



FINANCIAL AUDIT

23 DECEMBER 2021

Internal controls and governance 2021

NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

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 2021**'.

A handwritten signature in black ink, appearing to read 'Margaret Crawford'.

Margaret Crawford

Auditor-General for New South Wales
23 December 2021

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

contents

Internal controls and governance 2021

Auditor-General's foreword	1
Report highlights	2
Introduction	3
Internal control trends	10
Information technology	20
Cyber security planning and governance	29
Managing conflicts of interest	40
Masterfile management	52
Tracking recommendations	57

Auditor-General's foreword

This report analyses the internal controls and governance of the 25 largest agencies in the NSW public sector, excluding state owned corporations and public financial corporations, for the year ended 30 June 2021.

Our preferred approach is to table the 'Report on State Finances' in Parliament before any other cluster report. This is because the 'Report on State Finances' focuses on the audit results and observations relating to the Total State Sector Accounts, in effect a consolidation of all government agencies. This year the 'Report on State Finances' has been delayed due to significant accounting issues being considered in the Total State Sector Accounts and which may impact the Treasury and Transport clusters.

As there are no matters in this report impacting the Total State Sector Accounts we have decided to break with normal practice and table this report ahead of the 'Report on State Finances'.

Report highlights

What the report is about

This report analyses the internal controls and governance of the 25 largest agencies in the NSW public sector, excluding state owned corporations and public financial corporations, for the year ended 30 June 2021.

What we found

Internal control trends

The proportion of control deficiencies identified as high risk this year increased to 2.8 per cent (2.5 per cent in 2019–20). Six high risk findings related to financial controls while three related to IT controls. Two were repeat findings from the previous year.

Repeat findings of control deficiencies now represent 49 per cent of all findings (42 per cent in 2019–20).

Information technology

We continue to see a high number of deficiencies relating to IT general controls, particularly around user access administration and privileged user access which affected 82 per cent of agencies.

Cyber security

Agencies' self-assessed maturity levels against the NSW Cyber Security Policy mandatory requirements are low. Although

agencies are required to demonstrate continuous improvement against the CSP, 20 per cent have not set target levels and of those that have set target levels, 40 per cent have not met their target levels.

Policies, processes and definition around security incidents and data breaches lack consistency. Improvement is required to ensure breaches are recorded in registers and action taken to address the root cause of incidents.

Conflicts of interest

Agencies' policies generally meet the minimum requirements of the Ethical Framework set out in the *Government Sector Employment Act 2013*. However, few meet the Independent Commission Against Corruption's best practice guidelines. Policies could be strengthened in relation to requirements around annual declarations of interests from employees and contractors.

Masterfile management

Policies governing the management of supplier masterfiles and employee masterfiles existed in 79 per cent and 54 per cent of agencies respectively.

Weaknesses were identified in those policies. Access

restriction, segregation of duties and record keeping were the most common opportunities for improvement.

Tracking recommendations

Most agencies do not maintain a register to monitor recommendations from performance audits and public inquiries. Registers of recommendations could be improved to include risk ratings and record revisions to due dates. While recommendations can take several years to fully address, the oldest open items were originally due for completion by June 2016.

What we recommended

Agencies should:

- prioritise actions to address repeat control deficiencies, particularly those that have been repeated findings for a number of years
- prioritise improvements to their cyber security and resilience as a matter of urgency
- formalise and implement policies on tracking and monitoring the progress of implementing recommendations from performance audits and public inquiries.

Fast facts

The 25 largest NSW government agencies in this report cover all nine clusters and represent over 95 per cent of total expenditure for NSW public sector.

9

high risk audit findings were identified this year

40%

of agencies have not formally accepted residual cyber risk based on their self-assessed maturity levels

52%

of agencies do not have a policy on tracking recommendations from performance audits and public inquiries

50%

of all internal control deficiencies identified in 2020–21 were repeat findings

75%

is the average completion rate of annual staff declarations of interests

1. Introduction

1.1 State sector agencies

This report covers the findings and recommendations from our 2020–21 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.



1.2 Financial snapshot

The 25 agencies included in this report constitute an estimated 95 per cent 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 2021.

	Number of agencies	Assets \$ billion	Liabilities \$ billion	Income \$ billion	Expenses \$ billion
Departments	9	243.9	45.6	102.0	91.4
Public non-financial corporations	4	56.9	5.2	6.4	6.6
Statutory bodies	12	58.4	27.9	19.5	14.0
Total	25	359.2	78.7	127.9	112.0

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

The report focuses on elements of agencies' control environments relevant to their response to emergencies

The COVID-19 pandemic continues to have a significant impact on the people and public sector of New South Wales. With more people working from home and accessing services remotely, strong information technology controls are increasingly important. Risks around cyber security have increased as cyber criminals target organisations, particularly people and divisions responsible for making payments. This, and the disbursement of stimulus and relief funding has heightened risks around management of payroll and supplier masterfiles.

Public inquiries into the bushfires and natural disasters of 2020 brought to light the importance for agencies to track the progress of recommendations from those reviews. In this report we also look at agencies' processes for tracking the progress in implementing recommendations.

This report covers the following topics:

Cyber security planning and governance	Conflicts of interest
<p>Strong cyber security is 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. Cyber security covers all measures used to protect systems – and information processed, stored or communicated on these systems – from compromise of confidentiality, integrity and availability.</p> <p>This report focuses on whether agencies have:</p> <ul style="list-style-type: none"> established effective cyber security policies and procedures assessed their cyber risk maturity implemented tools to manage cyber risks. 	<p>Managing conflicts of interest is a central component of the public sector Code of Ethics and Conduct. In performing public duties and dealing with public funds, agencies must have effective processes for ensuring staff and service providers maintain integrity.</p> <p>This report focuses on whether agencies have:</p> <ul style="list-style-type: none"> established policy frameworks on managing conflicts of interest implemented processes to identify and respond to actual, potential or perceived conflicts monitored the level of compliance with their policies.

Masterfile management	Tracking and monitoring of recommendations
<p>Public sector agencies make significant payments through accounts payable and payroll systems, which rely on the accuracy of information in masterfiles. Completeness and accuracy of masterfiles is essential to ensure only valid payments are made by agencies. Strong internal control frameworks to manage supplier and payroll masterfiles reduce the risk of error and misappropriation of cash.</p> <p>This report focuses on whether agencies have:</p> <ul style="list-style-type: none"> • established policies and procedures on masterfile management • designed appropriate review of masterfile changes • ensured masterfiles are secure. 	<p>Government agencies are subject to public scrutiny and may be required to address recommendations from the Audit Office's performance audits and/or parliamentary or public inquiries. Strong internal control frameworks help to ensure recommendations are tracked, monitored and resolved, keep the agency accountable and reduce the risk of repeat findings.</p> <p>This report focuses on whether agencies have:</p> <ul style="list-style-type: none"> • established policies and procedures on tracking recommendations • effectively monitored the progress of actions to address recommendations • mechanisms for reporting on actions taken.

Agencies can use this report to enhance their internal control and governance frameworks

The report provides insights into the effectiveness of controls and governance processes in the NSW public sector by:

- highlighting the potential risks posed by weaknesses in controls and governance processes
- helping agencies benchmark the adequacy of their processes against their peers
- focusing on new and emerging risks, and the internal controls and governance processes that might address those risks.

The findings in this report should not be used to draw conclusions on the effectiveness of individual agency control environments and governance arrangements. Specific financial reporting, internal controls and audit observations are included in the individual 2021 cluster financial audit Reports to Parliament.

1.4 Sector-wide learnings

Our review identified sector-wide learnings that government agencies should consider in relation to their internal controls 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.
- 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 to only staff that require that level of access to perform their role and only for the period 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

- Set target levels of cyber maturity in the NSW Cyber Security Policy and Australian Cyber Security Centre Essential 8 frameworks applied in NSW that ensure controls are, at a minimum, able to mitigate basic or 'opportunistic' cyber attacks. Based on a gap analysis of the agency's current maturity level and target level, agencies should formally document their acceptance of risks associated with not achieving their target maturity level.
- Continue to roll out periodic cyber awareness training to all staff to build and support a cyber security culture, including:
 - moving to mandatory rather than 'opt in' models for cyber training delivery
 - 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 employees 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.
- Improve the quality of security incident registers to enable root cause analysis on the incidents and reduce the risk of issues recurring in future. Registers should record:
 - date/time of incident
 - date/time of actions to resolve the incident
 - detailed actions taken in response to the incident
 - categories of the nature of the incident.

Managing conflicts of interest

- Expand conflicts of interest policies to align with guidelines developed by the Independent Commission against Corruption, and apply the same standard of requirements of senior executives to all employees and contractors, namely:
 - make annual declarations of private financial, business, personal or other interests on relationships that result in actual or perceived conflict of interest
 - make fresh declarations as soon as practicable following a change in the individual's private interests or assignment to a new role or responsibilities
 - require submission of 'nil returns' from employees confirming they have no conflicts to declare.
- Identify units or divisions that are at higher risk of conflicts of interest arising, depending on the nature of their business. Policies should include additional measures at the unit/division level to mitigate the higher risks.
- Reinforce and improve the completion rates of staff annual declarations, through ongoing training and support to employees.
- Ensure that registers of interests are maintained for all staff and capture key information such as:
 - estimated value of the personal interest held
 - details of the related person or organisation causing the conflict of interest
 - assessment of the risk of conflict of interest
 - management plan details for actual conflicts
 - approval by manager or supervising officer.

Masterfile management

- Establish policies and procedures on managing supplier masterfiles that cover:
 - validating changes to supplier details directly with a designated supplier contact
 - recording the reason for amendment to masterfile records
 - periodic review of the masterfile to ensure compliance, validity and completeness of the records
 - a naming convention applied to avoid duplication of supplier names.
- Establish policies and procedures on managing employee masterfiles that cover:
 - independent review of the employee records created or amended
 - recording the reason for amendment to masterfile records
 - maintaining evidence to support record creation or amendment
 - periodic review of the masterfiles to ensure compliance, validity and completeness of records.
- Perform reviews of user access rights to masterfiles to ensure access is restricted to authorised personnel who require the access to perform their duties and there is appropriate segregation of duties.


Tracking recommendations

- Establish policies on assigning, tracking and monitoring the progress of implementing recommendations from performance audits and public or parliamentary inquiries.
- Maintain a register of recommendations from performance audits and public inquiries, which include features such as:
 - risk or priority rating to the issue or recommendation
 - expected completion dates
 - milestone due dates for larger implementation plans with multiple steps
 - record of revisions to due dates
 - comments to explain why due dates were changed
 - assigned ownership with responsibilities.
- Perform acquittals and subsequent reviews to ensure the agency's response to recommendations effectively address the issue and actions are still in place or operating as intended.
- Reporting the status of recommendations on a regular basis to management and those charged with governance.

1.5 Status of 2020 report recommendations

Our report on internal controls and governance for the year ended 30 June 2020 made a number of recommendations. The table below sets out the status of the recommendations we have made in previous reports where they were relevant to agencies within the scope of this report.

Recommendation	Current status	
Procurement		
Agencies should review their procurement policies and guidelines to ensure they capture the key requirements of the NSW Government Procurement Policy Framework, including NSW Procurement Board Directions.	<p>The progress of the implementation of the recommendation is outlined below:</p> <ul style="list-style-type: none"> 6 of the eight agencies have reviewed their procurement policies and guidelines to ensure they capture the key requirements for procurements greater than \$650,000 that are open to the market, unless exempt 11 of the 15 agencies have reviewed their procurement policies and guidelines to ensure procurements greater than \$500,000 in foreign currency are hedged 3 of the six agencies have reviewed their procurement policies and guidelines for authorising engagement consultants. 	—
<p>Agency procurement frameworks should be reviewed and updated to respond to emergency situations that arise in the future. This includes:</p> <ul style="list-style-type: none"> updating procurement policies and guidelines to define an emergency situation, specify who can approve emergency procurement and capture other key requirements using standard templates and documentation to prompt users to capture key requirements, such as needs analysis, supplier selection criteria, price assessment criteria, licence and insurance checks having processes for reporting on emergency procurements to those charged with governance and NSW Procurement. 	<p>The progress of the implementation of the recommendations are outlined below:</p> <ul style="list-style-type: none"> 13 of the 21 agencies have updated their procurement policies and guidelines in relation to emergency situations 3 of the five agencies have started using standard templates and documentation to prompt users to capture key requirements 4 of the six agencies have implemented processes for reporting on emergency procurements to those charged with governance and NSW Procurement. 	—
Delegations		
Agencies should ensure their financial and human resources delegation manuals contain regular set review dates and are updated to reflect the <i>Government Sector Finance Act 2018</i> , Machinery of Government changes and their current organisational structure and roles and responsibilities.	Three of the four agencies have addressed this recommendation.	—
Agencies should review financial and human resources delegations to ensure they capture all key functions of laws and regulations, and clearly specify the relevant power or function being conferred on the officer.	Three of the five agencies have addressed this recommendation.	—

Recommendation	Current status
Progress implementing last year's (2019) recommendations	
Agencies should re-visit the recommendations made in last year's report on internal controls and governance and action these recommendations.	
Gifts and benefits management (2019)	
<p>Agencies should:</p> <ul style="list-style-type: none"> ensure their gifts and benefits register includes all key fields specified in the minimum standards, as well as performing regular reviews of the register to ensure completeness provide ongoing training, awareness and support activities to employees, not just at induction establish an annual attestation process for senior management to attest compliance with gifts and benefits policies and procedures publish their gifts and benefits registers on their websites to demonstrate their commitment to a transparently ethical environment. 	<p>The progress of the implementation of the recommendations is outlined below:</p> <ul style="list-style-type: none"> all agencies (four of four) have updated their gifts and benefits register to include all the key fields specified in the minimum standards all agencies (three of three) have commenced providing training to employees 12 of the 20 agencies have implemented an annual attestation process for senior management 2 of the 23 agencies have published their gifts and benefits register on their website.
Agencies should regularly report to the agency executive or other governance committee on trends in the offer and acceptance of gifts and benefits.	Two of the six agencies have addressed this recommendation.
Internal audit (2019)	
Agencies should ensure there is a documented and operational Quality Assurance and Improvement Program for the internal audit function that covers both internal and external assessments.	All agencies (three of three) have addressed this recommendation.
Key  Fully addressed  Partially addressed  Not addressed	

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.

The scope of this year's report covers 25 general government sector agencies. Last year's report covered 40 agencies within the total state sector. For consistency and comparability, we have adjusted the 2020 results to include only the agencies remaining within scope of this year's report. Therefore, the 2020 figures will not necessarily align with those reported in our 2020 report.

Section highlights

- We identified nine high risk findings, compared to eight last year, with two findings repeated from last year. Six of the nine findings related to financial controls and three related to IT controls.
- The proportion of repeat deficiencies has increased from 44 per cent in 2019–20 to 50 per cent in 2020–21. The longer these weaknesses in internal control systems exist, the higher the risk that they may be exploited and consequential impact.

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 nine high risk findings out of a total of 324 audit findings this year, compared to eight high risk findings out of a total of 319 audit findings in 2019–20. As a proportion of total audit findings, high risk findings have also increased from 2.5 per cent to 2.8 per cent. Of concern, were two high risk findings, which were repeat deficiencies reported in the previous year. Six of the nine high risk deficiencies related to financial controls and three related to IT controls.

Agencies should continue to address high risk internal control deficiencies as a matter of priority.

High risk finding	Implication	Further reporting
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 will be included in the Report on Planning, Industry and Environment, which will be tabled in December 2021.
We noted deficiencies in an agency's system change management controls whereby developers had access to make changes to live business systems. There was no independent monitoring of these developers' system activity logs.	Lack of access controls in system change management increases the risk that unauthorised changes may be released in the live business system which could lead to system errors, system downtime, data error, incorrect financial reporting or fraud.	Further detail on this issue will be included in the Report on Customer Service, which will be tabled in December 2021.
We noted that controls assurance reports on IT general controls (ITGCs) 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 ITGCs 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 will be included in the Report on Customer Service, which will be tabled in December 2021.
We noted deficiencies in an agency's fleet revaluation process, and management's analysis and quality control over the valuation process.	Lack of quality control and review of the fleet revaluation process increases the risk of audit delays, additional audit costs and a higher risk of misstatement to the financial statements.	Further detail on this issue will be included in the Report on Stronger Communities, which will be tabled in December 2021.
An agency manages an event centre without having executed lease agreements. This creates uncertainty over the existing accounting treatment of certain assets that are material to the agency's financial statements.	Without an executed lease agreement, roles and responsibilities are not formalised and clearly defined. There is also an increased risk of material misstatement to the financial statements.	Further detail on this issue will be included in the Report on Stronger Communities, which will be tabled in December 2021.
We noted deficiencies in an agency's impairment assessment model for certain inventories. The agency was unable to substantiate some of the underlying data used in the impairment model.	Management's inventory impairment assessment is subject to significant estimation uncertainty, including inaccurate data, which could have a potential material impact on the impairment provisions.	Further detail on this issue will be included in the Report on Health, which will be tabled in December 2021.

High risk finding	Implication	Further reporting
We noted significant estimation uncertainty associated with an agency's expected credit loss (ECL) provision for major debtors due to data validation issues and limited debt recovery activity. Management reassessed and increased the ECL provision at 30 June 2021.	The agency may be exposed to further credit losses on outstanding debtors.	Further detail on this issue will be included in the Report on Health, which will be tabled in December 2021.
There is uncertainty in an agency's valuation of inventory which was received free of charge but is measured at fair value based on replacement cost. Cost information was not readily available for the year ended 30 June 2021, however it would increase the accuracy and reliability of the reported financial information.	As the inventory balance is expected to increase, there is a greater risk that these inventories are not valued correctly.	Further detail on this issue will be included in the Report on Health, which will be tabled in December 2021.
We noted deficiencies in the agency's management of conflicts of interest declarations in relation to land acquisitions. Instances noted were in breach of the agency's procurement policy which requires all staff involved in procurement activities to formally declare whether they have or do not have any conflicts of interest.	Absence of rigorous and consistent management of conflicts of interest, and non-compliance with established policies, increases the risk that the agency may be exposed to reputational damage or financial losses in relation to land acquisitions. This may result in lack of probity or value-for-money considerations during the land acquisition process.	Further detail on this issue will be included in the Report on Transport Agencies, which will be tabled in January 2022.

Note: Reporting of two of the high risk findings above have not been finalised at the date of this report. The draft findings were provided to management who have not yet provided their response.

Source: Audit Office findings.

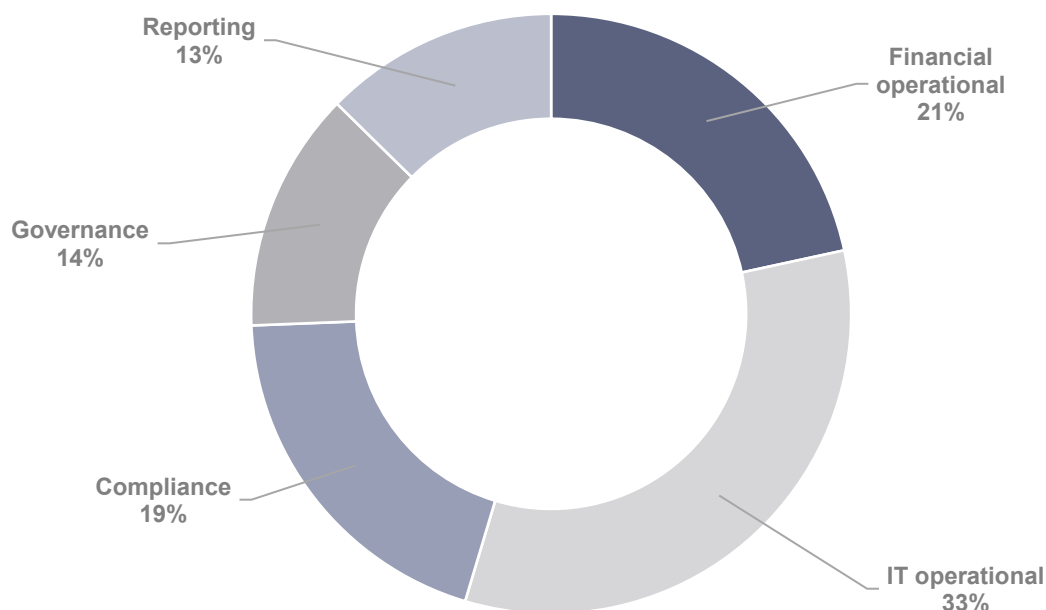
2.2 Common findings

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 324 internal control deficiencies we identified in 2020–21 into common categories as follows:

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

Internal control deficiencies 2020–21



Source: Audit Office findings.

The graph above shows that 54 per cent of the deficiencies (82 per cent in 2019–20) were financial or IT operational deficiencies, with the remainder split between compliance deficiencies (19 per cent compared to 16 per cent in 2019–20), reporting deficiencies (13 per cent compared to two per cent in 2019–20) and governance deficiencies (14 per cent; not separately reported in 2019–20).

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 (177)

⚠	High:	2 new	2 repeat
⚡	Moderate:	52 new	66 repeat
✅	Low:	29 new	26 repeat

Common issue	Findings/implications	Lessons for agencies
Maintaining master files	Controls were not established to: <ul style="list-style-type: none"> ensure sufficient segregation of duties over access to key masterfiles verify the validity, accuracy and/or completeness of changes to key masterfiles, such as vendor and payroll tables. 	Agencies should: <ul style="list-style-type: none"> review controls established over access to key masterfiles 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.

Common issue	Findings/implications	Lessons for agencies
Information technology	Control deficiencies were noted relating to IT governance, user access administration, program change and computer operations.	Refer to Section 3 of this report for further details.


Source: Audit Office findings.

Compliance (64)			
	High:	0 new	0 repeat
	Moderate:	20 new	16 repeat
	Low:	14 new	14 repeat

Common issue	Findings/implications	Lessons for agencies
Contract registers	<p>Agencies have not established contract registers or have incomplete or inaccurate contract registers. These agencies may face challenges with:</p> <ul style="list-style-type: none"> • complying with GIPA 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. 	<p>Agencies should focus on establishing complete and accurate contract registers. This includes:</p> <ul style="list-style-type: none"> • 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.
Document retention	<p>Agencies do not always maintain documents to evidence performance of key control activities. Deficiencies reduce accountability and reduce compliance with state records legislation.</p>	<p>Agencies should educate staff in their responsibilities and retain documentary evidence that they have discharged responsibilities.</p> <p>Agencies should ensure appropriate records management policies have been communicated to staff.</p>
Central registers, such as those used to manage conflicts and gifts and benefits	<p>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.</p>	<p>Agencies should ensure they have registers to capture staff disclosures in a way that complies with legislation and policies.</p> <p>Conflict of interest, gifts and benefits and other relevant policies should specify the timeliness of how such registers are updated.</p>

Source: Audit Office findings.




Reporting (41)

	High:	4 new	0 repeat
	Moderate:	9 new	9 repeat
	Low:	13 new	6 repeat

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.
Manual journals	Manual journals are prepared and posted by the same employee without an independent review. Supporting documentation is not attached to the general journal.	Management should implement controls so there is segregation of duties when posting manual journals. If this is not possible, management could implement a control where a periodic report of journals is independently reviewed. Management should ensure sufficient documentation is attached to the journal to explain its nature.
Accounting standard application	Agencies have not performed comprehensive assessments of the financial impact of the new leasing, revenue and related party accounting standards.	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.

Source: Audit Office findings.

Governance (42)

	High:	1 new	0 repeat
	Moderate:	9 new	13 repeat
	Low:	12 new	7 repeat

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.

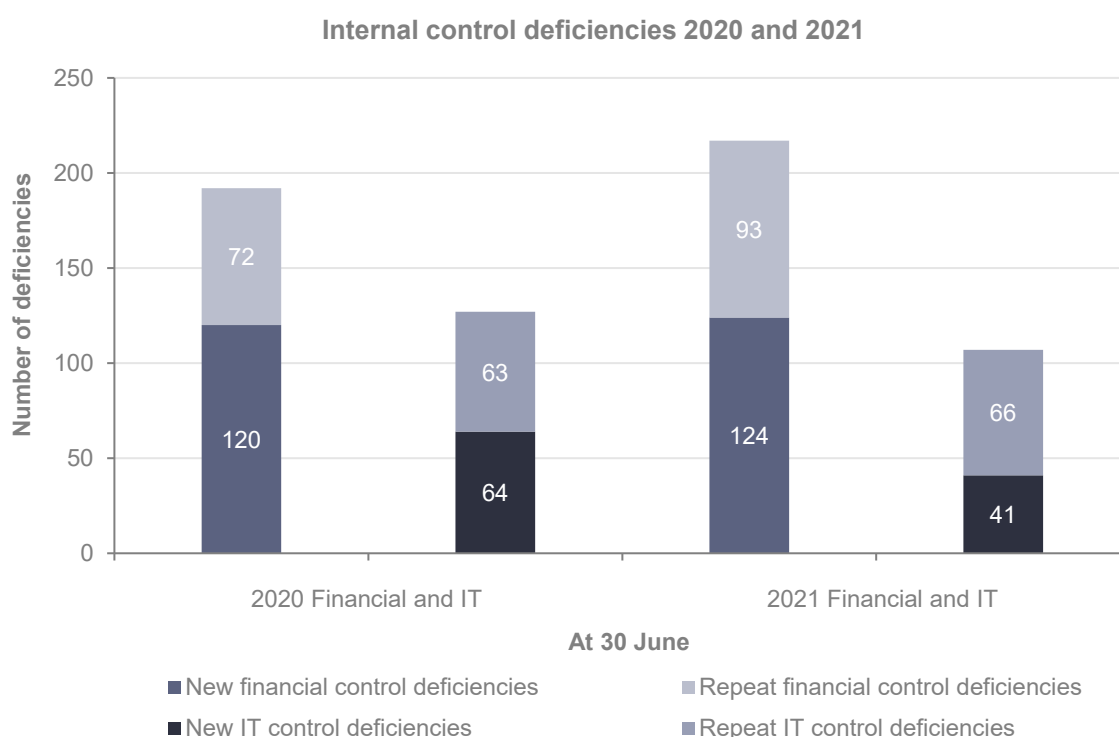
Our 2020–21 audits identified 324 internal control deficiencies, comprising:

- 217 financial related control deficiencies
- 107 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 increased by 1.6 per cent from last year

There were five more control deficiencies identified in 2021. The composition of the findings showed a 19 per cent decrease in IT findings versus a 13 per cent increase in financial control findings, and an overall 18 per cent increase in repeat findings across both categories.



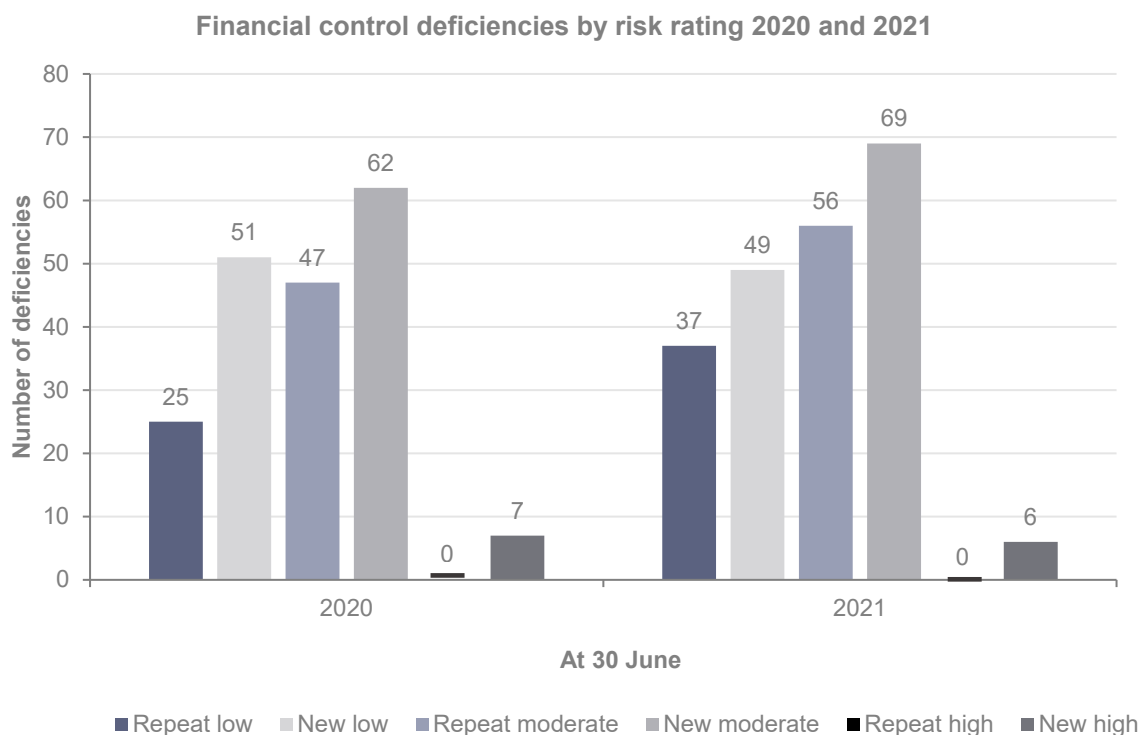
Source: Audit Office findings. 2020 numbers have been adjusted to exclude agencies not in scope of this year's report.

The number of financial control deficiencies increased by 13 per cent from last year

We found financial control deficiencies at 92 per cent of agencies (88 per cent in 2019–20).

While new financial control deficiencies increased by three per cent, repeat financial control deficiencies increased by 29 per cent from 2019–20. 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.



Source: Audit Office findings. 2020 numbers have been adjusted to exclude agencies not in scope of this year's report.

The number of IT control deficiencies decreased by 19 per cent from last year

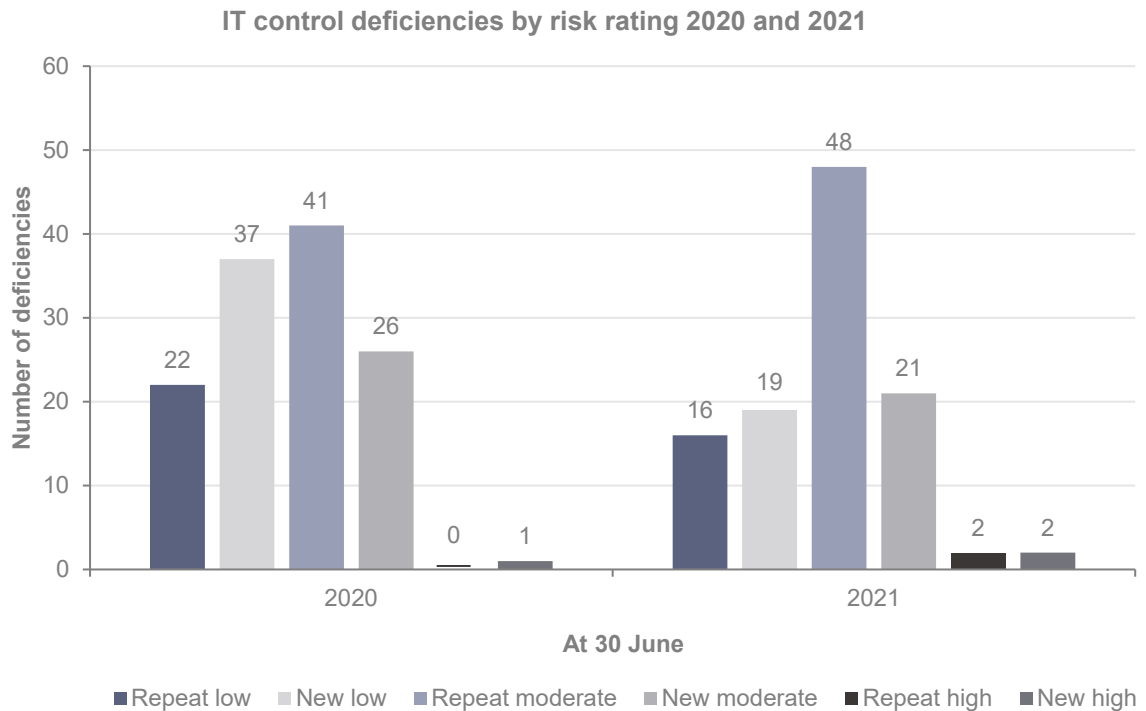
New IT control deficiencies decreased by 56 per cent and repeat IT control deficiencies increased by five per cent from 2019–20.

Repeat IT control deficiencies make up 62 per cent of the reported IT control deficiencies, indicating that a significant number of IT control deficiencies noted in previous years remain unresolved.

We found:

- 57 issues related to user access administration (60 per cent of agencies)
- 24 issues related to privileged users across (44 per cent of agencies)
- 21 issues related to third party arrangements (32 per cent of agencies)
- 17 issues related to password security (28 per cent of agencies)
- 16 issues related to change management (32 per cent of agencies)
- 13 issues related to disaster recovery plans (40 per cent of agencies)
- 11 issues related to policies and procedures (24 per cent of agencies)
- 6 issues related to business continuity plans (16 per cent of agencies)
- 4 issues related to patch management (16 per cent of agencies).

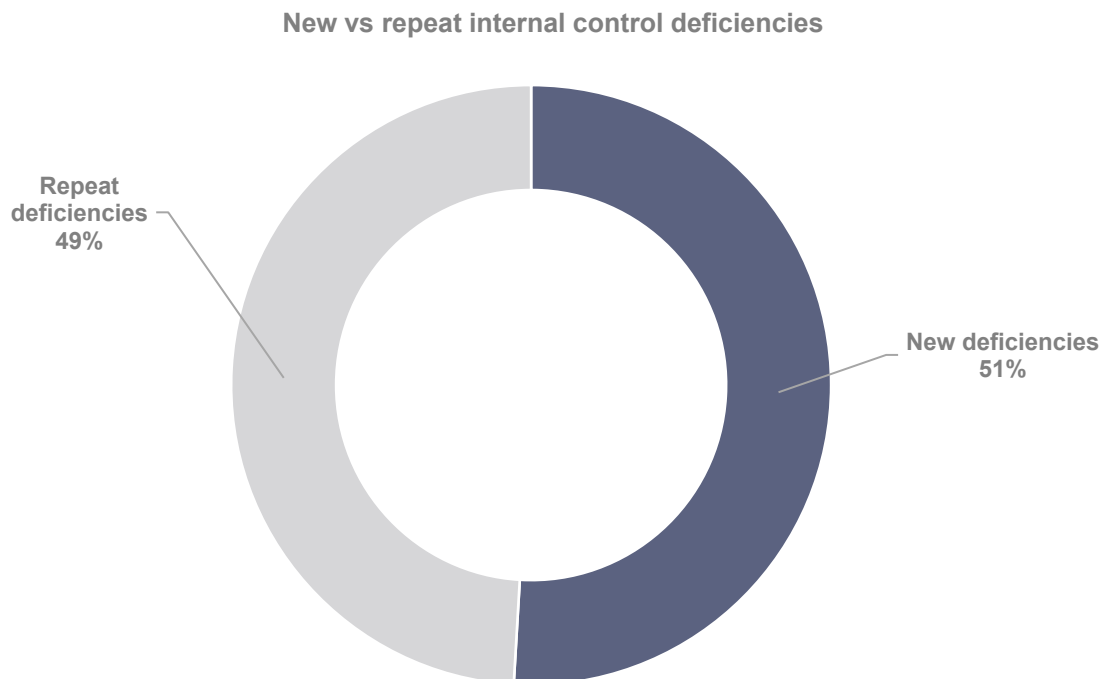
The graph below shows the risk rating of reported IT control deficiencies.



Source: Audit Office findings. 2020 numbers have been adjusted to exclude agencies not in scope of this year's report.

The proportion of repeat control deficiencies has increased from 2019–20

As a percentage of total internal control deficiencies, unresolved deficiencies from prior years now represent 49 per cent of all the internal control deficiencies identified (42 per cent in 2019–20).



Source: Audit Office findings.

We found at least nine per cent of repeat findings reported in 2021 had been repeated since 2018.

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

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.
- Agencies are increasingly contracting out key IT services to third parties, however, weaknesses in IT service providers' controls can expose an agency to cyber security risks.

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 (ITGCs) 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.

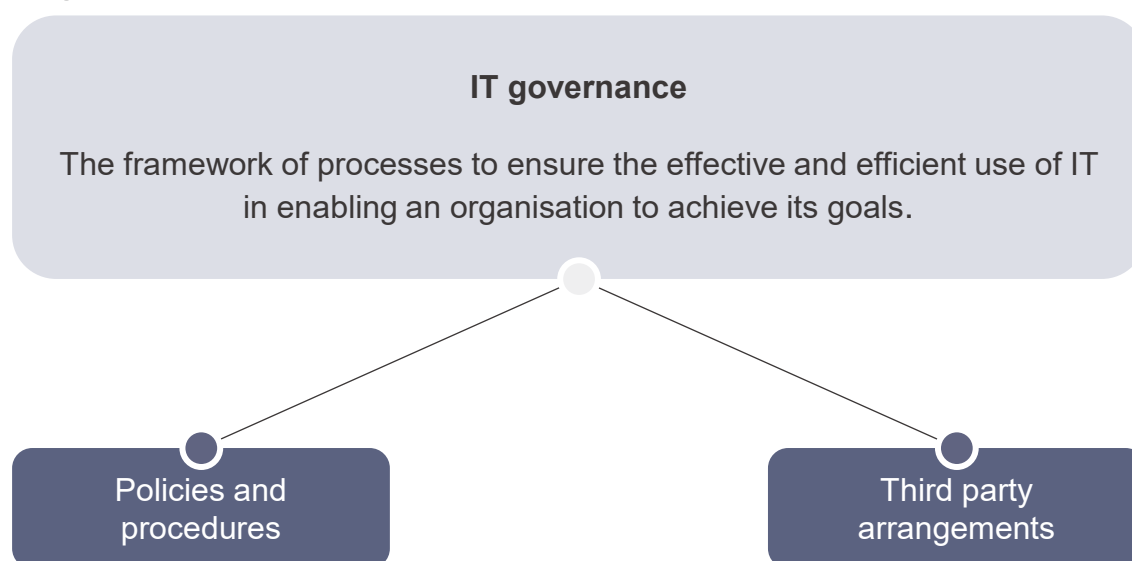
Poor IT controls increase agencies' vulnerability to the risk of:

- 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.

IT governance



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

We identified issues with 24 per cent of agencies' IT policies and procedures (48 per cent in 2019–20). 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.

Agencies can become exposed to cyber attacks via weaknesses in their outsourced/third party IT systems.

We identified issues at 32 per cent of agencies related to management of their IT service providers. The deficiencies related to:

- weaknesses in the third party IT service provider's backup procedures
- weaknesses in third party user IT service provider's access monitoring, timely removal of access, or privileged user audit log monitoring
- unencrypted storage devices used by third party IT service providers
- weakness in third party IT service provider's password controls
- lack of IT security policies and IT security monitoring at third party IT service providers
- lack of segregation of duties at third party IT service providers
- lack of adequate change management processes performed by third party IT service providers
- weaknesses in third party IT service provider's timely detection of cyber attacks
- 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 provider's controls assurance reports do not clearly show the agency's systems are covered by the report, or were qualified with significant issues in ITGC controls
- agency management not adequately reviewing or monitoring third party IT service provider's controls assurance reports
- agency management not completing the impact assessment of transition arrangements with third party IT service providers.

Risk

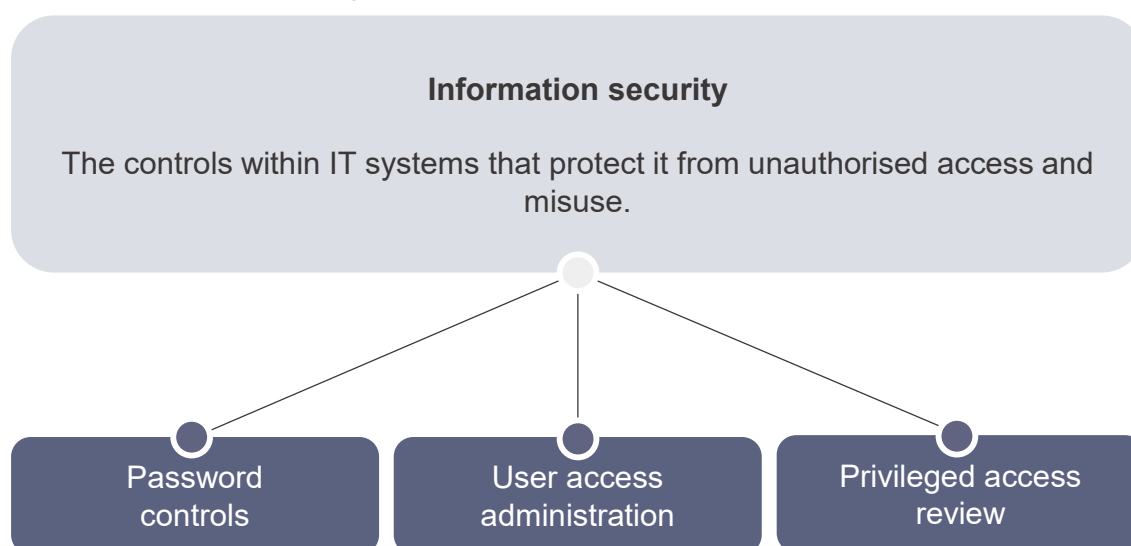
Appropriate management of third party service providers reduces the risk of:

- 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



Agencies are not complying with their own password policies

Twenty-eight per cent of agencies (32 per cent in 2019–20) 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 (i.e., the number of passwords remembered and restricting the recycling of recently used passwords)
- not applying minimum and maximum password age (i.e., prompting the change of passwords frequently)
- 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.

Most agencies have 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 60 per cent of agencies do not perform regular user access reviews (60 per cent in 2019–20) 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 to identify dormant user accounts, duplicate user accounts and default/generic accounts were not performed
- no 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
- 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 contribute to low maturity scores against the NSW Cyber Security Policy. 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.

Most 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 44 per cent of agencies do not periodically review the activities of privileged users to identify suspicious or unauthorised activities (40 per cent in 2019–20). 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 masterfile and manual journal responsibilities
- no segregation of duties in the privileged access review (i.e. 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.

People with privileged access may misuse that 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.

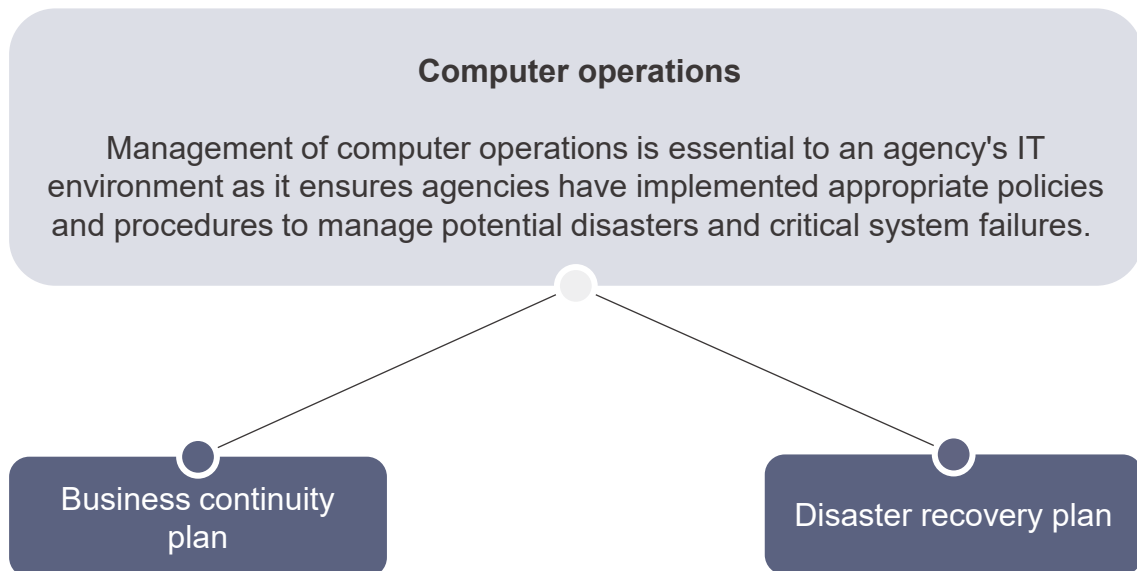
Poor management of privileged access may also lead to breaches of Section 3.6 of the *Government Sector Finance Act 2018* and the NSW Cyber Security Policy. This policy requires agencies to have appropriate security screening of users with privileged access rights, and remove access when it is no longer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

Poor cyber controls compound the risks associated with weaknesses in controls over privileged user accounts.

Agencies should:

- restrict privileged user access to only staff who 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



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.

We found deficiencies in disaster recovery processes at 40 per cent of agencies (48 per cent in 2019–20) and in business continuity processes at 16 per cent of agencies (28 per cent in 2019–20). 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

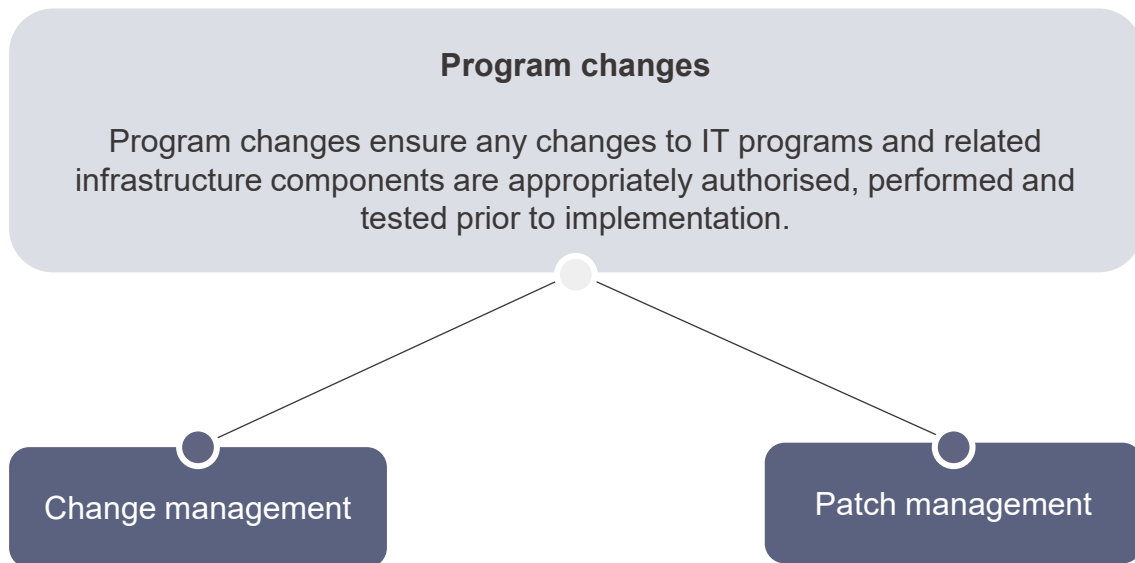
Without detailed analysis and planning for critical business functions and key IT systems and infrastructure, agencies cannot predict the impact of disruption, identify maximum tolerable outages, or plan informed recovery strategies. They also risk:

- 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



Change management: program changes should be reviewed and authorised, with 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 32 per cent of agencies (28 per cent in 2019–20). 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 develop and improve database and operating system patches are appropriately applied as required

A patch is additional code that updates vendor software products 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 in an information system.

We found deficiencies in patch management at 16 per cent of agencies. These deficiencies related to:

- patch management standards that had past their scheduled review date
- some systems had not been patched in the last six years
- 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
- no formal processes around exemption from patching and risk acceptance for unpatched systems.

Risk

As patching 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 8 controls.

Agencies should ensure:

- application, database and 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 planning and governance

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

Section highlights

- Agencies' self-assessed cyber maturity levels against the NSW Cyber Security Policy mandatory requirements are low and have not met their target levels. Forty per cent of agencies have not formally accepted the residual risk from gaps between their target and current maturity levels.
- Most agencies have conducted cyber awareness training to staff during 2020–21. Some have further enhanced this training through awareness exercises such as simulated phishing emails to test staff knowledge.
- Registers of security incidents and breaches are not consistent across agencies. Four agencies recorded nil breaches during 2020–21, however, their definition of incidents and breaches was not consistent with other agencies. For instance, they did not include account compromises or denial of service attacks. Only seven agencies' registers included details of actions taken to resolve issues.

4.1 Background

The Australian Cyber Security Centre (ACSC) was established in 2014 to lead the Australian Government's work to improve cyber security. ACSC is part of the Australian Signals Directorate within the Defence portfolio. The ACSC reports that:

the focus on cyber security is increasing for government agencies as the digital footprint of government expands. Risks have been further amplified by the COVID-19 pandemic as governments increasingly transact and deliver services to citizens through online platforms. Cyber attacks by criminals and state actors are becoming more sophisticated and complex and the attacks are more likely to be substantial in impact¹.

NSW Government agencies have recently experienced some well publicised cyber attacks, such as the global Accellion data breach which affected NSW Health and Transport for NSW in 2021. In July 2021, the Department of Education was impacted by a cyber attack that resulted in the agency deactivating internal systems to protect staff and student data.

¹ [ACSC Annual Cyber Threat Report 2020–21 | Cyber.gov.au](#)

In March 2020, Service NSW suffered two cyber security attacks in short succession. Technical analysis undertaken by the Department of Customer Service (DCS) concluded that these attacks resulted from a phishing exercise through which external threat actors gained access to the email accounts of 47 staff members. These attacks resulted in the breach of a large amount of personal customer information that was contained in these email accounts. The Auditor-General reported on the effectiveness of Service NSW's handling of personal information in In December 2020, finding that previously identified risks and recommended solutions had not been implemented on a timely basis². The Auditor-General has also reported on the effectiveness of how Transport for NSW and Sydney Trains manage their cyber risks detecting significant vulnerabilities in those agencies' most vital systems³.

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 25 mandatory requirements for agencies, including implementation of the ACSC Essential 8 Strategies to Mitigate Cyber Security Incidents (the Essential 8). The Essential 8 are key controls, which serve as a baseline set of protections for agencies to put in place to make it more difficult for adversaries to compromise a system. Agencies are required to self-assess their maturity against the CSP and the Essential 8, and report that assessment to Cyber Security NSW annually. A recently tabled report [Compliance with the NSW Cyber Security Policy](#) by the NSW Auditor-General focused on the poor levels of cyber maturity at nine key NSW agencies.

In this chapter of our report, we reviewed the governance structures agencies had in place to manage cyber security risks through:

- establishing appropriate roles and responsibilities
- assessing risks and the adequacy of controls to mitigate them
- training staff on cyber awareness
- handling of security incidents such as data breaches.

Implementation of the Essential 8 controls is not within the scope of this report.

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 March 2021.

Most agencies have implemented their own cyber security policy as required by the CSP. Some agencies rely on a central policy set by the principal department in the cluster. Two agencies' policies were not current at 30 June 2021. One was still in draft and the other has been overdue for review since 30 June 2020.

Reviewing policies on a timely basis helps agencies keep abreast of new developments, emerging vulnerabilities and best practice guidelines, particularly in an environment where threats can rapidly emerge such as in cyber security.

Most agencies have established roles and responsibilities for cyber security

As required by the CSP, agencies have defined and allocated roles and responsibilities in relation to cyber security. One agency was not compliant with the CSP as the agency head's accountability for cyber security was not established within their role description. While this oversight had been addressed in an updated policy, that policy remained in draft.

² [Service NSW's handling of personal information | Audit Office of New South Wales](#)

³ [Managing cyber risks | Audit Office of New South Wales \(nsw.gov.au\)](#)

All agencies have assigned a governance committee at the executive level that is accountable for cyber security. All are attended by the CISO/CIO or equivalent officer. Some agencies have a shared committee across the cluster, such as within the Transport, Stronger Communities, and Customer Service clusters. In these cases, the agencies have shared services and shared IT systems.

For 56 per cent of the agencies, a separate committee dedicated to cyber security has been established, which reports to a governance committee (usually the Board or Audit and Risk Committee) that meets at least quarterly. Three agencies do not have a formal charter for this separate committee. Without a defined charter, there may be less clarity over the committee's role and scope of oversight, and possible gaps in responsibility or duplication in the work performed by the governance committee to which it reports, or to other committees also overseeing risks aspects related to cyber security.

One agency, which assigns to its Audit and Risk Committee governance over cyber security, does not have cyber matters as a standing agenda item at each meeting, nor is it scheduled on a regular basis during the year. If cyber matters are only reviewed only on an ad hoc basis, there is a risk that insufficient attention is given to the risks, and emerging issues are not captured for consideration on a timely basis.

Most agencies have embedded cyber risks as part of their enterprise risks

One agency does not include cyber risks as part of its enterprise risk management assessment. Its enterprise risk register identifies a general IT risk for not effectively delivering services. Cyber risks are indirectly monitored through the agency's internal audit program. Lack of defined and articulated cyber risk management may limit an agency's consideration of those risks and the resultant mitigation strategies, and mean insufficient attention and resources are devoted to that area.

Cyber security plans

Agencies must prepare cyber security plans or strategies as required by the CSP, with consideration of the agency's cyber security threats, risks and vulnerabilities that impact the protection of the agency's information, information and communication technology (ICT) assets and services. These may include:

- a risk appetite statement
- specific programs or initiatives to mitigate and respond to cyber risks
- an approach or roadmap to uplifting the agency's cyber maturity
- identification of the agency's 'crown jewel' assets.

Most agencies have a current cyber security plan; but two agencies had plans that remained in draft at 30 June 2021. One agency did not have a plan at all.

Our review of the current cyber security plans identified the following gaps.

Element	Percentage of agencies that do not have this (%)
Plan identifies key cyber threats, vulnerabilities and risk events	4
Plan covers all IT systems used by the agency	12
Plan sets a risk appetite or target risk level that management has deemed acceptable	20

Source: Audit Office analysis.

The recently tabled report on [Compliance with the NSW Cyber Security Policy](#) by the NSW Auditor-General identified that there was no minimum standard to which agencies needed to aim for, or comply with. If an agency's governing body does not set risk tolerance against which management reports, it decreases their awareness of how risk is being managed. This in turn increases the risk that the current stance of the organisation is outside their risk appetite.

All agencies except one have specified in either their cyber security policy or plan how it applies to third party vendors, such as ICT service providers. However, even though the agency's policy encompasses third party vendors, 21 per cent of agencies do not require attestations or controls assurance reports from their ICT service providers to confirm achievement of any level of cyber maturity. This gap leaves agencies vulnerable. Being unaware of weaknesses in an ICT service provider's cyber security controls means agencies may respond slowly, or not at all to close vulnerabilities, which can be exploited by threat actors to gain access to the agency's systems, data and assets.

4.3 Managing cyber risks

Agencies must perform an annual assessment with regard to their compliance with the CSP's 20 mandatory requirements, which includes the Essential 8, by 31 August each year. Agencies must report their level of maturity for each requirement using the prescribed maturity model.

One agency received an extension to complete their 2020–21 maturity assessment, which they completed before the revised due date of 30 November 2021.

Maturity levels across the whole-of-government needs to be urgently improved

This year was the third time agencies have reported against the CSP's mandatory requirements and the Essential 8 mitigation strategies. The CSP outlines the mandatory requirements to which all NSW Government departments and public service agencies must adhere. It seeks to ensure cyber security risks to agencies' information and systems are appropriately managed.

Findings from our audit of nine key NSW agencies' [Compliance with the NSW Cyber Security Policy](#) included:

- the CSP did not specify a minimum level for agencies to achieve in implementing the mandatory requirements or the Essential 8
- the CSP did not require agencies to report their target levels, nor does it require risk acceptance decisions to be documented or formally endorsed
- agencies tended to over-assess their cyber security maturity - all nine participating agencies were unable to support all of their self-assessments with evidence
- there is no monitoring of the adequacy or accuracy of agencies' self-assessments.

Agencies' annual self-assessments of their maturity in implementing the requirements are not audited. The information below, which is based on those self assessments, is therefore also not audited.

Agencies assess their maturity in implementing the CSP requirements using a maturity rating on a scale of one to five. Detailed assessment criteria are provided in the CSP maturity model in relation to each requirement. The maturity model by which agencies measure their implementation of the core requirements uses the following broad 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, compliance requirements, etc.

The two tables below summarise the results across whole-of-government. 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 2021

1. Planning and governance

Agencies must implement cyber security planning and governance and report against the requirements outlined in the CSP and other cyber security measures. The 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 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	4	21	30	33	13	101
Cyber governance	8	16	20	50	8	102
Approved cyber plan	15	38	19	19	8	99
Cyber risk assessments	3	31	26	39	9	108
Service provider governance	8	53	29	15	4	109

Note: The total number of self-assessments for each requirement vary as 15 agencies included 'not applicable' ratings for at least one requirement. The 'not applicable' ratings were excluded from the table.

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

Number of self-assessments for 2021

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 cyber awareness and risk culture. Although cyber security education appears to be relatively well embedded, only level four and five maturity require that training is mandatory for all staff and ICT service providers. Maturity levels less than three only require that education is available to staff and ICT service providers.

CSP requirements	Maturity level one	Maturity level two	Maturity level three	Maturity level four	Maturity level five	Total
Cyber security education	2	32	52	6	5	97
Awareness and reporting of cyber security risk	5	56	26	6	6	99
Foster a culture of cyber risk management	3	39	26	34	8	110
Sensitive data access control	11	45	38	12	4	110
Cyber security threat sharing	2	20	27	33	16	98

Note: The total number of self-assessments for each requirement vary as 15 agencies included 'not applicable' ratings for at least one requirement. The 'not applicable' ratings were excluded from the table.

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

Number of self-assessments for 2021

3. Safeguarding information and systems

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 assuring the agency's crown jewels, tracking audit trails and activity logging, and commencing implementation of the Essential 8. We report the maturity of agencies in how advanced they are in implementing the Essential 8 in more detail in the section below.

CSP requirements	Maturity level one	Maturity level two	Maturity level three	Maturity level four	Maturity level five	Total
Appropriately assured ISMS to at least cover 'crown jewels'	25	36	31	9	1	102
Commence implementation of the ACSC Essential 8	15	40	34	8	4	101
Classify information and systems and adhere to labelling and handling guidelines	22	9	61	8	9	109
Build cyber security requirements into procurements	12	27	46	17	7	109
Ensure ICT system enhancements include audit trails and activity logging	38	38	21	6	4	107

Note: The total number of self-assessments for each requirement vary as 15 agencies included 'not applicable' ratings for at least one requirement. The 'not applicable' ratings were excluded from the table.

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

Number of self-assessments for 2021

4. Number of self-assessments for 2021

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 incident management process and the NSW Government Cyber Incident Response Plan, and testing those plans at least annually, involving senior business and IT executives, functional area co-ordinators, 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	7	46	18	14	17	102
Tested cyber incident response plan annually	21	42	18	18	1	100
Cyber monitoring tools to identify and respond to incidents	1	26	56	19	4	106
Report cyber incidents to Cyber Security NSW	5	8	39	48	3	103
Participation in whole-of-government exercises	14	8	29	41	4	96

Note: The total number of self-assessments for each requirement vary as 15 agencies included 'not applicable' ratings for at least one requirement. The 'not applicable' ratings were excluded from the table.

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

Maturity levels implementing the Essential 8 controls is of particular concern and need to be urgently implemented

The ACSC has defined 37 cyber security strategies, prioritising eight of these as a baseline for all organisations in mitigating cyber attacks. These eight highest priority strategies are called the 'Essential 8'. The table below reports the maturity levels of NSW Government agencies in implementing these essential cyber risk mitigation controls.

The CSP requires agencies to report maturity against the Essential 8 using a four-point scale. The broad definitions in the CSP for each maturity level effective at the reporting date were:

- 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.

Of significant concern are the large number of agencies that self-assessed at less than level two maturity, meaning their current maturity posture has notable gaps.

Number of self-assessments for 2021

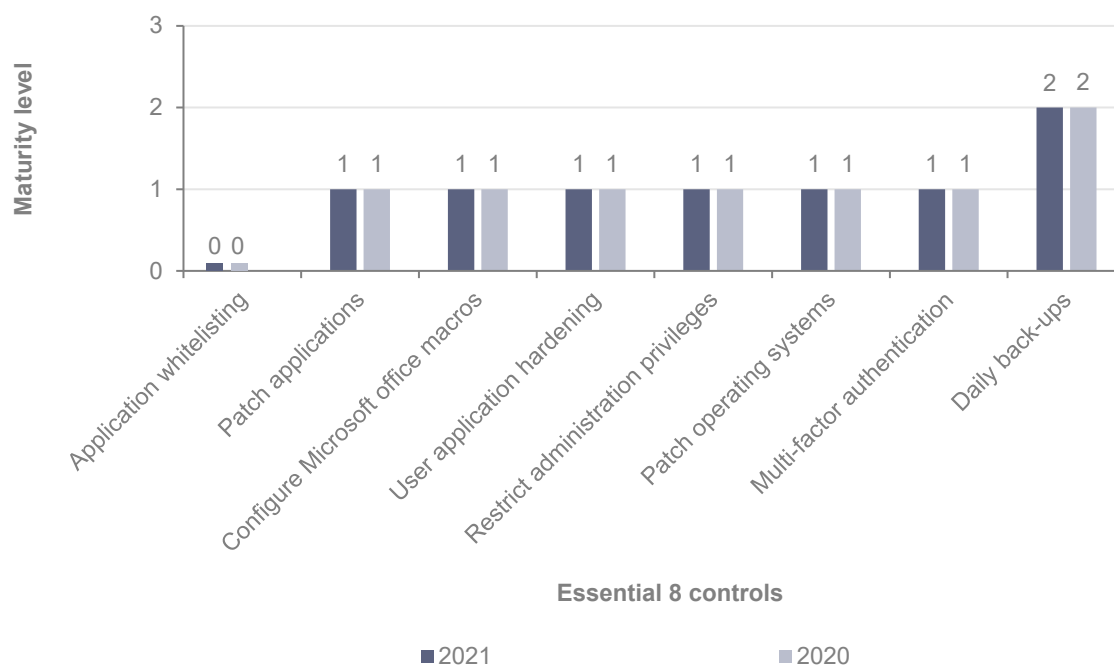
Essential 8 controls	Maturity level zero	Maturity level one	Maturity level two	Maturity level three	Total
Application whitelisting	76	12	11	7	106
Patch applications	36	32	28	10	106
Configure Microsoft office macros	32	49	15	8	104
User application hardening	41	31	22	11	105
Restrict administrator privileges	16	41	32	17	106
Patch operating systems	36	26	32	11	105
Multi-factor authentication	29	54	17	6	106
Daily back-ups	5	42	31	28	106

Note: The total number of self-assessments for each Essential 8 control vary as three agencies included 'not applicable' ratings for at least one requirement. The 'not applicable' ratings were excluded from the table.

Source: Individual self-assessed Essential 8 maturity returns (unaudited).

Of further concern are the median results for maturity implementing the Essential 8 controls in the current and previous years. The table below shows no improvement in agencies' implementation of the Essential 8 controls in the past year. 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.

Median maturity levels for Essential 8 controls



Source: Individual self-assessed Essential 8 maturity returns (unaudited).

Recommendation

As reported in 2020 Central Agencies and Compliance with the NSW Cyber Security Policy, agencies should 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
- report target levels of maturity for each mandatory requirement and Essential 8 control that they have determined is appropriate for the agency
- have processes whereby the agency head and those charged with governance formally accept the residual cyber risks.

Agencies are reviewing their self-assessed maturity levels

For 2020–21, over 80 per cent of agencies have engaged their internal audit division or contracted an independent review of their cyber maturity assessment to validate self-assessed ratings. In some cases, this has resulted in the 2021 maturity levels being revised lower than the level assessed in 2020. Most agencies aspire to achieve a rating of at least three for CSP requirements, with the exception of the Essential 8.

Installing new IT controls or upgrading systems to provide better protection may be complex and require funding, and is often cited as an impediment to achieving higher levels of maturity. Legacy systems can be an issue if they are no longer supported by the original vendor, particularly if the vendor is no longer releasing patching known vulnerabilities. However, progress on implementing these essential controls has been slow, and based on the target maturity levels agencies set for themselves, most aim only to achieve least level one within a two-year timeframe. As noted previously, a level one rating for the Essential 8 does not aim to protect against targeted attacks by cyber adversaries and level zero maturity indicates significant weaknesses.

Forty per cent of agencies have not formally accepted the residual risk where their current level of maturity does not meet the target level

Whilst agencies complete an annual attestation statement that they have managed cyber security risks in a manner consistent with the mandatory requirements set out in the CSP, maturity levels vary across agencies. While the current attestation does not require an explicit statement that the agency head or governance committee has accepted the residual risk represented by the gap between the target and actual maturity level, it does require that agencies have a plan to uplift their maturity continuously. Sixty per cent of agencies have assessed and accepted the residual risks in relation to risks associated with low maturity self-assessments, and the time scale in which they plan to address those risks.

Training and awareness

As part of the CSP requirement for agencies to build and support a cyber security culture, agencies must implement regular cyber security awareness training for all employees, contractors and outsourced ICT service providers. According to the agencies' self-assessments, 89 per cent of agencies make cyber awareness training available, but only 11 per cent of agencies make this training mandatory for all staff and contractors.

Cyber criminals aggressively target certain staff by sending fraudulent emails, stealing credentials and sending malicious attachments, which deploy because they entice people to interact with them. The most targeted staff are those in senior positions and finance roles. Completion of cyber awareness training by all staff, contractors and third party providers helps them recognise potentially malicious emails and avoid inadvertently activating attachments and software designed to infect devices and steal data to be used by cybercriminals.

Two agencies have not conducted cyber awareness training to staff

Processes at these two agencies are limited to cyber security awareness emails and optional self-learning modules. Opt-in training complies with the policy, but falls short of best practice to ensure all staff have undertaken training. Both of these agencies are developing plans to implement formal training and awareness programs in the next year.

For the remaining 23 agencies, in addition to all-staff training, some have provided:

- training to third parties with access to the organisation's systems, such as contractors, consultants, vendors and partners (68 per cent of agencies)
- targeted training to certain groups of employees who may be at greater risk of cyber attacks, such as procurement staff, payroll staff, executive and privileged users (47 per cent of agencies).

Some agencies have tested staff knowledge through awareness exercises

Fifty-six per cent of agencies have conducted awareness exercises in 2020–21 to test staff knowledge on responding to cyber threats, such as sending a simulated phishing email. Phishing involves cyber criminals sending fraudulent messages, which appear to come from a reputable source and trick the recipient into revealing sensitive or personal information. Agencies that do perform simulated phishing exercises find approximately three per cent of staff are unable to identify phishing emails.

Lack of awareness in staff means they are less likely to respond appropriately and compromise their agencies' cyber defences.

Security of agency information

Most agencies have defined sensitive information

Ninety-five per cent of agencies have defined sensitive information in the context of their operations and configured their system access controls accordingly.

Two agencies could improve their protocols for securing the exchange of sensitive information through secure online portals, minimising the use of email and eliminating the use of USB keys for the transfer of sensitive information. USB drives pose significant risks as they can be used to infect computers with malware once the drive is plugged in. They are also easily lost or stolen, causing a potential loss or misuse of data.

Security incidents registers lack consistency across agencies

All agencies maintain a register of security incidents or breaches. Fifty-two per cent of agencies reported nil data breaches in 2020–21. Superficially, this might seem an outstanding result, but given the ease and regularity with which these occur, the result is greeted with caution. We noted that four agencies' definition of a data breach does not include events such as account compromises or denial of service (DOS) attacks, even though there were recorded in the agencies' incident registers. Others do not record accidental breaches of personal information, which are also within the definition of a data breach⁴.

For other agencies, the number of data breaches recorded during the year ranged from one to 264. Data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a data controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

⁴ A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to an agency's data - [Data Breach Guidance for NSW Agencies](#).

We noted only seven registers recorded detailed actions taken in response to the breach, while other registers only recorded whether the issue was resolved or closed. An absence of detail about the nature of the breach makes it more difficult to perform root cause analysis on the incidents and reduce the risk of the issues recurring in future.

Agencies could improve the quality of their registers by including:

- date/time of incident
- date/time of actions to resolve the incident
- details of actions taken in response to the incident
- categories of the nature of the incident.

Agencies that retain personal information are subject to a range of legislative obligations. The *Privacy and Personal Information Protection Act 1998* (NSW) applies to NSW public sector organisations. While NSW Government agencies do not have a mandatory notifiable data breach reporting requirement, the NSW Privacy Commissioner has established a voluntary reporting scheme and is responsible for handling complaints by individuals who believe their privacy has been infringed.

NSW public sector agencies have obligations under the Notifiable Data Breaches scheme (established under the federal *Privacy Act 1988*) when a data breach occurs involving a Tax File Number (TFN). The collection, storage, use, disclosure, security and disposal of individuals' tax file numbers is regulated by the Privacy (Tax File Number) Rule 2015. This Rule requires organisations holding TFNs to implement reasonable security safeguards in the circumstances to protect the information.

5. Managing conflicts of interest

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

Section highlights

- Most agencies have established conflicts of interest policies consistent with the mandatory requirements of the Code of Ethics and Conduct for NSW Government sector employees. Agencies' policies could be strengthened to apply the standard they apply to senior executives to all employees and contractors. Currently, only senior employees are required to make annual declarations of interests, yet the ability to make or influence decisions is delegated to others in the organisation.
- Half of agencies' policies specify units or divisions that are at higher risk of conflicts of interest arising due to the nature of their business. Policies should identify additional measures at the unit/division level to mitigate these risks.
- On average, less than 75 per cent of staff completed annual declarations of interest where required. This could be improved with ongoing staff training and awareness, and follow up on incomplete conflicts of interest.

5.1 Background

All government sector employees are required to comply with the Ethical Framework as set out in the *Government Sector Employment Act 2013*, which outlines the core values for the government sector in acting ethically and in the public interest. The Public Service Commission established the Code of Ethics and Conduct for NSW Government sector employees (the Code). It includes mandatory requirements and best practice for conduct in accordance with the Ethical Framework.

The NSW Independent Commission Against Corruption's (ICAC) 2019 publication [Managing Conflicts of Interest in the NSW Public Sector](#) (ICAC Guide 2019) sets out ICAC's best practice guidance in relation to conflicts of interest.

Managing conflicts of interest is a critical component of demonstrating transparency and accountability for public servants to place the public interest over their personal interest. Good management of conflicts of interest is fundamental to ensuring public trust and confidence in the public sector. A conflict may arise when:

- there is a direct conflict between a person's current duties and responsibilities and their private interests (an 'actual' conflict of interests)
- a reasonable person might perceive that a person's private interests are likely to improperly influence the performance of their official duties, regardless of whether this is in fact the case (a 'reasonably perceived' conflict of interests)
- a person has a private interest that could conflict with their official duties in the future (a 'potential' conflict of interests).

In this chapter, we have focused on whether agencies have:

- implemented appropriate policies and procedures governing conflicts of interest
- maintained up-to-date and comprehensive registers of declared interests
- established monitoring and review processes to ensure that conflicts are addressed in accordance with the agency's policies.

5.2 Policy framework

Not all agencies' conflicts of interest policies are current

All agencies have established conflicts of interest policies that are applicable to all employees, regardless of level, and are readily accessible. However, 24 per cent of agencies' policies were not current. Three agencies' policies were within one year of their scheduled review date, one agency was within two years, and three agencies had not reviewed their conflicts of interest policy in over three years. Without regular review, agencies' policies may not reflect significant changes to government policy, legislation, agency structure and reporting lines or business practices.

Policies do not always define the types of conflicts of interest clearly

We identified a lack of clarity within the conflicts of interest policies:

- 8 per cent of agencies did not define 'actual' conflicts of interest
- 12 per cent of agencies did not define 'perceived' or 'potential' conflicts of interest.

It is important to define the types of conflicts of interest to ensure they are understood, declared and managed appropriately.

Twelve per cent of agencies' policies did not outline and explain all the personal interest categories that may trigger a conflict of interest or provide examples. These categories include:

- people who are close contacts (more than personal acquaintances)
- connections to people who have provided, or may provide income
- connections to people and entities who have given benefits or favours.

Over four per cent of agencies' policies do not include all mandatory requirements

The Code specifies mandatory requirements for senior executives with regard to declaring conflicts of interest in section 3.5. The table below details the proportion of agencies that have not mandated these requirements within their policies.

Requirement	Percentage of agencies that do not have this (%)
Senior executives must make a written declaration of private financial, business, personal or other interests on relationships that could result in conflict of interest or perceived conflict of interest	4
Senior executives must make annual declarations	12
Fresh declarations be made as soon as practicable, following a change in a senior executive's private interests	12
Fresh declarations be made as soon as practicable, following a senior executive's assignment to a new role or responsibilities	12
Submission of 'nil returns' if senior executives do not have any conflicts of interest to declare	16

Source: Audit Office analysis.

Agencies' declarations of interest could be expanded to apply to more employees

Although there is no requirement in the Code for all employees to declare private interests that could result in actual, perceived or potential conflict of interest, the majority of agencies have included this in their own policies. However, fewer agencies have extended the full suite of expressly stated requirements beyond their senior executives.

Agencies' policies could be strengthened to apply the same standard of requirements of senior executives to all employees and contractors.

Requirement	Percentage of agencies that do not have this (%)
All employees must make a written declaration of private financial, business, personal or other interests on relationships that could result in conflict of interest or perceived conflict of interest	20
All employees must make annual declarations	40
Fresh declarations, as soon as practicable, following a change in the individual's private interests	24
Fresh declarations, as soon as practicable, following the individual's assignment to a new role or responsibilities	28
Submission of 'nil returns' from all employees if they do not have any conflicts of interest to declare	48

Source: Audit Office analysis.

Agencies' conflicts of interest policies could be improved

Although all agencies have established policies, the level of detail and extent of requirements in each vary. The ICAC Guide 2019 states that agencies should have a conflicts of interest policy that clearly explains the principles and procedures for identifying, disclosing, managing and monitoring a conflict of interest. Key elements of a robust policy were lacking in some agencies, as set out in the table below.

Element	Percentage of agencies that do not have this (%)
Clearly articulating roles and responsibilities:	
• Policy outlines employee's obligations to declare all conflicts of interest as they arise promptly to a manager or the relevant authority	4
• Policy outlines employee's obligations to declare all changes in conflicts of interest promptly to a manager or the relevant authority	12
Defining activities to manage conflicts of interest:	
• Policy specifies recording senior executives' declarations in a 'register of personal interests'	32
• Policy specifies recording all employees' declarations in a 'register of conflicts of interest'	16
• Policy specifies conflict of interest management options and requirement to document and approve a management response plan	12
• Policy specifies actions if there is a breach of the policy	12

Element	Percentage of agencies that do not have this (%)
Outlining potential actions to manage declared conflicts:	
• Policy outlines potential actions that could be taken to manage the conflict of interests declared	16
• Where policy outlines potential actions for managing conflicts, it includes:	
– restricting staff involvement in matters where they have an actual, perceived, or potential conflict of interest	16
– removing staff from involvement in matters where they have an actual, perceived, or potential conflict of interest	16
– monitoring the perceived or potential conflict of interest if it continues and has no substantial impact which requires any action	16
– enlisting an independent third party who does not have an interest to advise on or participate in the matter	52
– staff relinquishing assets, membership, or other private interests to remove the actual, perceived, or potential conflict of interest	48
– resignation of staff (in rare circumstances)	40

Source: Audit Office analysis.

Conflicts of interest policies should clearly articulate the roles and responsibilities of employees to declare conflicts as soon as possible, as well as changes to conflicts of interest, so that appropriate action may be taken in a timely manner to address them.

The ICAC Guide 2019 states that one way of ensuring that conflict of interest policies have operational or practical effect is to incorporate them into employment contracts or contractual terms of engagement.

Activities to manage conflicts of interest should be defined so that they are consistently applied. A register of declared interests is a common tool for keeping track of declarations and conflicts. It also records the person(s) assigned responsibility for assessing and approving an appropriate response plan. In addition to having response plans, providing examples of potential actions to manage conflicts helps to provide standard options for staff to follow.

If a policy does not outline actions for managing conflicts, or actions in the event of a breach of policy, there is a greater risk of inconsistent application and measures taken to enforce the policy.

Half of agencies' policies specify units or divisions that are at higher risk of conflicts of interest arising

For some agencies, depending on the nature of their business, certain units or divisions are at higher risk of conflicts of interest arising. As detailed in the ICAC Guide 2019 these may include functions such as:

- procurement and tendering
- contract management
- human resources/recruitment
- grants administration
- issuing fines and penalties.

Forty-eight per cent of the agencies have identified such areas of higher risk. The ICAC Guide 2019 states that for high-risk units and branches, the best practice is to consider additional controls that go beyond the agency's standard policy requirements.

These include:

- providing additional, regular training and awareness-raising sessions (for example, probity training in the lead up to a major tender)
- providing additional written instructions, standard operating procedures, checklists and sign-offs
- modifying existing financial delegations
- providing additional information to parties affected by a matter, such as published reasons for the decision or making the decision in a public setting
- randomly allocating matters to staff, or preventing staff from self-selecting the tasks they work on
- enhancing recordkeeping requirements
- ensuring that electronic audit logs are used and monitored
- taking steps to restrict access to confidential information
- implementing additional segregation of duties and supervision
- adopting stricter gift and hospitality procedures for high-risk situations
- using data analytics and review to identify red flags.

Policies should identify additional measures at the unit/division level to mitigate the higher risks.

Half of agencies' policies do not require declarations of conflicts of interest for specific, higher risk processes

Forty-eight per cent of agencies have conflicts of interest policies that require declarations for specific processes, such as prior to tender evaluation decisions or at committee meetings. Incorporating these declarations as standing agenda items helps to ensure completeness of declarations and reduce the risk of omissions.

Not all policies specify conflict of interest requirements for outsourced internal audit providers

Seventy-six per cent of agencies outsource their internal audit function to an external service provider. Half of these agencies do not have a policy that governs, precludes or limits the services the external audit provider might perform, such as consulting or advisory services. This may create self-review threats if the consultancy relates to a current or future audit, or the quantum of the fees for the additional services gives rise to an actual or perceived lack of objectivity or independence on the part of the service provider.

We noted that 48 per cent of the agencies using outsourced internal audit providers have processes to assess potential conflicts of interest even though not required by the policy. These include processes to assess conflicts, or provisions within the internal audit charter requiring the committee to seek representation from the internal auditor to disclose possible conflicts. Not all agencies have an express requirement for prior approval of other services after considering possible conflicts.

Ten agencies engaged their internal audit provider to perform unrelated services during the year ended 30 June 2021. Other services provided by internal auditors at seven agencies exceeded the internal audit fees for the year. At three agencies, the amount of other services provided was greater than \$6.7 million (highest was \$9.5 million) and exceeded the internal audit fee by at least 6.9 times (highest was 11.2 times). The type of services included providing accounting advice, consulting advice on strategy and business cases, analytical reporting, valuations, and project implementation reviews. Even if the nature of the services provided did not pose a conflict, the quantum of the fees in relation to the internal audit should have been of sufficient concern to require justification.

5.3 Declarations of interest

Agencies have not applied the requirements in their own policies governing declarations of interest

Eighty-eight per cent of agencies' policies require senior executives to make annual written declarations in relation to their personal interests, but only 77 per cent of them had done so for the year ended 30 June 2021.

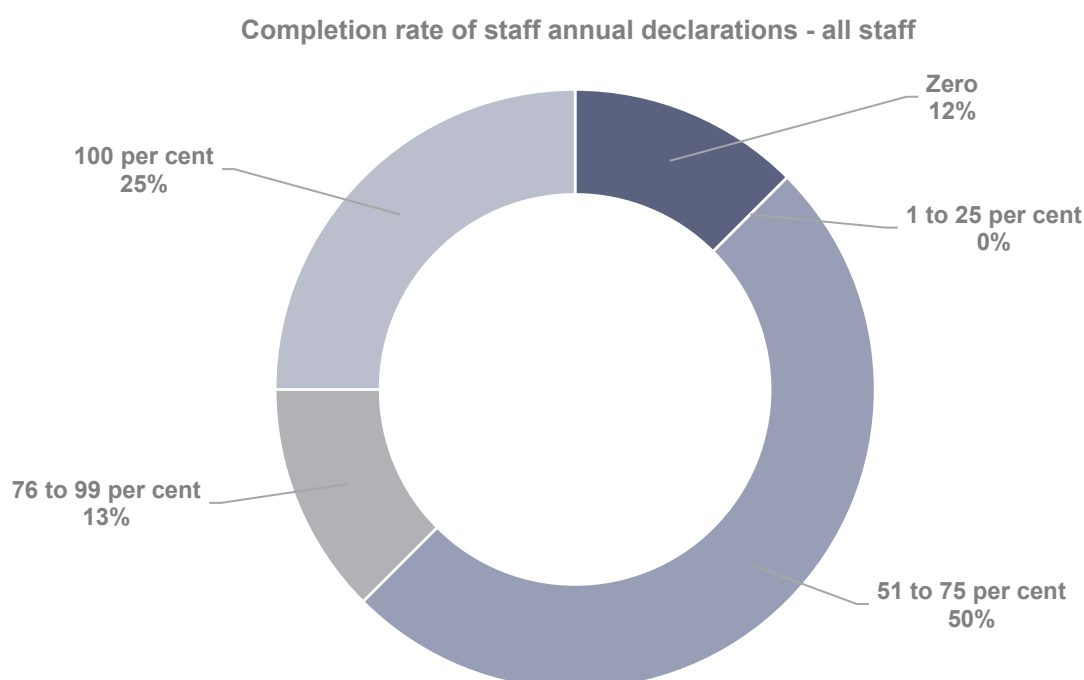
Sixty per cent of agencies state in their policies that all employees are required to make annual written declarations in relation to their personal interests. Only 53 per cent of those agencies had conducted an annual process for the year ended 30 June 2021.

On average, completion rates of staff annual declarations of interest are less than 75 per cent

The completion rate of staff submitting annual declarations when required to do so for the year ended 30 June 2021 ranged from zero to 100 per cent with an average of 73 per cent.

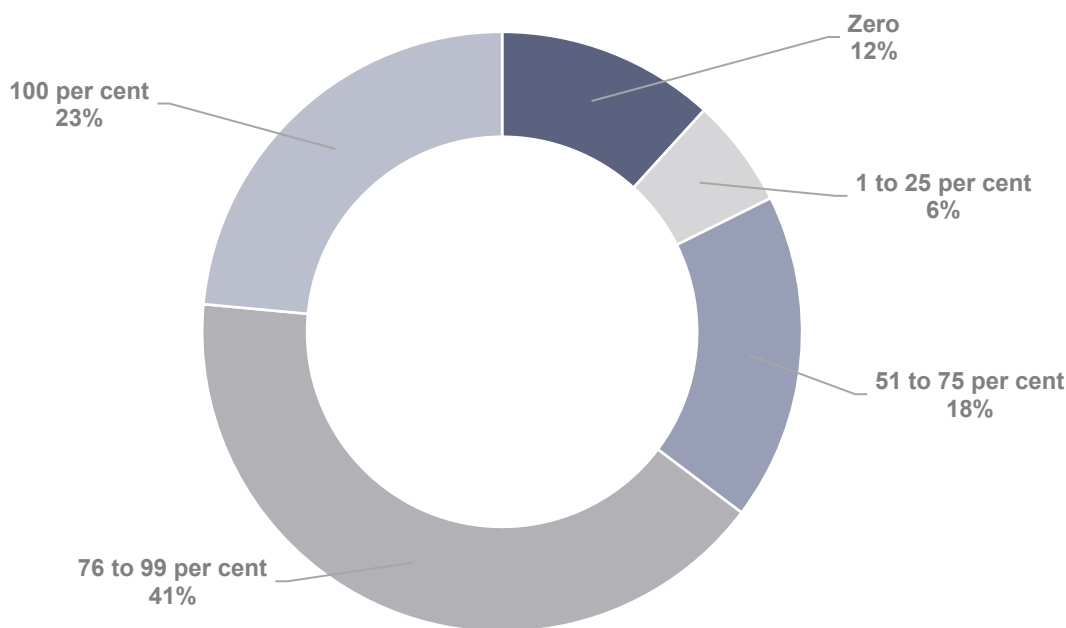
Thirty-two per cent of agencies required annual declarations from all staff. The average completion rates recorded at these agencies was 71 per cent. Sixty-eight per cent of agencies required annual declarations from senior executives only and recorded an average completion rate of 74 per cent.

The two graphs below show the range of completion rates for staff submitting an annual declaration of interest.



Source: Audit Office analysis.

Completion rate of staff annual declarations - senior executives only



Source: Audit Office analysis.

Some agencies' standard declaration forms do not capture key information

All agencies use a standard personal/conflict of interest declaration form for senior executives making a declaration. However, the design of the forms does not contain all the key fields suggested by the minimum standards, as set out in the table below.

Element	Percentage of agencies that do not have this (%)
Form includes management plan to address the conflict of interest	36
Form requires sign-off by the staff member making the declaration that it is true and correct	8
Form requires sign-off by the manager, governance or corruption prevention officer on the risk assessment and management plan	28

Source: Audit Office analysis.

Missing fields mean that not all pertinent information is captured, recorded in the register, and authorised. As shown in the table above, five agencies do not require a reviewer sign-off on the conflicts of interest declarations. This also makes it difficult to determine whether decisions regarding the treatment of each conflict of interest were appropriate in the circumstances and consistently applied.

Gaps in information diminish the usefulness of reporting to agency executive teams and/or governance committees on trends in conflicts of interest. It also reduces the transparency of agency reporting where agencies elect to make this information public, such as in financial statement disclosures on related parties⁵.

⁵ Australian Accounting Standard 'AASB 124 Related Party Disclosures'.

5.4 Registers of interests

Eighty-four per cent of agencies maintain a register of interests for all staff, while the remainder only maintain a register for senior executives' declared interests.

Some agencies' registers do not capture key information

The level of detail in registers of interests vary widely across agencies, and not all registers include the key fields suggested by the minimum standards, as set out in the table below.

Element	Percentage of agencies that do not have this (%)
Estimated value of the personal interest held	76
Description of the personal interest held	16
Details of the related person or organisation causing the conflict of interest	32
Assessment of the risk of conflict of interest	52
Management plan details	28
Approval by manager or supervising officer	16

Source: Audit Office analysis.

Missing fields means that not all pertinent information is captured, recorded in the register, and authorised. We further identified five agencies' registers were incomplete due to missing information in certain sections. This indicated the registers were not reviewed.

At 24 per cent of agencies, there is no formal requirement to update the registers immediately or in a timely manner following a new declaration. This increases the risk that decision-making by management does not take into account all potential conflicts nor exclude people with conflicts from making relevant decisions.

Two of the agencies that do not review the register of interests to ensure consistency with the policy mitigate the risk by requiring staff to make another conflict declaration prior to each major activity.

All agencies have security measures to protect the registers

As registers of interests contain sensitive personal information, it is important for agencies to ensure that the data is protected and only accessed or modified by authorised officers. Methods vary across agencies, however:

- 16 per cent use password protections only
- 32 per cent restrict access to relevant officers tasked with updating the register
- 52 per cent of agencies utilise both password protections and access restrictions to secure the register.

Eight per cent of agencies do not review the register of interests

Two agencies do not have a designated senior manager review the register of interests to ensure consistency with the conflicts of interest policy. The remaining agencies perform a review of the register at least annually, with over half performing the review at least quarterly.

Secondary employment

Secondary employment refers to any external employment or work activity that is in addition to an employee's position with the agency. It may include voluntary work or, work that the employee conducts while on leave. Secondary employment may pose risks to agencies if that employment conflicts with the business or interests of the agency. Secondary employment can also contribute to fatigue where the secondary employment consumes a substantial portion of the employee's time.

One agency does not require staff to declare secondary employment

Of the remaining agencies, 71 per cent use a standard form specific for secondary employment (including voluntary work) while the other 29 per cent use the same form for general conflicts of interest. A separate form allows for more relevant information to be captured and compared like-for-like in a separate register or database to ensure similar conflicts are handled consistently. Secondary employment creates a unique conflict for agencies. The agency has the right to determine that secondary employment is inconsistent with an employee's responsibilities. Many other conflicts of interest are unavoidable (such as related party and family associations) but nonetheless, the risks need to be mitigated.

Approval requirements of secondary employment vary across agencies

While all agencies require approval for a staff member's secondary employment, for one agency only certain types of secondary employment warrant approval. The delegation to approve secondary employment also differs:

- 4 per cent of agencies require approval by Human Resources
- 76 per cent of agencies require approval by a director level or above
- 20 per cent of agencies only require approval by the line manager.

It is important for senior executives to be aware of and authorise cases of secondary employment as they have a broader view of the agency's operations and may identify potential conflicts that a line manager would not. It also helps ensure that incidents are treated consistently across the organisation. Oversight by the Human Resources department also ensures that decisions comply with employment legislation, the terms of employment awards and contracts and other legislative and employee welfare considerations.

Forty-four per cent of agencies do not maintain a register of secondary employment

Of the remaining agencies that maintain a central register:

- 28 per cent do not include details of risk assessment
- 8 per cent do not include secondary employer (including name and role)
- 24 per cent do not include actions by management
- 16 per cent do not include approval of actions.

A third of agencies do not review the secondary employment register

Thirty-two per cent of agencies do not have a designated senior manager review the secondary employment register to ensure consistency with the secondary employment policy. The remaining agencies perform a review of the register at least annually, with over half performing the review at least quarterly.

Reporting processes

Agencies should regularly report on their register of interests and/or trends in conflicts of interest to a governance committee

Forty-four per cent of agencies do not report on their register of interests or trends in conflicts of interest to a governance committee. Of the remaining agencies that do, their reports are performed at least annually and included:

- any real or perceived conflicts of interest that have arisen during the period
- comparison of declarations from prior periods or by business unit
- statistics on completion rates of declarations
- risk ratings of conflicts.

Periodic review of the number, nature, and trends in conflicts of interests helps agencies support an ethical culture by:

- highlighting potential compliance issues or conflicts of interest and ensuring safeguards are appropriately and consistently applied to address such issues
- identifying, through trend analysis, where targeted activities are required, such as training and awareness programs
- providing assurance that actions taken in relation to conflicts of interest have been dealt with consistently and in compliance with agency policy.

Reporting and monitoring of this nature also helps reinforce to staff the importance of complying with the agency's conflict of interest policy.

Twenty per cent of agencies performed data matching exercises to identify any undisclosed conflicts of interest

Data matching exercises to identify potentially undisclosed conflicts of interest include comparing bank account details between the supplier masterfile and employee masterfile.

The ICAC Guide 2019 encourages agencies to be proactive in implementing measures to identify undisclosed (intentionally or unintentionally) conflicts of interest. The measures include a data analytics program that can identify suspicious transactions, red flags, events or relationships that may be associated with a conflict of interest especially in the case of high risk units detailed above on page 42.

Of the few agencies that performed data matching procedures, the most recent was performed on a monthly basis and the oldest had not been performed within two years.

Actions taken in the event of an undisclosed conflict of interest being identified included:

- referral to a governance division for investigation
- further reporting to governance committees
- decision made on the undisclosed interest.

Forty per cent of agencies' internal audit programs included a review of conflicts of interest

Forty per cent of agencies' internal audit programs included a review of conflicts of interest in the current financial year. They involved review of the conflicts of interest register and reporting to a governance committee.

The ICAC Guide 2019 states an agency's conflict of interest framework should be evaluated or audited from time to time, including testing:

- the completeness and accuracy of disclosures and registers
- whether documented management responses have been properly implemented
- whether cultures and systems are vigilant in detecting and addressing non-disclosure, such as internal audit function that has regard for suspicious transactions
- whether both employees and other relevant people and entities interacting with the agency are covered
- training and awareness.

5.5 Training and awareness

Agencies could improve their staff training and awareness on conflicts of interest

Twenty-eight per cent of agencies do not provide ongoing training on conflicts of interest to all employees. Three agencies do not provide new starters with the conflicts of interest policy on induction.

The ICAC Guide 2019 states it is important that there are clear requirements for conflicts of interest for all relevant groups of people including staff and contractors. The training should be tailored to target areas of greatest risk, clearly explain the key issues and the importance of properly dealing with conflicts of interest.

The results show that agencies could do more in providing ongoing training and support to employees. Ongoing training and awareness programs allow agencies to communicate to all staff their responsibilities and obligations in relation to conflict of interest situations. It also demonstrates the agency's commitment to maintaining an ethical environment which reduces the risk of inappropriate conduct by employees.

At a minimum, we recommend agencies remind staff of their obligations, manage conflicts of interest at least annually and integrate formal training into existing cyclical training or development activities, processes and in the agencies' culture (such as team meetings). The minimum standards also specify that the nature and type of awareness or training program should take into account the risk and likelihood of a conflict of interest based on the employee's role. Targeted training is ideal for those in high risk units/branches such as procurement.

Agencies could prioritise their focus on managing higher risk units and branches

Twenty-four per cent of agencies do not perform specific actions to manage higher risk units and branches, such as those responsible for procurement, recruitment, issuing fines and penalties, or rewarding grants or licences.

Specific actions taken by agencies include:

- targeted training, including training from ICAC
- mandatory declarations of interest to be provided before joining unit/committee
- regular review of fraud and corruption controls in place for the high-risk unit
- regularly seeking advice from legal and finance units
- robust policies in place for the high-risk units
- regular internal audits performed on high-risk units
- segregation of duties processes in place
- regular discussion of conflict of interest obligations as part of team meetings
- engagement of professional advisors (such as probity advisors) and committee review of transactions.

6. Masterfile management

This chapter outlines our audit observations, conclusions and recommendations arising from our review of agency's management of supplier and employee masterfiles.

Section highlights

- Most agencies have established policies or procedures on supplier masterfile management, however, only 56 per cent do for employee masterfile management.
- Less than half of agencies review user access rights to supplier or employee masterfiles which contain sensitive information and are susceptible to fraud. Access to edit the masterfiles should be limited to authorised personnel for whom it is required to perform their duties.

6.1 Background

Public sector agencies make significant payments through their accounts payable and payroll systems. These systems rely on the accuracy of information in masterfiles, which record key information about employees and suppliers, such as names addresses, bank account details, tax file numbers, Australian Business Numbers and other data, much of it sensitive in nature. Completeness and accuracy of masterfiles is essential to ensure only valid payments are made by agencies.

Strong internal control frameworks are required to manage supplier and employee masterfiles reduce the risk of error, misappropriation of cash misuse, or loss or theft of sensitive data. A limited number of employees will have the authority to make and approve changes to these files.

This section will focus on whether agencies have:

- established policies and procedures on masterfile management
- designed appropriate review of masterfile changes
- ensured masterfiles are secure.

In the conduct of our annual financial audits, the Audit Office regularly makes recommendations to management and those charged with governance to address internal control weaknesses for supplier and employee masterfiles. Common internal control deficiencies for masterfiles include:

- lack of or inadequate review of masterfile changes
- lack of segregation of duties that allow unauthorised changes to masterfiles.

Poor supplier masterfile management can lead to:

- supplier payments made to incorrect bank accounts
- duplicate supplier masterfiles can provide an opportunity for fraudulent activities.

Weak internal controls for employee masterfile management can lead to:

- employee payments made to incorrect bank accounts
- unauthorised users able to create new employees for fraudulent activities
- unauthorised users able to change pay rates or allowances
- payroll staff able to change their own payroll masterfile data.

Agencies with weak internal controls for supplier and payroll masterfiles, will often use exception reporting as a manual detective control procedure. However, employees that have access to generate these exception reports can also change or amend the parameters of the reports. The same employees that can amend masterfiles are also reviewing the exception reports.

Two agencies are heavily reliant on masterfile management systems from other departments due to the Machinery of Government changes in 2019–20. A number of agencies outsource masterfile management to GovConnect, an external service provider. However, even where another agency or outside service provider is engaged to perform this work, the originating agency remains responsible for the security of the service, and the accuracy and completeness of the masterfile information.

6.2 Policy framework

Eighty per cent of agencies have a policy on supplier masterfile management

Whilst 80 per cent of agencies have a policy on supplier masterfile management, 35 per cent of them are outdated. Thirty-two per cent of agencies outsource the supplier masterfile management process to GovConnect.

Some policies could be improved by including requirements to:

- validate changes to supplier details directly with a designated supplier contact
- record the reason for an amendment to masterfile records
- review the masterfile periodically to ensure compliance, validity and completeness of the records, such as removing duplicate suppliers or suppliers that have not been utilised in the past two years
- a naming convention applied to supplier records to avoid duplication of supplier names.

Agencies are exposed to phishing cyber attacks where cyber criminals impersonate others and intercept emails and communications for financial gain. Increasing numbers of transactions are processed daily, which are based on the data in master files. It is therefore important that controls around changes to masterfile data are robust.

Fifty six per cent of agencies have a policy on employee masterfile management

Only 56 per cent of agencies have a documented policy. Three agencies' policies are not current, one of which is an outdated manual from the 1990s.

The scope of agencies' policies is not as comprehensive as it could be. Agencies could improve their policies by including the elements as set out in the table below.

Elements of an employee masterfile policy	Percentage of agencies that do not have this (%)
Independent review of employee records created or amended	46
Reason for the amendment is recorded	77
Evidence is retained to support record creation or amendment	54
Periodic review (at least annually) of the employee masterfiles	69

Source: Audit Office analysis.

These policy requirements enhance internal controls over payroll processes so that:

- new records or amendments of records are checked for validity and accuracy by an independent officer
- appropriate reasons are documented for amendment to masterfile records
- documentary evidence is retained to support the creation and amendment of masterfile records
- periodic review of the masterfiles ensure compliance, validity and completeness of records.

Lack of documented policies on managing employee masterfiles may increase the risk of inappropriate or unauthorised changes to payroll data through fraud or error. There may be inconsistent practices across the organisation without a policy to ensure compliance with a standard set of requirements.

6.3 Review of masterfiles

Only 48 per cent of agencies review user access rights to supplier masterfiles

As supplier masterfiles are integral to agencies' procurement processes, they are susceptible to fraud. Access to edit the masterfiles should be limited to authorised personnel who require the access to perform their duties. Eleven agencies perform a review of user access rights to edit supplier masterfiles at least once a year. Of those agencies, three engage an external service provider to manage supplier masterfiles. These agencies review a controls assurance report from the service provider each year.

Two agencies did not have appropriate segregation of duties. The same employees established and amended masterfiles and also approved payments to suppliers. This increases the risk of fraudulent activity going undetected.

Thirty-two per cent of agencies review user access rights to employee masterfiles

Regular review of access rights ensures that staff who are authorised to view and edit sensitive personal information are limited to those where access is necessary. Only eight agencies review user access rights to edit employee masterfiles, including creating a payroll masterfile and making amendments. However, the timing of these reviews is not consistent and ranges from weekly to annually.

Twenty-eight per cent of agencies engage an external service provider to manage employee masterfiles. All agencies receive an ASAE 3402 Assurance Report on Controls at a Service Organisation. This report evaluates if the controls at the service provider are operating effectively. The service provider received a qualified opinion on information technology general controls (ITGC) as key controls over user access, system changes and batch process failed in all ITGC reports. Most of these deviations were not mitigated or sufficiently mitigated to address the risk of unauthorised user access. These control weaknesses increase the potential risk from a cyber attack on the IT environment.

The controls assurance reports also highlighted other internal control weaknesses:

- a lack of segregation of duties, with users able to change payroll masterfiles and process payroll payments
- a number of users had access to execute the pay run and generate the payment file but this access was not required for their roles.

These control weaknesses increase the risk of unauthorised user access to payroll masterfiles by the service provider.

One agency did not have appropriate segregation of duties. A number of employees have user access that allows them to amend masterfile information and approve payroll payments. A lack of appropriate segregation of duties increases the risk of fraudulent activity going undetected.

Review of the supplier masterfile

All 25 agencies use a standard supplier masterfile creation and amendment form to update and record supplier information. Using a standard form helps to keep the processes consistent, ensures relevant information is captured and fields are filled.

However, we found that 11 agencies did not validate changes to key details, including changes to bank account information directly with the supplier. In addition, we identified 11 agencies did not apply an appropriate naming convention to avoid and detect duplicate profiles for suppliers.

The table below shows how many agencies have applied standard processes for reviewing supplier masterfiles.

Process requirements	Percentage of agencies that include this (%)
Key details completed for a new supplier	100
Evidence kept to support creation of new supplier	100
Key details directly validated with the supplier	56
Evidence of independent review of details entered into the system	100
Naming convention applied	56

Source: Audit Office analysis.

Most agencies periodically review the supplier masterfile to identify incomplete or duplicate records. Of the 20 agencies that do, any control weaknesses are communicated to relevant stakeholders and remediation action is taken. Eight of these agencies have engaged an external service provider that conducts a quarterly review of the supplier masterfiles and sends reports to agencies to verify data. Only one agency reports the outcome of the review to a governance committee.

A number of control weaknesses were identified by those agencies that engage an external service provider. These include:

- a complete list of changes is not provided to the agency. The agency lodges a request for a change, but the agency is unable to ensure the requested change is complete and accurate
- no visibility over when requested changes are made to their systems
- the service provider can make changes to masterfiles without a request or approval from the agency
- no periodic review by the agency of all changes made to the supplier masterfiles.

Review of the employee masterfile

One new hire was selected from each agency to walk-through the creation process. It was noted that the employee masterfile for all agencies:

- completed the key details for the new employee
- contained evidence to support the creation of the new employee
- contained evidence of an independent review of key details entered into the employee masterfile.

For each agency an amendment to an employee masterfile was selected to ensure:

- evidence is maintained to support the amendment, including reasons for the change
- evidence of an independent review of changes made to the employee details.

All agencies had evidence to support amendments to the employee masterfile.

Only 52 per cent of agencies perform periodic reviews of the employee masterfile to identify incomplete or inaccurate records.

When agencies identify weaknesses, these are communicated to stakeholders and corrections are made to the records. Only three of these agencies also present the review outcome and any issues identified to a governance committee.

7. Tracking recommendations

This chapter outlines our audit observations, conclusions and recommendations arising from our review of agencies' processes to track and monitor the implementation of recommendations from performance audits and public inquiries.

Section highlights

- Less than half of all agencies have a formal policy on monitoring recommendations from performance audits or public inquiries. Agencies should formalise and implement policies on tracking and monitoring the progress of those recommendations.
- 56 per cent of agencies maintain a register of recommendations from performance audits or public inquiries. Registers could be improved to include features such as risk/priority rating, milestone due dates, record of revisions to due dates and explanatory comments.
- Recommendations can take several years to address, with the oldest unactioned items we noted dating back to 2016. Agencies reported completion of a third of recommendations that were raised within the last year.

7.1 Background

Government agencies are subject to public scrutiny and may be required to address recommendations from the Audit Office's performance audits and/or public inquiries including parliamentary inquiries and Royal Commission investigations. Effective governance arrangements that centrally monitor, review progress and track recommendations to completion help to keep agencies accountable and reduce the risk of repeat findings.

NSW Treasury Policy requires agencies to monitor the implementation of performance audit recommendations but there is no requirement specific to recommendations from other types of inquiries. There is also no specific requirement to verify that the implemented actions are appropriate and achieve the intended outcomes.

While there is no prescribed method for tracking and implementing recommendations, a well-maintained register with clearly articulated business rules has the following benefits. It:

- allows for alignment, and helps identify where overlaps or conflicts exist between recommendations or agency actions
- encourages early assessment of the relative priority, risk rating, governance arrangements, and monitoring requirements that should be adopted when addressing different types of inquiries and recommendations
- specifies expected milestones and timeframes, and highlights delays for escalation
- provides visibility for more consistent and routine reporting on public commitments.

Our review has focused on whether agencies apply a comprehensive approach to addressing external recommendations, which include:

- formal policies on tracking recommendations
- maintaining a centralised register of recommendations
- reporting and acquittal processes.

The importance of tracking recommendations was recently highlighted in the public inquiry and Royal Commission into the NSW bushfires of 2019–20⁶. The Royal Commission noted the extensive history of public inquiries into responses to natural disasters over the past ten years and the lack of action on recommendations:

Many recommendations are accepted by governments – and then disappear. Further, details of monitoring and implementation are not communicated to the public – and then there is another disaster and another inquiry, often into the same subject matter.

If a recommendation is not accepted, reasons should be provided for doing so. If it is accepted, steps should be taken to implement as soon as practicable, and to monitor, and report on, the extent of implementation.

Our 2021 report [Addressing public inquiry recommendations - Emergency response agencies](#) also found gaps in how agencies managed and monitored the implementation of recommendations.

7.2 Policy framework

Most agencies do not have a formal policy on monitoring recommendations

Only 48 per cent of agencies have a formal policy that involves monitoring recommendations from performance audits, public inquiries, or other external reviews. These policies contain varying degrees of detail regarding:

- roles and responsibilities of officers and business units
- documentation requirements
- updating and monitoring processes
- approval requirements for changes to plans
- reporting processes to executive or governance committees
- acquittal processes to ensure that actions address the intended outcomes.

While 52 per cent of agencies have informal processes in place for tracking these types of recommendations, they are not comprehensive in their approach nor are they centrally managed. There is a greater risk that agencies without a clear policy framework are not effectively responding to external recommendations in a timely way.

Recommendation

Agencies should formalise and implement policies on tracking and monitoring the progress of implementing recommendations from performance audits and public inquiries.

7.3 Recommendations register

Most agencies maintain some form of electronic register of recommendations that is regularly updated. However, this is often used only for recommendations arising from internal audit reviews and financial audits.

A centralised register allows management to demonstrate the completeness of recommendations captured, assign accountability for implementation plans for each recommendation, and monitor the progress and timeliness of actions.

⁶ [Royal Commission into National Natural Disaster Arrangements Report](#)

Fifty-six per cent of agencies maintain a central register of recommendations from performance audits or public inquiries

Fourteen of the 25 agencies within the scope of this report maintain a central register of recommendations that capture items from performance audits, public inquiries, or other external reviews. Seven of these agencies did not have a formal policy framework governing its use and content, but kept a register nonetheless. These registers were combined with internal audit and financial audit recommendations and managed through the internal audit actions monitoring process.

We noted evidence that all registers were updated during 2021. However, from our review, six agencies' registers were not complete. Their registers had incomplete fields such as due dates, or had not yet recorded recommendations from recent reports. Another agency had duplicated records when merging of the separate registers of former entities into a single register following Machinery of Government changes.

Two agencies who were the subject of our recent performance audit on '[Addressing public inquiry recommendations - Emergency response agencies](#)' have since established registers. One emergency response agency is still in the process of developing a register.

We found some agencies could improve the quality of their registers by including the features as set out in the table below.

Feature	Percentage of agencies' registers that do not include (%)
Risk or priority rating to the issue or recommendation	27
Milestone dates for larger implementation plans with multiple steps	100
Record of revisions to due dates	32
Comments to explain why due dates were changed	23

Source: Audit Office analysis.

Applying a risk or priority rating to recommendations allows decision-makers to focus greater attention and resources to those that are more critical.

Allocating milestone dates provides greater visibility of progress on long-term or complex action plans, particularly for those that involve multiple stages of implementation, or require the agency to work with other agencies or external parties.

Maintaining records of revisions to due dates enhances accountability and transparency, and allows those in governance charged with the implementation of recommendations to understand the causes for delays, and evaluate whether sufficient resources have been allocated to the matter to mitigate the risk.

All agencies except one require approval from senior management for revising due dates on actions. However, the one agency that did not require approval for changes noted that the status of recommendations is routinely presented to the executive team for endorsement.

Recommendations can take several years to fully address

Of the agencies that maintain a register of performance audit and public inquiry recommendations, the oldest actions that remain incomplete were originally raised in 2016, as detailed below.

Recommendation	Original due date	Risk rating	Management updates
To develop detailed performance indicators with baseline data	June 2017	Important and required prompt (but not urgent) attention	Delayed due to lack of expenditure authorisation
To formally document the process for managing and setting actions in response to key performance indicators (KPI) variation	June 2016	Not assigned	In development with current expected completion date in 2021

Source: Audit Office analysis.

From other registers of internal audit and financial audit recommendations, we also noted the oldest items being from 2016, as detailed below.

Recommendation	Original due date	Risk rating	Management updates
Financial audit recommendation for formalising service agreements between government agencies and consider accounting implications	June 2017	Moderate	Draft agreements being prepared
Internal audit recommendation for training and refresher courses for procurement staff	April 2019	Low	New training program being developed with expected completion by May 2021

Source: Audit Office analysis.

It is important that registers record status updates and changes to due dates, and are regularly reviewed so that the agency remains accountable for completing the actions. This helps to ensure that important recommendations accepted by the agency are not neglected and not progressed for years.

A third of recommendations were completed in the past year

Agencies that track recommendations from performance audits and public inquiries report that, on average they completed 36 per cent of recommended actions raised within the last 12 months. This calculation excludes those whose registers only display open action items where it is not possible to assess the completion rate.

Of those registers, half of them also incorporate internal audit recommendations. The number of recommendations on these registers from the past 12 months range from 15 to 226, with completion rates ranging from seven per cent to 53 per cent.

The other half of registers without internal audit recommendations show a total number of recommendations from the past 12 months from two to 143. The completion rates ranged from 12 per cent to 100 per cent.

All agencies track their overdue actions

One agency had not formally documented a policy requiring follow-up of overdue actions. Nonetheless, all agencies that maintain registers also review the status of overdue items and report on them to a Board or Audit and Risk committee either monthly or quarterly.

The oldest overdue action item we found in these registers was due in June 2016, as noted above.

The average percentage of overdue action items for recommendations raised within the last 12 months is 18 per cent. These registers also incorporate recommendations from internal audit and financial audit.

In 36 per cent of registers, there were nil actions reported as overdue for items raised within the last 12 months. Excluding those, the number of overdue actions on the registers range from two to 94, and the percentages of overdue actions ranged from four to 62 per cent.

Two agencies do not restrict access to their registers

While all other agencies have measures to protect the registers using passwords or secure locations so that only relevant officers can modify them, two agencies have not.

Access restrictions help ensure that only valid and authorised changes are made to the registers, such as revisions to due dates or progress commentary.

7.4 Reporting and oversight

All agencies report on the progress of recommendations to governance committees, such as the Board or Audit and Risk committee. This provides greater oversight on the monitoring process.

Five agencies do not report on the progress of recommendations externally

Of the 14 agencies that maintain registers of recommendations relating to performance audits and public inquiries, five do not report on their progress to an external body such as the Minister, the Parliament or the entity that made the recommendation.

Without public or external reporting, there is limited visibility of actions taken by the agency and reduced accountability.

Most agencies have a process to validate the implemented actions

Acquittals and subsequent reviews support the process of ensuring the agency's response to recommendations effectively address the issue. Acquittal processes comprise a review of completed recommendations and verifying evidence that they have been implemented in accordance with the stated aims. Subsequent reviews occur after a period of time to check that the implemented actions are still in place or operating as intended.

Of the 14 agencies that track recommendations from performance audits and public inquiries, we found that four did not perform acquittal processes. However, over half of the agencies do not perform subsequent reviews.

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)

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.