FINANCIAL AUDIT

20 DECEMBER 2022

Internal controls and governance 2022

NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

audit office
OF NEW SOUTH WALES

THE ROLE OF THE AUDITOR-GENERAL

The roles and responsibilities of the Auditor-General, and hence 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 add credibility to financial statements, 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 examine whether an entity is carrying out its activities effectively and doing so economically and 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.

As well as financial and performance audits, the Auditor-General carries out special reviews, compliance engagements and audits requested under section 27B(3) of the *Government Sector Audit Act 1983,* and section 421E of the *Local Government Act 1993*.

GPO Box 12
Sydney NSW 2001

The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 52B of the *Government Sector Audit Act 1983*, I present a report titled **'Internal controls and governance 2022'**.

Margaret Crawford
Auditor-General for New South Wales
20 December 2022

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

RECONCILIATION COMMITMENT STATEMENT

The Audit Office of New South Wales pay our respect and recognise Aboriginal people as the traditional custodians of the land in NSW.

We recognise that Aboriginal people, as custodians, have a spiritual, social and cultural connection with their lands and waters, and have made and continue to make a rich, unique and lasting contribution to the State. We are committed to continue learning about Aboriginal and Torres Strait Islander peoples' history and culture.

We honour and thank the traditional owners of the land on which our office is located, the Gadigal people of the Eora nation, and the traditional owners of the lands on which our staff live and work. We pay our respects to their Elders past and present, and to the next generation of leaders.

auditoffice
OF NEW SOUTH WALES

Banner image: 'Yarning Circle' by Caitlin Liddle, Audit Office Indigenous Internship Program participant used with permission.

contents

Internal controls and governance 2022

1. Introduction

1.1 State sector agencies

This report covers the findings and recommendations from our 2021–22 financial audits that relate to internal controls and governance at 25 of the largest agencies in the NSW public sector, excluding state-owned corporations and public financial corporations.

The agencies included in this report deliver a diverse variety of services and are exposed to numerous financial, operational and strategic risks. Effective internal controls and governance frameworks help to mitigate the likelihood of risks arising and their severity if they do.

A list of the 25 agencies included in this report is shown below in cluster groups.

Exhibit 1.

1.2 Financial snapshot

The 25 agencies included in this report constitute an estimated 95% of total expenditure for all NSW public sector agencies, excluding state-owned corporations and public financial corporations. The snapshot below provides an indication of the collective size of assets, liabilities, income and expenses of these 25 agencies for the year ended 30 June 2022.

	Number of agencies	Assets $ billion	Liabilities $ billion	Income $ billion	Expenses $ billion
Departments	9	263.4	42.1	107.7	100.3
Public non-financial corporations	3	69.7	7.6	6.4	6.7
Statutory bodies	13	65.9	29.7	23.7	18.4
Total	**25**	**399**	**79.4**	**137.8**	**125.4**

Note: The reported figures above include the impact of inter-agency transactions and balances, which are eliminated at a total state sector level. Income and expenses exclude income tax and other comprehensive income.

Source: Audited financial statements of agencies, for the consolidated entity (if consolidated).

1.3 Areas of focus

This report covers the following topics:

Cyber security planning and governance

Strong cyber security continues to be an important component of the NSW Beyond Digital strategy, enabling the effective use of emerging technologies and ensuring confidence in the services provided by NSW government. Increased cyber resilience and capability is required to respond to rapidly evolving cyber risks.

This report focuses on whether agencies have:

- developed effective cyber security policies and procedures
- implemented tools to manage cyber risks and uplift their cyber security maturity.

Engaging consultants and contractors

Consultants are frequently engaged to provide independent advice that supports decision-making in government. Contractors supply external labour to agencies, particularly for expert skills, but it is important for agencies to consider risks of creating a dependency on contractors.

This report focuses on whether agencies have:

- effective policies to maintain probity when engaging consultants for independent advice
- appropriate frameworks around workforce management with respect to engaging contractors.

Employment screening practices

Robust employment screening practices help to ensure that public service employees have appropriate skills and qualifications for their appointed roles.

This report focuses on whether agencies have:

- established policies on employment screening that ensure consistent practices
- conducted employment screening in line with better practice guidelines.

Contract management

Government agencies must ensure their internal policies and controls are consistent with the mandatory requirements of the NSW Government Procurement Policy Framework. The mandatory requirements include financial management obligations and policies relating to fraud and corruption control.

This report focuses on whether agencies have:

- established appropriate policies and procedures to manage procurement contracts
- complied with the *Government Information (Public Access) Act 2009* requirements on publishing details of government contracts.

1.4 Sector-wide learnings

Our review identified sector-wide learnings that government agencies should consider in relation to their internal control and governance frameworks, which we have summarised below.

Internal and information technology controls

- Address repeat control deficiencies by ensuring:
  - there is clear ownership of recommendations arising from internal control deficiencies, with timeframes and action plans for their implementation
  - audit and risk committees and agency executive teams monitor the implementation status regularly, focusing on those actions that are past due or have deferred implementation dates.
- Ensure compliance with Treasurer's Direction TD 21-04 'Gifts of Government Property' (TD 21-04) by annually certifying the accuracy and completeness of the agency's written register of gifts of government property, or attest that the agency has made no gifts.
- Review the implementation of user access controls to adequately protect the key financial and non-financial systems, focusing on the processes in place to grant, remove and monitor user access.
- Review the number of privileged users and the level of access granted to privileged users, and assess and document the risks associated with their activities. Based on this review, agencies should:
  - grant and restrict privileged user access only to staff who require that level of access to perform their role and only for the period for which they require that access
  - identify controls to address the risks associated with privileged user activity, including regular monitoring of activity logs
  - promptly remove access when it is no longer required.

Cyber security planning and governance

- Strengthen mechanisms that govern how third-party IT service providers comply with the agency's cyber security policy or plan, such as requiring:
  - compliance in standard term contracts with IT service providers
  - attestations or certifications from IT service providers confirming compliance
  - controls assurance reports relating to the IT service provider's controls around cyber security
  - the IT service provider notify the agency of any security incidents, regardless of whether they resulted in actual financial loss or breaches of information security.
- Continue to improve the agency's level of cyber maturity in the NSW Cyber Security Policy and Australian Cyber Security Centre Essential Eight Strategies to Mitigate Cyber Security Incidents frameworks to meet target levels.
- Ensure that the agency's reported level of self-assessed maturity is demonstrated by evidence, which could be verified by internal audit or an external expert.
- Continue to conduct mandatory, periodic cyber awareness training to all staff to build and support a cyber security culture, including:
  - reinforcing and improving the completion rates of staff mandatory training
  - ensuring third parties with access to the organisation's systems, such as contractors, consultants, vendors and partners are adequately trained in cyber risks
  - targeting training to certain groups of users who may be at greater risk of cyber attacks, such as procurement, payroll and executive staff
  - conducting simulated phishing exercises to test staff knowledge on responding to cyber threats.

Engaging consultants and contractors

- Improve the design of policies to include consideration of:
  - probity requirements and conflict of interests
  - rotation of independent consultants from time-to-time
  - additional review where multiple consultants are engaged on the same topic to address the risk of opinion shopping.
- Improve policy guidelines on engaging external labour/contractors that include consideration of workforce planning and strategy, such as:
  - Capability – if required specialist skills are not within the agency's core capability
  - Timing of work – if unpredictable or infrequent
  - Cost – if more efficient and effective to engage contractor
  - Timeframes for engagement – short-term rather than long-term.
- Agencies that have re-engaged the same contractor for multiple years for the same role should periodically reassess that contract against the market before renewing the contract to demonstrate that the contractor continues to represent value for money and effectiveness in achieving performance objectives.

Employment screening practices

- Ensure compliance with the *Government Sector Employment Act 2013* by screening citizenship requirements of public service employees.
- Perform credential checks for all appointments by validating educational and professional qualifications of the applicant, not just for roles which require a specific qualification.
- Non-permanent workers should be subject to the same employment screening checks as conducted for permanent workers.

Contract management

- Regularly review the completeness and accuracy of procurement contract registers to ensure compliance with the *Government Information (Public Access) Act 2009*.
- Establish central registers for contracts such as revenue or lease agreements.

1.5 Status of 2021 report recommendations

Our report on internal controls and governance for the year ended 30 June 2021 made a number of recommendations. The table below sets out the status of those recommendations being addressed by the relevant agencies.

Recommendation	Current status
Internal control trends	
Agencies should prioritise actions to address repeat control deficiencies, particularly those that have been repeated findings for a number of years.	15 of 24* agencies have addressed this recommendation. Seven agencies have partially implemented actions to address the recommendation. If control deficiencies are not addressed, the risks associated with the control deficiency increase with time, which is why they need to be addressed on a timely basis; refer to section 2.1 of this report for further details.
Cyber security planning and governance	
Agencies should prioritise improvements to their cyber security and resilience as a matter of urgency. Specific actions include:	Agencies' progress in implementing the recommendations is outlined below:
• ensuring their reported level of maturity is demonstrated by evidence	• 20 of 24* agencies have evidence to support their reported level of maturity
• report target levels of maturity for each mandatory requirement and Essential Eight control that they have determined is appropriate for the agency	• 20 of 24* agencies are reporting target levels of maturity for Essential Eight controls in accordance with NSW Cyber Security Policy mandatory requirements
• have processes whereby the agency head and those charged with governance formally accept the residual cyber risks.	• 22 of 24* agencies have implemented processes to report the residual cyber risks to those charged with governance for acceptance.
Tracking recommendations	
Agencies should formalise and implement policies on tracking and monitoring the progress of implementing recommendations from performance audits and public inquiries.	13 of 19 agencies to which this recommendation applies have implemented policies to track and monitor their performance audit or public inquiry recommendations.

Key **Fully addressed** **Partially addressed** **Not addressed**

* There is a total of 24 agencies reporting on the status of recommendations from 2021. One of the 25 agencies reported on last year, State Transit Authority of New South Wales, was dissolved in April 2022.

2. Internal control trends

Internal controls are processes, policies and procedures that help agencies to:

- operate effectively and efficiently
- produce reliable financial reports
- comply with laws and regulations
- support ethical government.

This chapter outlines the overall trends for agency controls and governance issues, including the number of audit findings, the degree of risk those deficiencies pose to the agency, and a summary of the most common deficiencies we found across agencies. The rest of this report presents this year's controls and governance findings in more detail.

For consistency and comparability, we have adjusted the 2021 results to incorporate additional audit findings that were reported after the date of the 'Internal controls and governance 2021' report. Therefore, the 2021 figures will not necessarily align with those reported in our 2021 report.

This section also covers how agencies have complied with TD 21-04 during 2021–22.

Section highlights

- We identified 23 high-risk findings, compared to 20 last year, with ten repeated from last year. Sixteen of the 23 findings related to financial controls and seven related to IT controls.
- The proportion of repeat deficiencies has increased from 47% in 2020–21 to 48% in 2021–22.
- We identified a low level of compliance with TD 21-04 during 2021–22. Most agencies do not have a policy on gifts of government property, and did not annually certify their register of gifts of government property or attest that the agency has not made any gifts.

2.1 High-risk findings

High-risk findings arise from failures of key internal controls and/or governance practices of such significance they can affect an agency's ability to achieve its objectives or impact the reliability of its financial statements. This in turn, increases the risk that the audit opinion will be modified.

We rate the risk posed by each control deficiency as high, moderate or low. The rating is based on the likelihood of the risk occurring and the consequences if it does. The higher the rating, the more likely it is that agencies will suffer losses, or its service delivery will be compromised. Our risk assessment matrix aligns with the risk management framework in NSW Treasury's Risk Management Toolkit for the NSW Public Sector.

The number of high-risk findings has increased from last year

We identified 23 high-risk findings out of a total of 279 audit findings this year, compared to 20 high-risk findings out of a total of 338 audit findings in 2020–21. As a proportion of total audit findings, high-risk findings have also increased from 5.9% to 8.2%. Of concern were ten high-risk findings that were repeat deficiencies reported in the previous year, including two deficiencies previously reported as high-risk in 2020–21. Sixteen of the 23 high-risk deficiencies related to financial controls and seven related to IT controls.

Agencies need to address high-risk internal control deficiencies as a matter of priority.

High-risk finding	Implication	Further reporting
We noted deficiencies in an agency's impairment assessment model for certain inventories. The agency was unable to substantiate and reconcile some of the underlying data used in the impairment model.	Management's inventory impairment assessment is subject to significant estimation uncertainty. Inaccurate or incomplete data underlying the impairment model can potentially have a material impact on the impairment provisions.	Further detail on this issue is included in 'Health 2022', which was tabled in December 2022.
The processing of time records remains an ongoing issue for an agency to meet its pay run obligations, with system administrators approving time records (forced-finalisation).	Management's practice of forced-finalisation of time records may result in over/under payment of staff. This may also increase the risk of errors, increased retrospective pay adjustments and material misstatement in the financial statements.	Further detail on this issue is included in 'Health 2022', which was tabled in December 2022.
An agency has an asset capitalisation threshold of $10,000. Treasury Policy and Guidelines TPG22-06 'Financial Reporting Code for NSW General Government Sector Entities' nominates a $5,000 asset capitalisation threshold (or a different threshold determined by the entity). The application of any threshold must be regularly reviewed to ensure that the risks of material misstatement do not outweigh the operational benefits. We identified assets that were incorrectly expensed and not capitalised.	Without regular review and assessment of the appropriateness of the asset capitalisation threshold, there is an increased risk that a material value of procurements that should be capitalised are expensed, which may materially impact the financial statements.	Further detail on this issue is included in 'Health 2022', which was tabled in December 2022.
We noted that controls assurance reports on IT General Controls (ITGC) at an agency's service providers reported significant deficiencies over user access, system changes and batch processing. Most of these deviations were not sufficiently mitigated to address the risk of unauthorised user access.	Control deficiencies in ITGC increase the risk of unauthorised transactions, system and configuration changes, and modifications to system reports. These increase the risk of material fraud and error in the financial statements.	Further detail on this issue is included in 'Customer Service 2022', which was tabled in November 2022.
A key management control over system change process is restricting or limiting the access of staff with system development responsibilities to the live business systems. This ensures appropriate segregation of duties, governance and integrity of the IT system change controls process. We identified these appropriate system controls were not in place at an agency to restrict developers from releasing or making changes to the live business systems.	Control deficiencies in change management increases the risk of system errors, system downtime, data error, incorrect financial reporting and fraudulent activity including cyber fraud.	Further detail on this issue is included in 'Customer Service 2022', which was tabled in November 2022.

High-risk finding	Implication	Further reporting
We identified deficiencies in controls over recording and reconciling an agency's significant database to its general ledger. The database system was not designed to facilitate financial reporting, resulting in extensive reconciliations and adjustments to information.	Control deficiencies in the completeness and accuracy of data can increase the risk of material misstatements in the financial statements. The agency may also not fulfil its responsibilities under applicable legislation.	Further detail on this issue is included in 'Planning and Environment 2022', which was tabled in December 2022.
A group of agencies did not comply with the *Government Sector Finance Act 2018* (GSF Act) to prepare annual financial statements. They also did not comply with Treasurer's Direction TD 21-03 'Submission of Annual GSF Financial Statements to the Auditor-General' to submit financial statements for audit within six weeks following the end of the annual reporting period.	Non-compliance with the reporting obligations under the GSF Act.	Further detail on this issue is included in 'Planning and Environment 2022', which was tabled in December 2022.
The financial statements of the NSW Total State Sector and the NSW Rural Fire Service do not recognise rural firefighting equipment, as the State is of the view that rural fire-fighting equipment vested to local councils under section 119(2) of the *Rural Fires Act 1997* is not controlled by the State. The agency should intervene to assess councils' compliance with legislative responsibilities, standards and guidelines.	The agency is not fulfilling its legislative obligations to assess councils' compliance with legislative responsibilities, standards and guidelines.	Further detail on this issue is included in 'Planning and Environment 2022', which was tabled in December 2022.
An agency had not restricted user access to key system functions including payroll management, vendor management and finance. Some users' level of access created a segregation of duties conflict.	Excessive user access and lack of segregation of duties enforcement increase the likelihood of inappropriate or unauthorised transactions/changes being made to the system.	Further detail on this issue is included in 'Planning and Environment 2022', which was tabled in December 2022.
An agency did not complete a comprehensive user access review in 2021–22 to validate all user accounts and the appropriateness of user access rights. This issue was first reported in 2018–19.	A lack of periodic user access review increases the risk of unauthorised access and breakdowns in segregation of duties controls and creates opportunities for fraud.	Further detail on this issue is included in 'Planning and Environment 2022', which was tabled in December 2022.
An agency did not review their third-party service providers' assurance reports or the review was not performed in a timely manner.	Without proper monitoring of process and controls operated by third-party service providers, there is an increased risk of unresolved/ unidentified issues.	Further detail on this issue is included in 'Planning and Environment 2022', which was tabled in December 2022.

High-risk finding	Implication	Further reporting
Control deficiencies were identified with an agency having no periodic comprehensive user access review performed to validate all user accounts and the appropriateness of user access rights. This deficiency was first reported in 2017–18. During September 2022 a user access review was initiated but not fully completed.	Lack of reviews over user access increases the risk of unauthorised access and breakdowns in segregation of duties controls because user profiles are inconsistent with a staff member's area of responsibility. Inappropriate access increases the risk that unauthorised or invalid transactions are processed, or confidential information is accessed or released.	Further detail on this issue is included in 'Stronger Communities 2022', which was tabled in December 2022.
Significant control deficiencies were identified with an agency's administration and financial reporting of grant programs.	The agency did not meet its performance obligations by obtaining the necessary approvals prior to recognising administration revenue. This may result in a breach of legislation and material misstatement in the financial statements.	Further detail on this issue is included 'Customer Service 2022', which was tabled in November 2022.
We noted deficiencies in an agency's provisioning, use and cancellation of purchasing cards. This included inappropriate usage and delays in submission and approval of transactions.	Weaknesses in purchasing card management elevates the risk of inappropriate or inaccurate transactions not being identified or detected in a timely manner.	Further detail on this issue is included in 'Education 2022', which was tabled in December 2022.
Some claims paid to injured workers between 2012 and 2019 may have been underpaid because indexation was incorrectly applied, or not applied at all.	Ineffective key controls including peer review and quality assurance frameworks designed to ensure the accuracy of payments, resulting in the potential underpayment of claims.	Further detail on this issue will be included in 'Treasury 2022', which will be tabled in December 2022.
We noted ongoing issues with internal processing of transactions. Internal controls were ineffective, unreliable and lacked supporting documentation.	Without sufficient controls in place the agency's calculations and payments are incorrect.	Further detail on this issue will be included in the 'Treasury 2022' which will be tabled in December 2022.
The quality and timeliness of financial reporting was significantly impacted for an agency due to a number of issues, including incorrect asset valuation, incomplete information used to produce the financial statements, and general ledger not reconciling to the financial statements submitted.	If the financial reporting process is not effective, it results in delays and increases the potential for significant misstatements in financial statements.	Further detail on this issue is included 'Enterprise, Investment and Trade 2022', which was tabled in December 2022.
An agency had not performed a regular comprehensive review of user access to validate user accounts and the appropriateness of user access rights. This deficiency had been reported as a repeat issue since 2017–18. The agency has a policy that user access reviews should be carried out at least quarterly.	The lack of periodic user access review increases the risk of unauthorised access and breakdowns in segregation of duties controls. Inadequate segregation of duties creates opportunities for fraud.	Further detail on this issue is included in 'Stronger Communities 2022', which was tabled in December 2022.

High-risk finding	Implication	Further reporting
Significant deficiencies were identified in the management and oversight of expenditure. There was insufficient evidence of the agency's documentation and review of the expenditure. A prior period error was also corrected retrospectively regarding these expenses.	Deficiencies in the management and oversight of expenditure increases the risk: • of inadequate management of public monies, and may result in incorrect payments to third parties • that expenditure of public moneys is not appropriately authorised in line with delegation instruments • of material misstatements and disclosure deficiencies • of non-compliance with the GSF Act.	Further detail on this issue will be included in 'Treasury 2022', which will be tabled in December 2022.
An agency's financial statements and supporting evidence submitted for audit included deficiencies that indicated a lack of quality review of information prior to its submission. This was a repeat high-risk finding from 2020–21.	A lack of quality review increases the risk of material misstatements and disclosure deficiencies in the financial statements.	Further detail on this issue will be included in 'Treasury 2022', which will be tabled in December 2022.
An appropriation to a fund had not been recorded on the basis that it was suspended. However, suspension of an appropriation was legally ineffective. The financial statements were subsequently amended to include disclosure of the appropriation.	The NSW Government does not have the power to suspend an appropriation made by Parliament.	Further detail on this issue will be included in 'Treasury 2022', which will be tabled in December 2022.
We identified significant deficiencies in accounting for the appropriation of hypothecated funds to Special Deposit Accounts and compliance with the GSF Act.	Not accounting for hypothecated appropriations results in the agency not complying with section 4.16 of the GSF Act in its capacity as responsible manager.	Further detail on this issue will be included in 'Treasury 2022', which will be tabled in December 2022.
We identified that monitoring and approval of administration costs of some grant programs, that required approval and sign-off, was not received before costs were deducted.	The absence of delegated approval of administration costs, prior to these being deducted, could lead to significant breaches of legislation and grant funding agreements.	Further detail on this issue will be included in 'Treasury 2022', which will be tabled in December 2022.

Note: Management letter findings are based either on final management letters issued to agencies, or draft letters where findings have been agreed with management.

2.2 Common findings

While it is important to monitor the number and nature of deficiencies across the NSW public sector, it is also useful to assess whether deficiencies are common to multiple agencies. Where deficiencies relate to multiple agencies, central agencies or the lead agency in a cluster can help ensure consistent, timely, efficient and effective responses to identified deficiencies.

We classified the 279 internal control deficiencies we identified in 2021–22 into common categories as follows:

- financial operational deficiencies
- IT operational deficiencies
- compliance deficiencies
- governance deficiencies
- reporting deficiencies.

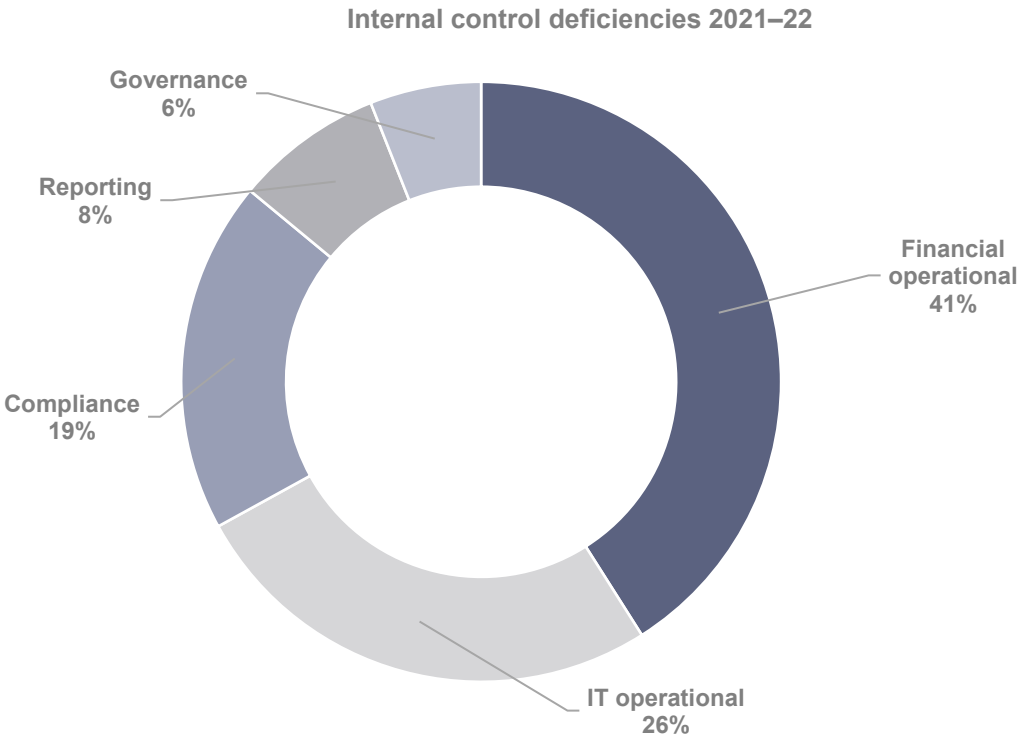

Exhibit 2.
Source: Audit Office findings.

The graph above shows that 67% of the deficiencies (50% in 2020–21) were financial or IT operational deficiencies, with the remainder split between compliance deficiencies (19% compared to 20% in 2020–21), reporting deficiencies (eight per cent compared to 15% in 2020–21) and governance deficiencies (six per cent compared to 15% in 2020–21).

The table below describes the most common deficiencies across agencies, including their risk rating, the number of repeat deficiencies and the recommendations we have communicated to management and those charged with governance.

Operational (185)	New Issues	Repeat Issues
High:	7	8
Moderate:	45	64
Low:	42	19

Common issue	Findings/implications	Lessons for agencies
Maintaining master files	Controls were not established to: • ensure sufficient segregation of duties over access to key master files • verify the validity, accuracy and/or completeness of changes to key master files, such as vendor and payroll tables • unauthorised access to change payroll master files.	Agencies should: • review controls established over access to key master files to prevent inappropriate access to, change or erasure of data • regularly review system access of business users to ensure incompatible duties are removed.
Use of purchase orders	Purchase orders were created and approved only after the goods and services were purchased.	Agencies should ensure staff are trained in their obligations to comply with proper procurement practices, policies, and legislation. Approval of purchase orders should occur before expenditure is incurred.
Purchase cards	The management of purchase cards lacks oversight and proper review. Our findings identified: • inappropriate use of purchase cards • purchases made over approved limits • terminated staff retaining the cards after resignation.	Agencies should ensure staff are trained in their obligations to comply with purchase card policies and procedures.
Fixed assets	A number of internal control deficiencies across many agencies were identified, including: • lack of timely capitalisation of completed capital work in progress or other asset additions • inadequate review over the appropriateness of asset capitalisation threshold • asset disposal documentation incomplete and/or not reviewed.	Agencies should: • capitalise asset additions or capital work in progress when the asset meets the requirements of capitalisation per AASB 116 'Property, Plant and Equipment' • review asset capitalisation threshold policy and determine if it is in line with the NSW Treasury Paper TPP06-06 'Guidelines for Capitalisation of Expenditure on Property, Plant and Equipment' • ensure asset disposals are documented and reviewed.

Common issue	Findings/implications	Lessons for agencies
Payroll controls	Internal control deficiencies were identified in 56% of agencies, including: • untimely deactivation of terminated users accounts • non-recoupment of overpaid salaries • poor management of recording overtime claims, input of new hires and timesheet/record keeping • excess salary payments made to terminated staff.	Agencies should ensure staff are trained in their obligations in relation to payroll controls and segregation of duties. Any changes made to payroll data must be authorised and reviewed, and stricter controls for payroll should be implemented to prevent overpayments, and payments to terminated staff.
Information technology	Control deficiencies were noted relating to IT governance, user access administration, program change and computer operations.	Refer to Section 3 'Information technology' for further details.

Source: Audit Office findings.

Compliance (54)	New Issues	Repeat Issues
High:	3	0
Moderate:	14	20
Low:	8	9

Common issue	Findings/implications	Lessons for agencies
Contract registers	Agencies have not established contract registers or have incomplete or inaccurate contract registers. These agencies may face challenges with: • complying with legislative obligations • identifying contracts that are nearing completion, and commencing timely procurement activity • effectively managing their contractual commitments • disclosing contractual commitments accurately in their financial statements.	Agencies should focus on establishing complete and accurate contract registers. This includes: • developing policies and procedures that govern the timely and accurate updating of the contracts register • monitoring the contracts register, including identifying contracts nearing completion so a new procurement can be commenced in a timely manner. Refer to Section 7 'Contract management' for further details.
Document retention	Agencies do not always maintain documents to evidence performance of key control activities. Deficiencies reduce accountability and reduce compliance with state records legislation.	Agencies should educate staff in their responsibilities and retain documentary evidence that they have discharged responsibilities. Agencies should ensure appropriate records management policies have been communicated to all staff.

Common issue	Findings/implications	Lessons for agencies
Central registers, such as those used to manage conflicts and gifts and benefits	Central registers are not kept or are not updated in a timely manner. Without a central register to capture information, agencies may not be able to monitor if their management of conflicts and/or gifts and benefits complies with requirements and internal policies.	Agencies should have registers to capture staff disclosures to ensure compliance with legislation and policies. Conflict of interest, gifts and benefits and other relevant policies should specify the timeframes of how and when registers are updated.
Non-compliance with legislation	Non-compliance with legislation and policies were identified.	Agencies should ensure central registers capture all key legislation and assign responsibility.

Source: Audit Office findings.

Reporting (23)	New Issues	Repeat Issues
High:	3	1
Moderate:	7	3
Low:	6	3

Common issue	Findings/implications	Lessons for agencies
Reconciliations	Key reconciliations were not prepared or were not reviewed in a timely manner. Reconciliations of inter-agency balances were not performed. There were unconfirmed balances in reconciliations.	Policies and procedures should require reconciliations be prepared and reviewed as part of month-end processes. Management should ensure this key control is performed. Inter-agency balances should be reconciled regularly. Reconciliation differences should be resolved in a timely manner.
Accounting standard application	Application of accounting standards continues to challenge agencies. Issues were identified including but not limited to: • revenue recognition • GST for cash flow purposes.	Agencies should ensure staff are provided with training to understand the key requirements of accounting standards and perform robust assessments of risk areas supported by appropriate documentation.

Common issue	Findings/implications	Lessons for agencies
Fair value assessment and revaluation of property, plant and equipment	Agencies engaging valuers did not conduct their own assessments as to the reasonableness of the valuations and did not assess the reasonableness of those valuations.	Agencies should ensure they comply with applicable Australian Accounting Standards and mandated Treasury guidance. Agencies continue to be responsible for the revaluation process and should: • assess the appropriateness of the methodology, key assumptions and judgements adopted in the valuation and impairment of plant and equipment • test key inputs and mathematical calculation of fair value and impairment assessments.
Expected credit loss provisions	Agencies have either not calculated their expected credit loss provisions correctly, or not applied the correct requirements in accordance with accounting standards.	Calculations that involve significant management judgements and assumptions should be documented and appropriately reviewed.

Source: Audit Office findings.

Governance (17)	New Issues	Repeat Issues
High:	0	1
Moderate:	7	4
Low:	2	3

Common issue	Findings/implications	Lessons for agencies
Policies and procedures	Agencies have not established policies, have gaps in policies or have policies that are past their scheduled review date.	Agencies should establish processes that ensure its policies reflect current requirements, the organisation's current structure and delegations, and avoid duplication, contradictions or gaps.
Service level agreements	Agencies do not always have service level agreements or Memoranda of Understanding in place for service provision arrangements with third parties.	Agencies should formalise service level agreements or Memoranda of Understanding with clearly defined roles and responsibilities, timeframes and deliverables.

Source: Audit Office findings.

2.3 Trends in findings

We assess trends in agency controls by measuring the number of internal control findings that emerged from our financial audits. We use three measures:

- number of findings
- number of new and repeat findings
- risk level of findings.

Our 2021–22 audits identified 279 internal control deficiencies, comprising:

- 204 financial related control deficiencies
- 75 IT related control deficiencies.

We reported these deficiencies to agency management and those responsible for governance at agencies, such as audit and risk committees and cluster secretaries. Our communications outline each audit finding, assess its implications, rate the level of risk and make recommendations.

The number of internal control deficiencies decreased by 17% from last year

There were 59 fewer control deficiencies identified in 2021–22. The composition of the findings showed a 30% decrease in IT findings and a 12% decrease in financial control findings, and an overall 17% decrease in repeat findings across both categories.

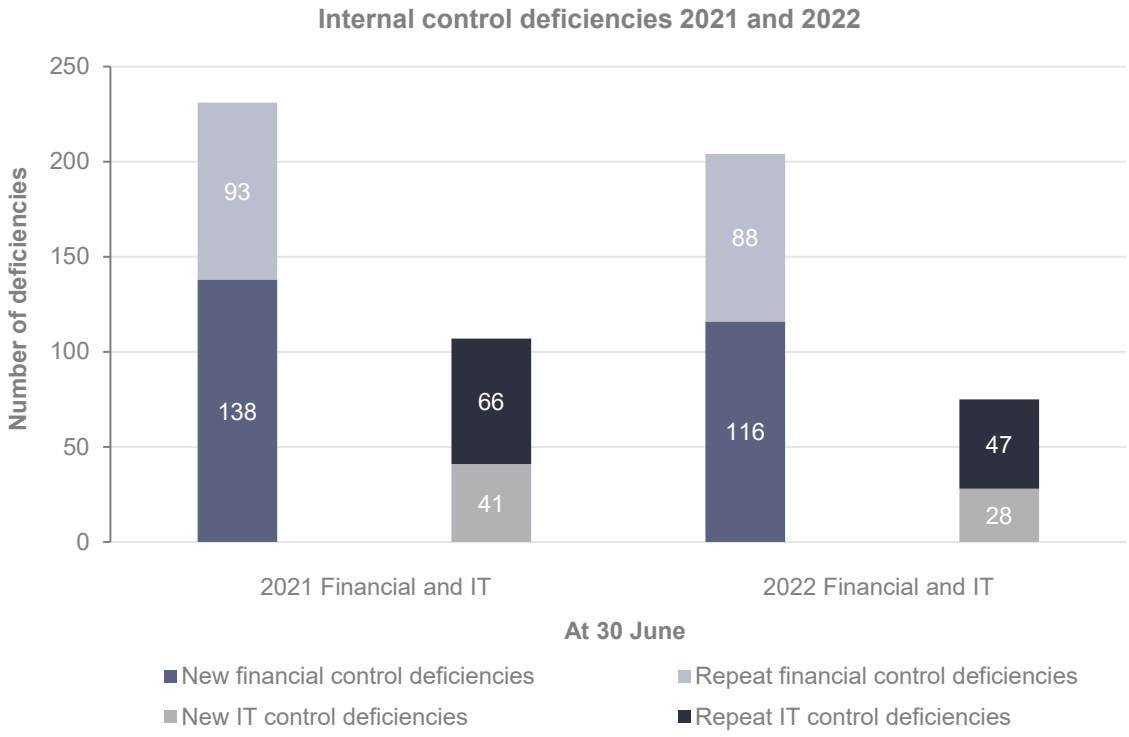

Exhibit 3.
Source: Audit Office findings.

The number of financial control deficiencies decreased by 12% from last year

We found financial control deficiencies at 96% of agencies (96% in 2020–21).

New and repeat financial control deficiencies decreased by 16% and five per cent respectively from 2020–21. Deficiencies in financial controls increase the risk of intentional and accidental errors in processing information, producing management reports and generating financial statements. This can impair decision-making, affect service delivery and expose agencies to fraud, financial loss and reputational damage. Poor controls may also mean agency staff are less likely to follow internal policies, inadvertently causing the agency not to comply with legislation, regulation and central agency policies.

The graph below shows the risk rating of reported financial control deficiencies.

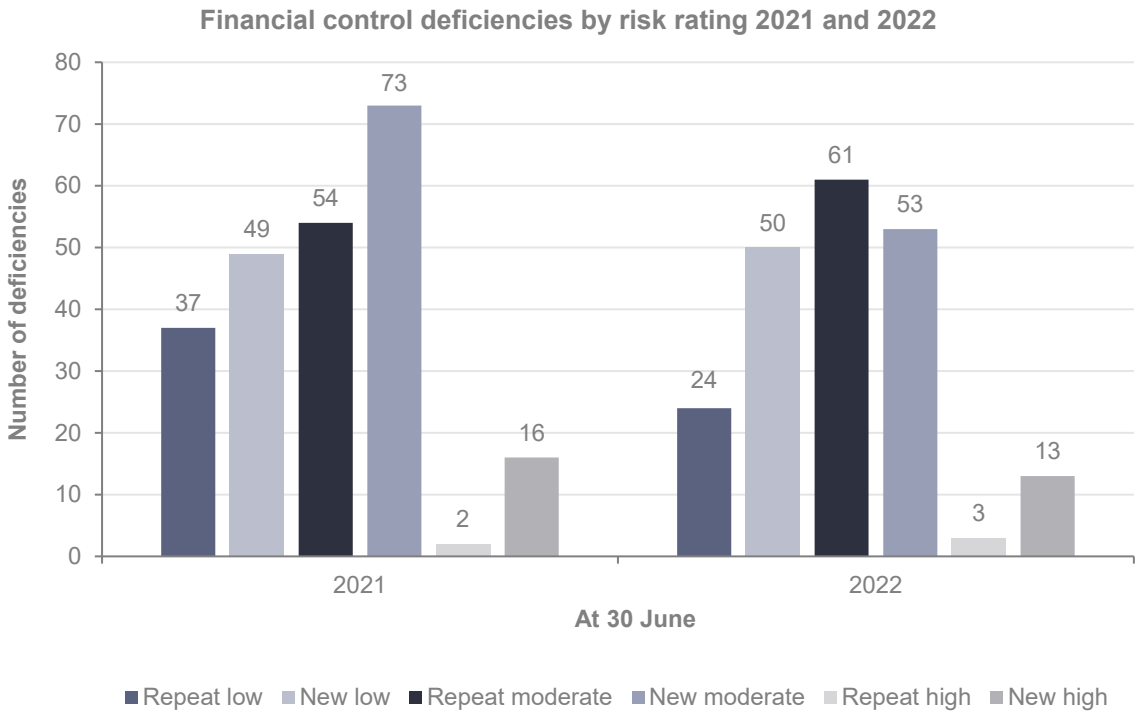

Exhibit 4.
Source: Audit Office findings.

The number of IT control deficiencies decreased by 30% from last year

New and repeat IT control deficiencies decreased by 32% and 29% respectively from 2020–21.

Repeat IT control deficiencies make up 63% of the reported IT control deficiencies, indicating that a significant number of IT control deficiencies noted in previous years remain unresolved.

We found:

- 40 issues related to user access administration (67% of agencies)
- 18 issues related to policies and procedures (33% of agencies)
- 8 issues related to privileged users (25% of agencies)
- 4 issues related to password security (8% of agencies)
- 4 issues related to disaster recovery plans (17% of agencies)
- 1 issue related to business continuity plans (4% of agencies).

The graph below shows the risk rating of reported IT control deficiencies.

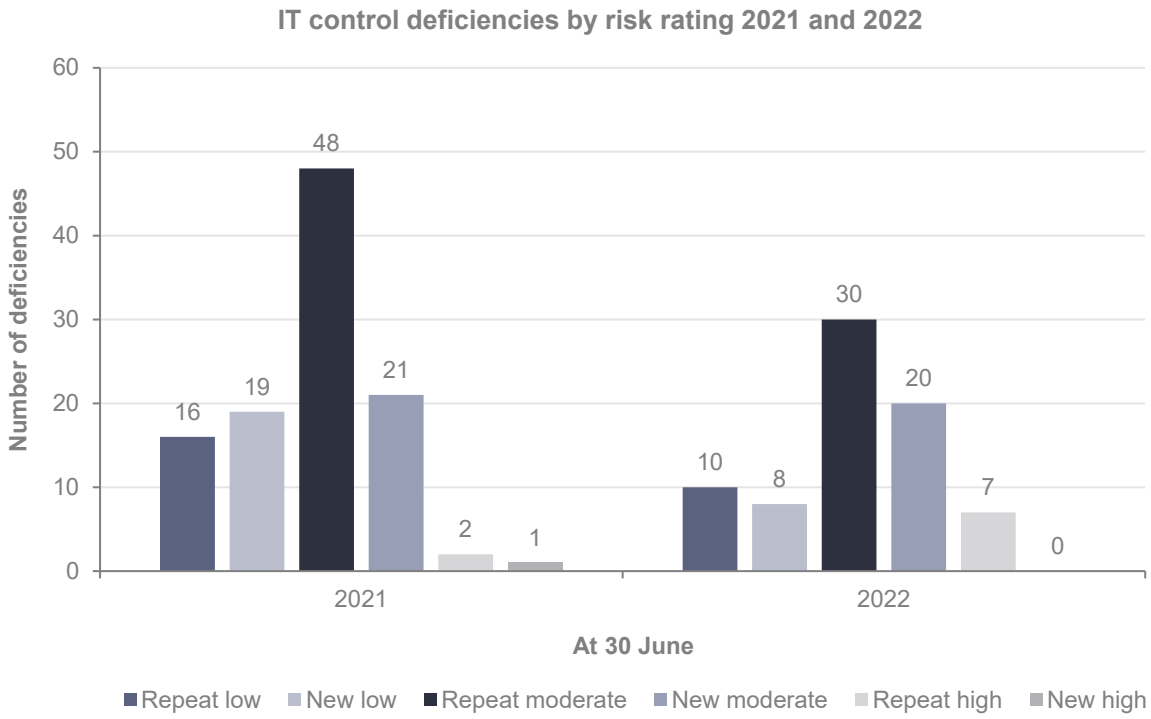

Exhibit 5.
Source: Audit Office findings.

As a percentage of total internal control deficiencies, unresolved deficiencies from prior years now represent 48% of all the internal control deficiencies identified (47% in 2020–21).

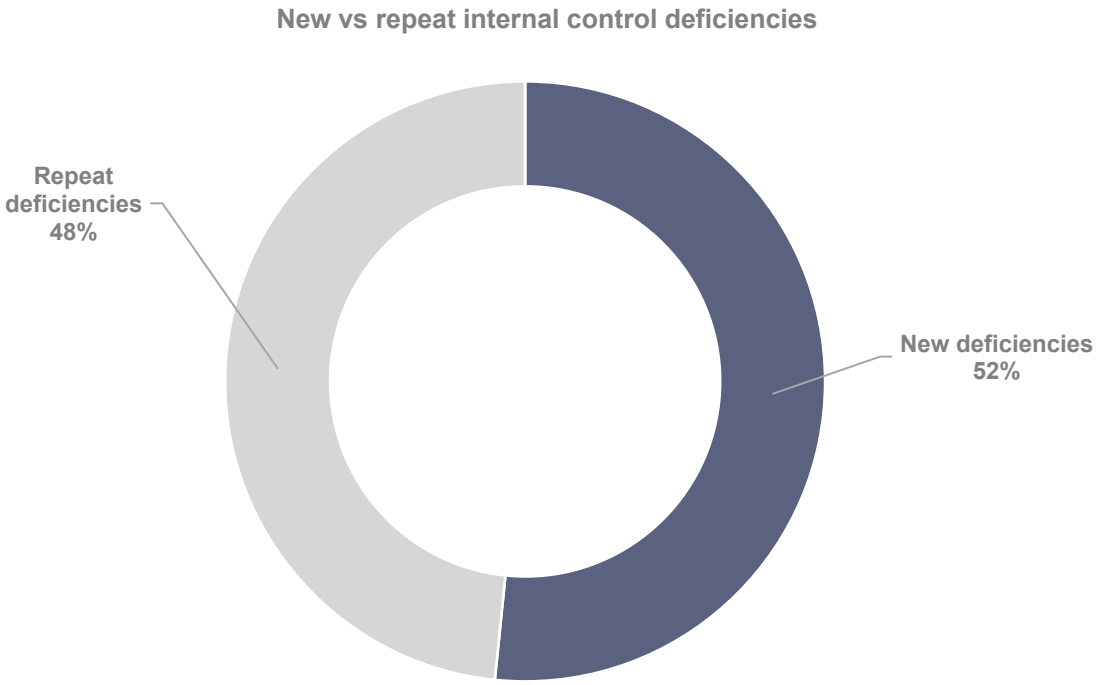

Exhibit 6.
Source: Audit Office findings.

We found at least five per cent of repeat findings reported in 2021–22 had been repeated since 2018. This is a decrease from nine per cent in 2020–21.

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 need to address these vulnerabilities by ensuring:

- there is clear ownership of the recommendations raised in respect of internal control deficiencies, including timeframes and action plans for their implementation
- audit and risk committees, and agency executive teams, monitor the implementation status regularly, focusing on those actions that are past due or have deferred implementation dates.

Recommendation

Agencies need to prioritise actions to address repeat control deficiencies, particularly those that have been repeated findings for a number of years.

2.4 Gifts of government property

Background

Agencies must comply with section 5.6 of the *Government Sector Finance Act 2018* (GSF Act) when making gifts of government property. Government property consists of all property held by, for or on behalf of the State or a government agency, but excludes money. A 'gift' is not defined in the GSF Act but by its ordinary meaning would include transfer of property for no or inadequate consideration. The GSF Act permits a person handling government resources to make a gift of government property only if it meets at least one of the following criteria:

- the property was acquired or produced to use as a gift
- the gift has been authorised by the Treasurer in writing
- the gift is made in accordance with the Treasurer's Directions
- the gift was authorised by or under any law.

The first category is not further defined in regulations or Treasurer's Directions, but may include awards, medals, prizes or complimentary hospitality items. The acquisition of such property would be subject to normal delegation and expenditure procedures.

Under the fourth category, agencies may expense government property for grants and subsidies in line with their operational objectives.

For the purpose of section 5.6(1)(c) of the GSF Act, NSW Treasury released a Treasurer's Direction TD 21-04 'Gifts of Government Property' which commenced on 23 April 2021. The direction authorises agencies to make a gift of government property if the agency is reasonably satisfied that the property meets all of the following criteria:

- it is genuinely surplus to the agency's requirements
- it cannot be transferred, with or without payment, to another agency which requires or can use the property
- a sale at fair value would be uneconomical.

Further, the gifted property must meet at least one of the following criteria:

- it holds historical or symbolic significance for the proposed recipient
- it holds some other special significance for the proposed recipient, and there are compelling reasons to justify the gift to that recipient
- it is a low value asset (an asset or group of assets below a total fair value of $500) and the gifting supports the achievement of a NSW government policy objective.

TD 21-04 required agencies to maintain a written register of all gifts of government property. On 5 September 2022, TD 21-04 was amended by Treasurer's Direction TD 22-27 'Amendment to TD21-04 Gifts of government property' to only require recording of gifts in the register if the gift has a fair value of over $10,000 when it is gifted. This change has allowed more gifts of government property to go unrecorded. Without recording those gifts, there is a heightened risk that agencies have inappropriately gifted government property that did not comply with the eligibility criteria.

Findings

Most agencies do not have a policy on gifts of government property

Only 20% of agencies have a policy or procedure for staff to follow in relation to gifts of government property. Although the Treasurer's Direction may be treated as a whole-of-government policy in itself, it lacks specific details for application within individual agencies.

Most agencies have not annually certified their register of gifts of government property or attested that the agency has not made any gifts

The Treasurer's Direction requires that agency heads annually review and certify the written register of gifts of government property, or attest in writing that the agency has not made any gifts. Only 16% of agencies have performed the certification/attestation, including submitting it to the agency's Audit and Risk Committee for review.

This low level of compliance may indicate a poor understanding of the scope and aim of the Treasurer's Direction.

Few agencies have recorded gifts of government property

Forty-four per cent of agencies have established a written record of gifts of government property in accordance with TD 21-04, although 55% of them have not recorded any gifts during 2021–22. In total, only 20% of agencies have made gifts of government property during the year.

Of the agencies that had gifted government property, not all have complied with the recording requirements of the Treasurer's Direction.

Register details	Percentage of agencies that recorded these %
Estimated fair value of the gift	100
Name and address of the gift recipient	40
Date that the government property was gifted	80
Name, position and financial delegation of the person handling government resources who approved the gift	60
Reasons for making the gift	80

Source: Audit Office analysis.

Only two agencies have published their registers on their websites, as required by the Treasurer's Direction.

3. Information technology

This chapter outlines our audit observations, conclusions and recommendations arising from our review of agency controls to manage key financial systems.

Section highlights

- We continue to see a high number of deficiencies related to IT General Controls, particularly those related to user access administration and privileged user access.
- We identified deficiencies within IT governance related to IT policies and procedures not effective in managing IT risks. We also identified weaknesses in arrangements with third-party IT service providers which can increase cyber security risk.

3.1 IT General Controls

Agencies rely on information systems to prepare their financial statements and deliver important services to the public. IT General Controls (ITGC) encompass policies, procedures and system settings, which support the effective functioning of operating system, database and application controls.

Robust IT controls are essential to support effective processes, policies and procedures for managing information systems, securing sensitive information, and ensuring the integrity and availability of agency data.

Poor IT controls increase agencies' vulnerability to the risk of:

- unauthorised access
- cyber security attacks
- fraud
- data manipulation
- privacy breaches
- information theft
- non-compliance with laws and regulations.

With the ever-increasing digital footprint of government, agencies should increase their focus on addressing IT weaknesses.

This summary provides a general indication of where control weaknesses exist. Agencies can use this information to improve the management of their overall control environments.

The following analysis is based on the IT internal control deficiencies identified at the 25 largest agencies in the NSW public sector, excluding state-owned corporations and public financial corporations. However, a number of these agencies provide IT shared services to other government agencies that may also be affected by these deficiencies. For the purposes of this report we have only identified the deficiency once at the responsible head agency.

IT governance

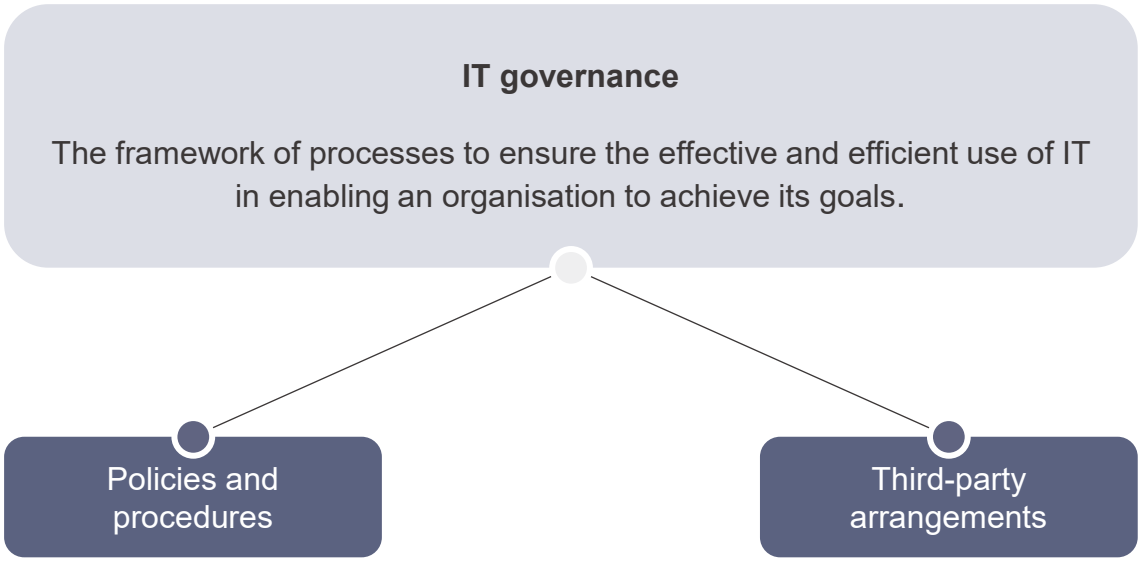

Exhibit 7.

Agencies should regularly review IT policies and procedures to ensure they effectively manage evolving and new IT risks

We identified issues with 33% of agencies' IT policies and procedures (24% in 2020–21). The deficiencies related to:

- IT policies that have not been reviewed by their scheduled review date (policies on data incident/breach management, security incident management, security patch management standards, information security)
- draft IT policies not yet finalised or approved
- gaps in policies (such as definitions, timeframes or follow-up actions required)
- inconsistencies in policies/procedures.

Risk

The absence of IT policies and procedures or sufficient periodic review of IT policies and procedures increases the risk of:

- policies and procedures not reflecting best practice or effectively managing new and evolving IT risks
- inconsistencies or gaps in policies/procedures
- lack of clarity on employees' roles and responsibilities in relation to IT
- non-compliance with laws and regulations.

Agencies should regularly review and update IT policies to ensure they meet current requirements, avoid duplication, contradictions or gaps.

Weaknesses in third-party IT service providers can expose an agency to cyber security risks

Agencies are increasingly contracting out key IT services to third parties. However, even when a service is outsourced, the agency remains accountable for risks.

We identified issues at 28% of agencies with their management of IT service providers (32% in 2020–21). The deficiencies related to:

- weaknesses in monitoring third-party user IT service providers' access, timely removal of access, or privileged user audit log monitoring
- weakness in third-party IT service provider's password controls, IT security monitoring
- lack of IT security policies at third-party IT service providers
- lack of segregation of duties at third-party IT service providers
- lack of clarity between the agency and third-party IT service providers about responsibilities to detect, manage and resolve cyber-attacks
- third-party IT service providers' controls assurance reports do not clearly show the agency's systems are covered by the report, or were qualified with significant issues in ITGC
- agency management not adequately reviewing or monitoring third-party IT service providers' controls assurance reports.

Risk

Appropriate management of third-party service providers reduces the risk of:

- interruptions caused by system outages
- fraud or cyber attacks
- loss of confidential information caused by cyber attacks and data security breaches
- threats to business continuity from failures in core infrastructure
- threats to compliance, disaster recovery and business continuity where roles and responsibilities between the agency and service provider have not been clearly defined.

Agencies should:

- ensure any gaps identified at the third-party IT service providers are addressed by the agency through mitigating controls or other processes
- review controls assurance reports from third-party IT service providers to identify IT control weaknesses and ensure gaps are suitably addressed.

Information security

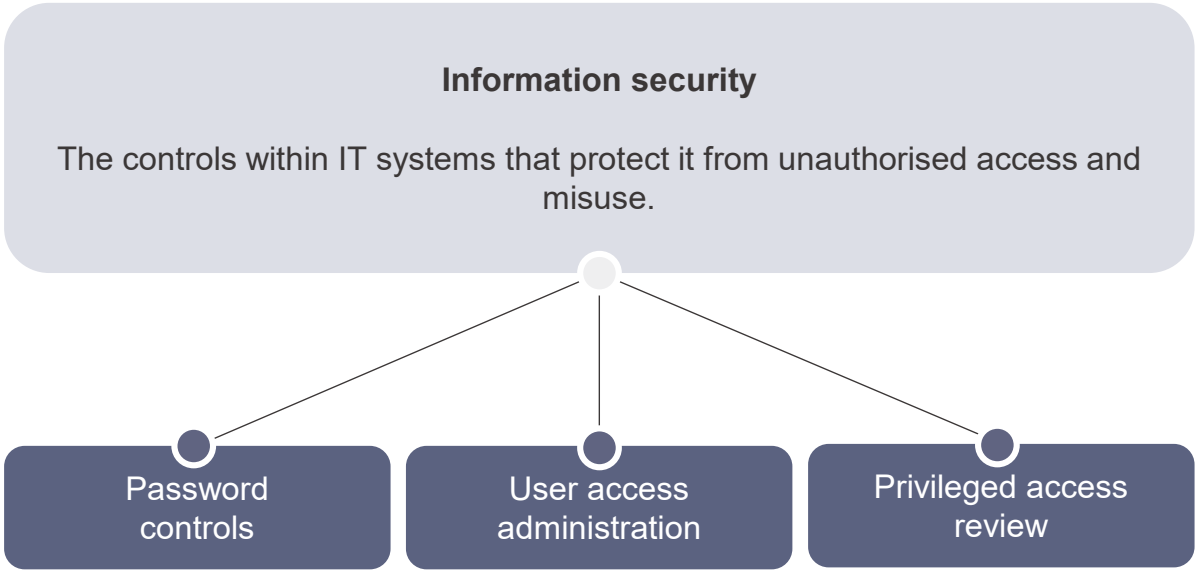

Exhibit 8.

Agencies are not complying with their own password policies

Twenty-four per cent of agencies (28% in 2020–21) either did not comply with their own policies on password parameters or did not enforce the minimum expected standard. The deficiencies identified related to:

- passwords not meeting minimum password lengths or complexity requirements
- not enforcing limits on the number of failed login attempts
- not enforcing controls for password history (such as the number of passwords remembered and restricting the recycling of recently used passwords)
- minimum and maximum password age not applied (such as prompting the periodic change of passwords)
- no internal formalised password policy or enforcement of the requirements
- use of default and generic passwords
- password policies lack definition of password parameters/good practice requirements.

Risk

Weaknesses in password configuration settings may make it easier for a user account to be maliciously compromised, allowing unauthorised access to use and change financial information. This can affect data in IT applications, databases and database servers.

Agencies should:

- implement and conduct regular reviews of password setting policies
- review IT password settings to ensure that they comply with minimum standards and the requirements of their password policies.

Agencies have significant weaknesses in their user access review processes

User access management relates to the process of managing access to applications and data, including how access is approved, removed, modified and reviewed periodically for appropriateness against an employee's role and responsibilities.

We identified 56% of agencies do not perform regular user access reviews (60% in 2020–21) to validate the currency and appropriateness of user access rights to an agency's business systems. The deficiencies related to:

- absence of periodic user access reviews performed to ensure access levels align with the user's role
- regular reviews of dormant user accounts, duplicate user accounts and default/generic accounts were not performed
- absence of a process to periodically review third parties' user access and remove profiles when they are no longer required, on a timely basis
- weaknesses in processes to ensure timely changes to access levels to reflect changes to staff responsibilities, new users and terminations, including lack of evidence of approval
- a lack of policies and procedures on user access administration
- non-compliance or inconsistencies in user access policies and procedures.

Risk

Weaknesses in user access management controls can result in inappropriate and unauthorised access to business systems. This can impact the completeness and accuracy of financial information by:

- exposing agencies to the risk of fraud or cyber attacks
- comprising data integrity and confidentiality
- increasing the risk of unauthorised and invalid transactions.

The deficiencies above increase the risk of low maturity scores when assessed against the NSW Cyber Security Policy and inadequate cyber security safeguards. Agencies should have processes in place to manage user access, including privileged user access to sensitive information or systems, and remove that access once it is not required or employment is terminated.

Agencies should regularly perform reviews of user access, and promptly action any changes including maintaining evidence of required changes.

Agencies do not periodically review the activities of privileged users

Privileged users are trusted or 'administrator' users with a heightened level of access to normally restricted systems and information including critical agency operational systems. They are able to alter user access profiles, make system changes and access sensitive agency data.

We identified that 36% of agencies do not periodically review the activities of privileged users to identify suspicious or unauthorised activities (44% in 2020–21). The deficiencies related to:

- system audit logs not enabled to track user account activities
- no defined process (gaps in current policy) or evidence of periodic review of privileged user activities where system audit logs are enabled and maintained
- no process to periodically review privileged user access and remove profiles when they are no longer required, on a timely basis
- inappropriately granting approval of privileged user access when not required/used in role
- gaps in the policy on privileged access review (frequency, exceptions handling and timeframes)
- review of privileged user activities not performed in accordance with policy
- limited segregation of duties of staff with privileged IT user profiles, especially in the areas of HR and payroll, supplier master file and manual journal responsibilities
- no segregation of duties in the privileged access review (such as system activity reports generated or reviewed by someone with privileged access).

Risk

The absence of periodic reviews of privileged user accounts increases the risk of inappropriate and unauthorised activities within the system going undetected.

Privileged users may misuse their access to:

- commit fraud
- access and extract confidential information for improper purposes
- access files, install and run programs, and change configuration settings
- maliciously or accidentally delete or distribute information.

Poor management of privileged access may also lead to breaches of Section 3.6 of the *Government Sector Finance Act 2018* and the NSW Cyber Security Policy. This policy requires agencies to have appropriate security screening of users with privileged access rights, and remove access when it is no longer required, or when employment is terminated.

Agencies should:

- restrict privileged user access to only staff that require that level of access to perform their role
- restrict or limit privileged access when incompatible with staff segregation of duties
- promptly remove access when it is no longer required
- identify controls to address the risks associated with privileged user activity, including regular monitoring of activity logs.

Computer operations

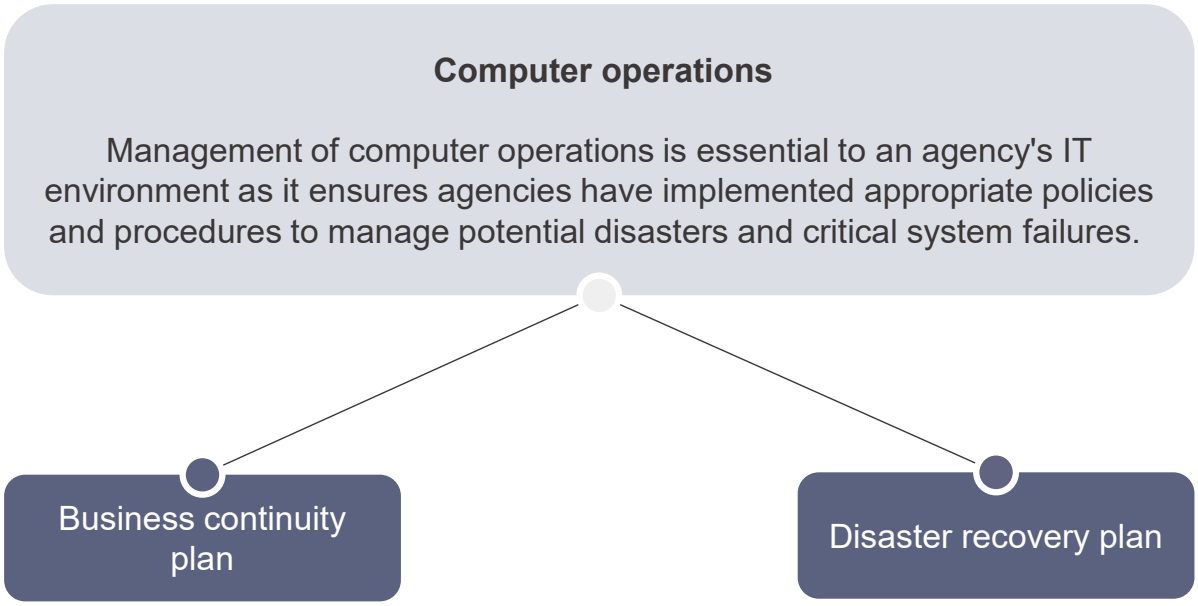

Exhibit 9.

Agencies should regularly review and test their business continuity and disaster recovery plans

Business continuity plans provide guidance and information to help teams to respond to a disruption and to assist an agency with response and recovery. A disaster recovery plan helps agencies maintain IT services in the event of an interruption, or restore IT systems and infrastructure in the event of a disaster or similar scenario.

We found deficiencies in disaster recovery processes at 24% of agencies (40% in 2020–21), and in business continuity processes at eight per cent of agencies (16% in 2020–21). These deficiencies related to:

- absence of business continuity or disaster recovery plans
- absence of regular review of business continuity or disaster recovery plans
- absence of annual business impact analysis and review by senior management
- not testing the business continuity or disaster recovery plans during the year
- not maintaining a business continuity or disaster recovery incident log
- absence of post-incident reviews (such as root cause analysis and actions to prevent reoccurrence) of business continuity events
- inadequate risk capture/identification as part of business continuity and disaster recovery plans such as health pandemic
- lack of recent review of the business continuity plan and disaster recovery plan by internal audit.

Risk

Without detailed analysis and planning for critical business functions and key IT systems and infrastructure, agencies cannot predict the impact of disruption, identify maximum tolerable outages, or plan informed recovery strategies. They also risk:

- data loss and delays in restoring data
- a plan not working in an actual emergency
- periods of vulnerability while transitioning between systems.

Agencies should:

- create, regularly review and test business continuity and disaster recovery plans
- conduct annual business impact analysis and ensure it is reviewed by senior management
- perform post-incident reviews (such as root cause analysis and actions to prevent reoccurrence) of business continuity events
- ensure all risks are identified and captured as part of business continuity and disaster recovery plans
- maintain a business continuity or disaster recovery incident log
- ensure the business continuity and disaster recovery plans are included in the internal audit program for cyclical testing.

Program changes

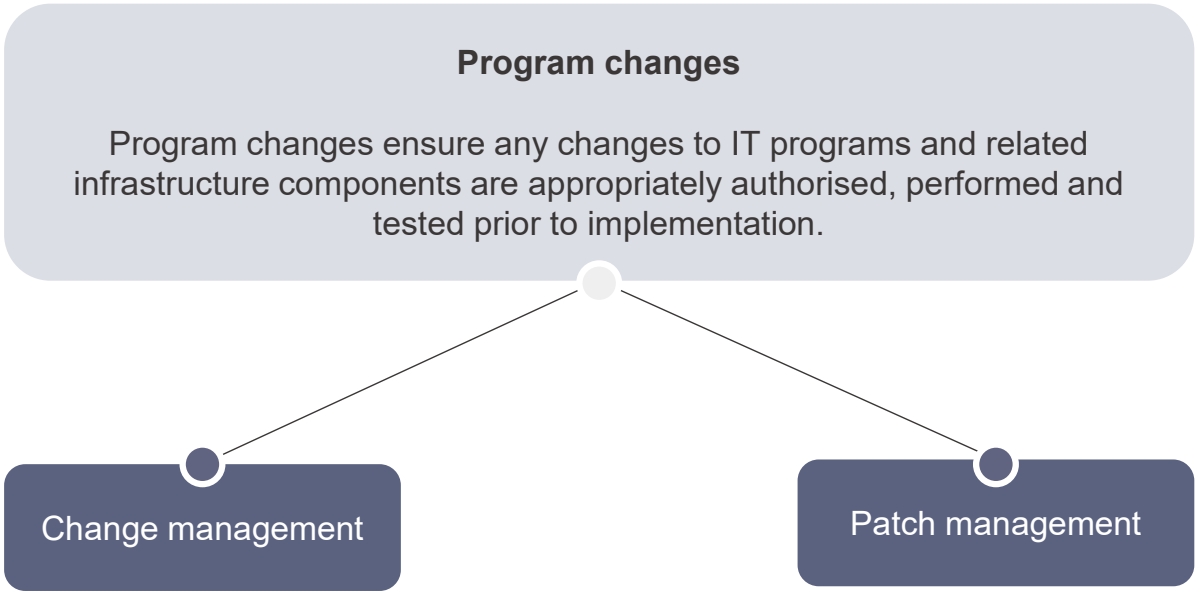

Exhibit 10.

Change management: program changes require appropriate review, approval and evidence of approval

Change management is a systematic and standardised approach to ensuring all changes to the IT environment are appropriate, authorised and preserve the integrity of the underlying programs and data.

We found deficiencies in agency IT program change controls at 20% of agencies (32% in 2020–21). These deficiencies related to:

- inappropriate segregation of duties over developing and releasing IT program changes to the production environment
- no evidence of approval of IT program changes prior to releasing changes to production
- change management policy and procedures were past their scheduled review date
- lack of closure report to detail what data has been migrated, manually added, or removed during data migration processes
- lack of formal process to review log of system changes.

Risk

Weak program change controls expose agencies to the risk of:

- poorly tested, inappropriate or unauthorised changes to systems or programs
- issues with data accuracy and integrity
- lack of completeness and accuracy of financial data
- incorrect functioning of the system.

Agencies should ensure:

- they perform user acceptance testing before system upgrades and program changes are deployed
- changes are not made without appropriate approval and documentation to support the approval
- change management policies and procedures are reviewed regularly.

Patch management: agencies should continue to develop and improve policies to ensure application, database or operating system patches are appropriately applied as required

A patch is an additional piece of software released by vendors to fix security vulnerabilities or operational issues. Patch management is the process of updating (acquiring, testing and installing) a set of changes or upgrades to support software, application and technology enhancements and to fix defects and vulnerabilities to an information system.

We found deficiencies in patch management at eight per cent of agencies (16% in 2020–21). These deficiencies related to:

- patch management standards were past their scheduled review date
- a formal process has not been established for patch management that includes identification, assessment, determining relevance and priority, escalation, timely rollout, and reporting of long outstanding patches to senior management and board
- an absence of a formal processes around exemption from patching and risk acceptance for unpatched systems.

Risk

Patch management addresses known vulnerabilities, leaving IT systems unpatched at the operating system, database or application levels increases the opportunity for attackers to exploit those known vulnerabilities. Patching is also used to provide system functionality updates and fix defects.

The deficiencies above increase the risk of low maturity scores when assessed against the Australian Cyber Security Centre Essential Eight Strategies to Mitigate Cyber Security Incidents.

Agencies should ensure:

- application, database or operating systems patches are appropriately applied as required and on a timely basis
- patch management standards, policies and procedures are reviewed regularly.

4. Cyber security

This chapter outlines our audit observations, conclusions and recommendations arising from our review of agencies' cyber security planning and governance arrangements.

Section highlights

- Only 80% of agencies specify how they monitor or ensure that third-party IT service providers comply with the agencies' cyber security policies. IT service providers may pose certain risks to the agency if the provider's cyber security controls have weaknesses.
- There are inconsistent practices and definitions of cyber security incidents across agencies with respect to maintaining incident registers. Five agencies reported nil incidents in their registers for 2021–22, while other agencies recorded up to 1,913 incidents.
- Agencies' self-assessed maturity levels against the NSW Cyber Security Policy mandatory requirements are lower than their target levels in at least one requirement. Maturity levels against the Australian Cyber Security Centre's Essential Eight controls have not improved since last year.

4.1 Background

Cyber security comprises technologies, processes and controls that are designed to protect IT systems and sensitive data from cyber attacks. The cyber security framework consists of threat identification, protection, detection, response and recovery of IT systems.

Cyber Security NSW, part of the Department of Customer Service, develops and manages the NSW Cyber Security Policy (CSP). The CSP sets out 20 mandatory requirements for agencies, including implementation of the Australian Cyber Security Centre (ACSC) Essential Eight Strategies to Mitigate Cyber Security Incidents (Essential Eight). The Essential Eight controls were developed by the ACSC to serve as a baseline set of protections for organisations to make it more difficult for adversaries to compromise a system.

Each year, agencies are required to self-assess their maturity against the CSP and the Essential Eight, and report that assessment to Cyber Security NSW. The Department of Customer Service administers the Digital Restart Fund which has allocated a total of $315 million in June 2021 towards continual uplift of agencies' cyber security maturity.

4.2 Policy framework

The CSP took effect from 1 February 2019, replacing the NSW Digital Information Security Policy following the Audit Office's 2018 performance audit 'Detecting and responding to cyber security incidents'. The CSP is subject to annual review, which includes agency feedback. The current version of the CSP was issued in January 2022.

All agencies have established up-to-date cyber security plans to manage their cyber security risks which:

- were approved within the agency
- referenced the NSW CSP and the agency's risk management framework.

Except for one agency, all other agencies' cyber security plans:

- identified the key potential cyber threats, vulnerabilities and risk events that could affect the agency
- were aligned to the identified cyber risks
- set a risk appetite or target risk levels regarding cyber security that management has accepted.

Sixteen per cent of cyber security plans do not cover all of an agency's IT systems

Most agencies' cyber security plans cover all IT systems used. The remaining agencies' cyber security plans only cover crown jewels, which are critical systems, but may leave other systems relatively more exposed with less protection. The graph below shows the different coverage levels of agencies' cyber security plans.

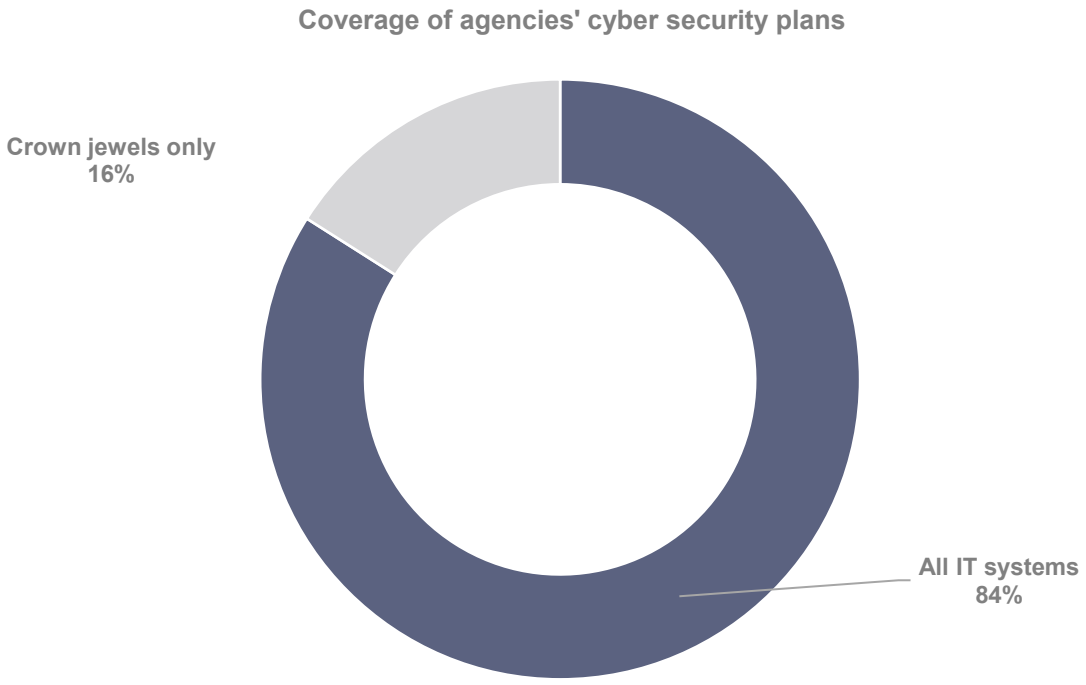

Exhibit 11.
Source: Audit Office analysis of cyber security plans.

4.3 Managing cyber risks

All agencies have conducted a periodic risk assessment of cyber security risks during 2021–22. Agencies' consideration of relevant cyber risks for their business are summarised in the table below.

Cyber risks	Percentage of agencies that have identified these as applicable (%)
Risk of data breaches that relate to unauthorised access to financial reporting applications, data and electronic assets	96
Risk of failures in preventive and detective controls to safeguard digital assets	88
Risk of misappropriation of digital assets	68
Risk of unauthorised access to the IT network	96
Risk of potential loss of data or inability to access data as required	100
Risk of IT system failure affecting the agency's primary business	96
Risks arising from lack of policies and procedures in place related to cyber security	80

Source: Audit Office analysis.

Sixty-eight per cent of agencies have not undertaken a process to identify digital or electronic assets that are intellectual property, such as patents, copyrighted material or trade secrets. Eleven of those agencies believe that they do not possess any intellectual property.

Twenty-four per cent of agencies have not undertaken a process to identify digital or electronic assets that are highly sensitive, such as Cabinet in confidence information, or data requiring security clearance to access, such as classified information.

All agencies report cyber risks to the board regularly, either monthly or quarterly. At a minimum, this has involved reporting of the enterprise risk register which includes cyber risk.

Third-party service providers

Agencies regularly use IT service providers to support their business operations as those vendors deliver specialised services and may offer cost savings or efficiencies. Consequently, third-party IT providers are part of the general IT ecosystem and embody certain risks that need to be managed. Being unaware of weaknesses in an IT service provider's cyber security controls means agencies may respond slowly, or not at all, to address vulnerabilities that can be exploited by threat actors to gain access to the agency's systems, data and assets.

One example of a cyber incident at a service provider that affected a wide group of entities was the data breach at Frontier Software in November 2021[1]. Frontier Software provides the widely used payroll system Chris 21, including cloud-based payroll system services. An unauthorised third-party gained access to Frontier Software's corporate network and removed a subset of data on that network. The data included personal information of client organisations' employees, including full name, date of birth, address, tax file number, banking details and superannuation information. Client employers were required to notify their affected employees (including former employees) and report the breach to regulatory bodies such as the Information and Privacy Commission NSW and Office of the Australian Information Commissioner. Although there was no reported direct financial loss from the incident, there has been reputational damage, and potential harm to individuals who may be subject to identity theft and further forms of cybercrime.

[1] Australian Update: Cyber Incident | Frontier Software Australia

Agencies need to improve their cyber risk management relating to IT service providers

As mandated by the CSP, 96% of agencies have ensured that their cyber security policy or plan specifies that it applies to third-party service providers. However, only 80% of agencies actually specify how they monitor or ensure that service providers comply with the relevant parts of the CSP. Without detailed actions or requirements, it is difficult for agencies to address the risks relating to third-party service providers.

The table below outlines how agencies manage compliance of service providers.

Compliance mechanisms	Percentage of agencies that have apply these (%)
Requirement to comply with CSP is included in standard term contracts with IT service providers	80
Attestations or certifications are required from IT service providers confirming compliance	52
Controls assurance reports are required from IT service providers relating to their controls around cyber security	60
IT service providers are required to notify the agency of any security incidents, regardless of whether they resulted in actual financial loss or breaches of information security	76

Source: Audit Office analysis.

Where IT service providers are required to notify agencies of security incidents, all of the agencies stipulate a timeframe of 48 hours or less from detection of the incident.

From 8 July 2022, amendments to the *Security of Critical Infrastructure Act 2018* (SOCI Act) require that organisations with 'critical infrastructure assets' report cyber incidents to the ACSC within 12 hours of detection for critical incidents that have a significant impact on the availability of the asset, or 72 hours for other incidents that have a relevant impact on the asset. Given that many government agencies operate in critical infrastructure sectors as defined in the SOCI Act, such as energy, financial services and markets, health care and medical, transport, and water and sewerage, it is increasingly important that agencies ensure their IT service providers notify them of incidents.

Where breaches or incidents are identified at service providers, all agencies treat and report these in the same way as internal incidents. However, we have found that there is no consistent definition of breaches or incidents across agencies, which has resulted in very different records of the number of incidents occurring.

Incident registers

One agency has not established registers to record security incidents. Practices vary across other agencies where:

- 4% have multiple registers rather than one central register
- 21% of registers do not include attempted/blocked attacks. However, these are recorded separately, such as in security monitoring applications.

All agencies that record incidents reported that attempted/blocked attacks are monitored and reported for further assessment. However, not all are reported to the head of the agency or those charged with governance. Monitoring of attempted attacks enables entities to locate weaknesses in their processes and identify areas that are targeted by threat actors and are subject to regular attack. Those charged with governance may fail to take appropriate action to minimise the risk of future attacks if they are not made aware of these events through summary reporting or trend analysis.

Details in incident registers need to be enhanced

We noted 96% of registers recorded detailed actions taken in response to incidents, while one agency's register only recorded whether the issue was resolved or closed. An absence of detail about the nature of the incident makes it more difficult to perform root cause analysis on the incidents and reduce the risk of the issues recurring in future.

It is important that senior management and those charged with governance appreciate the extent of the agency's risk exposure. Reporting the detail behind incidents, such as the type and number of incidents, is essential to their appreciation of the scale and gravity of the risks and informs their response to these risks.

Our review of the incident registers noted the points below.

Incident register features	Percentage of agencies' registers that include this (%)
Risk/priority rating for each incident	96
Categories for type of incident (for example, phishing, account compromise, malware)	75
Date the incident was reported, date of action taken, and date resolved	100

Source: Audit Office analysis.

Twelve per cent of registers were incomplete with blank fields that are expected to be remediated.

Twenty per cent of agencies recorded nil security incidents in their registers for 2021–22. As reported last year, we note again that agencies' definition of security incidents and data breaches is inconsistent. Agencies that do not disclose events such as account compromise, distributed denial of service (DDOS) attacks or data breaches to senior management and those charged with governance risk an inappropriate response to these potentially serious events.

For other agencies, the number of incidents recorded during the year ranged from two to 1,913. The percentage of incidents closed or resolved ranged from 61% to 100%. While only one agency reported a financial loss due to an incident, estimated to be under $50,000, all agencies have a responsibility to ensure the data they hold is kept secure and that reasonable steps are taken to secure the data they hold.

Control activities

All agencies have control activities in place to protect against DDOS attacks.

All agencies have conducted penetration testing and vulnerability scans for their crown jewel systems during the year, of which 72% engaged an external specialist to perform those tests.

All agencies have a patch management program including processes to:

- identify new patches or security vulnerabilities on a regular basis
- evaluate the potential impacts of the patches, test and implement authorised patches.

Two agencies do not have a formal process to periodically check and install security patches for applications such as Flash, web browsers, Microsoft Office, Java and PDF viewers.

Agencies have unpatched applications and operating systems

Twenty per cent of agencies do not patch or mitigate applications or operating systems for 'high-risk' vulnerabilities within 48 hours, as recommended by the Essential Eight.

One agency did not regularly update its operating systems with the latest patches, and three agencies only regularly updated their crown jewel systems rather than all systems.

Over 72% of agencies run applications and operating systems that are no longer supported by the IT service provider and are unpatched. Most agencies claim that there are mitigating controls in place or there is a plan to decommission or upgrade old legacy systems over the next two to three years. Four agencies do not have plans to decommission unsupported applications and did not have mitigating controls systematically in place.

With the reported increase in cyber fraud and online hoaxes since the COVID-19 pandemic, a small number of agencies are aware of incidents where third parties have attempted to impersonate the agency or its staff to defraud members of the public. Those agencies have alerted their customers using different mediums and also communicated to staff to be aware of phishing campaigns or targeted attacks on staff and their personal devices. These same agencies had reported nil incidents in their incident registers during the year.

4.4 Cyber maturity

Maturity assessments

This section of the report on maturity assessments covers all NSW government agencies that are required to report their self-assessed maturity ratings in implementing the CSP mandatory requirements for the 2022 financial year. Detailed assessment criteria are provided in the CSP maturity model in relation to each requirement. The CSP maturity model for the mandatory requirements uses the following scale:

1. Initial – the policy requirement is not practiced
2. Managed (Developing) – the requirement of the policy may only be performed on an ad-hoc basis and/or is not completely covering the scope of the requirement
3. Defined – the requirement is practiced on a consistent and regular basis and the relevant processes are documented
4. Quantitatively Managed – the requirement is reviewed/audited/governed on a regular basis to ensure that it is being performed as per the documented process/requirement and address any potential blockers
5. Optimised – the requirement is delivered with improved effectiveness such as through increased coverage/stakeholder involvement, automation of processes, continuous improvement and compliance requirements.

The tables below summarise the results across whole of government, with the exception of three agencies that have not provided their results as at the date of this report. The maturity assessments were due on 31 October 2022, with seven agencies receiving an approved extension. Fifteen agencies submitted late reports after 31 October 2022. The maturity data presented below are as reported by agencies. Our 2021 report on 'Compliance with the NSW Cyber Security Policy' recommended Cyber Security NSW to monitor and report compliance with the CSP by requiring agencies to resolve inaccurate or anomalous self-assessments where these are apparent. At the date of this report, Cyber Security NSW is still in the process of reviewing the self-assessments.

Maturity levels to the left of the dotted line signify the requirement has been implemented in an ad hoc manner or has not been implemented at all. Maturity levels to the right of the dotted line indicate that the requirement is practiced in at least a consistent and documented manner.

Number of self-assessments for 2022

1. Planning and governance

Agencies must implement cyber security planning and governance. Areas of relative weakness against this measure related to:

- agencies having approved cyber plans that are integrated with business continuity arrangements
- governance over cyber risks of Information and Communications Technology (ICT) third-party service arrangements.

CSP requirements	Maturity level one	Maturity level two	Maturity level three	Maturity level four	Maturity level five	Total
Allocate roles and responsibilities	8	11	35	40	18	**112**
Cyber governance	6	14	17	59	16	**112**
Approved cyber plan	13	37	26	22	14	**112**
Cyber risk assessments	5	34	25	34	14	**112**
Service provider governance	7	48	37	16	4	**112**

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

Number of self-assessments for 2022

2. Cyber security culture

Agencies must build and support a cyber security culture across their agency and NSW Government more broadly. Areas of relative weakness related to:

- ensuring appropriate access controls and security screening are in place for access to sensitive data
- fostering a culture where cyber security risk management is a demonstrable factor in decision-making and where cyber security risk management processes are understood and applied.

CSP requirements	Maturity level one	Maturity level two	Maturity level three	Maturity level four	Maturity level five	Total
Cyber security training	5	20	61	23	3	**112**
Awareness and reporting of cyber security risk	3	32	55	14	8	**112**
Foster a culture of cyber risk management	6	37	34	25	10	**112**
Sensitive data access control	13	42	36	14	7	**112**
Cyber security threat sharing	2	20	23	48	19	**112**

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

Number of self-assessments for 2022

3. Manage cyber security risks

Agencies must manage cyber security risks to safeguard and secure their information and systems. Weaknesses in this area is of particular concern as these are the practical safeguards to protect sensitive information. Areas of relative weakness relate to:

- implementing an Information Security Management System (ISMS) which enables a structured and systematic approach to protecting sensitive information
- ensuring audit trails and activity logging records are determined, documented, implemented and reviewed for new ICT systems and enhancements.

CSP requirements	Maturity level one	Maturity level two	Maturity level three	Maturity level four	Maturity level five	Total
Implement an ISMS	14	40	49	7	2	**112**
Implement the ACSC Essential Eight	13	37	51	8	2	**111***
Classify information and systems according to their business value	21	17	34	20	20	**112**
Build cyber security requirements into procurements	10	21	45	33	3	**112**
Ensure audit trails and activity logging	20	59	21	5	7	**112**

* The total number of self-assessments for this requirement excludes one agency that rated this as 'not applicable'.

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

Number of self-assessments for 2022

4. Resilience

Agencies must improve their resilience, including their ability to rapidly detect cyber incidents and respond appropriately. Areas of relative weakness include:

- having a current cyber incident response plan that integrates with the agency's incident management process
- testing cyber incident response plans at least annually, involving senior business and IT executives, functional area coordinators, as well as media and communication teams.

CSP requirements	Maturity level one	Maturity level two	Maturity level three	Maturity level four	Maturity level five	Total
Cyber incident response plan	10	38	21	15	28	**112**
Exercise cyber incident response plan annually	28	25	30	17	12	**112**
Cyber monitoring tools to identify and respond to incidents	2	20	51	20	19	**112**
Report cyber incidents to Cyber Security NSW	5	5	42	55	5	**112**
Participation in whole-of-government exercises	10	1	61	24	16	**112**

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

The scope of maturity assessment reporting for Essential Eight controls changed in 2022

In July 2021, the Australian Cyber Security Centre (ACSC) updated its Essential Eight maturity model to focus on using the maturity levels to counter the sophistication of different levels of adversary tradecraft and targeting, and consequently redefined a number of maturity levels[2]. In general, the changes introduced a number of new requirements for each control and lifted the standard required to meet each maturity level, but particularly Level One.

The Essential Eight maturity model uses a four-point scale. The definitions for each maturity level are:

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

The July 2021 update also included a statement that the Essential Eight are designed to protect Microsoft Windows-based internet-connected networks. Consequently, while parts of the Essential Eight may be applied to non-Windows environments (including cloud services, Linux/Unix and other operating systems), the ACSC noted that alternative strategies may be more appropriate to mitigate unique cyber threats to those environments[3].

Cyber Security NSW has estimated up to 80% of the crown jewel IT systems reported by agencies are based on non-Windows infrastructure. In August 2022, Cyber Security NSW issued guidance to agencies that outlined:

- for Windows-based systems, agencies should continue applying the Essential Eight controls and report their maturity assessment in accordance with the Essential Eight maturity model
- for non-Windows systems, agencies should consider alternative mitigation strategies and guidance from the ACSC, and apply a risk-based approach in implementing the Essential Eight controls as it may not be possible to uniformly implement the Essential Eight across all systems. These agencies may apply exceptions for maturity reporting under the updated Essential Eight maturity model.

Furthermore, agencies are required to assess their cyber maturity at 30 June 2022 against both the former and current Essential Eight models. Assessment against the former model allows direct comparability with previous years and visibility on year-on-year trends.

Agencies' self-assessed maturity levels at 30 June 2022 against the former ACSC Essential Eight maturity model have not improved

Using a consistent benchmark in the former Essential Eight model, agencies' 2022 assessments showed little change from 2021.

Of concern are the median results for maturity implementing the Essential Eight controls since 2020. The graph below shows no improvement in agencies' implementation of the Essential Eight controls in 2022 against the former model, and a decrease in median maturity for patching operating systems.

[2] ACSC Essential Eight Maturity Model - frequently asked questions on the July 2021 update.
[3] ACSC Essential Eight Maturity Model introduction section.

2022 maturity ratings against the updated model are even lower, given the higher standard of requirements for each maturity level. Additional requirements to meet Maturity Level One have meant that some agencies have reassessed some maturity levels to Level Zero. The Essential Eight framework requires all elements of a maturity level to be met across all systems before an entity can progress to the next maturity level. The highest rating score relates to daily back ups, which although key to restoring services, does not close vulnerabilities or prevent attackers from gaining access to systems.

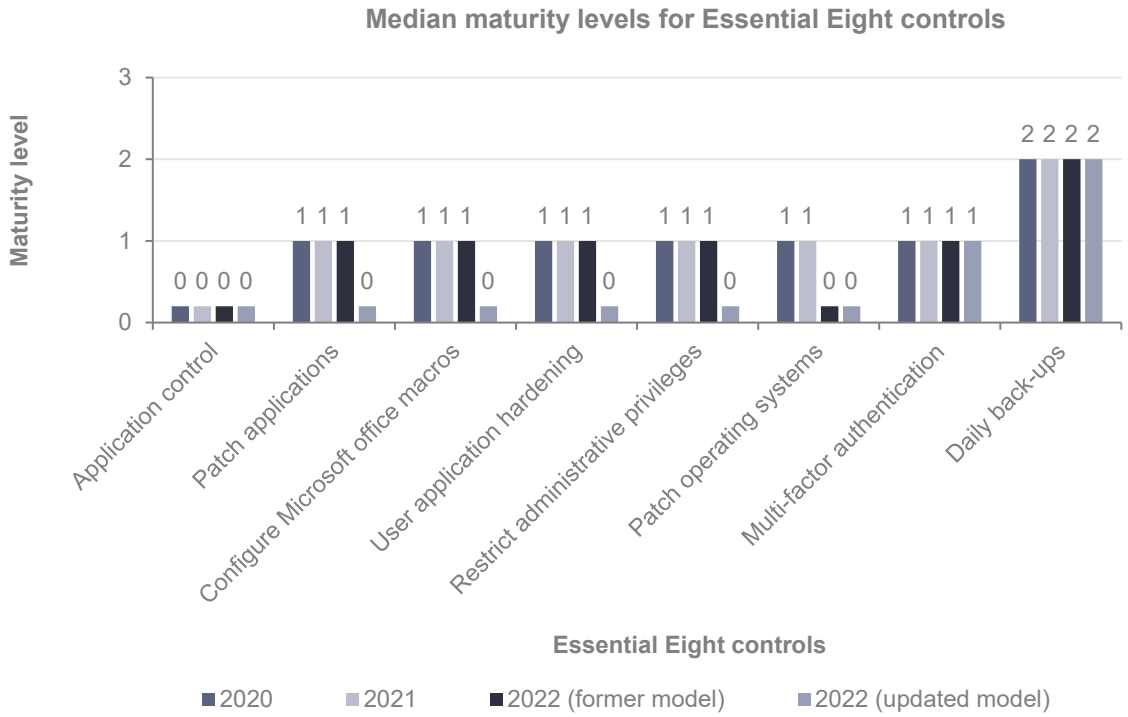

Exhibit 12.

Note: The median represents the level at which half of the agencies have reported they meet.

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

The table below reports the maturity levels of NSW government agencies in implementing the former model of the Essential Eight cyber risk mitigation controls, using the previously mentioned scale from zero to three. The movement indicator shows whether there has been an overall increase or decrease in maturity levels from 2021 based on the relative percentages of self-assessments in each maturity level.

Number of self-assessments for 2022 (former model)

Essential Eight controls	Maturity level zero	Maturity level one	Maturity level two	Maturity level three	Total*	Movement indicator**
Application control	68	25	7	7	**107**	↓
Patch applications	52	20	24	10	**106**	↓
Configure Microsoft Office macros	47	40	10	9	**106**	↓
User application hardening	45	40	12	8	**105**	↓
Restrict administrative privileges	33	37	26	11	**107**	↓
Patch operating systems	54	14	24	14	**106**	↓
Multi-factor authentication	26	51	26	4	**107**	↑
Daily back ups	11	41	30	25	**107**	↓

* The total number of self-assessments for each Essential Eight control vary as seven returns included 'not applicable' ratings or no response for at least one requirement. The 'not applicable' ratings were excluded from the table.

** Movement indicator shows an increase if the relative proportion of total self-assessments in Levels Two and Three have increased in 2022 compared to 2021. The indicator shows a decrease if the relative proportion of total self-assessments in Levels Two and Three have decreased in 2022 compared to 2021.

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

As noted earlier in this report, the updated Essential Eight maturity model includes changed and additional requirements compared to the previous version which has meant that agencies' maturity levels appear to have decreased in 2022.

The table below reports the maturity levels of NSW government agencies in implementing the updated model of the Essential Eight controls. Over half of all agencies are reporting a maturity level of zero for the first six of eight controls.

Number of self-assessments for 2022 (updated model)

Essential Eight controls	Maturity level zero	Maturity level one	Maturity level two	Maturity level three	Total*
Application control	70	25	8	3	**106**
Patch applications	77	12	15	2	**106**
Configure Microsoft office macros	57	37	7	4	**105**
User application hardening	67	27	9	2	**105**
Restrict administrative privileges	63	32	9	2	**106**
Patch operating systems	74	14	14	4	**106**
Multi-factor authentication	39	52	13	2	**106**
Daily back ups	22	26	39	19	**106**

* The total number of self-assessments for each Essential Eight control vary as eight returns included 'not applicable' ratings or no response for at least one requirement. The 'not applicable' ratings were excluded from the table.

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

Seventy-six per cent of agencies obtained independent or separate verification of this year's maturity assessment of the CSP mandatory requirements and Essential Eight requirements, such as by internal audit or an external expert. This was a recommendation from our 2021 report on 'Compliance with the NSW Cyber Security Policy'.

Maturity targets

This section of the report on maturity targets covers the top 25 agencies as listed in the introduction. Following the recommendations from our 2021 report on 'Compliance with the NSW Cyber Security Policy', the current version of the CSP requires all agencies to:

- set a target level of maturity for each key component of the 20 mandatory requirements and the Essential Eight
- have the agency head sign-off on any target maturity levels below a Level Three (out of five) for the mandatory requirements and/or a Level Zero or One for the Essential Eight.

Agencies' self-assessed maturity levels have not met target levels

All 25 agencies have set target levels of maturity for the year ending 30 June 2023 and designated a timeframe for achieving the target level for each component. All agencies continue to have gaps between their current self-assessed maturity levels and target levels in at least one component.

Sixty-four per cent of the agencies have set a target level of maturity of at least Level Three (out of five) for each of the 20 mandatory requirements in the CSP. Level Three indicates that the requirement is practiced on a consistent and regular basis, and the relevant processes are documented. The most common mandatory requirement for which the agencies have set a lower maturity target of Level One or Two relates to ensuring audit trail and activity logging records are maintained for new ICT systems and enhancements.

For the Essential Eight controls, only 36% of agencies have set a target level of maturity of at least Level Two for all components. Twenty-four per cent of agencies have set a maturity target of Level Zero for at least one component, with the most common components being application control and multi-factor authentication. Maturity targets for the Essential Eight controls are based on the updated model. As previously noted, given the higher standard of requirement for each maturity level, these targets will be more difficult to achieve than last year.

Ninety-two per cent of agencies have approved a plan or commitment to lift the maturity of Essential Eight controls to the targeted level within the targeted timeframe. However, three agencies have not set aside a specific budget to fund reaching the target level of maturity. Without quantifying and allocating a budget for specific activities to be achieved in order to raise the level of maturity, there is a greater risk that the target will not be met.

Eighty-four per cent of agencies formally accepted the residual risk through the head of agency where the current level of maturity does not meet the target level.

A related performance audit report on Cyber Security NSW's governance, roles and responsibilities is expected to be published in February 2023.

Recommendation

As reported last year, agencies need to prioritise improvements to their cyber security and resilience as a matter of urgency. Specific actions include:

- **ensuring their reported level of maturity is demonstrated by evidence**
- **improving Essential Eight maturity levels to meet target levels, which are more difficult to achieve under the updated Essential Eight model.**

Training and awareness

Agencies are required to implement regular cyber security awareness training in order to build and support a resilient cyber security culture under the CSP. Unlike system-based cyber security controls which can be expensive and take a long time to implement, training is one of the cheapest and simplest forms of improving cyber resilience. Training is also one of the quickest safeguards to put in place. Threat actors often target personnel. Humans are often the 'weakest link' in an organisation's cyber security defences and are targeted by cyber criminals to gain access to networks through phishing or related tactics.

Only one agency has reported 100% completion rate for staff training

Although all agencies have conducted some form of training and awareness programs on cyber security during 2021–22 applicable to all staff, the completion rates of mandatory training range from 20% to 100%, with over half of the agencies reporting completion rates of at least 85%. Agencies have used mostly online self-learning modules for training, but 32% also held face-to-face training sessions.

Few agencies have conducted additional training for higher risk groups

We noted:

- 12% of agencies carried out training to board members
- 28% of agencies carried out training to third parties with access to the organisation's systems (such as contractors, vendors and partners)
- 16% of agencies carried out training to certain groups who may be at greater risk of cyber attacks (such as procurement and payroll staff).

Over 90% of agencies performed awareness exercises such as simulated phishing tests. At least four agencies reported the results of their simulated phishing tests indicated a click-through rate of over ten per cent, where over ten per cent of the staff who received the test email clicked on the 'malicious' link. Click-through rates can vary depending on the sophistication of the simulated email and frequency of simulation exercises. It is important for agencies to monitor and report on these results over time, identify any repeat clickers, and adapt the exercise with new developments in cyber attacks.

Training content could be improved at 24% of agencies since COVID-19 changed the environment. Moves to higher levels of online service delivery and hybrid working models are reportedly increasing risks relating cyber fraud and online hoaxes. Examples include fraudulent requests:

- to change a supplier's or employee's bank details
- to add new suppliers to the master file
- for payment or invoices, which may purport to or appear to come from a legitimate user or senior officer.

Recommendation

Agencies need to reinforce their mandatory cyber awareness training to all staff and improve the completion rates.

Agencies should also conduct tailored training content for higher risk groups of users such as board members, procurement and payroll staff, and third parties with access to the agency's systems.

5. Engaging consultants and contractors

This chapter outlines our audit observations, conclusions and recommendations arising from our review of agencies' practices in engaging external experts, such as consultants and contractors.

Section highlights

- Agencies risk over-reliance on the same consultants, as some firms continue to be the highest paid consultants at 60% of agencies for at least three of the past five years.
- Agencies could improve their policies on engaging consultants to include consideration of:
  - probity requirements/conflict of interests
  - rotation of independent consultants from time-to-time
  - additional review where multiple consultants are engaged on the same topic to address the risk of opinion shopping.
- A quarter of agencies have re-engaged the same contractor over the past five years, with one contractor engaged for 19 years. Long-term engagements without reassessment against market increase the risk of dependency on the contractor.

5.1 Background

Engaging consultants

In the public service, many key decisions are based on, or supported by specialist advice, typically provided by an external subject matter expert. However, this process is subject to certain risks, such as:

- the advice is not impartial or has been deliberately manipulated, causing the decision-making process to be overly focused on achieving a desired outcome
- agencies becoming over-reliant on a single provider, and the advice not having been insufficiently canvassed from other perspectives or options
- 'shopping' for a consultant who will provide the advice that supports a desired outcome rather than considering alternative or better supported views.

Consultants are a subset of 'professional services' as defined by Procurement Board Direction PBD 2021-03:

> A consultant is defined as a person or organisation engaged under contract on a temporary basis to provide recommendations or professional advice to assist decision-making by management. Generally, it is the advisory nature of the work that differentiates a consultant from other contractors.

During the year ended 30 June 2022, the top 25 government agencies covered in this report recorded $127 million in combined consultant fees.

The trend in the agencies' combined consultant fees over the last five years is set out in the graph below.

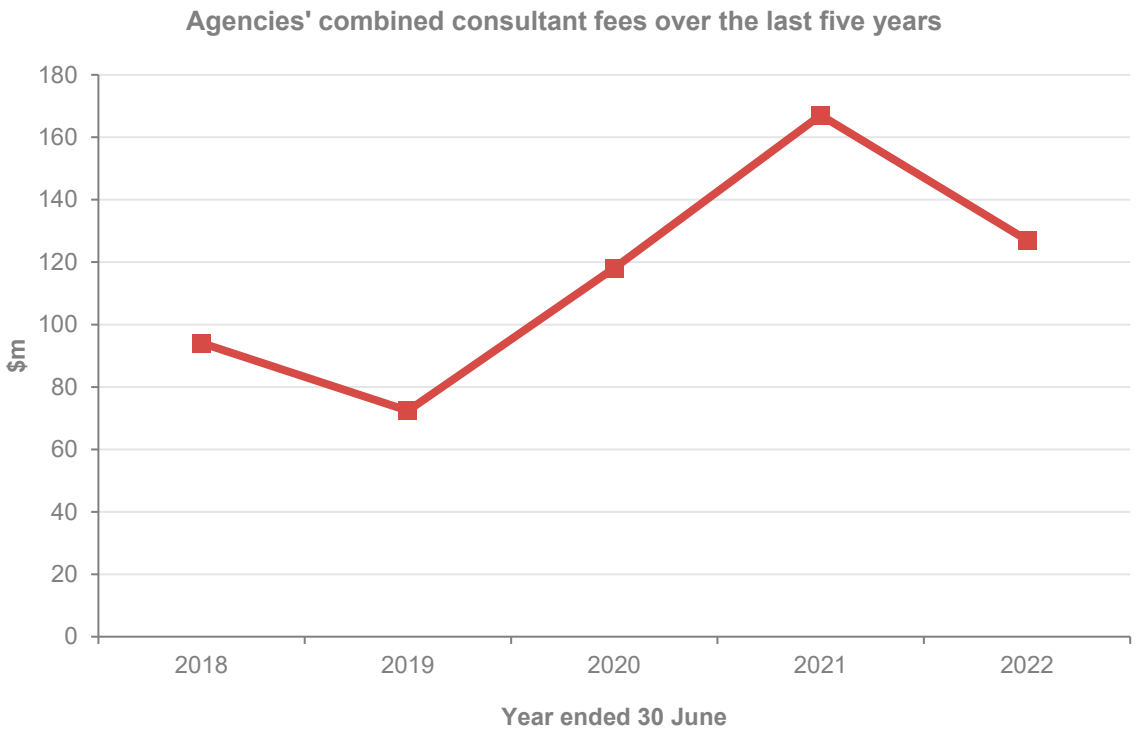

Exhibit 13.

Note: Due to Machinery of Government changes, four agencies did not exist in 2019 and five agencies did not exist in 2018.

Source: Agencies' financial data (audited).

Engaging contractors

Contractors are engaged as part of agencies' workforce strategy and management. They may provide capabilities that are otherwise unavailable in the agency. However, engaging a contractor to perform work that is a core capability of the agency or in government policy development is not desirable as it can create dependency on the contractor and may not achieve efficiency or value for money.

Contractors are an external source of labour and skills engaged under a contract or statement of work to provide services to an agency. They are often an individual providing services through their own private business, but can also be a group of individuals from a company or seconded staff from private firms.

We have not considered the following types of engagements within the scope of this report:

- casual, fixed-term or temporary employees directly employed by the agency
- contingent workers engaged through a labour supplier/employment agency.

During the year ended 30 June 2022, the top 25 government agencies covered in this report recorded over $1.2 billion in combined contractor fees.

The trend in the agencies' combined contractor fees over the last three years is set out in the graph below.

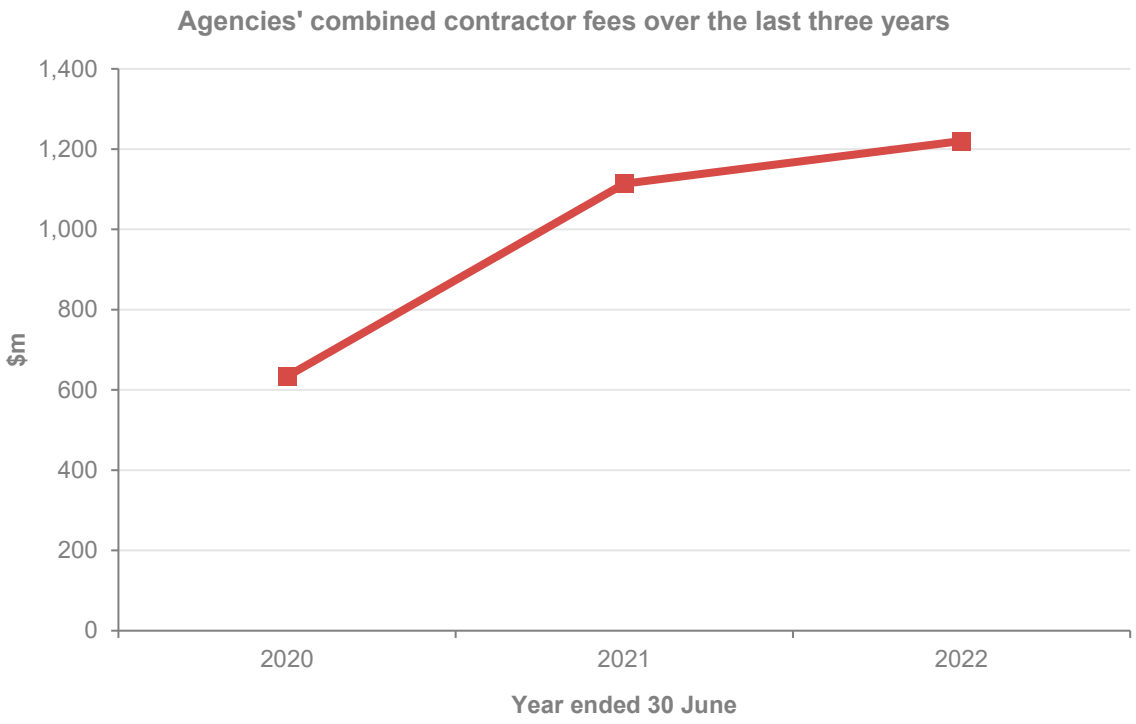

Exhibit 14.
Source: Agencies' financial data (audited).

5.2 Policy framework

Engaging consultants

NSW Procurement manages the Procurement Policy Framework and establishes whole-of-government schemes, such as the Performance and Management Services Scheme SCM0005 (PMS scheme). The PMS scheme has a pool of suppliers prequalified to supply professional services, including consultancy, to NSW government agencies.

The PMS scheme is not mandatory, so agencies are allowed to procure services outside of this scheme. In October 2021, the Procurement Board issued a Direction PBD 2021-03 which imposed additional conditions and governance arrangements for certain engagements outside the PMS scheme.

Under the PMS scheme, procurement rules require that:

- the agency must give specific instructions in a scope of work (SOW) to the supplier
- any variations to the SOW must be made in writing
- agencies must designate which agency personnel can instruct the supplier
- suppliers must disclose conflicts of interest at the point of engagement.

While there are guidelines from a whole-of-government scheme, it is important for agencies to establish their own policies and procedures, especially for circumstances where an agency may choose to procure outside of the PMS scheme.

Agencies' policies on engaging consultants could be improved

For consultants engaged to provide independent advice, the NSW Independent Commission Against Corruption (ICAC) released a better practice guide[4] on processes to reduce the risk of bias, conflict of interests and corruption. Agencies could improve the design of their policies in the areas below.

Policy requirement	Percentage of agencies' policies that do not require this %
For engagements outside of the PMS scheme/prequalified suppliers, only engage reputable independent consultants who are part of a professional association or peak body that has its own code of ethics and professional standards	100
Review the engagement fee for reasonableness, in comparison to other quotes or tender applications	4
Rotate independent consultants from time-to-time	72
Ensure probity/avoid conflict of interest in selection of consultant or setting the SOW – that is, if the advice relates to a person or division that could be the subject of adverse comment, that person or division should not be making procurement decisions	32
If the agency engages more than one consultant on the same issue or topic, appropriate reasoning must be provided and the engagement must be approved by another senior officer	72

Source: Audit Office analysis.

Engaging contractors

The Procurement Policy Framework also governs the use of contractors as a subset of suppliers. Whilst the NSW Public Service Commission has carriage of the Contingent Workforce Management Guidelines that specifies considerations around workforce management and planning, the guidelines only apply to contingent workers engaged through a labour supplier.

The Victorian Public Service Commission has published guidelines on engaging contractors[5] more generally which highlights the benefits and disadvantages for public sector. Contractors would be suitable for work that requires specialised skills, is infrequent or unpredictable in timing, or requires independence. Disadvantages include:

- loss of capability and increased dependency on external providers
- potential employee disengagement
- additional on-costs such as extensions and overruns, and diverting internal resources for contract management
- operational restrictions.

[4] NSW ICAC publication Obtaining independent advice - dos and don'ts.
[5] VPSC - External capability - things to consider before using contractors.

Agencies' policies on engaging contractors could be improved

Although all agencies have a policy on engaging external labour, whether it be in a broader procurement policy or a contingent labour policy, these could be improved in the following areas.

Policy considerations that support engaging a contractor	Percentage of agencies' policies that do not require this %
Capability – if required specialist skills are not within the agency's core capability	12
Timing of work – if unpredictable or infrequent	20
Cost – if more efficient and effective to engage contractor	12
Timeframes for engagement – short-term (less than six months)	20

Source: Audit Office analysis.

Guidelines on effectively managing contractors could also be enhanced in the following areas.

Policy requirements on managing a contractor	Percentage of agencies' policies that do not require this %
Clear designation of roles and responsibilities	32
Clear definition of requirements in the scope of work	20
Key performance indicators (KPIs) that are linked to the project/task outcomes	24
Rules or guidelines for managing costs and additional expenditure	24

Source: Audit Office analysis.

5.3 Managing consultants

Agencies risk over-reliance on the same consultants

In reviewing agencies' top three highest paid consultants for the last five years, 60% of agencies have relied on the same consultant for at least three of those years, and 28% have relied on the same consultant for at least four of those years.

Across the sector, there is a significant reliance on the 'Big 4' professional services firms which unsurprisingly make up the top four highest paid consultants over the past five years. The graph below shows the breakdown of consultant expenses for the agencies in this report from 2018 to 2019. The 'other' category comprises over 600 consultants.

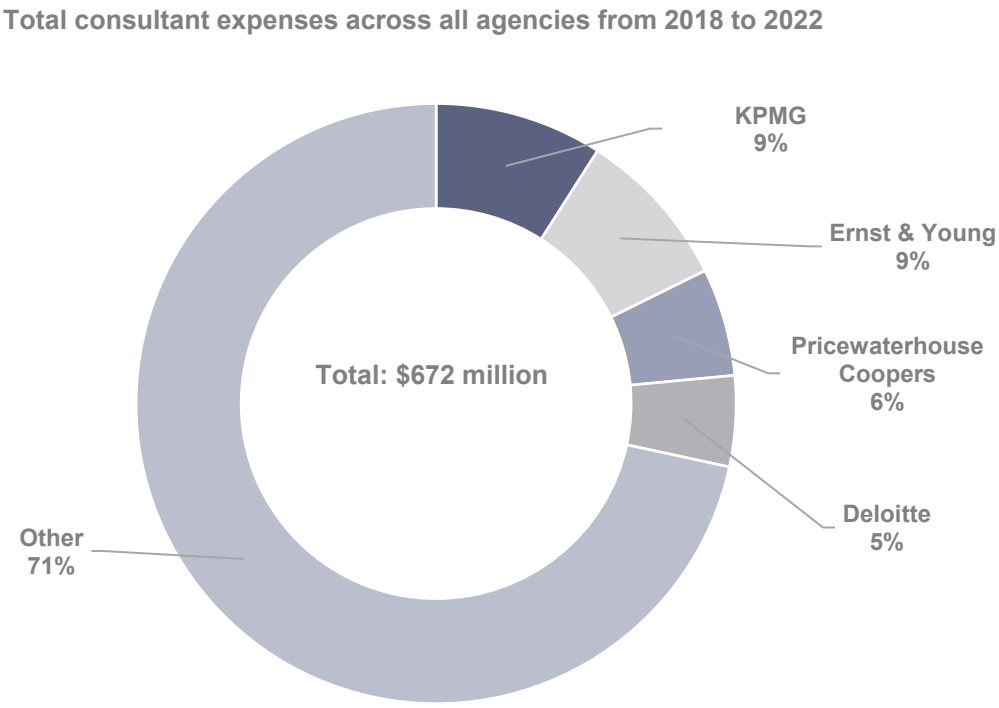

Exhibit 15.

Source: Agencies' published annual reports for 2018 to 2021, and agencies' financial data for 2022 (audited).

The guidance on defining a 'consultant' does not support consistent and accurate reporting on spend across the sector

The distinction between consultants and professional services is not always clear. As a result, agencies do not have consistent methods of classifying engagements as consultancies, given the degree of judgement involved in assessing whether the engagement is advisory in nature. Agencies' use of consultants will also vary depending on the nature of their business and whether significant projects are being run in a particular year. For annual reporting purposes, agencies are required to disclose in their annual reports the cost of consultant engagements over $50,000 by individual project, and a summary of engagements less than $50,000.

From our review of total professional services expenses in 2022 for the agencies in this report, nine per cent related to engagements outside the PMS scheme.

Our observations on consultancy spend noted the following statistics:

Year end 30 June	2018	2019	2020	2021	2022
Percentage of agencies that had less than ten engagements	16%	32%	28%	28%	32%
Highest number of engagements at one agency	130	273	1,774	671	1,146
Highest spend on consultants at one agency	$13.7 million	$16.4 million	$26.3 million	$39.2 million	$24.4 million
Highest spend on a single consultant at one agency	$5.9 million	$6.2 million	$7.9 million	$6.6 million	$5.9 million
Highest spend on a single consultant (above) as a percentage of that agency's total spend on consultants	42.9%	76.4%	85%	16.7%	24.2%

Source: Agencies' published annual reports for 2018 to 2021, and agencies' financial data for 2022 (audited).

A related performance audit report on use of consultants is expected to be published in March 2023 that will review how effectively NSW government agencies procure and manage consultants.

5.4 Managing contractors

One agency did not demonstrate probity in engaging contractors who are active and former employees

Although the agency has a secondary employment policy that prohibits staff who are Australian Business Number (ABN) holders from invoicing the agency under their private business, we identified the agency had paid at least ten vendors each year from 2018 to 2022 that are linked to active employees. None of those active employees identified in the agency's vendor register had declared secondary employment or pecuniary interests.

This agency had also transacted with at least 15 vendors each year from 2018 to 2022 that are linked to former employees. Total payments each year to those vendors ranged from $4 million to $11.2 million.

In one instance, a senior officer at the agency responsible for procurement had recommended a vendor for a $10 million contract in January 2018, left the agency in April 2018 and took a manager position with the vendor in September 2018. This individual then became a director at the vendor in 2019. No declaration of conflict of interest was made while the individual was an employee or as part of the procurement process. Agency management were unable to locate key documents relating to this transaction such as the signed briefing paper, original recommendation to award the contract, and tender evaluation records.

These practices may result in non-compliance with codes of conduct or other policies, and increase the risk of fraud. Undisclosed conflicts of interests can influence or be perceived to influence decisions at the agency that compromise the objectives of the Procurement Policy Framework around value for money and fair and open competition.

Sixteen per cent of agencies reported that they have engaged contractors who are former employees of the agency. Whilst this may be appropriate in some circumstances, it is important that these relationships are disclosed for transparency.

It would be prudent for agencies to consider additional policies or conditions in employment agreements addressing probity in the procurement process for contractors linked to active or former employees to mitigate risks of:

- fraud
- theft or inappropriate use of intellectual property
- familiarity threats – where procurement proposals by former employees are approved by former colleagues, or former colleagues are responsible for managing project delivery and quality of the work of former employees.

Over 40% of agencies have re-engaged the same contractors for more than five years

Eighty per cent of agencies have engaged contractors on a recurring basis over the last five years, and 11 of these agencies have re-engaged the same contractor for five or more years. All of these agencies have re-engaged contractors for the same role or type of work, and 37% had also re-engaged contractors for different work.

The highest number of contractors who have been re-engaged by an agency was 1,913 in the last five years.

The longest period a contractor was engaged continuously at an agency ranged from 12 months to 19 years. For those agencies with contractors engaged for more than five years, only 55% of them had reassessed the contract against the market before renewing the contract. More generally, this occurred at 63% of agencies for the longest term re-engaged contractor. While there are benefits from re-engaging a contractor who has already gained experience and familiarity working with the organisation, agencies may not be achieving the best value for money if they have not reviewed the market. This risk is particularly heightened the longer a contractor has been re-engaged as technological, regulatory and other environmental developments may have occurred to bring new suppliers on the market. There is also a risk that long-term contractors are also addressing a core capability and the role would be better addressed through recruitment of a permanent staff member.

Recommendation

Agencies need to ensure that contractor engagements that have been renewed over multiple years for the same role are periodically reassessed against the market to demonstrate that the contractor continues to represent value for money and effectiveness in achieving performance objectives.

Thirty-six per cent of agencies are outsourcing work that is a core capability

In 36% of agencies, we found that the highest paid contractors have been engaged to perform work that is considered a core capability for the agency. Examples include:

- temporary placements to fill a director, executive or senior management role
- a Big 4 accounting firm engagement linked to the core functions of an agency
- ensuring legislative compliance and delivering projects that are part of an agency's core function.

At 46% of agencies, the timing of work the contractor performed was not unpredictable or infrequent. For three agencies, the nature of the contractor's work was both a core capability and the timing was not unpredictable or infrequent.

In 2022, the highest paid individual contractor earned over $599,000, which represented 0.3% of the agency's total contractor expenses for the year. This contractor was engaged in a senior management role.

In 2021 and 2020, the highest paid individual contractor was the same person in both years and earned over $609,000 and $590,000 respectively (but was not the same contractor noted for 2022). Those costs represented less than 0.8% of the agency's total contractor expenses for each year. This contractor was also engaged in a senior management role.

6. Employment screening practices

This chapter outlines our audit observations, conclusions and recommendations arising from our review of agencies' employment screening practices.

Section highlights

- We identified that most agencies do not include the risk of employment application fraud in their risk registers.

  Post-employment screening has an important role in preventing fraud and managing risk as roles often change and the initial employment screening procedures may not be sufficient to control risk over time. Only 57% of agencies that have an employment screening policy include post-employment screening guidance.

- Screening and induction practices for non-permanent workers are often less stringent than for permanent employees. There is an increased risk that agencies will:
  - fail to identify an applicant with a past history of corrupt or criminal conduct
  - not identify applications with false credentials
  - hire a worker with unsuitable qualifications, skills or experience.

6.1 Background

Employment screening is used to ensure the suitability, integrity and identity of people employed in the NSW public sector. Agencies are subject to a number of legal and regulatory requirements that are relevant to employment screening practices, including:

- the *Government Sector Employment Act 2013*
- the Government Sector Employment (General) Rules 2014.

Undetected employment application fraud can undermine merit-based selection and result in hiring an employee who lacks not only the requisite expertise for the role, but also basic integrity. This can have a range of detrimental effects for an agency, including health and safety risks, poorer provision of public services, and impairment of public trust and confidence.

Agencies can address employment application fraud by implementing a range of measures, including but not limited to designing a risk-based employment screening framework, assigning roles and responsibilities, improving the quality of employment screening checks and conducting checks on non-permanent workers.

The Independent Commission Against Corruption (ICAC) published a report in February 2018 on 'Strengthening Employment Screening Practices in the NSW Public Sector'. Overall agencies can improve their processes by benchmarking to this report.

6.2 Policy framework

Most agencies have developed their own specific policy for employment screening checks and procedures. We have noted that opportunities still exist to make these employment screening policies more comprehensive.

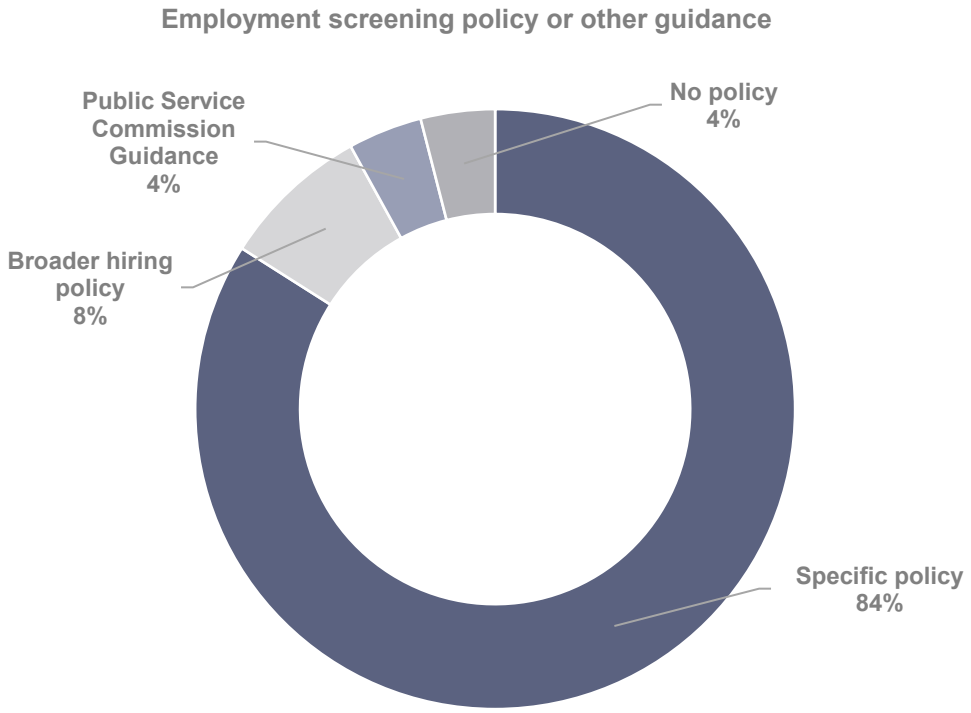

Exhibit 16.
Source: Audit Office analysis.

Fifty-seven per cent of agencies that have developed a specific policy for employment screening conduct a single approach instead of a risk based/role based approach. The NSW Public Service Commission (PSC) pre-employment guidelines also recommends considering the essential requirements of the role, identifying any risks associated with the requirements, and deciding on screening checks required to manage risks identified. The selected approach taken by the agency will determine the level of employment screening required. Another key component of a good policy should also assign roles and responsibilities for employment screening, which all agencies with their own policies have addressed. This key component is also referred to in the PSC guidelines.

Post-employment screening has an important role in preventing fraud and managing risk as roles often change and the initial employment screening procedures may not be sufficient to control risk over time. Only 57% of agencies that have their own policy include post-employment screening guidance.

Without policies and procedures for employment screening, there is an increased risk of employment application fraud. Employment application fraud is an indicator of future corrupt conduct and other acts of dishonesty.

Most agencies do not include the risk of employment application fraud in their risk register

Only 40% of agencies have included the risk of employment application fraud in their risk register. Having policies and procedures in place without defining the risk itself may lead to less effective or less targeted controls, particularly if the screening approach is risk-based. Identification of employment application fraud on the risk register will record the likelihood and consequences of this risk occurring, the actions required to reduce the risk and assign responsibility to manage the risk. The risk rating applied to employment application fraud should also be monitored in accordance with the overall risk policy.

Some agencies have not complied with screening citizenship requirements in the *Government Sector Employment Act 2013*

The *Government Sector Employment Act 2013* (GSE Act) specifies that the engagement of public service employee may be subject to specific conditions such as:

- citizenship or residency requirements
- formal requirements
- security and other clearances
- health clearances.

Twenty-four per cent of agencies have not complied with the employment screening requirements of the GSE Act with regard to citizenship or residency requirements. Rule 6 of the Government Sector Employment (General) Rules 2014 (GSE Rules) states that a person is not to be employed as a public service employee unless they are:

- an Australian citizen
- a permanent resident of Australia
- a New Zealand citizen with a current New Zealand passport
- citizen of another country with a current visa that allows the person to work in Australia.

Most agencies conduct post-employment screening. Post-employment screening may be required when:

- the role is inherently risky and ongoing checks need to be conducted
- the role requires ongoing evidence that relevant qualifications and licences have not lapsed
- a person is promoted or moved to a different role
- a person has the same role but is given new or different responsibilities
- a contractor becomes an employee.

Post-employment screening includes triggered re-screening and periodic re-screening. For example, a triggered re-screening may occur when an employee changes role within the agency. A periodic re-screening is conducted for high-risk roles or reapplied after a set period of time. Most agencies conduct re-screening procedures, either triggered, periodic or a combination of both, as an agency does not need to choose one approach over the other. However, agencies' policies do not clearly specify circumstances where post-employment screening should be performed. This may result in inconsistent application of post-employment screening or expose agencies to greater risks.

All agencies use external providers to perform employment screening, either on its own or in conjunction with internal processes. Where a combination approach is used, all agencies have guidelines on circumstances when in-house or external screening is to be performed.

Twenty-one per cent of agencies that perform in-house employment screenings have a decentralised process. If adequate procedures and guidelines are in place, this may suit the operations of the agency. However, a decentralised approach can lead to inconsistency, duplication of work and non-conformance with policy.

6.3 Conducting checks

The rigour/extent of security and credential checks vary across agencies

Pre-employment criminal record, qualification and employment history checks verify the credentials, identity and integrity of a prospective or current employee. Most agencies perform criminal record checks with all new appointments.

Agencies that require Working With Children Checks (WWCC) for all new appointments also require these checks for their non-permanent workers such as casual staff or contractors.

Only 40% of agencies conduct credential checks for all appointments by validating the educational/professional qualifications of the applicant, while other agencies only perform the credential check if a certain qualification is required for the role description. Not all positions in NSW government require qualifications or licences. However, if an applicant has purported to possess a qualification, even if it is not required for the role, this may have formed part of the merit assessment which favoured that applicant over other candidates. Credential checks for all appointments reduce the risk of applicants gaining the role through dishonest means.

Re-screening checks ensure relevant professional credentials exist and have not expired

Of those agencies that do not conduct credential checks on all appointments, 40% will conduct these important checks on roles considered as high-risk positions only. If guidance is not clear when checks should be conducted, this may increase the risk of under-screening which may lead to employment application fraud, including internal applications and acting roles.

Nearly half of all agencies report they have experienced barriers to conducting employment screening in the last 12 months, that is, from a lack of resources or time constraints. One agency responded that due to resource pressures (criticality to filling a role, often related to safety or legal obligations), employees have been commenced prior to the completion of their criminal history screening, conditional on the eventual clearance.

Non-permanent workers

Screening and induction practices for non-permanent workers are often less stringent than for permanent employees

The ICAC report on 'Strengthening Employment Screening Practices in the NSW Public Sector' noted that, due to the nature of their engagement, non-permanent workers can pose greater corruption risks to an organisation and should be subject to the same employment screening checks as done for permanent workers.

While all agencies perform screening of non-permanent workers, 48% of agencies' screening checks differ for permanent and non-permanent workers. One agency's policy does not require the same employment screening practices for contractors such as contingent labour. As a result, there is an increased risk that agencies will:

- fail to identify an applicant with a past history of corrupt or criminal conduct
- not identify applications with false credentials
- hire a worker with unsuitable qualifications, skills or experience
- rely on screening practices of individuals in their organisation, which may be inconsistent, ad hoc and may not access all data available for applicants.

For 28% of agencies, the human resources/people management division is not responsible for recruiting and inducting non-permanent workers. This is assigned to the business departments. For some agencies, human resources may oversee and own the process with individual hiring managers conducting recruitment and induction. For other agencies, a third-party supplier is responsible for selection and induction of contract labour. These practices can lead to inconsistent screening activities or non-compliance with policy requirements where the business departments and hiring managers are less familiar with the process. These inconsistencies may increase the risk of fraudulent applications if the individuals involved in the process are not experienced with identifying false or misleading applications, particularly when screening checks are limited or not conducted.

7. Contract management

This chapter outlines our audit observations, conclusions and recommendations arising from our review of agencies' contract management processes.

Section highlights

- All agencies maintain a central contract register but 40% are incomplete, risking non-compliance with the *Government Information (Public Access) Act 2009* (GIPA Act).
- The contract renewal process could be improved. We identified only 76% of agencies assessed value for money before deciding to renew/extend the contract.
- Most agencies provide some training and support to staff on procurement procedures. Ongoing training and awareness programs allow agencies to communicate to all staff their responsibilities and obligations in relation to procurement activities.

7.1 Background

The NSW Government Procurement Policy Framework (the Framework) sets the following objectives: value for money, fair and open competition, easy to do business, innovation, economic development, social outcomes and sustainability.

NSW government agencies must ensure their internal policies and controls are consistent with the mandatory requirements set out in the Framework. The mandatory requirements include financial management obligations and policies relating to fraud and corruption control. However, the Framework does not provide detailed guidance for contract management. It refers to other specific guidelines and policies for different types of contracts.

The NSW Public Service Commission (PSC) developed a capability framework for use across NSW government agencies. The capability framework describes the capabilities and associated behaviours that are expected of all NSW public sector employees. Whilst the framework is recommended, it is not mandatory. NSW Procurement, in consultation with the PSC, has developed a program called the Procurement Capability Compass. The compass program is a whole-of-government procurement capability assessment tool that is aligned with the PSC’s capability framework. The compass program is designed to measure the baseline of procurement knowledge across a team by helping individual staff identify their strengths and development areas.

7.2 Policy framework

All agencies have a policy governing contract management that is easily accessible. Twelve per cent of these policies are overdue for review.

The Framework recommends the following points as best practice. Agencies could improve how they establish contract management plans for high value contracts.

Elements of best practice	Percentage of agencies that implement these %
Establish systems and processes to ensure compliance with contract terms and performance requirements	100
Determine who is responsible for key tasks and activities	100
Define and maintain the appropriate level of management and resources of the procurement arrangement	96
Manage performance	100
Track and report benefits to demonstrate how value for money is being delivered	96
Establish contract management plans for high value goods and services procurement	88

Source: Audit Office analysis.

All agencies use the PSC capability framework for position descriptions for all staff. Seventy-six per cent of agencies use the compass program to assess the procurement capability of their staff annually.

Ninety-six per cent of agencies use a range of approaches to validate performance data which contributes towards ensuring the agency is achieving value for money. These include:

- risk reviews included as part of regular performance reviews
- risk and complexity-based approach to levels of management, frequency and reporting requirements for contracts.

All agencies' policies and procedures provide instructions on how and when contract managers should monitor and review contract performance.

7.3 Managing contracts

All agencies maintain a central contract register, but many are incomplete risking non-compliance with the GIPA Act

The GIPA Act aims to improve the transparency and integrity of the NSW public sector by requiring agencies to proactively publish information in relation to their contracts with the private sector. If an agency does not maintain a central contract register, it increases the risk of non-compliance with the GIPA Act. A centralised contract register can also enhance procurement and contract management outcomes because it:

- allows an agency’s central procurement team to monitor contract end dates, contract extensions and commence new procurement in a timely manner
- helps agencies manage their contractual commitments, budgeting and cash flow requirements.

We have previously identified concerns with the completeness and accuracy of contract registers maintained by agencies, and this remains an ongoing area of concern.

Twenty-four per cent of agencies do not have a proactive approach to identifying issues that may be systemic. They tend to rely on self-reporting and monitoring. Agencies should conduct monitoring activities throughout the life of the contract by:

- collecting and validating relevant performance information
- regularly monitoring and rigorously reviewing contract performance
- identifying and responding to contract performance issues in a timely and effective manner
- providing regular reporting to the senior management.

Three agencies do not have a specialised contract management system

Eighty-eight per cent of agencies have a contract management system that can support effective planning for end of contracts by alerting contract managers of pending expiry dates.

One agency is in the process of implementing a system that is capable of that function.

Only 60% of all agencies' contract registers are complete

One agency did not record details of contracts over $150,000 as required by the GIPA Act.

Five agencies record all contracts regardless of dollar value, while others set lower thresholds than the mandatory $150,000, ranging from $30,000 to $50,000.

Forty per cent of all agencies' contract registers are incomplete, with either missing contracts or missing details such as:

- contractor reference number
- contract effective/end dates
- contract category
- the manager assigned.

Sixteen per cent of agencies do not regularly review the contract register for accuracy and completeness

Most agencies' policies require the contract register to be reviewed for accuracy and completeness at least annually. Thirty-six per cent of agencies review their contract registers monthly.

For one agency, the contract register is reviewed on an ad hoc basis. There was no evidence this was done in the last financial year. A lack of periodic review has contributed to this agency's incomplete and inaccurate contract register.

Half of all agencies do not maintain registers for revenue or lease agreements

Whilst not related to the Procurement Policy Framework, it is best practice for agencies to maintain a central register for other types of contracts such as revenue/grant agreements, leases, and service level agreements (including inter-agency service agreements that do not go through a procurement process).

Only half of the agencies have central registers for revenue or lease agreements. The management and monitoring of these agreements is decentralised in most agencies and reference to these types of agreements is not included in agencies' procurement policies.

This may increase the risk of financial reporting errors if contracts are not accounted for correctly or not in the correct period. It is important for finance staff to be aware of the existence of legal agreements to understand the accounting consequences. From an operational perspective, central registers for other types of key agreements help to ensure completeness of records and monitoring of updates and obligations.

Overall, 64% of agencies have central registers for other types of agreements. One-third of the agencies do not regularly review those registers to ensure accuracy and completeness.

Compliance with GIPA Act reporting requirements

Part 3, Division 5 of the GIPA Act states that information about contracts worth more than $150,000 between agencies and private sector bodies must be recorded in a register of government contracts. A copy of an agency's government contract register is to be published on the government tenders' website.

For Class 1 contracts (value of $150,000 or more), the agency must enter the following information in the government contracts register within 45 days of the contract becoming effective.

Required information	Percentage of agencies that complied %
Name and address of the private sector contractor	92
Details of any related company that may be involved in carrying out the contractual obligations	75
Date the contract became effective and its duration	96
Particulars of the project or goods or services to be provided under the contract	88
Estimated amount payable to the contractor and any allowable variations to that amount	100
Any renegotiation provisions	67
Method of tendering and criteria for assessment, if appropriate	92
Any provisions for payment to the contractor for operational or maintenance services	67

Source: Audit Office analysis.

For Class 2 contracts, further information is required.

Class 2 contracts are Class 1 contracts to which any of the following applies:

- there has not been a tender process, the proposed contract has not been made publicly available and the terms and conditions have been negotiated directly with the contractor
- the proposed contract has been the subject of a tendering process and the terms and conditions have been substantially negotiated with the successful tenderer
- the obligations of one or more parties to maintain or operate infrastructure or assets could continue for ten years or more
- the contract involves a privately financed project as defined by guidelines published by Treasury
- the contract involves a transfer or a significant asset of the agency to another party in exchange for the transfer of an asset to the agency.

Required information	Percentage of agencies that complied %
Particulars of any future transfer of significant assets to and from the agency	62
Results of any cost-benefit analysis	77
Particulars of how risk will be apportioned, if relevant	69
Particulars of any significant guarantees or undertakings between the parties	77
Any other key elements of the contract	85

Source: Audit Office analysis.

Contract renewal assessments could be improved

When contracts are renewed or extended without going through a competitive process, only 76% of agencies assessed value for money before deciding to renew/extend the contract. However, only half of the agencies used a standard template for the assessment, which included consideration of all of the following:

- supplier performance (including meeting customer expectation and performance against KPIs)
- business needs (whether there is still a need for the goods and services and/or have requirements changed)
- market analysis (including analysis of how the market changed/technology advances)
- coordinated procurement arrangement (consideration of procurement arrangements or activities planned or in place that may impact the extension or renewal).

Without a standard template or guidelines, agencies may have inconsistent application of their value for money assessment.

Twelve per cent of renewals were not approved by a delegated authority. For those renewals approved by a delegated authority, 14% of agencies' approval was only for the value of the contract from the date of extension, not the total value of the contract including extension. This practice may increase the risk that approvals for contract extensions are not reviewed by the appropriate level of authority as lower value contract extensions can add up.

7.4 Training and support

Ninety-two per cent of agencies provide some training and support to staff on procurement procedures

Of those agencies that provided training in 2021–22, it was recently conducted and placed emphasis on personal accountability, probity and transparency in relation to procurement procedures. However, we noted gaps in some aspects of their procurement procedures when reviewing contracts, including:

- procurement documentation not specifying certain key details such as the conditions for participation including any financial guarantees and dates for the delivery of goods or supply of services
- purchase orders were not raised and approved for the total value of the contract
- request for tender was not issued
- the evaluation plan was not signed off by the Evaluation Committee.

Ongoing training and awareness programs allow agencies to communicate to all staff their responsibilities and obligations in relation to procurement activities which results in:

- effective management and monitoring of contracts
- compliance with procurement policies, frameworks and guidelines
- improvement in risk management processes.

Professional people with purpose

OUR VISION

Our insights inform and challenge government to improve outcomes for citizens.

OUR PURPOSE

To help Parliament hold government accountable for its use of public resources.

OUR VALUES

Pride in purpose

Curious and open-minded

Valuing people

Contagious integrity

Courage (even when it's uncomfortable)

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

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

PHONE +61 2 9275 7100

mail@audit.nsw.gov.au

Office hours: 8.30am-5.00pm
Monday to Friday.

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au