NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

Internal controls and governance 2025:

Procurement and technology

FINANCIAL AUDIT | 29 OCTOBER 2025

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*.

AUDITOR-GENERAL NEW SOUTH WALES

GPO Box 12
Sydney NSW 2001

The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 52B of the *Government Sector Audit Act 1983*, I present a report titled **'Internal controls and governance 2025: Procurement and technology'**.

Bola Oyetunji
Auditor-General for New South Wales
29 October 2025

RECONCILIATION STATEMENT

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

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

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

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

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

contents

Internal controls and governance 2025: Procurement and technology

Section 1 – Internal controls and governance 2025: Procurement and technology

Section 1 –

Internal controls and governance 2025: Procurement and technology

1. Report snapshot

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

Key findings

Internal control findings have decreased

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

IT controls need to improve

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

Deficiencies in procurement practices

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

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

Agencies can better integrate AI into their existing governance and strategy arrangements

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

Cyber security control deficiencies expose supply chains to vulnerabilities and undermine investment effectiveness

Control deficiencies make agencies vulnerable to supply chain cyber security threats and reduce investment effectiveness.

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

Recommendations

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

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

Fast facts

5
high-risk audit findings relating to IT controls

33%
of reported audit issues were repeat findings

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

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

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

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

Tabled in NSW Parliament 29 October 2025

2. Executive summary

This report analyses the internal controls and governance of 26 of the NSW public sector's largest agencies. These agencies account for 95% of the NSW Government's budgeted expenditure for 2024–25. The report provides Parliament with insights into the effectiveness of internal controls and governance in these agencies, including:

- an overview of the results of interim financial audits for 2024–25
- analysis of the effectiveness of these controls at selected agencies for certain important areas of public sector governance:
  - procurement
  - technology, including cyber security and emerging technologies like artificial intelligence
- key areas of improvement and practical lessons for NSW government agencies in considering the effectiveness of their internal controls and governance.

Refer to Chapter 3 for key areas of improvement and practical lessons for agencies and Appendix 1 for details of the agencies selected for inclusion in each chapter of this report.

This is the first of four financial audit reports focused on financial audits undertaken in the NSW public sector for 2025. The other three reports in the series are:

- State agencies, which will bring together the final results of, and insights from, audits of financial statements of all NSW public sector agencies for 2024–25
- State finances, which will focus on the NSW Government's consolidated financial statements of the general government and total state sectors for 2024–25
- Capital projects, which will assess procurement and project management of major infrastructure and investment projects in NSW.

2.1. Key findings

Internal controls and governance

Internal control findings have decreased, but agencies should take action to address repeat findings

Audit findings were reported on internal controls and governance at all 26 agencies, but the total number of findings decreased in 2024–25 compared to 2023–24 interim audits.

Repeat audit findings have increased and now represent 33% of all findings, compared with 19% in 2023–24. Repeat audit findings are findings previously reported that have not been addressed by the agency by the initially agreed due dates.

Common findings identified indicate that agencies need to improve the design or effectiveness of internal controls and governance relating to two of the largest areas of expenditure by the NSW Government - payroll and supply of goods and services expenses - to mitigate the risk of loss, error or fraud.

Agencies should improve information technology controls

There were five high-risk findings reported - all related to ineffective information technology (IT) controls, including those intended to prevent cyber security risks and events. Around half of all findings reported relate to IT controls over key financial systems.

Procurement

Deficiencies in end-to-end procurement and contract management practices mean that value-for-money could be eroded. Agencies' procurement policies and procedures do not consistently incorporate all mandatory and recommended requirements of the Framework.

All agencies have procurement policies and procedures, though oversight controls could be enhanced

Agencies' procurement policies and procedures do not consistently incorporate all mandatory and recommended requirements of the NSW Procurement Framework (the Framework). While all agencies have procurement policies, some have not been reviewed by their scheduled revision dates. Not all agencies are using internal audit functions to assess procurement controls. Reporting to executives on procurement matters is generally undertaken, but the scope and formality varies and could be strengthened to improve oversight of procurement outcomes.

Capability for procurement could be enhanced

Not all agencies provide their staff with mandatory training on procurement policies and requirements. Having an appropriate level of procurement capability reduces the risk of errors, waste and non-compliance.

There are gaps and inconsistencies in procurement accreditation policies across the sector. Of the 10 Level 1 accredited agencies in this report, only two included the mandated concurrence thresholds and requirements to seek concurrence from Level 2 accredited agencies in their procurement policy.

While most agencies submit Annual Procurement Plans to the NSW Procurement Board, Public Non-Financial Corporations (PNFCs) and non-accredited agencies are not required to. This could limit visibility in procurement opportunities across the sector.

Business case procedures are not consistently tailored to agency needs

Strengthening business case procedures also presents an opportunity to enhance strategic decision-making. While most agencies reference NSW Government guidelines, not all have developed tailored, agency-specific procedures for business case preparation.

Most agencies have established policies to govern complex market engagements. Three agencies either lack policies or do not require approving officers to assess compliance with legislative and policy obligations related to complex procurement approaches.

All agencies have policies mandating due diligence checks at the planning and sourcing stages of the procurement lifecycle. However, agencies with construction contracts are not meeting mandatory requirements to assess financial capacity of suppliers across the contract period.

Inconsistent approaches to Best and Final Offer

Around half of all agencies do not have formal policies for best and final offer use. Robust and transparent best and final offer processes ensure compliance with the Framework, uphold competitive integrity, maintain supplier trust and secure value-for-money outcomes.

There are gaps in the way contracts are disclosed, which limits the public's ability to understand contracts with suppliers and how public funds are spent. Audits in three agencies found issues with incomplete and inaccurate supplier contract reporting on the buy.nsw Supplier Hub.

Inconsistent review, reporting and oversight of conflict of interest disclosures

Conflict of interest policies are in place across all agencies, but some are outdated and some agencies lack mechanisms for managing complaints about conflicts. Two agencies do not maintain a centralised register for personal and conflict of interest disclosures, relying on decentralised business unit arrangements, which may limit transparency and compliance.

More than half of all agencies do not formally review centralised conflict of interest registers to detect undeclared conflicts before awarding procurement contracts. This may limit the ability to detect undisclosed conflicts as part of procurement processes or may impede their management. Most agencies do not have a policy of undertaking structured, periodic reporting to governance bodies or executive management on compliance with conflict of interest plans for high-risk procurement activities.

In one agency, 15 employees and contractors had positions in external entities that had financial dealings with the agency. These had not been previously disclosed as part of conflict of interest processes by these officials.

Not all agencies adopt a supplier relationship management approach when managing suppliers

Supplier management practices are inconsistently applied, with eight agencies lacking a structured supplier relationship management framework. Not all agencies have a policy to set key performance indicators to manage supplier performance.

Four agencies did not have a process to undertake any formal contract closure or evaluation activities, including documenting whether intended benefits were realised or benchmarking performance. This may limit the ability of these agencies to determine whether a procurement represents value-for-money. A lack of contract evaluation may also limit the effectiveness of future procurement decisions, particularly where poor performance or delivery has not been documented.

Most agencies do not have a requirement to undertake periodic reviews to identify waste in procurement.

The extent to which agencies have begun applying anti-slavery frameworks and guidance in their procurement practices is variable

Most agencies advised that they considered modern slavery risk in procurement. Four agencies advised they had not documented roles and responsibilities related to addressing modern slavery in procurement, nor had they incorporated responsible procurement principles into their procurement strategy.

Artificial intelligence

Agencies are adopting artificial intelligence but have not fully integrated it into their existing governance and strategic planning processes

Agencies are adopting artificial intelligence (AI) for a wide range of purposes, and its use will continue to grow. However, fewer than half of the agencies have implemented formal AI policies and most have yet to fully integrate the specific and unique risks posed by AI into their existing governance frameworks, such as risk management, procurement, IT, and monitoring and reporting systems.

AI has not yet been integrated as a strategic or operational tool across the sector. Only a quarter of agencies have developed a strategy for the use of AI. Senior leaders need more oversight of AI use, risks and challenges so that they can address barriers and align adoption to agency priorities and objectives.

Cyber security

Gaps in cyber security controls may result in supply chain vulnerabilities and less effective investments

Cyber security risk management practices vary across agencies. Three agencies do not have formal policies addressing supply chain cyber security risks, and eight lack strategies to maintain complete IT asset registers, limiting visibility of IT systems. Weak third-party oversight was observed, including unclear contractual roles and limited post-termination risk planning.

Not all agencies conduct cost–benefit analyses, track return on investment or benefits realisation, or ensure alignment of cyber security spending with current threat landscapes. Only seven agencies identify and manage underutilised, redundant, or outdated cyber security tools and services.

Information technology general controls

Agencies have faced challenges in implementing appropriate controls to manage risks for key financial systems

Some agencies lack current and comprehensive IT policies, with critical documents outdated or in draft form for extended periods. Three agencies did not review independent assurance reports from their third-party IT service providers, resulting in increased exposure to unmanaged external risks.

Access management controls were inconsistently applied. Agencies granted system access without proper approval, delayed deprovisioning following staff termination, and did not conduct regular user access reviews. Privileged user activities were not adequately monitored and password configurations frequently failed to comply with policy, increasing the risk of unauthorised access and data compromise.

There were weaknesses in change management and operational practices. Several agencies did not segregate duties between developers and implementers, bypassing independent review processes. Others lacked documentation for system changes or had not formally approved and tested disaster recovery plans and backups.

One agency was found to lack cyber security safeguards, including Distributed Denial of Service protection measures, multi-factor authentication and event monitoring for critical systems. This agency operated unsupported legacy infrastructure without formal risk assessments. In 2025, it experienced a cyber-attack targeting a key system also used by other agencies. This incident is further detailed in Chapter 9 as a case study.

2.2. Recommendations

By 30 June 2026, agencies should enhance their procurement frameworks by:

1. adopting all mandatory and relevant recommended requirements of the NSW Procurement Policy Framework
2. implementing guidance recommended by the NSW Anti-slavery Commissioner on managing modern slavery risks.

By 30 June 2026, agencies should improve cyber security control frameworks by:

3. strengthening supply chain risk management governance
4. improving investment accountability by introducing cost–benefit analysis, return on investment tracking, aligning the cyber spending with current threat landscapes, and managing underutilised, redundant and or outdated cyber security tools and services.

By 30 June 2026, agencies should support the adoption of AI by:

5. establishing and implementing an AI policy, and embedding the consideration of AI use into governance frameworks
6. creating a central AI inventory to document its purpose, uses and limitations for transparency, oversight and accountability
7. considering the benefits of developing an AI strategy that can be integrated into a broader organisational plan to ensure that AI initiatives are coordinated and aligned with agencies' strategic objectives
8. establishing regular reporting to senior management or an appropriate governance committee to ensure AI initiatives are aligned with organisation strategies and mandates, and to monitor and evaluate the use of AI.

3. Key areas of improvement and practical lessons

This chapter outlines key areas of improvements and practical lessons that can be applied by all agencies in designing and maturing internal controls and governance in respect of procurement and technology, including cyber security and emerging technologies like artificial intelligence.

Procurement

Procurement policies and frameworks

Procurement and contract management are foundational activities that support the delivery of public services in NSW. Ensuring the right oversight mechanisms are in place will promote value-for-money outcomes and mitigate risk. Agencies should:

- use internal audit to obtain assurance on how procurement is being managed and delivered within an agency, in support of continuous improvement
- establish structured reporting mechanisms, including use of key performance indicators, to executive management to enhance visibility of procurement activities and support executive-level accountability
- develop centralised systems or formal processes to track procurement performance and supplier outcomes, enabling better oversight and data-driven decision-making.

People and capability

Building capability for procurement within agencies will promote procurement that achieves value-for-money outcomes. Agencies should strengthen learning and development frameworks by mandating procurement training for all relevant staff, including non-specialist roles, to ensure consistent capability across the agency.

Business cases

If business cases are not prepared, agencies risk delays, non-compliance and poor value-for-money outcomes. Agencies should take steps to embed business case procedures into procurement policies and guidance. Procedures should be tailored to the context of agencies and with appropriate staff capability to ensure that they address key risks.

Due diligence

Supplier performance risk can be mitigated from the outset of a contract by having in place robust due diligence processes. Agencies should:

- strengthen due diligence frameworks by implementing clear, risk-based procedures that align with guidance from ICAC
- undertake financial assessments at engagement and regular intervals throughout the construction contract lifecycle in accordance with the requirements of the Framework.

Procurement

Conflicts of interest

Management of conflicts of interest is fundamental to ensuring procurement outcomes that promote public trust and ensure value-for-money. Agencies should take steps to promote effective management of conflicts by:

- ensuring that centralised conflict of interest registers capture declarations across all staff categories and business units, where possible, to provide oversight and assurance that conflicts are being actively identified and associated risks are being managed
- implementing structured, periodic reporting to governance bodies or accountable authorities on conflict of interest compliance, with particular focus on high-risk procurement processes
- reviewing centralised conflict of interest registers prior to awarding procurement contracts to identify any undeclared conflicts and ensure that associated risks are appropriately managed.

Contract extensions

Poorly managed contract extensions can undermine procurement integrity by bypassing competitive processes, diminishing value-for-money outcomes and exposing agencies to financial and governance risks. Extending contracts should be undertaken where there are clear value-for-money outcomes. Agencies should:

- mandate formal value-for-money assessments
- document contractor performance
- consider market alternatives before approving extensions.

Best and Final Offer

Without robust and transparent Best and Final Offer processes, agencies risk undermining competition, eroding supplier trust and compromising value-for-money outcomes. Agencies should have a clear policy and approach to best and final offers to promote competition, support transparency and maximise value-for-money outcomes. Agencies should take steps to:

- clarify procedures within their procurement policies and processes
- communicate requirements clearly in tender documentation.

Contract and supplier management

In the absence of robust contract and supplier management processes, agencies face increased risks of supplier underperformance, missed cost-saving opportunities and diminished accountability in achieving procurement outcomes. Agencies should strengthen procurement management by:

- adopting a formal supplier relationship management framework
- mandate the use of key performance indicators, regular performance reviews, root cause analysis, structured contract closure processes and evaluate outcomes.

Artificial intelligence (AI)

Governance and oversight

As AI becomes increasingly common in agency IT environments, it is necessary for agencies to maintain suitable governance and oversight of both the AI pipeline and AI tools used in production.

While it is not mandatory for NSW public sector agencies to apply the National framework for the assurance of artificial intelligence in government, it specifically identifies that:
'Governments should ensure their use of AI is disclosed to users or people who may be impacted by it. Governments should maintain a register of when it uses AI, its purpose, intended uses, and limitations'.

Strategic use of artificial intelligence

When senior leaders are kept informed of both the opportunities and the challenges associated with AI, they are better positioned to champion strategic initiatives, address resource needs, and ensure that ethical and governance standards are upheld throughout the organisation.

Cyber security

Managing supply chain cyber security risks

The foundation of an effective cyber security strategy is knowledge about the IT environment. Maintaining an IT asset inventory is crucial for strong cyber security as it provides visibility into what needs to be protected, enabling better risk management, threat detection and incident response.

Unmonitored external systems, such as those managed by third-party vendors and overall supply chain, can introduce further risks if they do not adhere to the agency's security standards.

Furthermore, not including supply chain risk in the risk register means that these risks are not being tracked or managed effectively. This oversight can result in a lack of preparedness for potential cyber incidents involving third-party vendors.

Cyber security spending

Effective management of cyber security investment helps agencies to ensure that their investments are yielding the desired results, in compliance with regulations, and ultimately safeguarding their operations while ensuring an effective and efficient spending on cyber security.

4. Introduction

This report provides Parliament with insights into the effectiveness of internal controls and governance at 26 of the largest NSW public sector agencies (excluding state owned corporations and public financial corporations). A list of the agencies included in each the analysis included chapter of this report is available at Appendix 1.

Internal controls and governance support the achievement of agencies' outcomes by promoting effective operations, reliable financial reporting, and compliance with applicable laws and regulations.

Effective internal controls and governance are particularly important for the agencies included in this report because they collectively accounted for 95% of the NSW Government's total budgeted expenditure in 2024–25. These agencies also deliver diverse services and are exposed to financial, operational and strategic risk.

Australian Auditing Standard ASA 315 'Identifying and Assessing the Risks of Material Misstatement' requires an auditor to obtain an understanding of the design and implementation of the internal controls relevant to the preparation of financial statements. Observations and findings drawn from the application of this standard in financial audits of agencies form the basis of the report.

The table below details the elements of internal controls and governance that are detailed in this report.

Chapter	Overview
Internal controls and governance	Chapter 5 provides an overview of the findings and deficiencies in internal controls and governance identified in interim audits at all 26 agencies.
Procurement	Procured goods and services are one of the NSW Government's largest areas of expenditure. Chapter 6 examines the extent to which 17 agencies, with more material procurement activities, comply with selected NSW Government mandatory requirements and recommendations.
Technology - Artificial intelligence	Agencies are increasingly integrating emerging technologies like AI to streamline operations, foster innovation and enhance delivery of public services. To safeguard ethical standards and uphold the integrity of public institutions, as well as the rights of the public, it is essential that agencies establish robust internal controls and governance frameworks to guide the development, deployment and oversight of AI technologies. Chapter 7 examines the current and future planned use of AI and governance, risk and assurance mechanisms to support ethical adoption of AI by 21 agencies who advised they had implemented AI.
Technology - Cyber security	Cyber risk is a critical concern. Cyber threats can disrupt operations and compromise sensitive data and assets. The dependence on third-party vendors and overall supply chains introduces risk, as these external partners may not have the same level of cyber security maturity as is expected of agencies. Chapter 8 examines how 20 agencies are managing and mitigating cyber risks in supply chains and maximising the return on investment in tools that mitigate and manage cyber security.
Technology - Information technology controls	Chapter 9 examines the key IT control findings and deficiencies internal controls identified in interim audits at all 26 agencies.

5. Internal controls and governance

A strong system of internal controls and governance enables agencies to operate effectively and efficiently, produce reliable financial statements, comply with laws and regulations, and support ethical and transparent decision-making. Good governance promotes public confidence in the integrity and effectiveness of agencies' systems and operations.

Financial audits include:

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

This chapter highlights findings relating to internal controls and governance from 2024–25 interim audits at 26 agencies. A list of agencies included in this chapter is included at Appendix 1.

Chapter highlights

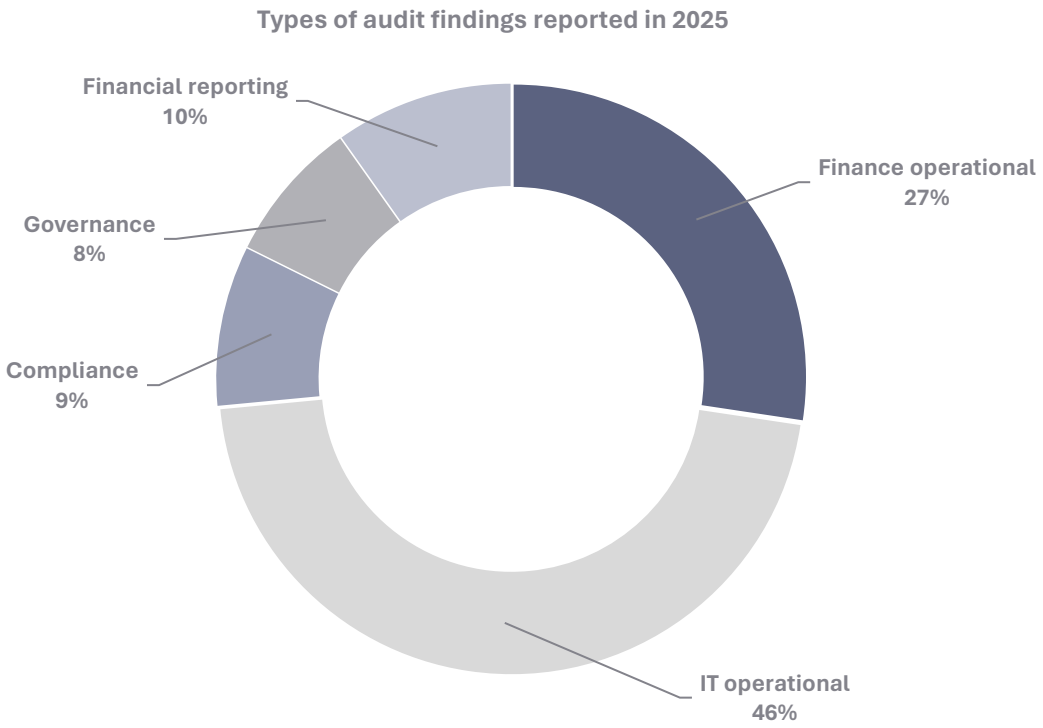
- Internal control findings decreased, but agencies should take action to address repeat findings. Repeat findings have increased and now represent 33% of all findings, compared with 19% in 2023–24. Findings on the design, implementation or operating effectiveness of internal controls and governance were identified at all agencies.
- IT controls and governance need to improve. Approximately half of all findings reported related to IT controls. Five high-risk findings were reported, all of which related to ineffective IT controls, including those that prevent cyber security risks.
- Common findings identified indicate that agencies need to improve the design or effectiveness of internal controls and governance processes relating to two of the largest areas of expenditure for the NSW Government, payroll and supply of goods and services expenses, to mitigate the risk of loss, error or fraud.

5.1. Audit findings

Deficiencies identified in internal controls and governance in our interim financial audits were reported to the accountable authority, management and audit and risk committee for each agency, so they can take appropriate action to mitigate the identified risk.

Agencies should take action to reduce repeat audit findings

We made audit findings on internal controls and governance at all 26 agencies included in this report. The total number of audit findings reported to agencies in 2024–25 decreased compared to 2023–24 interim audits. Of the 105 reported issues identified, 46% related to deficiencies in IT controls over key financial systems.



There was an increase in repeat audit findings, representing 33% of all reported findings. Repeat audit findings are those findings previously reported that have not been addressed by an agency by initially agreed due dates.

Vulnerabilities in internal control systems can be exploited by internal and external parties and pose a threat to agencies. The longer these vulnerabilities exist, the higher the risk that they will be exploited and the higher the expected losses. Agencies should prioritise resolution of these vulnerabilities by:

- assigning ownership of the recommendations raised in respect of internal control deficiencies
- regularly reporting progress on the actioning of recommendations to audit and risk committees and to executive management.

5.2. High-risk findings

High-risk findings arise from failures of key internal controls and/or governance practices of such significance that they can affect an agency's ability to achieve its objectives or impact the reliability of its financial statements.

Five high-risk findings were reported and all related to IT control deficiencies

High-risk deficiencies in internal controls identified included:

- operation of IT unsupported servers, including some connected to critical systems, without conducting a formal risk assessment or developing an action plan
- not requiring a third-party vendor to provide independent assurance reports on controls relevant to financial reporting and system delivery
- unclear roles and responsibilities between an agency and vendor for new system implementation and changes
- two findings relating to inadequate controls to detect or prevent a cyber security incident in which a threat actor went undetected in a key financial system.

Further details on findings related to IT controls are discussed in Chapter 9.

5.3. Common audit findings

Agencies need to improve the design or effectiveness of internal controls and governance relating to the two of the largest areas of expenditure for the NSW Government, payroll and supply of goods and services expenses.

Agencies should increase security over payroll records to reduce the risk of fraud or error

Common deficiencies in controls identified included:

- instances of inappropriate access to amend employee master file data
- payroll payment files uploaded to banking systems are unencrypted
- delays in processing cessation of employees in the payroll system
- payroll summary and exception reports not accurate or missing key information.

Ineffective controls in the payroll process can expose an agency to loss as demonstrated in the case study below.

Case study – Segregation of duties in payroll processing

At one agency a payroll officer was able to modify their own employee master file record due to insufficient segregation of duties and system restrictions.

These payments went undetected at the time because they fell below the monetary detection thresholds set out in payroll exception reports which were established by the agency to assist in detecting payment anomalies.

Subsequently, the agency has implemented a control to restrict payroll officers from modifying their own employee master file record.

Weak procurement controls increase the risk of error, waste and fraud

Common deficiencies in controls identified included:

- amending accounts payable vendor master file information without proper supporting documentation or verification
- invoice payments made without purchase orders, or purchase orders raised after invoice receipt
- credit card transactions unauthorised, unacquitted or above mandated transaction limits.

Ineffectively designed controls relating to purchasing and expense management can expose an agency to loss as demonstrated in the case study below.

Case study – Prevention of fraud in vendor management

An individual impersonating an agency's supplier contacted the agency to request an email address change. Although the agency's policy required verifying such requests by forwarding them to the existing email address in the vendor master file, this was not performed. Instead, the email address was updated based on a phone call with the individual.

Using this email address, the individual later requested and received copies of the legitimate suppliers' invoices. The agency's internal controls to prevent error or fraud relating to updating supplier bank account details rely on the supplier providing three current invoices and using an email address that matches the vendor master file record before the change is made. As the individual had already updated the email address in the master file and was able to provide the invoices, the agency's control failed to detect this instance of fraud.

The agency later approved a payment to be made to the fraudulent bank account. The payment was reversed by the agency's bank.

Subsequently, the agency has:

- updated the process for verifying changes to vendor details, by requiring the use of independent contact number from a vendor website to contact a vendor's accounts team to confirm the request
- implemented a review process to check that the required steps for confirming vendor details have been undertaken.

6. Procurement

Effective internal controls and governance over procurement should enable an agency to deliver services to the public efficiently and effectively and ensure that value-for-money is achieved for each dollar of public funds invested.

This chapter examines the extent to which agencies:

- procurement policies comply with the selected NSW Government mandatory and recommended procurement requirements
- have established controls to ensure they deliver value-for-money in procurement outcomes.

This chapter focuses on the selected key mandatory requirements and best practice outlined in the NSW Procurement Policy Framework (the Framework). The accountable authority for each agency holds ultimate responsibility for managing agency procurement activities in accordance with the Framework.

As explained in Appendix 1, this chapter includes 17 of the agencies included in this report. These agencies were selected for analysis as they undertook more material procurement of goods and services. Seven of these agencies also undertake more significant construction activities. For other agencies, procurement was less material or mainly involved expenditure with other NSW government agencies, for which some of the mandatory requirements of the Framework do not apply.

Chapter highlights

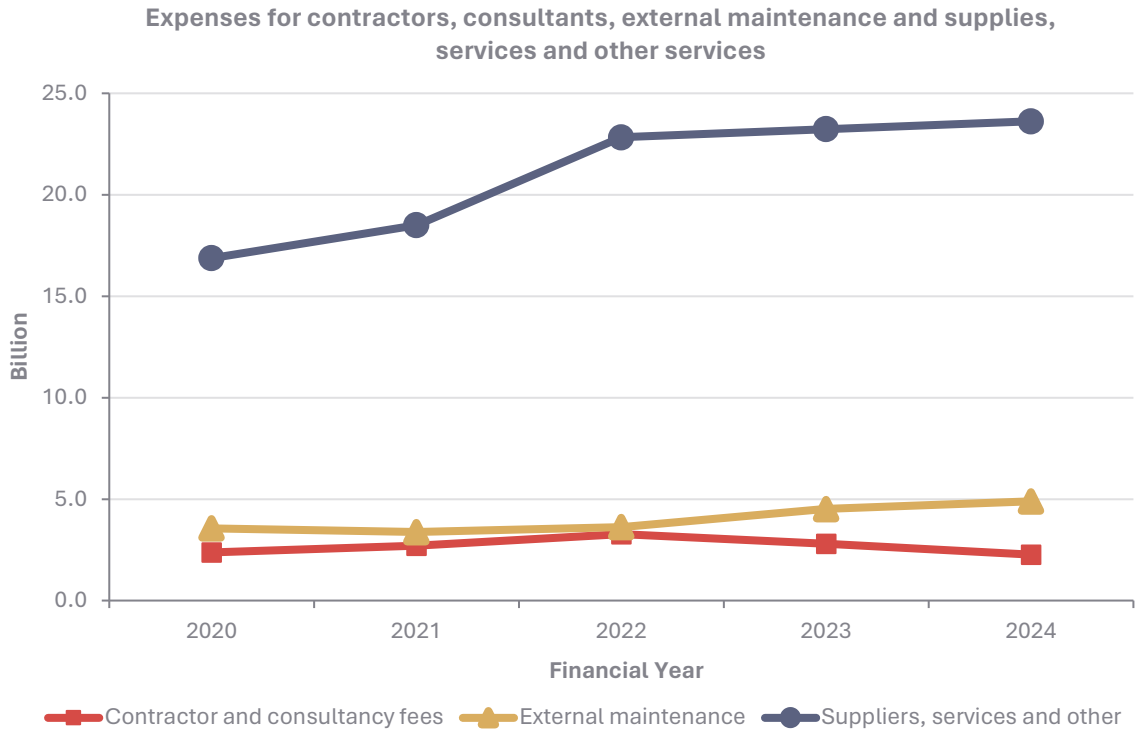
- Deficiencies in end-to-end procurement and contract management practices mean that value-for-money could be eroded. Agencies' procurement policies and procedures do not consistently incorporate all mandatory and recommended requirements of the Framework examined in this chapter.
- Not all agencies provide mandatory training on procurement to their staff. Lack of knowledge and capability around procurement processes can expose agencies to risk and limit achievement of value-for-money.
- Agencies have developed guidance or require due diligence procedures to be undertaken when planning a procurement, however some agencies were not applying the guidance in the Framework to assess supplier viability for high-value construction contracts at periodic intervals.
- There are inconsistent practices for the review, reporting and oversight of conflict of interest disclosures. More than half of the agencies do not formally review centralised conflict of interest registers to detect undeclared conflicts before awarding procurement contracts.
- Not all agencies have developed formal policies and processes for the application of Best and Final Offer principles, reducing opportunities to achieve value-for-money outcomes.
- Agencies have inconsistent approaches to assessing the value for money of contract extensions. Contract extension practices vary, with inconsistent documentation and limited post-project reviews.
- Not all agencies adopt a supplier relationship management approach to managing suppliers. Not all agencies set key performance indicator to manage supplier performance. Inadequate supplier performance management and evaluation can limit the ability to demonstrate that procurement decisions represent value-for-money or achieve intended benefits.
- The extent to which agencies have begun applying Anti-slavery frameworks and guidance in their procurement practices is variable.

6.1. Background

The Total State Sector Accounts for the year ending 30 June 2024 recorded expenses for:

- $2.2 billion on contractors
- $0.1 billion on consultants
- $4.9 billion on external maintenance
- $23.6 billion on supplies, services and other services.

These expenses will include a component of procured goods and services. The table below shows the expenses recorded in the Total State sector Accounts for the period 2020 to 2024.



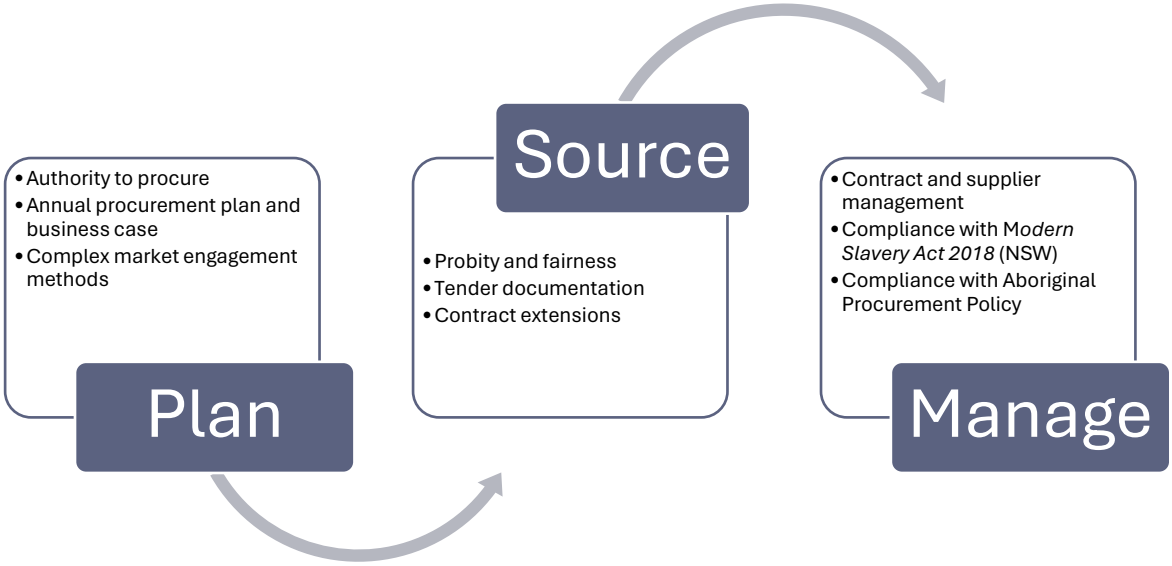
Procurement activities must comply with the requirements of the *Public Works and Procurement Act 1912*

The *Public Works and Procurement Act 1912* (the PWP Act), including associated policies issued by the NSW Procurement Board, establishes the framework within which agencies must approach procurement. The NSW Procurement Board issues policies and directions for procurement under the PWP Act. The PWP Act and the NSW Procurement Board's policies and directions apply to all government agencies except for State owned corporations.

In addition to the PWP Act, when undertaking procurement agencies must also comply with the:

- *Government Sector Finance Act 2018*
- *Independent Commission Against Corruption Act 1988*
- *Government Information (Public Access) Act 2009*.

The NSW Procurement Policy Framework (the Framework) outlines the NSW Procurement Board's requirements as they apply to each step of the procurement process. The Framework is a policy under the PWP Act and agencies must comply with its mandatory requirements. The Framework outlines three stages of the procurement process: plan, source and manage.



6.2. Agency procurement policies and frameworks

Effectively designed policies and procedures provide officials with clear instructions on how to comply with Framework requirements and undertake procurement within the risk appetite of an agency.

The Framework requires agencies to regularly test their compliance with the mandatory requirements and other Procurement Board policies and directions.

All agencies have procurement policies and procedures

The Framework requires agencies to have internal policies and controls and to ensure that these are consistent with the obligations of the Framework.

All agencies included in this analysis have established policies and guidance to direct and support their procurement activities.

Most agencies had established a process for regular review of their procurement policies. Two agencies did not set a period for regular review or undertook review at the scheduled date. Ongoing review and revision of procurement policies is important to ensure that organisational processes reflect best practice and incorporate current NSW Procurement Board requirements.

Most agencies had conducted an internal audit into procurement in the last three years

TPP20-08 Internal Audit and Risk Management Policy for the General Government Sector requires internal audit functions to provide timely and useful information to management about the adequacy of, and compliance with, the system of internal controls, whether agency results are consistent with established objectives, and whether operations or programs are begin carried out as planned.

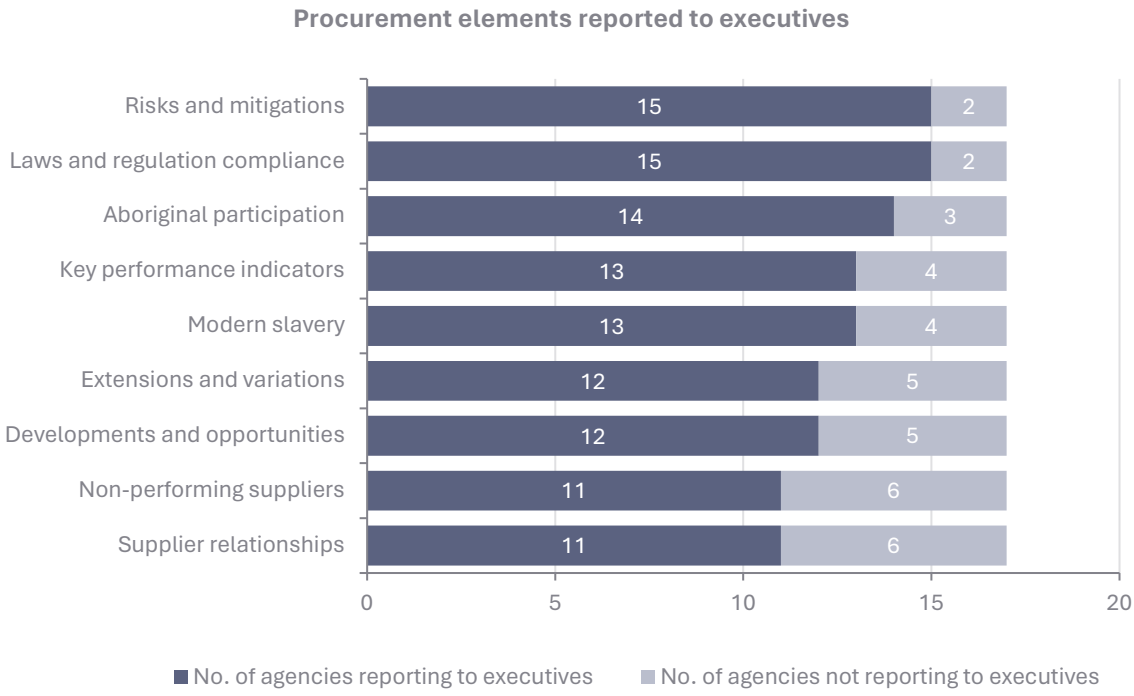
Internal audits of procurement can provide accountable authorities with assurance of the effectiveness of internal controls and governance for procurement and may be an opportunity to identify inefficiencies or financial wastage in their procurement practices.

Most agencies advised they had undertaken an internal audit of procurement, including specific procurements, during the last three years. Three agencies had not directed any specific internal audit work in this area during the period.

All agencies report on procurement to executive management, though the scope, detail and formality of reporting differs

Good practice in internal controls and governance for procurement includes regularly providing executive management with clear, comprehensive updates to ensure they maintain effective oversight of activities and outcomes.

Six agencies advised that they are not providing information to executive management on strategic oversight of supplier relationship management and the evaluation of underperforming suppliers. The figure below outlines the extent to which procurement related items are reported to executive management, highlighting variability in the frequency and depth of oversight.



Not all agencies provide their staff with mandatory training on procurement policies and requirements

Training provides staff with the knowledge to understand and consistently apply policies, procedures and ethical standards. Having an appropriate level of procurement capability should reduce the risk of errors, waste and non-compliance.

Four agencies did not require their staff to undertake procurement training. Some agencies assessed that mandatory training was only required for only some roles, such as procurement specialists.

Of the agencies with training on procurement available, topics covered included procurement fundamentals, ethics, contract management and compliance with government policies. Training was delivered through a mix of eLearning, face-to-face sessions and internal workshops.

Of the agencies with mandatory procurement training, some agencies reported completion rates of less than 100%.

While some agencies require training for procurement staff, especially for complex or high-value activities, others only provide optional or ad hoc sessions for broader staff groups. Given the complexity, value and risk, associated with procurement agencies should require officials undertake mandatory training before engaging in procurement to ensure they have the appropriate skills and capabilities.

6.3. Plan

Authority to procure

Procurement accreditation is formal recognition granted by the NSW Procurement Board, administered by NSW Procurement, to assess and authorise an agency's procurement capabilities. Agencies may be accredited under two distinct programs: 'Accreditation Program for Goods and Services Procurement' and 'Accreditation for Construction Procurement'. Accreditation levels determine the maximum contract value for a procurement that an agency can manage and its degree of autonomy in conducting procurement activities.

There are gaps and inconsistencies in procurement accreditation policies across agencies

The Framework mandates that agencies adhere to the terms of their accreditation as set by the Procurement Board in planning their procurement activities. If these terms are not clearly defined within an agency's procurement policies, there is a heightened risk that staff may fail to comply with them during procurement processes.

Of the ten Level 1 goods and services accredited agencies[1] sampled in this report, only two incorporated the NSW Government's mandated concurrence thresholds and the requirement to seek concurrence from Level 2 accredited agencies[2] in their procurement policies and guidance.

One agency did not require checks for existing whole-of-government contracts and prequalification schemes before initiating new procurements.

Procurement authority policies should be enhanced by embedding mandatory requirements.

Agency procurement planning – Annual Procurement Plans and business cases

Procurement planning enables agencies to strategically manage upcoming procurement activities, align purchasing with organisational priorities and provide transparency to the market.

The Framework requires accredited agencies to submit an Annual Procurement Plan to the Board by 31 August each year. A summary of the plan is also published on eTendering. Unaccredited agencies are encouraged to publish an Annual Procurement on eTendering. TPG24-29 NSW Government Business Case Guidelines requires agencies to prepare business cases and submit to the relevant gateway coordination agency for significant capital, recurrent and ICT investment proposals.

Greater transparency of whole-of-government procurement can be achieved by encouraging broader participation across all government sectors

All agencies mandated to submit procurement plans have submitted these plans to the NSW Procurement Board.

Public Non-Financial Corporation (PNFC) sector agencies and non-accredited agencies are not required to submit these plans. This could limit visibility in procurement opportunities across the sector.

[1] Level 1 agencies may independently conduct goods and services procurement activities up to a maximum contract value based on the following risk profile of the procurement: Low risk <$50 million, Medium risk <$35 million, High risk <$20 million. Concurrence from a Level 2 accredited agency or NSW Procurement is required to conduct procurements above these thresholds.

[2] Level 2 agencies may independently conduct goods and services procurement activities. Their responsibilities also include taking a leadership role in relation to procurement in the portfolio and taking lead buyer status for a category to establish and manage whole-of-government contracts.

Most agencies have referenced NSW Government business case guidelines in their procurement policies and framework

Four agencies do not reference the requirement for business cases as outlined in the guidelines. Two of these agencies advised that they have not formalised requirements, assuming they will not undertake major projects in the future. A reactive approach risks delays and governance gaps when significant procurement needs arise.

Agencies should embed tailored, capability-supported business case procedures into their procurement frameworks.

Complex market engagement methods

When NSW government agencies need to procure goods or services not covered by existing contracts or whole-of-government arrangements, they may adopt sourcing strategies such as direct dealings, multi-phase tenders and structured negotiations. In doing so, agencies must refer to the guidance contained within the Non-traditional and Complex Market Approaches and Direct Dealing Guidelines.

Agencies are navigating complex market engagements with varying levels of policy maturity and procedural clarity

Policies to govern complex market engagements have been established by 14 agencies. Three agencies either lack policies or do not require approving officers to assess compliance with legislative and policy obligations related to complex procurement approaches.

Agencies should formalise internal policies that clearly define approval responsibilities and procedural requirements for complex market engagements.

First Nations participation in procurement

The Aboriginal Procurement Policy (APP) applies to the procurement of goods and services by agencies. The objective of the APP is to:

- support employment opportunities for Aboriginal and Torres Strait Islander people
- support sustainable growth of Aboriginal businesses by driving demand via government procurement of goods, services and construction.

The APP aims for the NSW Government to direct one per cent of total spend to Aboriginal businesses, including three per cent of the total of awarded contracts for goods and services. All NSW government agencies, excluding state owned corporations, are required to adhere to the requirements of the APP.

Most agencies have prepared and published an Aboriginal Participation Strategy

The APP requires agencies to publish an Aboriginal Participation Strategy detailing how they will meet their obligations under the APP. This strategy must be publicly accessible on an agency's website. Two agencies had not prepared a strategy, which they advised was due to a change in portfolio arrangements a result of machinery of government changes. Not all agencies had published their strategy on their website.

6.4. Source

Probity and fairness – due diligence

The Framework indicates that agencies should conduct supplier due diligence checks that reflect the value, nature and risk of each procurement and contract. This requirement is supported by Appendix 1 of the Independent Commission Against Corruption's (ICAC) Supplier Due Diligence: A Guide for NSW Public Sector Agencies, which outlines the relevant legislative and regulatory frameworks. As described by ICAC, due diligence checks involve ensuring that a supplier:

- is genuine
- is capable and reliable
- is financially viable
- is of good repute and integrity
- has the required authorities, licences and status.

All agencies require due diligence procedures to be undertaken when undertaking procurement

All agencies have policies mandating due diligence checks at the planning and sourcing stages of the procurement lifecycle. However, two agencies do not have policies or procedures that provide guidance for staff on conducting these due diligence activities.

Inconsistent processes for evaluating supplier financial viability for construction contracts

Of the agencies included in this report, seven manage high-value contracts for construction services.

For these contracts, the Framework requires that agencies use the Financial Assessment Services Scheme to assess the financial capacity and viability of prospective or existing contractors at the start of construction contracts and throughout their duration.

Agencies are responsible for determining the appropriate level and frequency of rolling financial assessments for construction projects or contractors. Unless there are valid reasons to apply different intervals, contracts valued between $1 million and $10 million require a financial assessment report at least every six months from the start of the contract, while contracts exceeding $10 million require a report at least every three months.

Most agencies had a policy in place to meet the requirements of the Framework around assessing supplier financial viability for contracts. However:

- five agencies did not require financial assessments every six months for contracts valued between $1 million and $10 million
- only one agency mandated quarterly assessments for contracts exceeding $10 million.

Agencies advised us that they did not undertake these periodic assessments due to:

- high turnover of projects
- cost of assessments
- reliance on other assurance processes
- assessments being conducted based on risk or in response to specific triggering events.

Agencies should strengthen due diligence frameworks to ensure procurement policies mandate financial assessments at engagement and throughout the construction contract lifecycle.

Probity and fairness – conflict of interest

Agencies must implement procurement procedures that uphold the principles of fairness, transparency and ethical conduct throughout the entire procurement lifecycle. This includes management of conflict of interest, both perceived or actual.

All agencies had conflict of interest policies in place

All agencies have policies in place relating to the disclosure and management of conflicts of interest. Three agencies had not reviewed their policies in more than three years. Ongoing review and revision of conflict of interest policies is important to ensure that processes reflect best practice and incorporate current policy requirements.

Three agencies could improve their conflict of interest policies by including additional information as to how officials can make complaints around conflict of interest, as they do not have a process or guidance for addressing complaints related to undisclosed or poorly managed conflict of interest.

Most agencies had a centralised process or register in place to record declarations

Two agencies did not maintain a centralised register for conflict of interest disclosures. The agencies indicated that their organisation-wide registers do not fully capture conflicts managed at the individual business unit level, where separate processes may exist.

Decentralised or locally managed processes:

- impede the effectiveness of conflict of interest processes as they may not be applied consistently across an organisation
- limit visibility of compliance with conflict of interest requirements and ability to report and monitor on an organisation wide basis.

The following case study illustrates the risks that can arise when agencies do not identify and manage conflicts of interest.

Case study – Undisclosed conflicts of interest and lack of oversight in secondary employment

At one agency, 15 employees held roles as directors in external entities that had financial dealings with the agency through contracts and procurement. None of these employees had submitted a conflict of interest declaration regarding their relationship with these entities.

The agency did not maintain a secondary employment register, and the agency does not actively monitor secondary employment arrangements.

Failure to disclose and manage conflicts of interest and secondary employment can pose a significant fraud and integrity risk. Consequences can include reputational damage, financial loss, legal and ethical breaches.

Most agencies do not report to governance bodies or executive management on compliance with conflict of interest requirements

Regular reporting to governance bodies executive management on compliance with conflict of interest requirements, particularly in relation to formal or high-risk processes, such as large or complex tenders, can provide transparency in relation to whether risks are being appropriately addressed. Reporting may include disclosures made, actions taken to manage identified conflicts, outcomes of assessments, and any breaches or non-compliance.

Ten agencies do not have a practice of reporting information on conflict of interest compliance to governance bodies or executive management.

More than half of agencies do not formally review centralised conflict of interest registers when undertaking procurement

A centralised register of conflict of interest allows agencies to systematically record and monitor disclosures and support transparency and accountability in procurement processes.

Twelve agencies do not have a policy or requirement to undertake formal checks of centralised conflict of interest registers before awarding contracts.

Agencies should maintain conflict of interest registers across all staff and business units, implement structured and periodic conflict of interest compliance reporting to governance bodies, and review these registers prior to contract awards to identify and manage any undeclared conflicts.

Tendering

A tender evaluation is the process by which agencies assess supplier submissions against defined criteria to determine which offer best meets the procurement requirements and delivers value-for-money.

A multi-stage market process is an effective approach to tendering, enabling agencies to shortlist suppliers using broad criteria, then refine selection through detailed evaluation. As part of this, agencies may request a best and final offer, giving suppliers a final chance to present their most competitive price and terms, ensuring optimal contract outcomes.

The Framework allows the use of complex market engagement methods, such as a multi-stage market approach with best and final offer, as long as processes comply with the PBD-2019-05- Enforceable Procurement Provisions Direction (EPP).

Not all agencies have developed formal policies and processes for the application of best and final offer principles, reducing opportunities to achieve value-for-money outcomes

Nine agencies have policies or procedures which indicate how to best and final offers are obtained during supplier selection or contract finalisation. The remaining agencies rely on general NSW Government guidance or other practices. Best and final offer approaches were inconsistently disclosed in market documentation by agencies.

Agencies should establish robust and transparent best and final offer processes to ensure compliance with the EPP, uphold competitive integrity, maintain supplier trust and secure value-for-money outcomes.

Contract extensions

Agencies may include extension options in their contracts. The Framework requires agencies to only exercise contract extension options where it can be demonstrated the contract will continue to deliver value-for-money.

To ensure value-for-money, the Framework requires that agencies conduct an assessment of the market prior to rolling-over or extending a contract, including how the extension will impact competition and create (or continue) barriers to new suppliers.

Most agencies' procurement policies require an assessment that a contract demonstrates continued value-for-money, including at the point of considering a contract variation. All policies required that the assessment of whether the contract meets the agency's needs and suppliers performance is satisfactory.

Supplier registration

Agencies must keep appropriate records of procurement planning, management and decision-making. This includes complying with contract disclosure and open access information requirements of the *Government Information (Public Access) Act 2009* (GIPA Act).

Gaps in disclosure of contracts on agency contract registers and buy.nsw limits the ability of the public to understand contracts with suppliers and how public funds are being spent

The Framework requires agencies to confirm that suppliers are registered on the buy.nsw Supplier Hub when the total engagement value exceeds the GIPA Act contract disclosure threshold of $150,000. This confirmation should occur prior to issuing a select or closed market approach, or upon closure of open market approaches. Additionally, contracts must be publicly disclosed on the buy.nsw website within 45 days of award, as mandated by the GIPA Act.

Inaccurate and incomplete contract reporting on buy.nsw was identified in interim financial audits for three agencies, where:

- one agency had 24 of its contracts not published on the buy.nsw within the required 45-days timeframe
- one agency had eight of its contracts not published on the buy.nsw within the required 45-day timeframe
- one agency had 17 contracts not published on buy.nsw within the required 45-day timeframe.

6.5. Manage

Contract and supplier management

Contract and supplier management involves overseeing both the contractual obligations and the supplier relationship to ensure that procurement outcomes are delivered effectively and sustainably.

The Framework encourages adoption of a supplier relationship management approach to contract managing an agency's engagement with suppliers of goods and services in accordance with the Supplier Relationship Management Guidelines for NSW Practitioners. Supplier relationship management involves segmentation of suppliers, categorising them based on their strategic importance, spend volume, risk or innovation potential. The approach emphasises maximising the value of these relationships by fostering collaboration, improving performance and reducing risk.

Half of agencies have not formalised their management of suppliers using the recommended supplier relationship management approach

Eight agencies advised that they have not adopted a supplier relationship management approach in their procurement policies and framework.

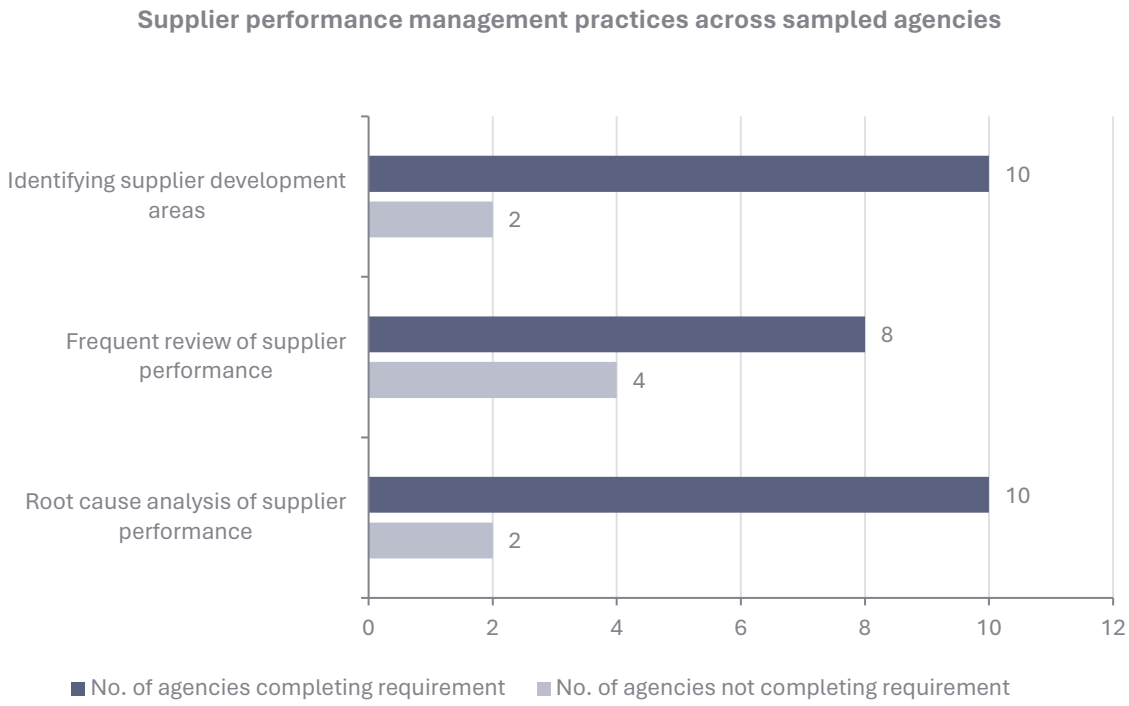
Where agencies did not adopt a supplier relationship management approach, management is typically conducted on an ad hoc basis, either at the business unit level based on local guidance or practice or guided by draft policies that had not yet been implemented.

Not all agencies have a policy to consider key performance indicators to manage supplier performance

The Framework requires agencies to manage supplier performance, drive continuous improvement and encourage innovation in coordination. This can be supported by the use of key performance indicators to evaluate supplier outcomes.

Key performance indicators for evaluating supplier performance are not consistently applied across agencies. Five agencies did not have a policy to consider key performance indicators in managing supplier performance and expectations.

The figure below demonstrates supplier performance management practices across the twelve agencies who use key performance indicators to manage and evaluate supplier performance.



Lack of evaluation of contract performance by some agencies may limit the ability to demonstrate that procurement decisions represent value-for-money or achieve intended benefits

The Framework requires agencies to track and report benefits to demonstrate the delivery of value-for-money for each procurement. Agencies meet this requirement by assessing supplier performance throughout the contract lifecycle and upon its completion.

Four agencies did not have a mandatory process to undertake any formal contract closure or evaluation activities. This included not formally documenting contract outcomes, not assessing whether intended benefits had been realised or not conducting supplier performance benchmarking.

The lack of a formal evaluation of supplier performance on contract completion limits the ability of an agency to determine whether a procurement has fulfilled its intended benefits or achieved value-for-money. Additionally, a lack of benchmarking of supplier performance may limit the effectiveness of future procurement decisions, particularly where poor performance or delivery has not been documented.

Most agencies do not consider waste in evaluating previous procurements

Most agencies do not have a requirement to undertake periodic reviews to identify waste and inefficiency in previous procurements.

Agencies should strengthen their controls and oversight of supplier performance by adopting a supplier relationship management approach, including establishing key performance indicators, where appropriate, and structured contract closure and evaluation processes.

6.6. Modern slavery

The PWP Act requires agencies take reasonable steps to ensure that goods and services procured by and for an agency are not the product of modern slavery. Modern slavery refers to serious violations of human rights and dignity, including practices such as slavery, servitude, forced labour, debt bondage, human trafficking and forced marriage.

Agencies must comply with the *Modern Slavery Act 2018 NSW*, including annual reporting obligations and co-operation with the Anti-Slavery Commissioner (the Commissioner).

The 'Commissioner's Guidance on Reasonable Steps (GRS) to Manage Modern Slavery Risks in Operations and Supply-Chains' sets out measures agencies should take to comply with mandatory requirements to manage modern slavery risk in their procurement, including:

- map supply chain risks for each procurement
- report on steps taken by an agency to develop a risk reducing procurement strategy.

Failure to manage modern slavery risks appropriately may expose agencies to reputational damage, legal non-compliance and ethical accountability failures.

This section analyses agencies' responses to inquiries about how that they had incorporated anti-slavery measures in the Act, Framework and Guidance into their procurement practices.

Agencies used different approaches to assessing modern slavery risks in procurement

Agencies advised they considered modern slavery risk in procurement. The method by which agencies undertook their risk assessments varied, relying on a range of different tools, techniques and methods including enterprise risk or procurement templates, management plans or the Commissioner's Inherent Risk Identification Tool.

Not all agencies have incorporated recommended steps in relation to in relation to modern slavery risk

The Framework requires that agencies consider the Commissioner's Guidance during procurement planning. The Framework also recommend that procurement strategies include:

- a clearly defined scope of modern slavery concerns to be considered during procurement
- standards expected from suppliers
- specific methods for managing modern slavery risks throughout the procurement process
- defined roles and responsibilities for modern slavery oversight
- integration of responsible procurement principles into category management strategies for higher-risk procurements
- consideration of the agency's potential to cause, contribute to or be directly linked to modern slavery through its supply chains

Most agencies advised that they have developed some guidance that incorporates modern slavery risk considerations into their procurement practices. This guidance is often embedded within procurement standards, policy statements or risk management processes.

Four agencies advised that they had not documented roles and responsibilities related to addressing modern slavery in procurement, nor had they incorporated responsible procurement principles into their strategic or policy frameworks.

Agencies should review the Commissioner's Guidance and confirm that their procurement strategies align with its recommendations.

Most agencies advised that they consider modern slavery as part of the procurement process

The Commissioner's Guidance recommends that agencies can mitigate the risks associated with modern slavery in the procurement of goods and services by:

- enhancing the procurement process to incorporate modern slavery risks as part of tender evaluation processes, including through using model tender clauses and specifications and supplier self-assessment questionnaires, and by conducting due diligence before awarding contracts
- including modern slavery clauses in contracts, aligned with model contract clauses.

Most agencies advised that they had a policy to consider the use of modern slavery clauses in procurement tenders and contracts and as part of due diligence activities. There was inconsistency in agencies adopting the recommendation for supplier self-assessment questionnaires.

Most agencies do not provide modern slavery risk capability development for suppliers

The Commissioner's guidance indicates that agency can use a range of capability development activities, such as providing guidance or training to suppliers in order to increase capability.

Most agencies advised that they did not provide training and development for suppliers. Some agencies advised that they referred suppliers to existing whole-of-government resources such as buy.nsw for information on modern slavery.

Agencies should take steps to enhance the capability of their suppliers in relation to the risks of modern slavery through provision of capability development as recommended by the Commissioner.

Agencies met their annual reporting obligations in the Modern Slavery Act

Agencies are required to report annually on the reasonable steps taken to ensure that goods and services procured are not the product of modern slavery (and where applicable) any significant operational issues raised to them by the Commissioner. All agencies met this annual reporting obligation for 2023–24, either within their annual reports or through separate stand-alone reports.

Mandatory annual modern slavery reporting requirements came into force from 1 January 2022.

7. Technology - Artificial intelligence

Agencies are increasingly integrating emerging technologies like artificial intelligence (AI) to streamline operations, foster innovation and enhance delivery of public services.

This chapter examines:

- the use of AI in the 21 agencies that reported having adopted AI
- whether appropriate governance, risk and assurance mechanisms are in place to support ethical adoption in line with NSW Government policy and framework requirements
- future plans and strategies for use of AI by agencies.

As explained in Appendix 1, this chapter includes 21 of the agencies included in this report. These agencies were selected as they had implemented AI.

Chapter highlights

- Agencies are using AI for a variety of purposes, and its use will continue to grow. The adoption of a total of 357 different AI tools, either in pilot or fully implemented, was reported across 21 agencies. Several challenges and barriers affecting the adoption and use of AI have been noted by agencies, including the development of governance frameworks, management of data sensitivity, security and quality, limited AI literacy, and technical issues such as integration with existing IT systems.
- Agencies should better integrate AI considerations into their existing governance arrangements. Fewer than half of the agencies have implemented formal AI policies and most have yet to fully integrate the specific and unique risks posed by AI into their existing governance frameworks. This includes evaluating its broader impacts on accountability structures, policies and procedures (such as information technology, procurement, risk management), and monitoring and reporting systems.
- Agencies can improve the information they centrally capture about their AI tools by documenting information about purpose, intended use and limitations. A comprehensive inventory provides a clear, consolidated view of all AI in use, enabling agencies to monitor their deployment, assess their impact and manage risks, and ensure alignment with ethical and governance standards.
- Around a quarter of agencies have a strategy to help maximise the benefits of AI. AI has not yet been integrated as a strategic or operational tool across the sector. Senior leaders need more oversight of AI use, risks and challenges to address barriers and align adoption to agency priorities and objectives.

7.1. Background

To safeguard ethical standards and uphold the integrity of public institutions, as well as the rights of constituents, it is essential that agencies establish robust governance frameworks to guide the development, deployment and oversight of AI technologies.

The NSW Government's AI Framework includes the:

- Artificial Intelligence Strategy
- Artificial Intelligence Ethics Policy
- NSW Artificial Intelligence Assessment Framework.

This is supported by DCS-2024-04 – Use of Artificial Intelligence by NSW Government Agencies, which requires all agencies to comply with the Artificial Intelligence Ethics Policy and NSW Artificial Intelligence Assessment Framework.

While there is no single definition of AI, the Artificial Intelligence Ethics Policy defines AI as intelligent technology, programs and the use of advanced computing algorithms that can augment decision-making by identifying meaningful patterns in data.

7.2. Adoption of artificial intelligence

Agencies are using AI for a variety of purposes, with use expected to grow

Twenty-one agencies have adopted a total of 357 different AI tools, either in pilot or fully implemented. This included use of AI for:

- productivity and workflow enhancement
- customer (citizen) interaction and support
- fraud detection and cyber security support
- legal and compliance monitoring
- capability development and training
- supporting service delivery in agency core functions, including across areas like Health, Transport, Education, and Family and Community Services.

Agencies expect the use of AI will continue to grow. Of the agencies included in this report, 18 advised that they had AI tools under consideration, planning or development that were not yet in use at time of this report.

Agencies reported challenges and barriers that hinder effective AI adoption

Agencies identified challenges and barriers to the adoption and use of AI, including the following.

- **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 lack of coordinated approaches and clear decision-making structures further complicates responsible AI adoption.
- **Data sensitivity, security and quality** – Managing sensitive information, such as personal or community-impacting data, is a major barrier to AI adoption. Agencies struggle with data classification, ensuring privacy, preventing data loss, and maintaining high data quality and availability for AI systems.
- **Education, skills and change management** – A lack of AI literacy, training and understanding among staff hinders responsible and effective AI use. Agencies report difficulties in engaging staff in professional learning, managing workforce impacts, and ensuring that employees understand both the risks and capabilities of AI tools.

- **Integration with legacy systems and operational complexity** – Integrating AI into existing, often fragmented or legacy IT systems, presents technical and operational challenges. Agencies must also manage change across processes and workflows, balance productivity with transparency and safety, and ensure consistent application of AI to business needs.

Some agencies lack oversight of the AI they have adopted

Of the agencies having adopted AI, 15 advised they had identified and documented all AI tools implemented in a centralised inventory.

A centralised inventory of AI tools in use is important for transparency, oversight and accountability. Without such oversight, agencies cannot assure themselves that they have fit-for-purpose governance arrangements in place to oversee the use of AI.

7.3. Policies for responsible use of artificial intelligence

Good governance and assurance arrangements support the effective delivery of ethical and lawful AI. There is no one-size-fits-all governance model. The National framework for the assurance of artificial intelligence in government outlines that governance structures should be proportionate and adaptable to encourage innovation while maintaining ethical standards and protecting public interests.

Fewer than half of all agencies have adopted an AI policy

Only 38% of agencies have established formal AI policies or embedded consideration of AI into existing policies. Some agencies reported that a policy was under development or review, while other agencies reported that they rely on the Artificial Intelligence Ethics Policy. While the policy sets out overarching principles that are designed to ensure best practice use of AI, in isolation, it is unlikely to be sufficient. This is because an agency level policy is required to deal with elements that go beyond the NSW Government's ethical principles. These may include:

- 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.

Agencies should better integrate AI into their existing governance arrangements

Agencies need to more effectively integrate AI considerations into their governance frameworks to address the specific and unique risks posed by AI. This includes evaluating AI's broader impacts on accountability structures, policies and procedures (such as IT, procurement, risk management), and ensuring staff are adequately trained to both take advantage of AI and ensure its responsible use. As more AI tools are developed and deployed, ensuring there is appropriate integration with current governance structures will become more important.

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

Element	Details	Percentage of agencies that considered the element
Accountability	While exact responsibilities may differ, generally, an overall owner would be responsible for overseeing the deployment, ethical use and maintenance of AI tools, as well as ensuring that they align with the agency's objectives and legal and regulatory standards.	67%
Risk management	Reviewing an agency's risk management framework when adopting and rolling out AI is essential because AI introduces new, complex and evolving risks that traditional frameworks may not adequately address.	33%
Procurement	While not mandatory for the NSW public sector, the National framework for the assurance of artificial intelligence in government specifically outlines that careful consideration must be applied to procurement documentation and contractual arrangements. This includes consideration of: • AI ethics principles • clearly established accountabilities • transparency of data • access to information assets • proof or performance testing throughout an AI system's lifecycle.	5% (Given the prevalence of procured AI solutions, agencies may need to develop specific procurement guidelines tailored to AI tools. The NSW Government also provides detailed guidance on AI procurement essentials, see Artificial intelligence (AI) procurement essentials | info.buy.nsw)
Information technology	The unique nature of 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.	33%
Training	Training in the responsible use of AI is essential for staff to ensure AI is used ethically and within guardrails set by the agency, enabling agencies to maximise benefits and minimise risks.	67%
Reporting process	Regular reporting to senior management or governance bodies ensures ongoing oversight of AI adoption, aiding strategic alignment, risk management and transparency.	29% (had policy or procedures for monitoring, evaluating and reporting on adoption and use of AI) 52% (had undertaken some reporting to senior management or a relevant governance committee)

7.4. Artificial intelligence assessment framework

The NSW AI assessment framework helps to ensure responsible use of AI

The NSW Artificial Intelligence Assessment Framework has been established to guide NSW government agencies through the ethical development, deployment and use of AI. Its primary aim is to ensure AI solutions are designed, built and operated with a strict adherence to the mandatory Artificial Intelligence Ethics Policy.

Different requirements apply depending on the quantum of the project and funding source. While all agencies will generally be required to complete the self-assessment, projects above $5 million or funded by the Digital Restart Fund must be registered with the Department of Customer Service and be assessed under the NSW Digital Assurance Framework. The NSW Artificial Intelligence Assessment Framework also notes that agencies may not need to apply the framework to projects that are:

- using an AI system that is a widely available commercial application (which the agency is not training or customising), or
- conducting exploratory research that does not meet the criteria for elevated risk.

Further analysis was undertaken on AI projects across agencies that met the requirements above. This analysis found that:

- 13 of 15 relevant agencies with projects under $5 million had completed the NSW AI Assessment tool. One agency that completed the assessment did not have an appropriate senior officer approve the assessment.
- The three relevant agencies with projects above $5 million had completed the NSW AI Assessment tool and had it approved by a senior officer within the agency. However, one agency had not registered the project with the Department of Customer Service.

7.5. Strategic use of artificial intelligence

Around a quarter of agencies have a strategy to help maximise the benefits of AI

Although agencies have implemented AI and plan to expand its use further, only 29% report having a supporting strategy in place. More focus on the strategic use of AI could help maximise benefits from AI and ensure alignment with agencies' objectives. Seven of the agencies advised that they are currently developing either a dedicated AI strategy or integrating one into a broader plan.

Greater visibility over the use, challenges and risks may help to remove barriers to adoption of AI

Earlier in this chapter, it was observed that agencies encounter several challenges and barriers in adopting AI effectively. Increased transparency regarding the use, challenges and risks of AI may address some of these barriers; however, agencies currently experience gaps in senior level oversight.

Only half of the agencies are actively identifying or monitoring risks related to AI initiatives. This limited level of awareness may result in missed opportunities to mitigate potential issues early or to leverage opportunities. Moreover, just half of all agencies report to senior management or governance committees on the adoption and use of AI.

This lack of routine reporting can hinder informed decision-making at the leadership level, making it difficult to align AI activities with broader organisational objectives or to allocate resources effectively. Without consistent communication and oversight, there is a risk that AI projects may operate in silos, with limited coordination or shared learning across the organisation.

8. Technology - Cyber security

Cyber security risk has become a critical concern for government. Cyber threats can disrupt operations, compromise sensitive data and damage reputations. The dependence on third-party vendors and overall supply chains introduces risk, as these external partners may not have the same level of cyber security measures in place as agencies. Understanding and managing cyber risk, including those from third parties, is essential for maintaining business continuity and protecting valuable assets.

Agencies have responded to such risks by implementing controls and investing in cyber security measures to protect their assets and data, in accordance with the requirements of the NSW Cyber Security Policy (CSP).

This chapter analyses how agencies:

- manage their internal and supply chain cyber security risks
- control and monitor their cyber security investments.

As explained in Appendix 1, this chapter includes 20 of the agencies included in this report. These agencies were selected as they were required to submit their own cyber security attestations to Cyber Security NSW. The other agencies rely on shared service arrangements and cyber security controls from other agencies.

Chapter highlights

- Three agencies do not have a formal cyber security risk management policy that covers supply chain risks. Of 19 agencies that have established IT asset registers for internal and external systems, only twelve have a strategy to ensure the completeness of the register.
- There are weaknesses in agencies' management of supply chain cyber security risks. These included not clearly specifying cyber security roles and responsibilities in supplier contracts, excluding key third-party service providers in their cyber incident response plan testing, not enforcing third-party cyber security responsibilities and lacking formal processes to maintain cyber security and resilience after IT partnership or service agreement termination.
- Agencies have weaknesses in their management of cyber security spending. Agencies are not consistently performing cost and benefit analysis, setting and monitoring investment/benefit realisation on cyber security investments, or ensuring security investments are aligned with agency cyber security needs and threats. Only seven agencies identify and manage underutilised, redundant or outdated cyber security tools and services.

8.1. Background

The Cyber Security Insights 2025 report summarised how agencies are meeting the requirements of the CSP. It also offered insights that can further improve the annual cyber security attestation process. This report also presented a summary of gaps in cyber security governance controls identified between 2018 and 2025 across NSW state agencies, universities and the local government sectors.

Agencies have responded to such risks by implementing controls and investing in cyber security measures to protect their assets and data, in accordance with the requirements of the CSP. All NSW Government departments and public service agencies must report the following to Cyber Security NSW (Department of Customer Service) by 31 October each year, in a format provided by Cyber Security NSW:

- an assurance assessment against all mandatory requirements in the CSP for the previous financial year
- cyber security risks with a residual rating of high or extreme
- an attestation on cyber security of the reporting entity, including adherence to the requirements of the CSP.

Cyber threats can disrupt agency operations, compromise sensitive data and damage reputations. Dependence on third-party vendors and supply chains introduces further risk, as these third parties may not have appropriate cyber security measures in place. Understanding and managing cyber risk, including risks associated with third parties and an agency's supply chain, is essential for maintaining business continuity and protecting valuable data and assets.

Agencies have responded to these cyber risks by implementing controls and investing in cyber security measures to protect their assets and data. It is crucial to continuously assess and monitor these investments to ensure they are effective, up-to-date and capable of addressing the latest threats. This ongoing evaluation also helps agencies achieve their cyber protection goals while ensuring an effective and efficient spending on cyber security.

8.2. Managing supply chain cyber security risks

As organisations increasingly rely on complex technologies and third-party services, the potential for cyber threats originating from these third parties has grown significantly. Understanding and managing cyber risk in supply chains, including with third parties, is essential for maintaining business continuity and protecting valuable data and assets.

We reviewed the process in place for managing cyber security risk, including those arising from supply chains. This assessment focused on determining whether agencies:

- effectively maintain, manage and monitor their cyber security risks, encompassing both internal threats and those associated with third parties and overall supply chains
- maintain an up-to-date inventory of all assets related to both external and internal systems, supported by robust procedures to ensure completeness and appropriate risk classification of each asset
- employ structured protocols for third-party management, including rigorous due diligence practices, clear definition and oversight of roles and responsibilities, as well as ongoing management of security risks throughout the lifecycle of IT partnerships.

Three agencies do not have a cyber security risk management policy that covers supply chain risks

The CSP has mandatory requirements regarding management of cyber security risk. The CSP mandatory requirement 1.9 obligates agencies to ensure that cyber security risks in all areas of the agency are identified, assessed, managed, documented and reported as part of the agency's enterprise risk management framework.

Seven agencies do not have a formal strategy to ensure the IT asset register for external and internal systems is complete

IT asset registers have been established by 19 agencies, covering internal hardware and software, as well as third-party systems in use. Of these agencies, 12 have a formal strategy to ensure completeness of their registers.

Weaknesses in managing third-party cyber security risks

Agencies that do not manage third-party cyber security risk effectively may expose themselves to significant vulnerabilities, leading to data breaches, operational disruptions, financial losses and reputational damage.

A formal due diligence process is in place for 18 agencies. This process needs to be performed before entering vendor relationships. The two agencies without a due diligence process explained that they normally perform an assessment, but it is not based on a formal process and may not be properly documented.

In addition:

- four agencies have not specified cyber security roles and responsibilities for vendor or other third-party relationships within their contract
- five agencies have not included relevant third-party service providers in their cyber incident response plan testing
- four agencies do not monitor and enforce third-party cyber security responsibilities throughout the technology product and service lifecycle
- five agencies do not have a formal process or plan to ensure security risks and resilience are maintained after termination of IT partnership or service agreements.

Mandatory Requirement 1.10 from the CSP sets out minimum expectations for third-party security risk management and the recent DCS-2025-04 - Cyber Security NSW directive– Targeted Initiatives for NSW Government document outlines several targeted initiatives to strengthen cyber security across NSW Government agencies, with a clear emphasis on managing third-party risks.

- Agencies that outsource Information Technology (IT) services rely on third-party platforms and are reminded that accountability for cyber risk remains with the agency, not the vendor. This includes ensuring compliance with the CSP and maintaining visibility into the security posture of external providers.
- Agencies must conduct regular cyber risk assessments of third-party systems and services.
- The directive recommends that agencies embed cyber security requirements into contracts with third-party vendors, including minimum security standards, reporting obligations for incidents and audit right to verify compliance.

The Cyber Security Insights 2025 report identified third-party risk management as one of the most significant and persistent challenges facing NSW public sector agencies. The report emphasises that while agencies are increasingly reliant on third-party service providers, many lack adequate oversight and assurance mechanisms to manage associated cyber risks effectively. Case studies of cyber incidents involving third parties were highlighted in this report, highlighting the reality of cyber security risks coming from third parties.

8.3. Management of cyber security spending

In responding to ongoing cyber threats, agencies are increasingly allocating resources to cyber security to protect their assets and data. However, technology is constantly evolving in response to evolving cyber threats, making it crucial to continuously assess the effectiveness of these investments. Regular monitoring ensures that the security measures in place are up-to-date and capable of addressing the latest threats and risks. It also helps in identifying any gaps or outdated systems that may no longer provide adequate protection.

We analysed process in place for managing cyber security procurement and benefit realisation including identification and management of duplicate/redundant cyber security tools and services. Our assessment focused on whether agencies:

- perform and document a cost–benefit analysis during the procurement process for cyber security tools and services, and if they compare outsourcing versus in-house options
- have an established process for setting and monitoring return of investments/benefit realisation related to cyber security spending
- have a mechanism to monitor ongoing cyber security investments for alignment with current threat landscapes and organisational needs
- have a formal strategy to prevent resource wastage or duplication of efforts in cyber security initiatives.

Eight agencies do not perform a cost–benefit analysis when procuring cyber security tools and services

Conducting a cost–benefit analysis for cyber security investments is crucial for efficient resource allocation, justifying expenditures, managing risks, ensuring stakeholder confidence, maintaining regulatory compliance and enabling continuous improvement. Most agencies conduct a cost–benefit analysis as part of the business case when reviewing or defining their cyber strategy.

Lack of process to set and monitor benefit realisation on the cyber security spending

Thirteen agencies do not have a process to set and monitor the return of investment or benefit realisation on the investments they have made in cyber security. Of these agencies, 12 did not measure the effectiveness of cyber security spending with specific metrics and they do not have a formalised procedure for action when cyber security investments are not meeting the return of investment expectation.

Seven agencies have a process in place to set and monitor investments, such as an assessment as part of the program evaluation cycle, regular contract performance assessments, use of specific metrics and alignment of compliance levels with certain cyber security framework.

Some agencies do not have a formal process in place to ensure security investments are aligned with current threat landscapes and organisational needs

Two agencies do not have a formal process to monitor if cyber security investment is aligned with current threat landscapes and organisational needs. Cyber threats are constantly evolving, therefore what has worked in the past may not be sufficient to protect against new and emerging risks. By staying updated with the latest threat landscape, agencies can implement the most appropriate and effective security measures to protect against cyber threats.

Some agencies have identified underutilised, redundant or outdated cyber security tools and services

Most agencies have a formal process to maintain a register or inventory of their cyber security tools and services. Of these agencies, thirteen do not have a formal process for identifying and managing underutilised, redundant and/or outdated cyber security tools and services.

Managing underutilised, redundant or outdated cyber security tools and services is essential as it:

- helps maintain a robust security posture by ensuring that all tools and services are effective and up-to-date, thereby reducing vulnerabilities and potential entry points for cyber attackers
- optimises resource allocation, allowing agencies to reallocate funds from ineffective tools to more impactful security measures, which not only enhances overall security but also ensures that the cyber security budget is used efficiently.

Additionally, managing cyber security tools reduces complexity within the cyber security infrastructure, making it easier to monitor and manage. This streamlined approach helps prevent oversight and errors, further strengthening security.

We identified that:

- five agencies have at least one underutilised cyber security tool due to unresolved issues, configuration gaps or limited coverage
- four agencies have current cyber security tools that are outdated and no longer suitable for meeting operational needs. These tools have either been replaced, are in the process of being updated, or are scheduled for future replacement
- two agencies have cyber security tools that were redundant and have now been replaced. One of these agencies shared that removing this redundant tool had resulted in savings of approximately $50,000.

9. Technology - Information technology general controls

Agencies rely on information technology (IT) systems to prepare their financial statements and deliver services to the public. Deficiencies related to Information Technology General Controls (ITGC) continue to be a key area of concern, accounting for half of all findings reported to the agencies included in this report. Of the five high-risk findings identified, all related to ITGCs for key financial systems.

Australian Auditing Standard ASA 315 Identifying and Assessing the Risks of Material Misstatement requires an auditor to:

- understand the entity's information system relevant to the preparation of the financial report
- identify the specific risks arising from the use of IT (including cyber security risks) and evaluate the effectiveness of the entity's controls that address those risks.

A list of agencies included in this chapter is included at Appendix 1.This chapter provides analysis of the reported ITGC and cyber security findings identified as part of financial audits for the 26 agencies included in this report.

Chapter highlights

- Agencies have continued to face challenges in implementing appropriate controls to manage risks for key financial systems, including in relation to IT governance, user access, change management and cube security.
- Three agencies did not have appropriate IT governance in place, including gaps in key policies, procedures and standards. Three agencies did not have appropriate assurance over controls at third-party vendors.
- Not all agencies have taken steps to manage user access to key financial systems appropriately, increasing the risk of unauthorised access and loss. Key deficiencies include proper approval of user access provisioning, removal of user access on termination, regular revalidation of user access, monitoring of privileged user activities and implementation of password configurations.
- Three agencies did not segregate developer access from access to migrate changes into the production systems. These ineffective change management controls may reduce system integrity at these agencies.
- Three agencies lacked a formal disaster recovery plan (DRP) and testing for a key financial system, including two that did not undertake a disaster recovery test, increasing the risk that critical systems or operations may not be restored in a timely manner during a major disruption at these agencies.
- One agency does not have adequate cyber security controls to detect or prevent cyber security incidents, including operating unsupported systems (including those that host crowns jewel applications) without a formal risk assessment or plan.

9.1. Background

While IT enhances efficiency and accuracy, where not properly managed it can introduce risk to financial reporting and management. ITGCs are foundational controls essential for ensuring the integrity, reliability and security of financial systems, including:

- IT governance
- access management
- change management
- IT operations.

Risks arising from weak ITGCs include:

- unauthorised access to data that may result in destruction of data or improper modification
- unauthorised changes to IT applications or other aspects of the IT environment that undermine the integrity of processing or reporting of transactions
- inability to recover from IT incidents
- compromised segregation of duties and management override of established controls that may lead to fraudulent transactions made through the system
- potential loss of data or inability to access data as required.

9.2. Information technology governance

IT governance provides a framework that aims to ensure IT is managed in alignment with an agency's objectives. For each agency we evaluated whether:

- policies and standards are defined and are current across all key areas of IT
- IT management identifies and documents risks and reports significant risks to senior management of the agency
- management obtains independent assurance that service providers maintain an appropriate level of control over their environment, proportionate to the reliance placed by the agencies.

Three agencies have gaps in creating, updating and adopting IT policies, standards and procedures

One agency had a division that operated its systems independently from established enterprise governance and central IT functions without formal IT policies and procedures.

Two agencies had a number of key IT policies, standards and procedures that were outdated, including some that had been in draft without endorsement for the previous three to four years. These included policy and standards related to access management, system vulnerability management, system interface, identity and access management, and cyber incident response planning.

Agencies should ensure IT policies are current and properly adopted to ensure alignment with current business processes, generally accepted practices and regulations.

Three agencies did not evaluate their third-party IT service providers

These agencies have deficiencies in their oversight of IT service providers, including:

- an agency that did not have a process to review independent third-party assurance reports on the effectiveness of its service provider's controls, which is essential for holding third parties accountable to meet their obligations, including for security
- two agencies, while receiving third-party assurance reports, could not demonstrate they had reviewed the reports.

Failure to identify and respond to risks from third-party service providers may lead to business disruption due to system outages or weaknesses and loss of confidential information caused by fraud, cyber-attacks and security breaches.

Agencies should ensure that third-party IT providers comply with contractual obligations or service level agreements, maintaining effective controls in their environments. By examining independent assurance reports, agencies can evaluate vendor environments and verify that any identified issues are appropriately resolved.

9.3. Access management

IT access management ensures that transactions and changes made to data are performed in the normal course of business by authorised individuals. For each agency we evaluated whether:

- access is appropriately approved for new and modified access requests
- access is removed when no longer required
- access rights are reviewed periodically and excessive access, if identified, is removed
- highly privileged accounts are restricted and monitored
- systems are configured to reduce the risk of guessing or otherwise determining an account password.

Four agencies granted user access to systems without proper approval

Four agencies had deficiencies in ensuring that user access is approved before it is provided to users. One of these agencies could not provide evidence to support the approval of a new account creation in their key system database. Two agencies did not follow standard processes and provided user access to financial systems before approval was provided. These two agencies offer shared services to other agencies. The remaining agency has business units that did not perform a formal user access management process as required by the policy and procedures set by the central IT team.

Agencies should ensure access to the system is granted only after obtaining the necessary approvals. Evidence of user access approval should be formally documented and retained.

Five agencies delayed deactivating system access for users who no longer needed it

Five agencies did not promptly remove users' access. Contributing factors included delayed offboarding requests and incomplete execution of the access removal process. Four of these agencies offer shared services to other agencies.

Agencies should ensure that access removal is timely at employee termination and that processes are in place allowing timely communication by people/payroll teams to system administrators to disable or delete inappropriate access.

Weaknesses in user access provisioning and deprovisioning can lead to inappropriate and unauthorised system access, increasing the risk of fraud, cyber attacks and invalid transactions. This can compromise the integrity, confidentiality and accuracy of financial data.

Eight agencies did not effectively review and revalidate user access

Eight agencies had deficiencies in their review and revalidation of user access. Four of these eight offer shared services to other agencies. These deficiencies included:

- a failure to conduct user access reviews for key financial systems during the financial year, or reviewers providing incomplete or late reviews
- limited review coverage where a review did not include all key areas/functions or only covered the validity of the user without checking their access level.

In the case of four agencies, we identified users with inappropriate access to key transactions, such as the ability to modify others' basic pay and bank account details, modify batch jobs configurations or excessive access to other branches.

Weaknesses in user access review controls may lead to users retaining invalid access after role changes or departure, which potentially enables inappropriate access for unauthorised transactions.

Agencies should regularly perform reviews of user access to ensure existing access permissions are appropriate and user accounts are still required. Review and corrective action should be prompt and evidence of changes retained.

Seven agencies are not effectively monitoring privileged user activities

Seven agencies failed to effectively monitor privileged user activities due to gaps, such as no established formal process, no audit log available, use of a generic privileged account without a way to identify who uses it, and delay or incomplete review.

The absence of periodic reviews of privileged user activities increases the risk that inappropriate and unauthorised activities within the system are undetected**.**

Agencies should ensure privileged user activities are regularly reviewed by a suitably independent and qualified individual, with appropriate action taken when required. Formal evidence of the review should be documented and retained to demonstrate effective oversight and compliance.

Four agencies have not complied with their password policies

Deficiencies identified included discrepancies in password configurations, such as minimum length, complexity, maximum age, number of invalid login attempts, password history and lockout duration upon invalid login attempts.

Weaknesses in password configuration settings may make it easier for a user account to be compromised, allowing a party with unauthorised access to use and change financial and non-financial information for malicious or fraudulent purposes.

Agencies should ensure that their password policy and standards are in line with current good practice for the effective use of passwords or passphrases. Agencies should ensure their own standards are enforced through system configuration.

Case study – Vendor governance and user security issues

One agency had weaknesses in the governance of its vendor provided IT system. Issues included the absence of system implementation controls, and problems with user security management such as the allocation of privileged user access rights to users. These control deficiencies were identified in a business unit operating a public facing system independently from the central IT team. These control gaps may be present in many other business units that the agency has across NSW.

In addition, each business unit had a choice of agency approved vendor system, but there was a reliance on the vendor to manage the implementation without appropriate controls performed by the business units or the agency to ensure successful system implementation. These control gaps created weaknesses at the business units for the approval of invoicing and refunds.

Deficiencies in controls included:

- user creation and approval, user access removal, validation of user access, limiting privileged access and monitoring privileged activities that did not follow agency policies or standards
- no formal approval that all user training, system configuration, security set up and data migration was completed during the system implementation process. The vendor managed the system implementation project with the business unit, performed the data migration and provided the user training, but did not communicate the outcomes of these deliverables
- while the agency performed limited reviews of the vendor security and certifications, they did not require the vendor to provide independent assurance reports over the process and controls performed by the vendor. The vendor did not meet the agency's policy for monitoring of privileged user activities.

Failing to follow policies and standards, document actions appropriately, identify breaches of security standards and restrict privileged access exposes the agency to the risk of unauthorised access, system breaches and inappropriate financial transactions. Gaps in system implementation processes could expose the agency to a delayed system that uses the incorrect data, processes transactions incorrectly and is used by staff who have not been trained in its use.

9.4. Change management

Controls over IT changes ensure that changes to how programs work are in line with requirements, and that unintended or unauthorised changes are not made. For each agency we evaluated whether:

- changes are appropriately tested before implementation to validate that systems operate as intended
- changes are authorised to ensure they are in line with business requirements and expectations, and have been adequately documented and reviewed
- duties are segregated to prevent people from making changes and then implementing them without independent approval
- as part of new system implementation, overall project management, user acceptance testing, data migration testing, go-live approval and training are performed by management.

Three agencies do not segregate developer access from the access to migrate changes into production systems

This lack of segregation allows changes to be made without going through the formal change management process where an independent check on the validity of the change is undertaken.

Lack of appropriate segregation of duties may lead to unauthorised, untested or erroneous changes that compromise system integrity and audit reliability.

Agencies should ensure that there is a segregation of duties between those who can make changes and those who can implement changes. Where agencies allow these practices due to the small size of their specialist teams, additional governance and monitoring processes should be implemented to mitigate the risk.

Two agencies did not keep sufficient records for system changes

Two agencies did not retain records of controls performed to support changes made to their financial systems (including in the implementation of new systems). Deficiencies included:

- evidence of testing and approval for changes were not always documented
- system patching was performed without adequate testing prior to implementation
- evidence of data migration testing for a key system migration was not fully documented.

An absence of records supporting system changes undermines controls intended to ensure changes to systems work as intended and that data is transferred accurately and completely.

Agencies should formally record significant decisions and approvals during system implementations.

9.5. Information technology operations

Management and control of IT operations ensures that key IT processes operate as expected, and that systems are recoverable in the event of a disaster. For each agency we evaluated whether:

- key processes are monitored and action is taken to resolve issues identified
- key financial data is backed up, and agencies validate that backed up data can be restored
- DRPs are documented and tested.

Three agencies do not have current DRPs or have not tested those plans

A DRP helps agencies maintain IT services in the event of a service disruption or restore IT systems and infrastructure in the event of a disaster or similar scenario.

Three agencies have deficiencies in their planning for recovering from disasters. Deficiencies included:

- not having a DRP for a key financial system
- not testing of one or more DRPs for key financial systems
- limitations in time period in which data is backed up.

There is a heighted risk that without an approved and tested DRP, critical systems or operations may not be restored in a timely manner during a major disruption. Inadequate back up processes may not support system restoration and recovery.

Agencies should:

- have approved DRP documents that are tested periodically to validate the effectiveness, completeness and readiness of agency response to technology disruptions
- periodically test their back-ups and ensure appropriate back up configuration is applied.

9.6. Cyber security risks over financial statements

We evaluated the following as part of financial statement audits to assess relevance of cyber security risks to the financial statement generation:

- cyber security policies and procedures are documented and appropriately approved
- cyber risks are identified, recorded and managed through a formal risk management process
- key processes are in place to protect systems and financial data from cyber threats through preventive, detective and responsive security measures.

Chapter 8 includes analysis relating to risks in the supply chain and investments in cyber security tools.

One agency does not have adequate cyber security controls to prevent or detect cyber security incidents

Weaknesses in cyber security controls may limit an agency's ability to detect, prevent or respond to cyber threats. Agencies should implement key cyber security controls that allow them to detect or respond to cyber security threats in a timely manner as described in the case study below.

Case study – Cyber security

One agency runs unsupported operating systems on a number of servers without a:

- formal risk assessment
- action plan as to how to safely continue using the systems and/or work towards replacing them.

Some of these servers also host 'crown jewel' applications. Unsupported operating systems do not receive regular security updates from a vendor. The absence of vendor support increases the vulnerability of the systems to cyber security threats.

In addition, the risk of cyber security incidents was increased as a result of ineffective controls including:

- distributed denial of service attack prevention not implemented
- multi-factor authentication not configured for access into key systems
- event monitoring tools not utilised for all 'crown jewels'
- unsupported systems in use without a formal risk assessment or a management action plan.

The agency experienced a cyber-attack affecting another key financial system. As a result of inadequate event monitoring controls, the cyber attacker remained within the environment for around a month without being identified.

Section 2 –

Appendices

Appendix 1 – Agencies included in this report

This report includes the largest 26 NSW public sector agencies (excluding state owned corporations and public financial corporations). These agencies are included in this report as they:

- collectively account for approximately 95% of the NSW Government's 2024–25 total budgeted expenditure
- deliver a diverse variety of services and are exposed to numerous financial, operational and strategic risks.

The tables below outline which agencies have been included in each chapter of this report. The inclusion of these agencies in this analysis provides representative cross-section of NSW Government entities, chosen based on relevance to the subject matter and operational significance. Further information on why these entities were selected is available in the corresponding chapter of the report.

Key

Report analysis status			
Agency included in chapter analysis	✓	Agency not included in chapter analysis	–

Agencies selected for thematic analysis by chapter

Agency	Chapter 5: Internal Controls	Chapter 6: Procurement	Chapter 7: Artificial intelligence	Chapter 8: Cyber security	Chapter 9: IT general controls
Ministry of Health	✓	✓	✓	✓	✓
Transport for NSW	✓	✓	✓	✓	✓
Sydney Trains	✓	✓	✓	✓	✓
Department of Education	✓	✓	✓	✓	✓
Department of Climate Change, Energy, Environment and Water	✓	✓	✓	–	✓
Department of Communities and Justice	✓	✓	✓	✓	✓
NSW Land and Housing Corporation	✓	✓	–	–	✓
NSW Police Force	✓	✓	✓	✓	✓
Department of Primary Industries and Regional Development	✓	✓	✓	✓	✓
Department of Customer Service	✓	✓	✓	✓	✓

Agency	Chapter 5: Internal Controls	Chapter 6: Procurement	Chapter 7: Artificial intelligence	Chapter 8: Cyber security	Chapter 9: IT general controls
Department of Planning, Housing and Infrastructure	✓	✓	✓	✓	✓
TAFE Commission	✓	✓	✓	✓	✓
Corrective Services NSW	✓	✓	✓	–	✓
Infrastructure NSW	✓	✓	✓	✓	✓
Sydney Metro	✓	✓	✓	✓	✓
Transport Asset Manager of New South Wales	✓	✓	–	–	✓
NSW Treasury and Crown Finance Entity	✓	✓	✓	✓	✓
NSW Self Insurance Corporation (Insurance for NSW)	✓	–	✓	✓	✓
State Insurance Regulatory Authority	✓	–	–	–	✓
NSW Rural Fire Service	✓	–	✓	✓	✓
Property and Development NSW	✓	–	–	–	✓
Service NSW	✓	–	✓	✓	✓
Premier's Department	✓	–	✓	✓	✓
Fire and Rescue NSW	✓	–	✓	✓	✓
Department of Creative Industries, Tourism, Hospitality and Sports (formerly Department of Enterprise, Investment and Trade)	✓	–	✓	✓	✓
NSW Reconstruction Authority	✓	–	–	✓	✓

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