performance and compliance would allow CFOs to:

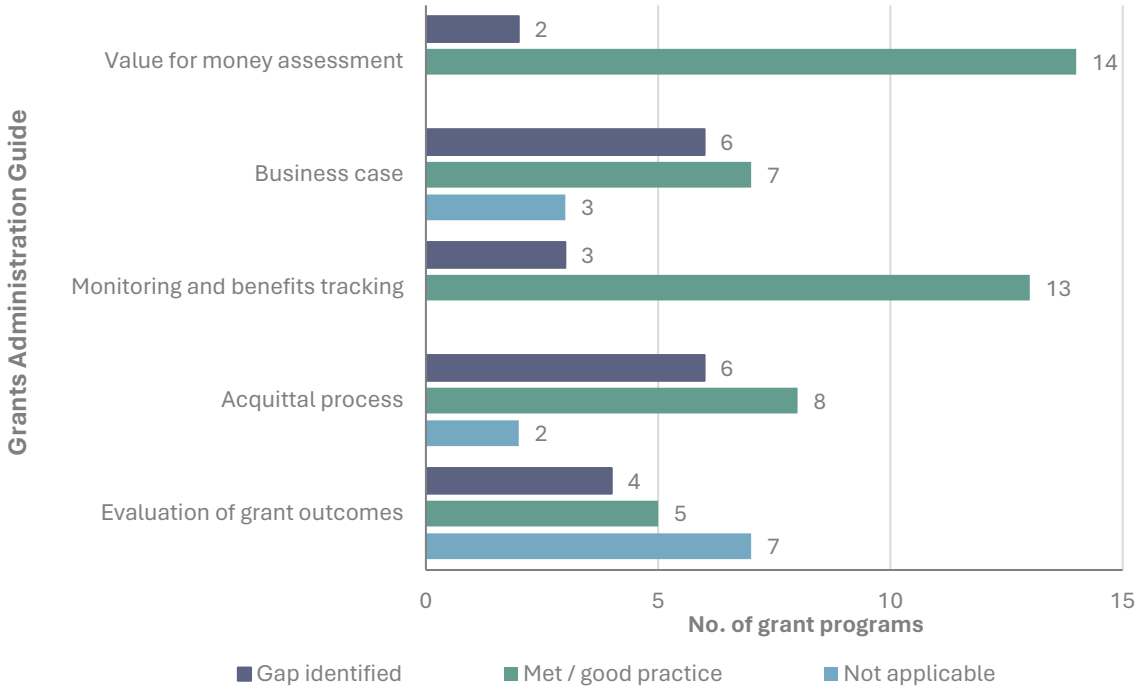
- assess control effectiveness
- identify and take action on issues in a timely manner
- provide assurance over the completeness and accuracy of financial and non-financial information.

5.3. Grant administration frameworks

The Guide requires that agencies establish procedures to ensure compliance, manage risks in line with the GSF Act, and use clear and specific written funding agreements.

Figure 2 below summarises the extent the 16 selected grant programs complied with the requirements and principles of the Guide.

Figure 2: Selected grant programs: alignment with key Guide principles and requirements



Note: Some requirements were not applicable where the grant program had not concluded or where the relevant requirement did not apply to the sampled program.

Source: Analysis based on16 selected grant programs reviewed at 9 agencies.

Policies and procedures

All but one agency had established policies and procedures for grants

The Guide requires agencies to establish appropriate practices and procedures. Of the 9 selected agencies, only one had not established centralised policies, procedures and guidance for grants. Most had reviewed their policies within the last 12 months.

Most agencies conduct internal audits into grants

The GSF Act requires accountable authorities to maintain effective systems of internal control and assurance, including conducting internal audits. Internal audits assure the effectiveness of internal controls and governance for grants administration and can identify inefficiencies or financial waste. Two of the 9 selected agencies had not undertaken internal audits into grants administration since 2023–24.

Lack of training hindered capability development for grants administration

The Guide asserts that training officials in grant administration builds necessary skills and capabilities. Only one selected agency mandates training in grants administration.

Appropriate training builds assurance that staff understand and apply policies.

Agencies did not consistently identify grant risks in enterprise risk management frameworks

Assessing and managing risk is critical to planning and designing grant opportunities. The Guide requires officials to identify and manage risks. Four agencies have not identified any program, grantee and governance risks in their enterprise risk assessment. Three agencies do not require risk appetite statements for medium to high-risk grants.

Strengthening risk identification and embedding risk appetite frameworks aligns risk management practices and grant decision-making.

Planning and design

The Guide requires agencies to demonstrate how grant opportunities achieve value for money by identifying expected costs and benefits over the lifecycle of the grant. Agencies are required to consider economic, social, cultural and environmental impacts, including both monetary and non-monetary factors, that are proportionate to the value and risk of the grant.

The Guide recommends the use of business case and cost–benefit analysis (CBA) for NSW Government investments above $10 million. A benefit–cost ratio (BCR) greater than one and positive net present value (NPV) indicate expected benefits exceed costs.

Robust value-for-money analysis at the planning stage informs funding decisions, strengthens accountability for the use of public funds and enables ongoing monitoring of program performance against intended outcomes.

Agencies did not always specify requirements to demonstrate value for money, reducing assurance over the optimal use of public funds

Analysis of the policies, procedures and guidance at the 9 selected agencies found:

- 6 did not specify the analysis required to demonstrate value for money in grant opportunities
- 4 did not reference key outputs such as NPV and BCR analysis for business cases for grant programs valued at more than $10 million.

Further, analysis of the selected grant programs identified 4 agencies (across 6 programs) did not complete business case analysis, including:

- A Department of Communities and Justice program, originally budgeted at $15 million, did not include NPV or BCR analysis. The agency advised it considered value for money at design stage by appointing an external probity adviser and developing program guidelines aligned to program objectives, however these elements of the process did not provide insight on the value to be delivered by the grant.
- Transport for NSW allocated approximately $30 million over 3 successive funding rounds between 2024 and 2028 under a grant program without a business case. The agency advised that the program was delivered on a round-by-round basis rather than as a single overarching program. While it designed each round to remain below $10 million, funding increased due to higher-than-expected demand. The agency has acknowledged future funding requests will need a short-form assessment to support its expansion as a multi-year initiative.

Insufficient policies, procedures and guidance for officials increases the risk that inadequate analysis of value for money is undertaken when planning a grant program, reducing assurance that the optimal use of public funds is achieved.

Assessing and managing risk at the grant program level

The Guide requires agencies to undertake due diligence on applicants for higher-risk grants, with the scope proportionate to value and risk profile.

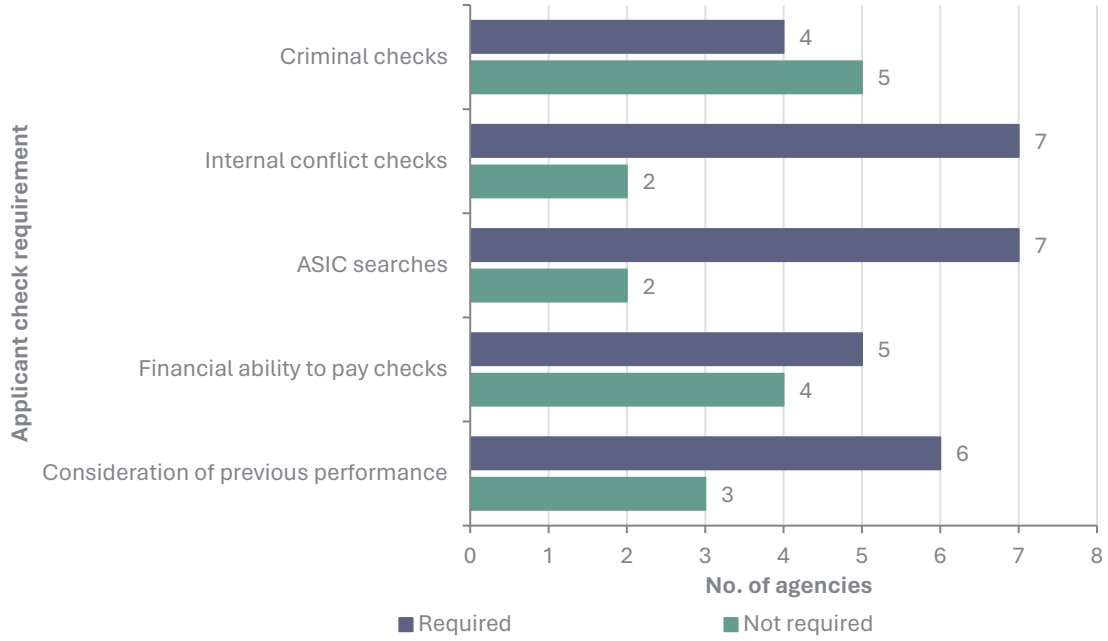
The nature and depth of due diligence checks vary, increasing the risk that higher risk applicants will not be identified at early stages

Analysis of agency policies indicates that 5 agencies do not perform criminal history checks, 4 do not require financial capacity checks and 3 do not consider recipients' past performance when assessing grant applications.

Insufficient due diligence processes, including understanding past performance of recipients, increases the risk that higher risk applicants will not be identified and considered from the outset of a program.

Figure 3 outlines the types of due diligence checks on potential grant recipients required by agencies.

Figure 3: Due diligence checks on grant recipients required by agencies



Source: Audit Office analysis.

Monitoring

The Guide requires agencies to monitor overall grant opportunities and individual grant recipients throughout the life of the grant. This involves the ongoing reviews to:

- assess progress
- confirm that funding is used as intended
- evaluate outcomes, benefits and overall value for money.

Weak monitoring limits oversight of public funds and delivery of outcomes

The Guide recommends agencies use performance measures, milestone reporting and benefits realisation management.

Benefits realisation management tracks expected benefits throughout the life of a program to support investment decisions and improve outcomes. This includes maintaining a benefits plan and register, and aligning these with change management processes.

Of the selected agencies:

- all but one policy required reporting and performance measures to be included in funding agreements
- 4 agencies' policies do not embed a benefits realisation approach.

Analysis of the selected grant programs indicated that 2 agencies (across 3 programs) did not use performance measures, benefits realisation planning, or milestone reporting to monitor the selected programs.

The case study below highlights the need for active monitoring and oversight in grants administration.

Case study 1 - Inadequate monitoring of grant program

In February 2021, the Department of Planning, Housing and Infrastructure awarded a grant to fund capital works and maintenance to the Bathurst Thoroughbred Racing Club totalling $4.1 million (inclusive of GST). The grant was part of a broader NSW Government COVID-19 stimulus package. In September 2025, the department approved a change in project scope for the remaining unspent grant funding. As of April 2026, the department advised that the funded works were not yet completed and $2.4 million was unspent.

The department's monitoring of this grant was limited. The funding agreement did not clarify requirements for milestone monitoring, reporting or acquittals, nor did it address unspent funds. The department has not undertaken internal monitoring or prepared progress reports about the status of the program. The department did not require reporting from the recipient from 2022 to 2025, and its monitoring of the grant was irregular and not timely during this period.

Due to the ineffective and limited monitoring across the grant lifecycle, the department did not have:

- assurance that the funds have only been used for the purposes of the grant
- sufficient information to ascertain the progress of the works or status of unspent funds.

The department has taken some actions since 2025 to request reporting from the recipient.

Acquittal processes

Acquittals provide assurance that public funds are used for delivering the intended outcomes. The Guide recommends agencies assess each individual grant and each grantee's compliance with the terms of the funding agreement and any relevant requirements. The level of acquittal should be commensurate with the grant's size and risk.

Oversight of the use of public funds is not effective when acquittals are not requested, monitored or reviewed by agencies

Two agencies do not have policies, procedures or guidance that specify the extent of acquittal requirements to be included in funding agreement, for example, reviews of financial statements, supporting documentation and progress or completion reports.

Not specifying acquittal requirements from the outset in funding agreements, limits visibility of performance and reduces assurance that grants are only used for their intended purpose.

Analysis of the selected grant programs identified that there were delays in obtaining and reviewing acquittals from grant recipients, including the recovery of unspent funds, at 3 agencies (across 6 programs).

This includes the Department of Education which had 62 acquittals outstanding from recipients for a program (approximately 9%), and was yet to recover up to $2.4 million in unspent funding for a separate program.

Obtaining and reviewing acquittals in a timely manner helps agencies to identify and track outstanding items, address delays and non-compliance, and recover unspent funds where required.

Analysis also identified that the Department of Communities and Justice was taking action to recover $670,000 in unspent funding for a program, including amounts relating to a recipient that had entered deed of company arrangement (voluntary administration) and another that had withdrawn from the program.

Evaluation of grant outcomes

A formal evaluation process collects and analyses information to assess the relevance, efficiency, effectiveness and overall value or net benefit of a grant program at its conclusion. The Guide recommends the following types of evaluations:

- process evaluation of how an initiative is delivered, whether implementation aligns with the original design, and any issues during delivery
- outcome evaluation of whether and how the initiative achieved intended outcomes
- economic evaluation of the costs and benefits of an initiative to determine value for money and overall social benefit.

Evaluation processes are inconsistently applied

Of the selected agencies policies and procedures, 1 agency's policy does not require any evaluations and 1 agency only requires evaluation for programs above $10 million.

Analysis of the selected grant programs indicated that 2 agencies (across 4 programs) with a requirement for evaluation in their policy did not complete evaluations covering all relevant considerations.

Timely post-completion evaluations will demonstrate achievement of intended outcomes, assess value for money, inform future programs and support transparency and accountability.

6. Consultants

Over-reliance on consultants can result in increased costs, weaken internal capability, and create risks around accountability and transparency. Agencies should have in place robust internal controls and governance which support the justification and approval to engage consultants that meet the mandatory requirements established in legislation and NSW Government policy.

This chapter examines:

- expenditure on consultants by the 26 agencies
- the effectiveness of internal controls and governance at 6 agencies with the highest budgeted consultancy expenditure for 2025–26.

6.1. Context

The NSW Procurement Board defines a consultant as 'a person or organisation engaged to provide recommendations or professional advice to assist decision-making by management'. The Board indicates that consultants are distinguished from other professional services and contractors by:

- the advisory nature of the work
- the output reflects the independent view or findings of the consultant
- the consultant's performance of the work is not, or mostly not, under the client's direct supervision and direction
- the consultancy being the sole or majority element of the contract in terms of relative value or importance.

Non-consultancy professional services generally involve implementation or delivery of an existing proposal or strategy, output that is not the independent view of the supplier and there is more direct supervision and control by an agency.

Agencies must exercise judgement and care when determining if services provided by a supplier represents a 'consultancy', particularly as these suppliers provide a range of other professional services to agencies. The Auditor-General's 2023 performance audit *NSW Government agencies' use of consultants* found examples of consulting engagements which were not reported as consulting expenditure, indicating that the audited agencies did not apply the NSW Procurement Board's definition of consultant consistently. If a consultancy is not correctly identified at the outset of a procurement, the mandatory procurement and annual reporting requirements will not be applied.

Agencies must comply with legislation and NSW Procurement Board directions when engaging consultants

When engaging a consultant, agencies must comply with:

- *Public Works and Procurement Act 1912* (PWP Act)
- *Government Information (Public Access) Act 2009*
- TPG25-10 *Framework for Financial and Annual Reporting*
- NSW Procurement Board policies and directions for procurement issued under the PWP Act.

PBD-2026-02 *Engagement of professional services suppliers* specifies that, when engaging consultants, agencies must:

- define the need to use a consultant, rather than other resource types
- make the duration of the consultancy as short as possible to undertake the required work
- justify any variations to the contract
- subject the engagement to appropriate confidentiality provisions
- declare and manage potential, perceived or actual conflicts of interest prior to and throughout the engagement
- assess the consultant's work
- put appropriate documentation and record keeping practices in place
- identify the consultant when working within agencies, for example in email systems, security passes or staff directories
- not give the consultant decision-making authority in recruitment or selection processes for other consultants and contractors.

PBD-2026-02 does not apply to state-owned corporations, however, is better practice for these agencies.

PBD-2026-02 requires agencies to consider the Core NSW Public Service Work Policy, which sets expectations for identifying and delivering core work to strengthen internal capability and reduce reliance on consultants. It defines core work as activities central to government decision-making and public sector functions, including work that must be performed by government employees or progressively brought in-house.

TPG25-10 requires agencies to separately report consultancy engagements over $50,000 in annual reports, with engagements below this threshold reported in aggregate.

Agencies use suppliers to provide both consulting and other professional services

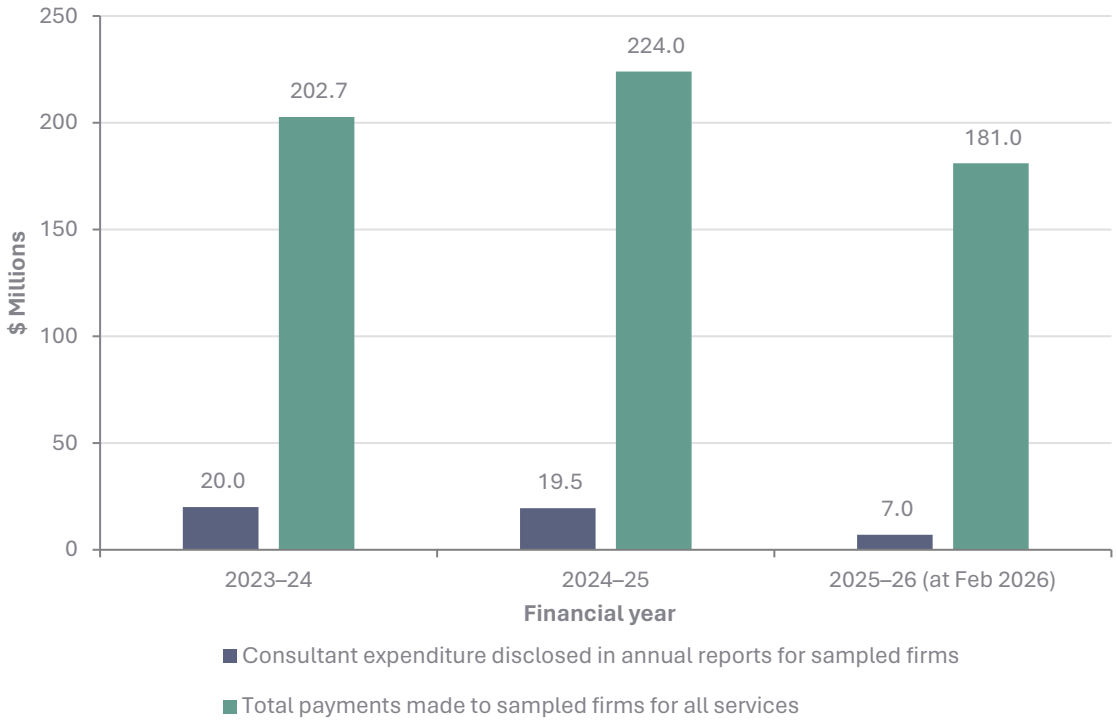
Agencies reported a decline in expenditure on consultants. Total consultancy expenditure reported in the NSW Government Total State Sector Accounts decreased from $193 million in 2022–23 to $78 million in 2024–25.

Suppliers of consulting services may also provide a range of other professional services beyond consulting, for example audit, business advisory, legal, IT and project management.

For example, from 1 July 2023 to 28 February 2026, the 26 agencies reported $46.6 million in expenditure on a sample of 85 suppliers engaged to provide consulting services. These suppliers provided $607.7 million in total services to the agencies over the period.

Figure 4 compares amounts classified as consulting expenditure with total payments to a sample of 85 suppliers who also provided consultancy services during the period 1 July 2023 to 28 February 2026.

Figure 4: Consultants expenditure versus total payments made to sampled firms (2023–24 to 2025–26)



Source: Annual reports and accounts payable data of the 26 agencies (unaudited). Consultant expenditure included in Figure 4 excludes $11 million of contracts with value less than $50,000.

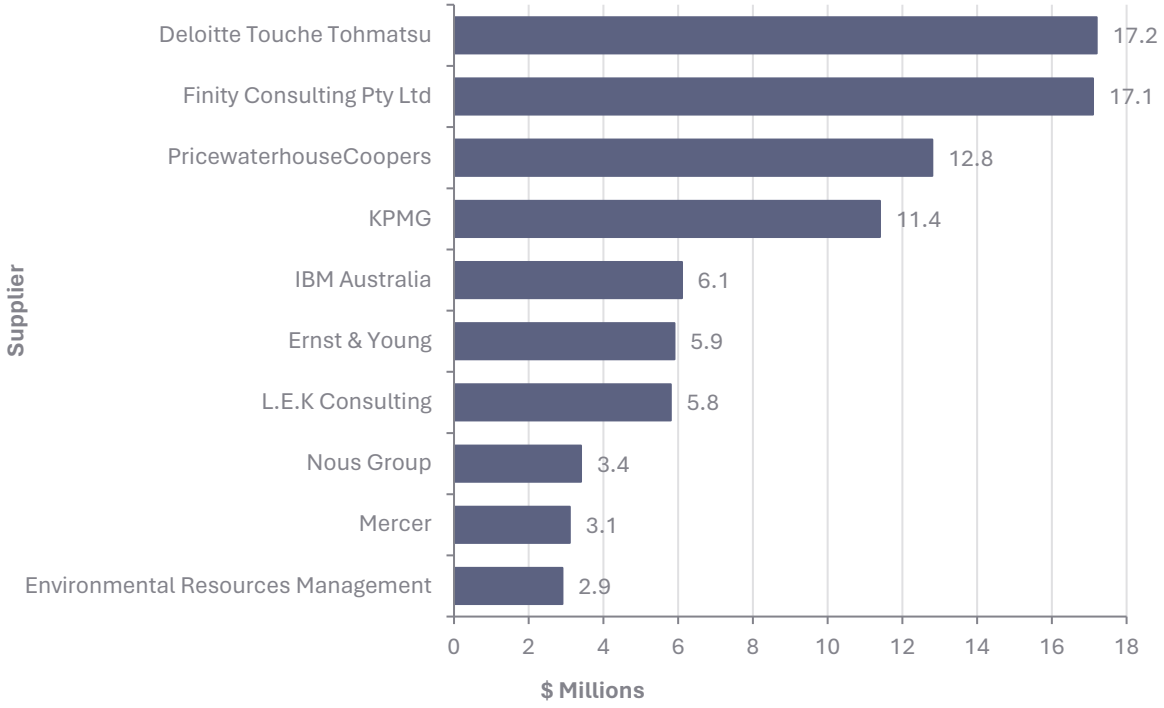
6.2. Engaging consultants

Almost half of expenditure on consultants was paid to 10 consultants

Since 2022–23, the 26 agencies paid $85.8 million or 45% of consultancy expenditure to 10 consultants.

Figure 5 shows the expenses across these consultants between 2022–23 and 2024–25. The amounts below exclude $20.4 million in expenditure for contracts valued at less than $50,000. Agencies are not required to disclose these arrangements separately in annual reports.

Figure 5: Spending on consultants by the 26 agencies on the top 10 consultants, 2022–23 to 2024–25



Source: Audit Office analysis of annual report disclosures of the 26 agencies (2022–23 to 2024–25).

As shown in the table below, the use of the highest paid consultants has changed since 2022–23.

Ranking of top 10 consultants by expenditure, by year, 2022–23 to 2024–25

Rank	2022–23	2023–24	2024–25
1	Deloitte Touche Tohmatsu	Finity Consulting Pty Ltd	Finity Consulting Pty Ltd
2	PricewaterhouseCoopers	Deloitte Touche Tohmatsu	KPMG
3	Finity Consulting Pty Ltd	IBM Australia	Deloitte Touche Tohmatsu
4	KPMG	Environmental Resources Management	L.E.K. Consulting
5	Ernst & Young	KPMG	Mercer

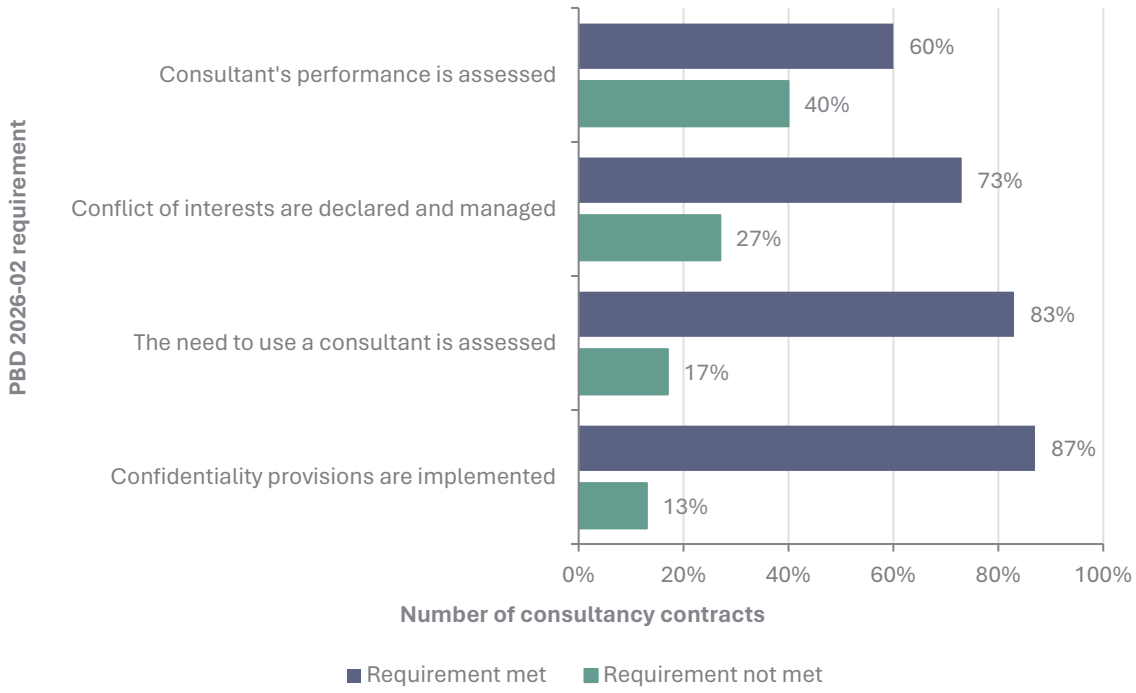
Source: Audit Office analysis of annual report disclosures of the 26 agencies (2022–23 to 2024–25).

Agencies are not engaging consultants in line with mandatory requirements

Analysis of 48 selected contracts for the period 1 July 2024 to 28 February 2026 at the 26 agencies identified that mandatory requirements of PBD-2026-02 were not fully met.

Figure 6 summarises compliance with PBD-2026-02 for the 48 selected contracts.

Figure 6: Consultant engagement practices across agencies



Source: Analysis of 48 selected consultancy engagements.

Consultant performance was not evaluated for 40% of contracts

PBD-2026-02 requires agencies to evaluate consultant performance throughout the engagement and on completion. For 40% out of selected contracts, agencies did not complete a formal evaluation nor:

- benchmark consultant performance
- document outcomes
- assess whether the intended benefits were realised.

Limited evaluation practices inhibit how an agency can determine if consultants met intended outcomes or achieved value for money. Lack of evaluations reduces the ability to inform future procurement decisions.

Agencies inconsistently managed conflicts of interest

PBD-2026-02 requires ongoing identification and management of conflicts. Agencies need procedures to uphold fairness, transparency and ethical conduct throughout the engagement and manage both actual and perceived conflicts of interest.

Twenty-seven per cent of selected contracts did not have evidence of formal conflict of interest declarations, limiting agencies' ability to monitor and manage risks.

Confidentiality provisions were not included in all consultancy contracts

Confidentiality clauses protect sensitive government information and provide enforceable controls over its use and disclosure by consultants. Agencies should tailor confidentiality provisions to the risks of the engagement, particularly where consultants have access to sensitive information. Analysis of the selected contracts identified 13% did not include confidentiality clauses, including where consultants had access to sensitive information.

17% of selected contracts did not contemplate alternative methods at the initial procurement decision stage

Not all agencies evaluated the need for a consultant during initial procurement decisions, indicating that they had not considered alternatives such as the use of internal capability. This increases the risk of consultants being engaged without sufficient justification, potentially leading to unnecessary costs and reduced value for money.

Consultants were often engaged in direct source procurements

Preferred supplier arrangements are pre-approved panels or schemes established by the NSW Procurement Board. These arrangements enable agencies to engage suppliers without conducting a full open-market tender process. For example, under the Performance and Management Services Scheme (SCM0005), for contracts less than or equal to $250,000 (excluding GST), agencies may directly engage an approved full prequalified supplier by inviting the supplier to provide one written quote. Half of the consultancy engagements analysed were conducted through preferred supplier arrangements. Of these engagements, 60% were awarded based on a single quote or following direct negotiation with a single supplier.

Further, of the contracts analysed:

- 2 agencies approved exemptions from their procurement policies to directly engage consultants
- 2 agencies directly engaged consultants that had previously performed similar work. This included the NSW Police Force, which entered into a $1.7 million engagement without a documented procurement approach.

While approved exemptions may be consistent with agency procurement policies, excessive reliance on exemptions can:

- reduce transparency in procurement decision-making
- increase dependence on sole suppliers, limiting competitive tension and potentially reducing value for money
- increase the risk of perceived or actual conflicts of interest.

6.3. Reporting of consultancy expenditure

Incomplete reporting of consultancy expenditure in annual reports

The Audit Office analysed a sample of payments from the 26 agencies made to suppliers who provided consultancy, as well as other services, between 1 July 2023 and 28 February 2026. The analysis identified at least $18.3 million in expenditure which were consultancy engagements but not reported as such by agencies in their 2024 and 2025 annual reports. These agencies include the Department of Education, Essential Energy, Ministry of Health and the NSW Land and Housing Corporation. We also identified $3.6 million in payments to suppliers in 2025–26 that were not classified as consultancy expenditure. Agencies have acknowledged this and will report the expenditure as consultancy expenditure in their 2026 annual reports.

Additionally, there were other contracts, which analysis undertaken by the Audit Office indicated may have met the definition of consultancy services but were not disclosed as such by the agency. While agencies disagreed with this assessment, several could not explain whether payments to these consultants were appropriately excluded from reporting. As a result, the extent of unreported consultancy expenditure may be greater than the amount identified.

Moreover, disclosures in 3 agencies' annual reports between 2022–23 and 2024–25 were lower than amounts reported in the agency's audited financial statements, indicating these agencies' annual report disclosures are incomplete.

6.4. Internal controls and governance over consultants

This section analyses the design and effectiveness of internal controls and governance related to consultants at 6 selected agencies. These agencies have the highest budgeted consultancy expenditure for 2025–26.

Plan, source and manage

Inconsistent engagement and management of consultants, limit agencies' ability to demonstrate value for money, build internal capability, and maintain effective oversight.

Not all of the Auditor-General's previous recommendations to improve the strategic management and engagement of consultants have been implemented

The Auditor-General's 2023 performance audit found most agencies engaged consultants on an ad hoc basis, without a strategic approach. The report made recommendations for all agencies to improve internal controls and governance relating to engaging and managing consultants.

The table below shows the extent to which the selected agencies revised policies, procedures and internal controls in response to selected recommendations.

Performance audit recommendation	Percentage of agencies which addressed recommendations (%)
Provide guidance for staff on when consultants should be used	50%
Conducting regular assessments of the quality of work done by consultants	67%
Use consistent approaches for transferring and retaining knowledge from consulting engagement	33%
Improve record-keeping practices to ensure all relevant documents relating to consulting engagements are retained in accordance with the *State Records Act 1998*	67%

Source: Audit Office analysis.

Agency policies do not align with mandatory requirements

Not all of the selected agencies align their policies with mandatory requirements outlined in PBD 2026-02, including:

- only half mandate staff to document the need to engage a consultant rather than alternatives
- 67% provide no guidance to keep consultancy engagements to the minimum duration
- 83% do not require clear identification of consultants in email and security systems or organisational directories
- 67% do not restrict consultants from decision-making authority in recruitment or selection processes.

Core work

Core Work policy requirements have not been translated into operations

Three of the 6 selected agencies were required to comply with the Core Work Policy. The accountable authority is responsible for setting targets to reduce reliance on external resources for core work. While all 3 agencies developed plans and targets, they did not consistently:

- identify affected roles or classifications
- incorporate the principles of the Core Work Policy objectives into their procurement or consultancy engagement policies and procedures.

The absence of clear policies, procedures or guidance limits agencies' ability to direct officials and ensure compliance with requirements.

7. Purchasing cards

Purchasing cards can be an efficient means of payment for agencies for low value and high volume transactions, though carry risks around acceptable use. Purchasing cards include physical purchasing cards and virtual card arrangements. Purchasing cards are a type of credit card used for government purchasing.

This chapter examines the extent to which agencies implemented effective internal controls and governance over purchasing cards, by:

- analysing purchasing card expenditure across all 26 agencies from 1 July 2023 to 28 February 2026
- assessing whether the frameworks of 6 selected agencies align with NSW Government mandatory and recommended requirements. The agencies were selected to reflect a range of agency sizes and expenditure.

7.1. Context

Purchasing cards are now a significant part of the NSW Government's procurement processes. There are approximately 42,500 purchasing cards issued by the 26 agencies as at 28 February 2026. The agencies advise expenditure on purchasing cards from 1 July 2023 to 28 February 2026 comprised 5.7 million transactions, totalling $2.3 billion.

Use of purchasing cards must comply with NSW Treasury's mandatory requirements

NSW Treasury has minimum requirements relating to the use of purchasing cards. TPG24-01 *Management of NSW Government Payments* applies to all agencies under the *Government Sector Finance Act 2018*. It sets out requirements for making payments to vendors and suppliers and requires agencies to use purchasing cards for ad hoc, low value supplier payments up to $10,000.

TPP21-02 *Use and Management of NSW Government Purchasing Cards* (TPP21-02) establishes core requirements and provides operational guidance to help agencies establish and maintain an effective, efficient and appropriate use of purchasing cards. This includes:

- The accountable authority is ultimately responsible for the proper management and administration of purchasing cards within the agency.
- Cardholders understand and are accountable for the responsible use of purchasing cards.

TPP21-02 also emphasises that agencies should have effective preventative and detective controls.

7.2. Expenditure

Cardholders must ensure that purchasing cards are used responsibly. Key to this responsibility is that purchasing cards should not be used for non-official purposes or to circumvent established controls.

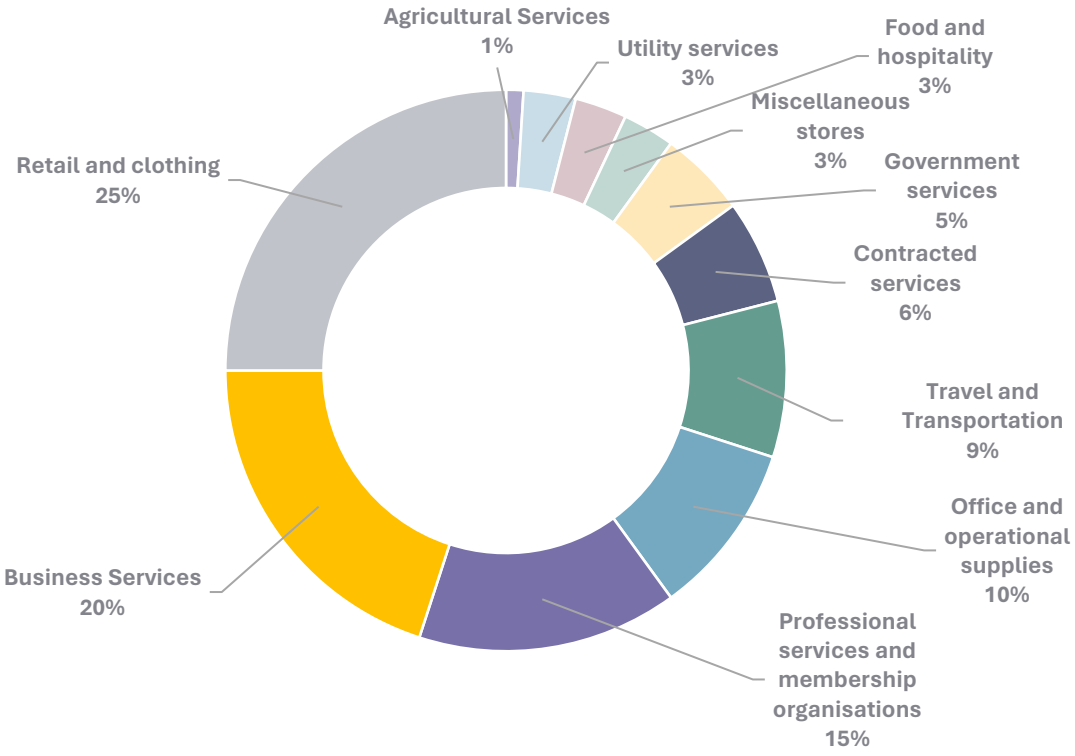
This section provides insights into the result of analysis of purchasing card expenditure from 1 July 2023 to 28 February 2026 for the 26 agencies. The analysis was undertaken applying data analytics to identify usage trends and at-risk transactions.

Purchasing cards are mainly used for low value transactions, including office supplies, travel and food, attracting a higher risk of misuse

Purchasing cards generally used for purchases below $10,000. Analysis of expenditure indicates that officials use cards for low value purchases such as food, supplies and travel. These categories are at a higher risk of misuse as judgement is required as to what constitutes an acceptable official expense. As a result, agencies need effective preventative and detective controls to confirm purchasing card transactions are for official purposes.

Figure 7 below shows purchasing card transactions by merchant category.

Figure 7: Purchasing card expenditure by merchant type, 1 July 2023 to 28 February 2026



Note: Purchasing card expenditure is classified by merchant category codes (MCCs), a 4-digit code that identifies a vendor's primary line of business. Some vendors operate across multiple lines of business; however, the MCC reflects the vendor's registered primary business activity. Some agencies were unable to provide MCC information for all transactions. The analysis was performed on transactions for which MCC information was available.

Source: Agencies' purchasing card transactions – 1 Jul 2023 to 28 Feb 2026.

For the 2-year period ended 28 February 2026, our analysis identified approximately $18 million in transactions that may be appropriate, but which could represent purchasing card misuse and raise questions about their official purpose. These transactions included purchases from vendors associated with:

- gift cards ($12.9 million)
- entertainment services ($4.3 million)
- alcohol and tobacco products ($0.5 million).

Some expenditure with these vendors may be for official purposes. For example, the Department of Communities and Justice issues gift cards as a form of payment to vulnerable members of the community through child protection and disaster welfare programs.

However, the existence of these types of transactions on purchasing cards highlights the importance of cardholders providing evidence to demonstrate the official purposes of such transactions, and of agencies having clear guidance on prohibited expenditure and merchant categories. In some cases, agencies advised that some of the transactions were fraudulent charges involving stolen credentials or were reimbursed by cardholders.

Approximately 7% or just over 374,000 transactions were incurred on weekends. Weekend use may be required due to operational needs, however warrants consideration of its purpose to confirm it is an acceptable official expense.

Personal and non-compliant transactions were incurred on purchasing cards

Between 1 July 2023 and 28 February 2026, the agencies assessed 2,761 transactions or $173,000 as non-official or non-compliant with agency policies. These required reimbursement by the staff member.

Data analytics undertaken as part of interim audits also identified transactions incurred for personal purposes or without sufficient evidence to support that it was incurred for an official purpose. Some of these transactions were approved by a line manager as part of acquittal purposes as being consistent with acceptable use, others had also been identified by agencies and a reimbursement sought from the card holder. Transactions identified included:

- personal or non-official transactions
- purchase of gift cards, despite an agency's prohibition of these transactions
- expenditure on minor equipment and technology where there was insufficient information included in an acquittal to confirm an official purpose.

Where these transactions were approved as part of an acquittal, this could indicate there are deficiencies in the primary detective control designed to confirm expenditure is appropriate and only for official purposes. When approving acquittals and transactions, line managers should have regard for the type of transaction and ensure that the evidence provided verifies official purposes.

Split payments indicate that limits are being circumvented

Data analytics undertaken also identified instances of intentional invoice splitting at 13 agencies. Invoice splitting refers to where a single purchase is divided into multiple transactions to bypass transaction limits or approval thresholds. Splitting of transactions may indicate deliberate circumvention of procurement processes, controls and delegation which may apply to higher value or higher risk procurements. Split transactions may indicate an increased risk of inappropriate and unauthorised expenditure.

High-value purchases are being made on purchasing cards

TPG24-01 requires agencies to use purchasing cards for supplier payments of up to $10,000. Alternative payment methods should be considered for supplier payments exceeding this amount. Between 1 July 2023 and 28 February 2026, approximately 9,350 transactions totalling $137 million exceeded $10,000. The largest identified transaction was $199,330.

The use of purchasing cards for transactions above $10,000 increases compliance and governance risks. Higher-value purchases typically warrant greater procurement oversight and scrutiny, increasing the potential for inappropriate, unauthorised or non-compliant expenditure.

7.3. Acquittals

Purchasing card acquittals verify that transactions are for official purposes, correctly allocated and compliant with agency policies. Acquittals are generally subject to a review by an official's line manager.

One in 5 purchasing card transactions are not acquitted and approved within 30 days

TPP21-02 recommends that purchasing card acquittals be completed within 30 days, with review and approval by a line manager. From 1 July 2023 to 28 February 2026 approximately $350 million or 21% of transactions took longer than 30 days to be acquitted. Just over 7% of transactions took more than 60 days.

The table below summarises the time taken for purchasing card acquittals to be submitted and approved.

Time taken to prepare and approve purchasing card transactions across all agencies	Percentage of total purchasing card transactions (%)
Less than 30 days	79%
31 – 60 days	13%
61 – 90 days	3%
91 – 365 days	4%
More than 1 year	1%

Source: Audit Office analysis of agencies' purchasing card transactions – 1 Jul 2023 to 28 Feb 2026.

Delays in acquitting purchasing card transactions reduce agencies' ability to detect problematic transactions. There is a risk that:

- inappropriate expenditure, non-compliance, or errors will not be identified in a timely manner
- transactions cannot be disputed or recovered.

7.4. Internal controls and governance over purchasing cards

Effective policies, procedures and internal controls guide staff on how to comply with TPP21-02 and set expectations for the appropriate use of purchasing cards. Detective controls over purchasing card transactions help agencies identify misuse, non-compliance or unusual spending.

This section analyses the design and effectiveness of internal controls and governance related to purchasing cards at 6 agencies, selected to reflect a range of agency types and expenditure.

Policies, procedures and risk management

Agencies' procedural guidance on prohibited transactions and transaction splitting should be clearer

All of the selected agencies have policies and procedures to guide purchasing card use. Most agencies have processes for periodic review.

TPP21-02 recommends that agencies ensure cardholders understand and are held accountable for the responsible use of purchasing cards. Analysis of the selected agencies' policies and procedures indicates that guidance for officials could be improved by providing more clarity over:

- Prohibited transactions. All agencies specified some prohibited transactions or merchant categories. However, the way in which these were articulated differed in detail and clarity. Some agencies provide comprehensive lists of prohibited transactions, while others relied on broader descriptions such as personal or non-official purchases. Examples of prohibited expenditure identified include cash withdrawals, gift cards, entertainment and purchases that circumvent established procurement processes.
- Invoice splitting.

Integration of risks related to purchasing cards into enterprise risk management frameworks is limited

TPP21-02 requires agencies to identify and manage purchasing card risks consistent with their risk management framework. Formal identification of purchasing card risks boosts visibility at the enterprise level and supports effective monitoring and mitigation.

Only one of the 6 agencies captures purchasing card risks in its enterprise risk register, including those risks identified in TPP21-02, such as inappropriate use.

Some agencies had not conducted an internal audit of purchasing cards in the past 3 years in line with better practice

TPP21-02 recommends regular internal audits of purchasing card controls. Internal audits can provide assurance over the effectiveness of controls and governance arrangements, and help identify inefficiencies or non-official expenditure. Two selected agencies have not undertaken an internal audit on purchasing cards use since 2023.

Inadequate training may heighten the risk of inappropriate use, fraud and loss

TPP21-02 requires agencies to provide training to cardholders at induction or before issuing a purchasing card. Training builds cardholder understanding of their responsibilities, accountability and policy requirements, reducing the risk of misuse. Two agencies did not require staff to undertake training on purchasing cards prior to issuance.

Data analytics

TPP21-02 recommends using detective data analytics to identify potential fraud and non-official transactions, including but not limited to unusual spending patterns, suspicious merchants, duplicate transactions and transactions outside normal business activities.

Use of data analytics to oversight transactions is inconsistent

The extent and maturity of data analytics vary across the 6 selected agencies. Two agencies did not use data analytics. Other agencies limit analysis to expenditure coding checks or a narrow focus on specific risks, such as identifying dormant cardholders or duplicate transactions. Two agencies apply more targeted data-driven techniques, identifying and targeting risks specific to that agency.

The case study below illustrates one agency's approach to data analytics.

Case study 2 - Better practice data analytics used to detect irregularities in purchasing card transactions

The Department of Customer Service performs periodic audits to detect errors and potential fraud in purchasing card transactions. Using an analytics tool, its internal audit team reviews a range of risk indicators, including:

- active cards held by inactive employees
- transactions exceeding individual transaction limits
- potential split transactions and duplicate transactions within purchasing card data
- monitoring cardholders with recurring direct debit charges
- transactions linked to restricted or unapproved purchasing card expense categories
- inactive cards held by employees
- transactions missing supporting documentation
- delayed submissions and approvals
- multiple active cards held by the same employee.

Results are provided to line managers for investigation.

Card limits

Most agencies did not undertake regular reviews of purchasing card limits

TPP21-02 requires agencies to establish, embed and regularly review their purchasing card frameworks. Regular reviews support alignment with genuine needs and delegated authority levels. Four of the 6 selected agencies did not have policy requirements to regularly assess whether limits are appropriate.

8. Technology - Cyber security

Agencies submit an annual cyber security attestation to Cyber Security NSW, detailing the extent of their compliance with the NSW Cyber Security Policy for the previous financial year. This chapter analyses the self-assessed compliance of all agencies with the policy using data in annual attestations for 2024–25.

For 10 selected agencies, the chapter also analyses:

- the effectiveness of attestation preparation, including robustness of evidence and assurance over assessed compliance
- how entities address gaps identified through attestations, specifically those relating to legacy systems.

The 10 agencies represent a range of technology environments and levels of complexity, including some that provide shared services to other agencies.

8.1. Context

Cyber Security NSW aims to strengthen cyber resilience across all entities. Its Cyber Security Policy specifies mandatory requirements for agencies which are also recommended for state owned corporations.

There are 31 mandatory requirements, divided into 114 detailed requirements, grouped into 3 domains:

- govern and identify
- detect, respond and recover
- protect.

By 31 October each year, agencies must report to Cyber Security NSW on the extent of their compliance with the policy, cyber security risks (with a residual rating of high or extreme), and an attestation on cyber security.

In July 2026 Cyber Security NSW released a new revision to the policy. Key changes include more detailed requirements for agency heads to attest to approval of non-compliance, increased requirements for oversight and management of third-party suppliers, and guidance covering AI and quantum computing.

Leaders of the cyber security agencies in Australia, Canada, New Zealand, the UK and the US (collectively the 'Five Eyes' security alliance) warn that AI is fundamentally transforming cyber security and accelerating the speed, scale and sophistication of cyber threats. Their recommended areas of focus align with areas where many NSW agencies did not meet minimum cyber security policy requirements.

Cyber Security NSW also highlights the heightened risks from AI in its 2026–2028 Cyber Security Strategy and its advisories to agencies.

8.2. Cyber security attestation results

The February 2024 update of Department of Customer Service Circular DCS-2021-02 for the NSW Cyber Security Policy stated:

> Agencies are not expected to have fully met all Mandatory Requirements in the 2023–2024 financial year of NSW Cyber Security Policy reporting. This reporting year is intended to be a transition period and will serve as a baseline only.

The data for 2025 shows that mandatory requirements are not fully implemented in most cases.

Cyber Security will be the subject of a future performance audit, as detailed in the Audit Office Audit Work Plan 2026–2029.

Insufficient levels of compliance with Cyber Security Policy requirements

As indicated in the figure below, less than half the agencies self-assessed that they comply with the 'govern and identify' and 'protect' domain mandatory requirements.

Figure 8: Compliance with CSP mandatory requirements

Note: percentage displayed above refers to self-assessed compliance rate of the Mandatory Requirements across all 71 reporting agencies in 2024–25. In our analysis, Mandatory Requirement is considered compliant when all the detailed requirements within it are compliant. Mandatory Requirements with mixed Detailed Requirement ratings are generally treated as partially compliant. 'Not Applicable' ratings, which require Cyber Security NSW approval, are treated as neutral. Requirements managed by third parties were not assessed by agencies and are therefore shown separately where it was not assessed.

Source: Audit Office analysis of agency cyber security compliance returns to Cyber Security NSW for 2025.

Most agencies did not comply with 'govern and identify' domain controls

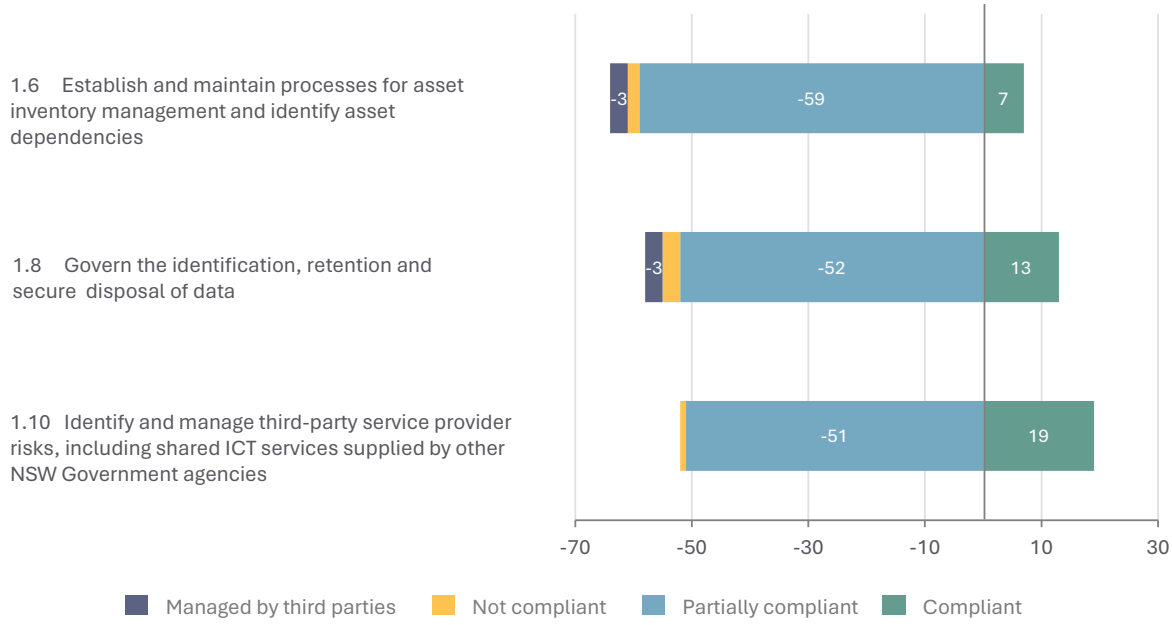
Controls in the 'govern and identify' domain relate to understanding IT assets, their dependencies, governance of cyber security, data identification retention and disposal and management of third-party relationships. In 2024–25, 43% of agencies reported that they were compliant with the mandatory requirements.

Weak asset visibility, poor data lifecycle management and limited oversight of third-party cyber security controls can leave agencies with:

- unmanaged or unprotected assets
- weaker safeguards for sensitive information
- greater exposure to data breaches
- slower responses to vulnerabilities.

Figure 9 below, identifies the 3 least compliant requirements in the 'govern and identify' domain cover IT asset inventory, disposal of data and management of third-party relationships.

Figure 9: Number of reporting agencies meeting the 3 least compliant requirements in the 'govern and identify' domain



Source: Audit Office analysis of agency cyber security compliance returns to Cyber Security NSW for 2025.

Overall, poor compliance with the 'govern and identify' domain may result in incomplete or ineffective cyber security implementation across an agency.

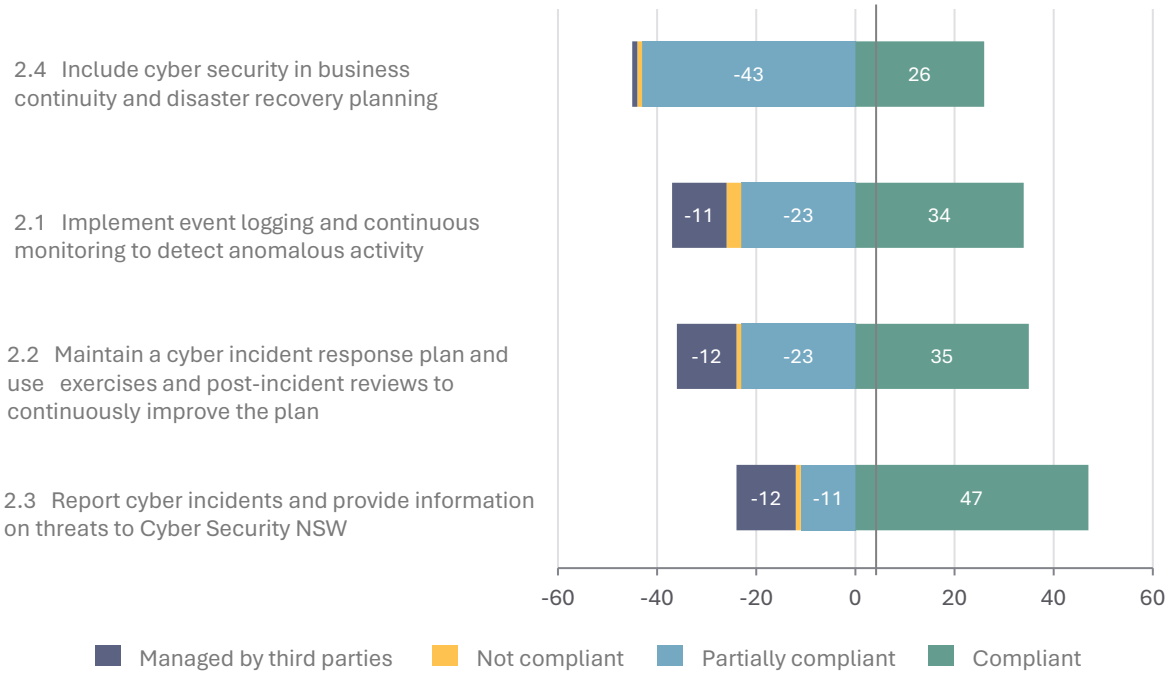
Half of the agencies comply with 'detect, respond and recover' domain

Controls in the 'detect, respond and recover' domain relate to cyber security event logging, monitoring and incident response. In 2024–25, 50% of agencies complied with mandatory requirements.

Weaknesses in event logging and monitoring reduce visibility of potential cyber incidents. Gaps in business continuity, disaster recovery and incident response planning weaken the timeliness and effectiveness of actions taken during and after an incident.

Figure 10 below demonstrates the compliance of agencies in meeting ‘detect, respond and recover’ mandatory requirements.

Figure 10: Number of reporting agencies compliant with all 4 of the 'detect, respond and recover' mandatory requirements



Source: Audit Office analysis of agency cyber security compliance returns to Cyber Security NSW for 2025.

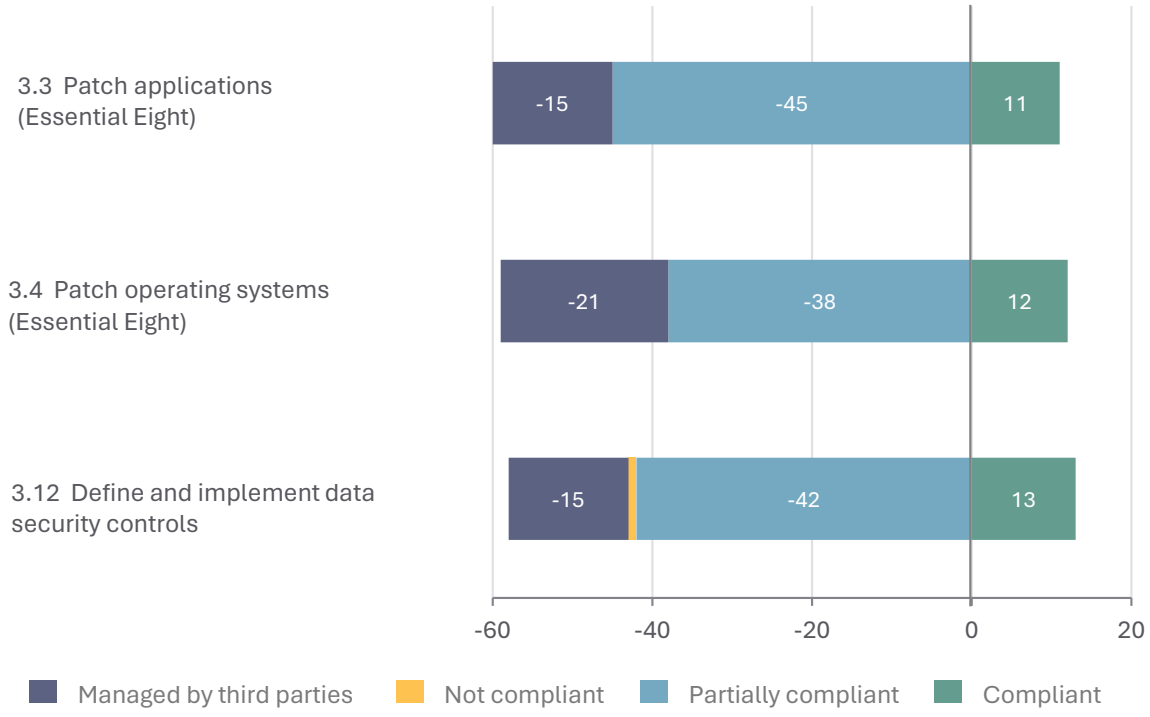
Most agencies did not comply with ‘protect’ domain controls

Controls in the ‘protect’ domain aim to prevent cyber security incidents. Controls cover requirements to implement the ACSC Essential Eight, network security controls and cyber security training. In 2024–25, only 33% of agencies complied with mandatory requirements, with a further 22% stating that a third party manages that requirement.

Weaknesses in patching and data security controls can leave system vulnerabilities and data protection gaps unresolved, increasing the likelihood of a cyber-attack.

Figure 11 below indicates the 3 least compliant requirements in the 'protect' domain cover patching applications and operating systems and implementing data security controls.

Figure 11: Number of reporting agencies meeting the 3 least compliant requirements in the 'protect' domain



Source: Audit Office analysis of agency cyber security compliance returns to Cyber Security NSW for 2025.

Agencies do not report control compliance when performed by third parties

Some mandatory requirements are performed by a third party, which may be another government agency or shared service, or may be a private company.

Third-party compliance with mandatory policy requirements may be known to the agency but does not need to be reported to Cyber Security NSW. These are reported as 'managed by a third party' rather than as either implemented or not implemented. While agencies may outsource services and technology, they retain accountability for the effective management of associated risks.

The highest level of third-party reliance not reported or assessed against policy requirements is in the 'Protect' domain.

The absence of transparent reporting on controls managed by third parties could increase the risk that agencies and Cyber Security NSW do not know about non-compliance with the policy.

Aggregated reporting could mask issues at individual agencies

The number of agencies that report to Cyber Security NSW does not reflect the actual number of agencies responsible for cyber security. Agencies that operate a common technology environment and substantially share infrastructure and services are permitted to report at an aggregate level.

The 110 reports to Cyber Security NSW in 2020–21 declined to 71 reports (for 189 agencies) in 2024–25.

	FY2021	FY2022	FY2023	FY2024	FY2025
No. of reporting agencies	110	112	110	66	71

Source: Audit Office analysis of agency cyber security data returns to Cyber Security NSW for 2021–2025.

This reduction reflects changes in aggregated reporting at a portfolio level instead of an individual agency level. Aggregated reporting could hinder transparency of individual agencies or obscure uniquely weak cyber control compliance. This is especially so where responsibility for cyber security in portfolios of agencies is mixed or unclear.

Agencies report 128 significant, high and extreme residual cyber security risks

Of the 71 reporting agencies, 33 reported 128 cyber security risks with a significant, high and extreme residual risk. Agencies define these risk categories differently; generally high risk means there is an impact on a critical agency function, whereas extreme is an impact on the entire agency's operations.

Accuracy of cyber security attestation results

Reviews of attestations did not always validate all policy requirements or draw from evidence

Agencies may engage external parties or an internal function to assess policy compliance in response to CSP requirements aimed at achieving a more robust assurance, validation and evidence based reporting model. We observed a mix of assurance practices:

- 2 agencies engaged a third-party service provider to obtain independent assurance
- 4 self-assessed compliance using their IT governance, risk and control team or the cyber security team
- 4 combined these approaches, either by dividing review scope between internal and external reviewers or performing self-assessment with support from a third-party provider.

Agencies did not always base their assessment on sufficient evidence for all requirements. Two self-assessing agencies told us they validated evidence only for requirements that were self-assessed as 'compliant'. This reduces confidence in accurate assessment of partial compliant requirements, including which parts were met and which were not.

Agencies did not always capture all required evidence

The policy specifies that 'agencies must compile and retain, in accessible form, evidence that demonstrates the basis of their assurance assessment'. Nine of the selected agencies compiled and retained evidence to support their policy assessments.

From these agencies, we selected a sample of the detailed requirements to assess evidence compiled by agencies. Four agencies could not provide full evidence to support their assessment, therefore we could not validate the accuracy of the ratings for all the selected sample. The policy requires agencies to retain auditable evidence against all mandatory requirements.

The absence of sufficient evidence is not consistent with policy requirements. Gaps in documentation could indicate that assessments are incomplete and that agencies' determination of their cyber security maturity may not be accurate or reliable.

8.3. Actions to address deficiencies in controls

Remediation strategies indicate some agencies at least 4 years away from compliance

Agencies typically incorporate remediation plans into their cyber security and/or technology strategies and outline the activities required to achieve full compliance with policy requirements assessed as partially met or non-compliant. All 10 agencies have identified the stakeholders for the uplift program including their roles and responsibilities.

Remediation plans generally include implementation timeframes from a few months to 4 years. Information on prioritised remediation activities is based on risk and available funding and/or resourcing.

The remediation plan timeframes indicate full compliance with the Policy is at least 4 years away for some agencies.

Agencies need to address legacy systems and compensating controls for systems that can no longer be patched

Legacy systems often support critical operations while introducing operational and cyber security risk. It presents an asset lifecycle management, risk acceptance and compensating control challenge. Without clear inventories, formal risk assessments, compensating controls or plans for upgrades, replacement or decommissioning, agencies may be unable to manage these risks.

Analysis of the 10 selected agencies identified:

- all 10 agencies maintain an inventory of legacy systems in use, however not all of them recorded this information in a centralised listing
- 3 have not formally assessed the risks associated with each legacy system, although most have an approved strategy to upgrade, replace or decommission of these systems
- 2 agencies have not formally assessed and implemented compensating controls to mitigate risks from legacy systems that can no longer be updated or patched
- approaches from agencies that have implemented compensating controls vary depending on the systems, including measures such as network segmentation, system isolation and restricted access.

9. Technology - Artificial intelligence

The NSW Government is implementing a policy framework aimed at establishing safe, ethical and effective use of AI across agencies.

This chapter examines whether appropriate governance, risk and assurance mechanisms are in place in line with the NSW Government's policy and framework. The analysis covers 10 selected agencies that have the highest AI use or greatest potential benefit, while also providing assurance across a range of entities.

9.1. Context

Digital NSW defines AI as 'the ability of a computer system to perform tasks that would normally require human intelligence, such as learning, reasoning, and making decisions. AI encompasses various specialised domains that focus on different tasks.' Examples include generative AI, machine learning, chatbots and virtual assistants.

Agencies expect AI use to continue to grow. At the 10 agencies current uses of AI include:

- productivity and workflow improvement, including workforce planning
- analysis of data, documents, images and videos to identify patterns, events and summaries
- AI assistants and chatbots
- learning and development support
- cyber security.

Agencies need robust governance frameworks to guide the development, deployment and oversight of AI to safeguard ethical standards, uphold integrity and meet public expectations.

The NSW AI Operational Policy was issued in July 2026, replacing the NSW Ethics Policy which was in effect during the period of this audit.

The NSW Government's AI Framework now consists of:

- AI Strategy which sets direction
- NSW AI Operational Policy which mandates requirements
- NSW AI Assessment Framework which is the process for assessing risks in AI projects
- AI Review Committee which advises on high risk AI uses.

DCS-2026-02 - *Use of Artificial Intelligence by NSW Government Agencies* mandates compliance with the Operational policy, including the requirements to adhere to Australia's AI Ethics Principles when using AI and to apply the AI assessment framework.

The Office of AI advised that the new NSW AI Operational Policy will improve some of the matters raised in this report.

NSW government agencies' use of Artificial Intelligence is the subject of a performance audit, as detailed in the Audit Office Audit Work Plan 2026–2029.

9.2. Adoption of AI

Risks can be mitigated in AI program design

The case study below demonstrates the application of the NSW Government's AI Framework and how AI risks can be mitigated by effective controls in program design.

Case study 3 - Using AI to detect seatbelt offences

Background

In July 2024 Transport for NSW introduced automated enforcement of seatbelt offences, building on mobile phone detection camera processes and infrastructure. This uses AI elements to recognise patterns in photographs and make probabilistic classifications to determine if the image shows an infringement of seatbelt laws. A private company that works with other jurisdictions provides this AI-enabled process.

Applying the NSW AI framework

This project was among the first to be subject to the AI Review Committee under the NSW AI Assessment Framework. The framework builds on the NSW AI Ethics Policy principles:

- community benefit
- fairness
- privacy and security
- accountability
- transparency.

Community benefit

The starting point should not be whether AI is available, but whether using it is in the public benefit

Manual enforcement alone could not achieve the objectives of reducing deaths and serious injuries caused by improper seatbelt use. The automated solution enables scanning of over 100 million trips and aims to reach close to 100% of NSW drivers each year.

Transport for NSW considered academic research indicating that high levels of detection and enforcement will increase compliance and that automated enforcement would be suitable and appropriate. They also engaged Monash University Accident Research Centre to model the outcomes of the program, which gave an estimated prevention of 17-26 fatalities and 41-62 serious injuries over 5 years.

Privacy and security

Agencies should build in privacy and security as a foundational requirement and enforce compliance throughout the lifecycle

Transport for NSW already used images to enforce road rules and understands legal and privacy considerations. It developed controls with internal legal teams and the Privacy Commissioner and built privacy protections into requirements, and the procurement and contract. It identified legislative modifications early, such that amendments passed in 2023 ahead of the program commencing in mid-2024.

Privacy controls ensure:

- Most images are never seen by a human.
- Images that do not indicate offences are deleted promptly and permanently.
- Images escalated for human review are cropped to retain only those parts of the image relevant to the offence.
- Reviewed images are cropped and pixelated to remove identifying information.
- Additional pixelation may be applied to faces to remove identifiable features of the occupants.
- Access to images is restricted to authorised and trained staff.

Accountability

AI should support decision-making, not replace it

The AI system performs an initial filtering role only. At least 3 human decision-makers review all potential offences before an infringement is issued. Potential offences can be rejected if a human reviewer does not observe the offence is shown in the images. The final decision to issue a penalty remains with the trained Revenue NSW officers. Drivers can request a review of their penalty through Revenue NSW.

Transparency

The public should be able to understand the AI data and methodology and challenge decisions based on AI

Transport for NSW has published how the enforcement works, including YouTube videos covering every stage of the process.

Existing review rights remain, and infringements are accompanied by documentation on how to contest or ask for a review of the infringement. Individuals can elect to have the matter heard in court. Decisions can be challenged and corrected, and accountability remains with human decision-makers.

Ongoing monitoring and improvement

Transport for NSW monitors the effectiveness of the process and oversees and manages ongoing risks through regular audits, tracking of metrics and comparing data across several sources to identify trends in the AI-enabled process, complaints and other indicators.

Early data suggests the program is improving compliance with seatbelt rules. Transport for NSW communicates the results of monitoring through awareness programs to complement the enforcement activity.

Insights

- AI creates additional governance requirements. These are developing over time but broadly converge on the principles covered under the NSW AI Framework.
- The principles for governing AI are also features of good public administration. The presence of AI may increase the need for discipline, but the underlying principles apply to any program that affects people's rights, obligations or access to services.
- The practical lesson for agencies is to build these controls into program design from the start.

Agencies report challenges and barriers that hinder effective AI adoption

The 10 selected agencies identified challenges and barriers to the adoption and use of AI:

- **Governance, policy and ethical frameworks**. Agencies face challenges in establishing and maintaining effective AI governance, including developing policies, frameworks and ethical guardrails that keep pace with rapidly evolving technology and regulatory requirements. The responsible adoption of AI is complicated by a lack of coordinated approaches, clear decision-making structures, and defined roles and responsibilities.
- **Data sensitivity, security and quality**. Managing sensitive information, such as personal or community-impacting data, is a major barrier. Agencies struggle with data classification, privacy, data loss, and maintaining high data quality and availability for AI systems.
- **Education, skills and change management**. Limited AI literacy, training and staff understanding hinder responsible and effective use. Agencies report challenges in engaging staff in professional learning, managing workforce impacts, and ensuring employees understand the risks and capabilities of AI tools, including public or unauthorised generative AI tools. Rapid advances in AI increase the challenge.
- **Integration with legacy systems and operational complexity**. Integrating AI into existing, often fragmented or legacy IT systems presents technical and operational challenges. Agencies must manage change across processes and workflows, balance productivity with transparency and safety, and consistently apply AI to business needs.

Some agencies lack oversight of the AI they have adopted

There are gaps in the completeness of the selected agencies' AI registers. Six agencies capture all AI use, while 4 capture only AI use assessed under the framework. While not captured, these AI uses may warrant greater oversight without this assessment. Further risks exist with agencies needing to understand third party use of AI on their behalf, and the use of unapproved AI solutions.

A complete inventory of AI solutions will build transparency, oversight and accountability. It will give agencies a complete view of current or planned AI technologies, and increase their ability to confirm that governance arrangements are fit for purpose.

Most agencies did not centrally track the cost or set budgets for AI solutions. AI cost models are evolving rapidly, and are trending towards consumption-based pricing models driven by token usage (representing compute power used) rather than per-user licencing models. Token prices and usage can be volatile which may result in unexpected costs to agencies.

The Auditor-General's *Internal controls and governance 2025* report recommended agencies create a central AI inventory to document its purpose, uses and limitations for transparency, oversight and accountability.

Greater use of the NSW AI Assessment Framework would support responsible AI usage

The framework aims to ensure AI solutions are designed, built and operated with a strict adherence to the mandatory AI Ethics Policy.

Of the 15 selected projects (10 below $5 million and 5 above $5 million):

- 13 had the framework performed against them
- 2 did not use the framework assessment as it was not in place when AI solution was implemented
- 4 did not perform a cyber risk assessment

The framework requires its application across the AI solution lifecycle. This means existing AI solutions need to be assessed as part of the ongoing governance of all AI solutions.

These gaps reduce confidence that agencies have adequately assessed the reliability, security and appropriateness of the AI tools implemented.

Half the agencies have a strategy to help maximise the benefits of AI

While the agencies have already implemented AI and plan to expand its use, only half the selected agencies have a formal AI strategy. A greater focus on the strategic use of AI could help maximise benefits from AI and ensure alignment with agencies' objectives.

9.3. Governance for the responsible use of AI

All selected agencies use AI but only half have an AI policy

Some agencies are developing or reviewing policies; others rely on the AI Ethics Policy. While the AI Ethics Policy sets out overarching principles, it is not sufficient; agency-level policy is required to deal with elements specific to that agency, including:

- policy ownership, scope and application
- roles and responsibilities, including internal review processes for new use cases
- compliance and internal reporting requirements, including how and to whom to report misuse or concerns.

The Auditor-General's *Internal controls and governance 2025* report recommended agencies establish and implement an AI policy and embed the consideration of AI use into governance frameworks.

AI adoption is outpacing the establishment of effective governance arrangements

Agencies need to more effectively integrate AI considerations into their governance frameworks to:

- evaluate AI's broader impacts on accountability structures, policies and procedures (such as IT, procurement, risk management)
- adequately train staff to take advantage of AI and ensure its responsible use.

The table details the governance over the adoption and use of AI by agencies, focusing on whether agencies have considered the specific and unique risks posed by AI.

Element	Details	Number of agencies that have considered the element (out of 10 selected agencies)
Accountability	While exact responsibilities may differ, generally, an overall owner is responsible for the deployment, ethical use and maintenance of AI solutions and that the solutions align with the agency's objectives and legal and regulatory standards.	**10** Ownership of each AI use case and its lifecycle may remain with the relevant business or product owner.
Risk management	Reviewing an agency's risk management framework when adopting and rolling out AI introduces new, complex and evolving risks that traditional frameworks may not adequately address.	**5**
Procurement	While not mandatory for the NSW public sector, the National framework requires careful consideration of procurement documentation and contractual arrangements	**1**
IT	AI may require revisions to IT policies and procedures, including enhanced pre- and post-implementation testing protocols to identify and mitigate potential risks associated with AI systems, such as unintended biases and vulnerabilities.	**4**
Training	Training in the responsible use of AI will help to ensure ethical AI use within agency requirements, enabling agencies to maximise benefits and minimise risks.	**8**
Reporting process	Regular reporting to senior management or governance bodies ensures ongoing oversight of AI adoption, aiding strategic alignment, risk management and transparency.	**7** reported regularly **3** ad hoc reporting at project level

Appendix 1 – Agencies included in this report

This report includes the largest 26 NSW public sector agencies. These agencies are included in this report as they:

- collectively account for approximately 91% of the NSW Government's 2025–26 total budgeted expenditure
- deliver a diverse variety of services and are exposed to numerous financial, operational and strategic risks.

The table below lists the agencies which are included in this report.

Agencies included in this report
Corrective Services NSW
Department of Climate Change, Energy, the Environment and Water
Department of Communities and Justice
Department of Creative Industries, Tourism, Hospitality and Sport
Department of Customer Service
Department of Education
Department of Planning, Housing and Infrastructure
Department of Primary Industries and Regional Development
Essential Energy
Fire and Rescue NSW
Insurance and Care NSW
Lifetime Care and Support Authority of New South Wales
Ministry of Health
New South Wales Treasury Corporation
NSW Land and Housing Corporation
NSW Police Force
NSW Reconstruction Authority
NSW Self Insurance Corporation
NSW Treasury
Property and Development NSW
Sydney Metro
Sydney Trains
Sydney Water Corporation
Technical and Further Education Commission
Transport Asset Manager of NSW
Transport for NSW

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)

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

© Copyright reserved by the Audit Office of New South Wales. All rights reserved. No part of this publication may be reproduced without prior consent of the Audit Office of New South Wales. The Audit Office does not accept responsibility for loss or damage suffered by any person acting on or refraining from action as a result of any of this material.