FINANCIAL AUDIT

20 DECEMBER 2023

Internal controls and governance 2023

NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

audit office OF NEW SOUTH WALES

THE ROLE OF THE AUDITOR-GENERAL

The roles and responsibilities of the Auditor-General, and hence the Audit Office, are set out in the *Government Sector Audit Act 1983* and the *Local Government Act 1993*.

We conduct financial or 'attest' audits of state public sector and local government entities' financial statements. We also audit the Consolidated State Financial Statements, a consolidation of all state public sector agencies' financial statements.

Financial audits are designed to give reasonable assurance that financial statements are true and fair, enhancing their value to end users. Also, the existence of such audits provides a constant stimulus to entities to ensure sound financial management.

Following a financial audit the Audit Office issues a variety of reports to entities and reports periodically to Parliament. In combination, these reports give opinions on the truth and fairness of financial statements, and comment on entity internal controls and governance, and compliance with certain laws, regulations and government directives. They may comment on financial prudence, probity and waste, and recommend operational improvements.

We also conduct performance audits. These assess whether the activities of government entities are being carried out effectively, economically, efficiently and in compliance with relevant laws. Audits may cover all or parts of an entity's operations, or consider particular issues across a number of entities. Our performance audits may also extend to activities of non-government entities that receive money or resources, whether directly or indirectly, from or on behalf of government entities for a particular purpose.

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

AUDITOR-GENERAL
NEW SOUTH WALES

GPO Box 12
Sydney NSW 2001

The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 52B of the *Government Sector Audit Act 1983*, I present a report titled **'Internal controls and governance 2023'**.

Margaret Crawford PSM
Auditor-General for New South Wales
20 December 2023

RECONCILIATION COMMITMENT STATEMENT

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

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

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

auditoffice
OF NEW SOUTH WALES

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

contents

Internal controls and governance 2023

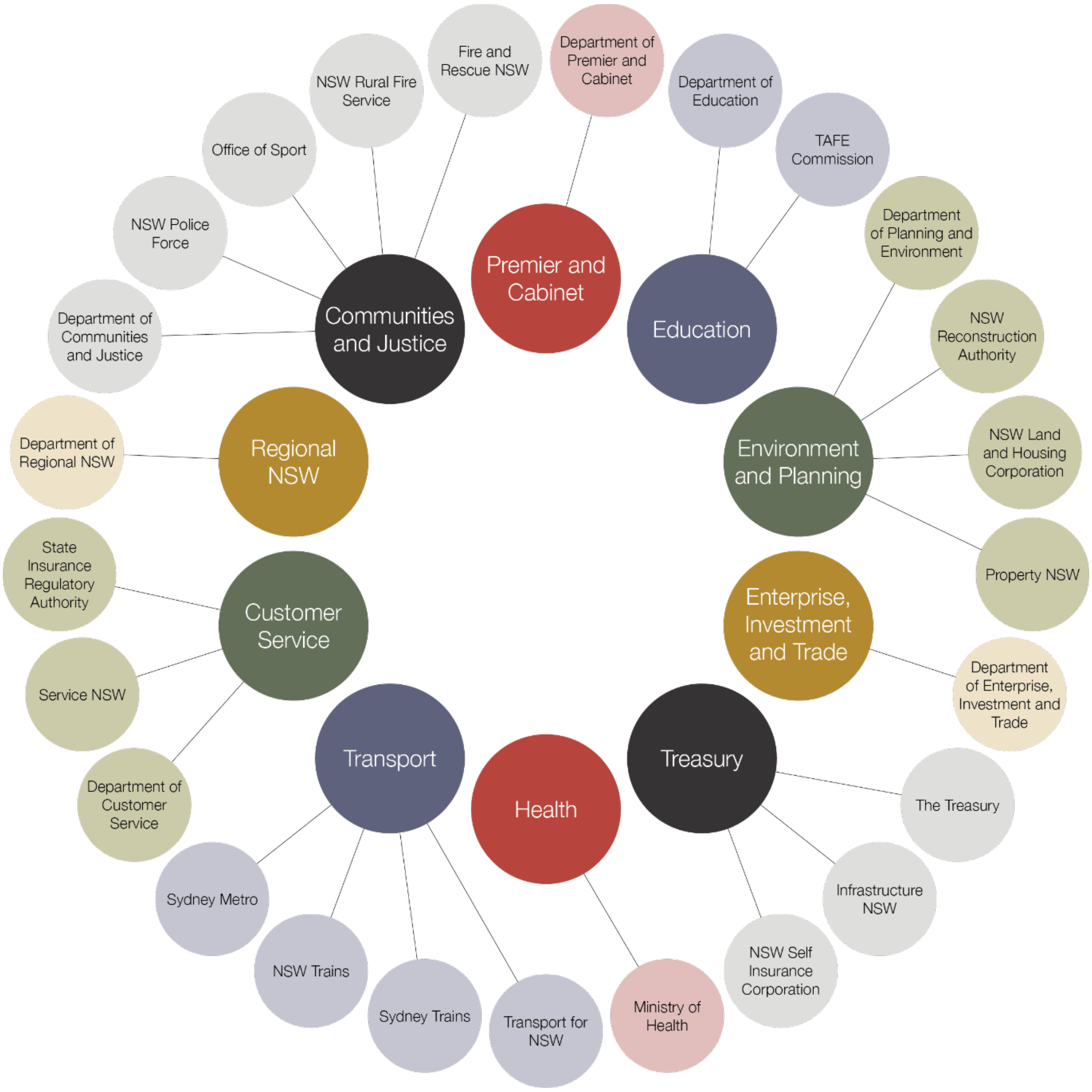
1. Introduction

1.1 State sector agencies

This report covers the findings and recommendations from our 2022–23 financial audits that relate to internal controls and governance at 25 of the largest agencies in the New South Wales (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 portfolio groups as at 30 June 2023.



Premier and Cabinet
Department of Premier and Cabinet
Education
Department of Education
TAFE Commission
Environment and Planning
Department of Planning and Environment
NSW Reconstruction Authority
NSW Land and Housing Corporation
Property NSW
Enterprise, Investment and Trade
Department of Enterprise, Investment and Trade
Treasury
The Treasury
Infrastructure NSW
NSW Self Insurance Corporation
Health
Ministry of Health
Transport
Transport for NSW
Sydney Trains
NSW Trains
Sydney Metro
Customer Service
Department of Customer Service
Service NSW
State Insurance Regulatory Authority
Regional NSW
Department of Regional NSW
Communities and Justice
Department of Communities and Justice
NSW Police Force
Office of Sport
NSW Rural Fire Service
Fire and Rescue NSW

Exhibit 1.

Note: The structure and name of agencies included in the diagram above are as at 30 June 2023.

A number of Machinery of Government changes were announced during 2023 through Administrative Orders, which have affected the structure and names of some agencies in the scope of this report. These are listed in the table below.

Instrument	Description	Further reporting
Administrative Arrangements (Administrative Changes—Miscellaneous) Order (No 2) 2023	Effective on 5 April and 5 May 2023, this Order transferred sport-related agencies including the Office of Sport from the Enterprise, Investment and Trade portfolio to the Communities and Justice portfolio.	Report on Stronger Communities 2023
Administrative Arrangements (Administrative Changes—Miscellaneous) Order (No 4) 2023	Effective 1 July 2023, this Order changed the name of the Department of Premier and Cabinet to the Premier's Department and transferred parts of the former Department of Premier and Cabinet to The Cabinet Office.	Report on Premier and Cabinet 2023
Administrative Arrangements (Administrative Changes—Miscellaneous) Order (No 6) 2023	Effective on 1 January and 1 February 2024, this Order will change the name of the Department of Planning and Environment to Department of Planning, Housing and Infrastructure, and create a new Department of Climate Change, Energy, the Environment and Water.	Report on Planning and Environment 2023

1.2 Financial snapshot

The 25 agencies included in this report constitute an estimated 95% of total expenditure for all NSW public sector agencies, excluding state owned corporations and public financial corporations. That is, they represent the general government sector and public non-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 2023.

	Number of agencies	Assets $ billion	Liabilities $ billion	Income $ billion	Expenses $ billion
Departments	10	299.9	41.9	116.5	108.9
Public non-financial corporations	3	72.0	8.1	7.4	7.6
Statutory bodies	12	77.1	33.0	25.0	21.0
Total	**25**	**449.0**	**83.0**	**148.9**	**137.5**

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

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

1.3 Areas of focus

This report covers the following topics:

Topic	Description
Maturity of cyber security	Accountability for cyber security maturity enables agencies to be transparent on their preparation and capability to prevent, detect, respond and recover from cyber security incidents. This report focuses on maturity self-assessments from agencies, analysis of those assessments and the function of Cyber Security NSW.
Cyber security resilience	Cyber resilience is an important component of the NSW Cyber Security Policy, with the objective for agencies to be able to rapidly detect cyber incidents and respond appropriately. This report focuses on how well agencies are monitoring and responding to cyber incidents, including: • having and exercising a current cyber incident response plan • monitoring systems to identify cyber incidents • reporting of cyber incidents.
Governance framework	Governance frameworks refer to the structures, processes and mechanisms by which agencies are held accountable for their decisions and operations. Ethics, risk management and compliance are all elements of good governance. This report focuses on whether agencies have established appropriate governance arrangements and risk management practices in line with NSW Treasury policies.
Managing payroll and work health and safety (WHS)	For the NSW public sector where employee related expenses comprise over a third of total expenditure, payroll controls are critical for effective financial management. Employee safety is also an important consideration as employers are required to comply with the *Work Health and Safety Act 2011* to manage hazards and risks in the workplace. This report focuses on: • whether agencies have implemented appropriate payroll controls • how agencies manage their WHS responsibilities and staff wellbeing, including management of overtime.

1.4 Sector-wide learnings

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

Internal and information technology controls

- Address repeat control deficiencies by ensuring:
  - there is clear ownership of recommendations arising from internal control deficiencies, with timeframes and action plans for their implementation
  - audit and risk committees and agency executive teams monitor the implementation status regularly, focusing on those actions that are past due or have deferred implementation dates.
- Focus on monitoring privileged users and their access permissions, assess risk management and document the risks associated with their privileges. Agencies should:
  - provide and limit privileged user access only to staff and contractors who require the level of access to perform their role and only for the period for which they require access
  - identify controls to address the risk associated with privileged user activity, including monitoring of activity logs
  - promptly remove access when it is no longer required.
- Establish and review segregation of duties over key payroll functions to reduce the risk of fraud and improve the quality of payroll processing.

Cyber security maturity and resilience

- Prioritise and improve cyber maturity, implementing the mandatory requirements of the NSW Cyber Security Policy in a consistent way, and implementing the Essential Eight at a level appropriate for the risk agencies face.
- Implement effective oversight to ensure that maturity uplift initiatives deliver the benefits of higher cyber security maturity.
- Review and build in information security and cyber security obligations with service providers and organisations that have access to their systems and data.
- Regularly test cyber incident response plans, including response teams and third-party providers to maximise learning and improvements to cyber resilience.
- Maintain sufficient records for cyber security incidents to ensure correct, timely and consistent classification, and therefore response.

Governance framework

- For agencies that operate governing boards, they should formalise their board charter or terms of reference to:
  - define the responsibilities of the board compared to the responsibilities of management
  - periodically evaluate their performance against defined criteria.
- Risk management frameworks should be improved to:
  - ensure that policies are kept up-to-date and periodically reviewed
  - establish risk appetite statements and tolerance levels
  - require external evaluation of internal audit functions at least every five years.
- Agencies should perform periodic assessments/reviews of their risk maturity and implement action plans where required.

Managing payroll and WHS

- Agencies should improve their controls around payroll masterfile maintenance, such as enforcing segregation of duties in system access levels and ensuring changes to data are reviewed by an independent officer.
- Agencies should improve their management of overtime, including:
  - establishing policies or guidelines for when the use of overtime is appropriate to support effective workforce management
  - monitoring overtime hours at an organisational level, analysing trends to inform resource planning, or identify staff outliers who may have unsustainable workloads.
- Agencies should update their WHS policies and procedures to include current legislative requirements, including management of psychosocial hazards.
- Agencies should regularly report WHS matters to those charged with governance, including risks, review activities, and notifiable incidents. Officers, including those charged with governance, have duties of care under the WHS Act.
- WHS training could be improved to provide a mandatory annual refresher for all employees, and tailored induction training for contractors and visitors who are also in the scope of the WHS Act.

1.5 Status of 2022 report recommendations

Our report on internal controls and governance for the year ended 30 June 2022 made a number of recommendations. The table below sets out the status of those recommendations being addressed by the relevant agencies.

Recommendation	Current status*	
Internal control trends		
Agencies need to prioritise actions to address repeat control deficiencies, particularly those that have been repeated findings for a number of years.	Fourteen out of 24* agencies have addressed this recommendation. Eight agencies have partially implemented actions to address the recommendation. If control deficiencies are not addressed, the risks associated with the control deficiency may increase with time, which is why they need to be addressed on a timely basis; refer to section 2.1 of this report for further details. Two agencies did not have any repeated findings from the prior year.	⊖
Cyber security		
As reported last year, agencies need to prioritise improvements to their cyber security and resilience as a matter of urgency. Specific actions include:	Agencies' progress in implementing the recommendations is outlined below:	
• ensuring their reported level of maturity is demonstrated by evidence	• Thirteen out of 24* agencies have evidence to support their reported level of maturity. Eleven agencies have a plan in place, but actions did not commence in 2022–23.	⊖
• improving Essential Eight maturity levels to meet target levels, which are more difficult to achieve under the updated Essential Eight model.	• Three out of 24* agencies have demonstrated improvement in their maturity levels. Twenty-one agencies have a plan in place, but had not achieved improvement in maturity levels for 2022–23.	⊖

Recommendation	Current status*	
Agencies need to reinforce their mandatory cyber awareness training to all staff and improve the completion rates. Agencies should also conduct tailored training content for higher risk groups of users such as board members, procurement and payroll staff, and third parties with access to the agency's systems.	Eighteen out of 24* agencies have conducted cyber awareness training for staff, some of which include phishing simulation exercises. One agency has not addressed the recommendation. Five agencies have made progress in addressing the recommendation or have scheduled training programs that will commence after 30 June 2023. Agencies need to improve their cyber security maturity complying with Cyber Security NSW's Mandatory Requirements and the Essential Eight, as detailed in section 4 of this report.	⊖
Engaging consultants and contractors		
Agencies need to ensure that contractor engagements that have been renewed over multiple years for the same role are periodically reassessed against the market to demonstrate that the contractor continues to represent value for money and effectiveness in achieving performance objectives.	Sixteen out of 24* agencies have addressed the recommendation. Five agencies have not addressed the recommendation. Two agencies have action plans in progress. One agency is newly formed and does not have long-term contractors.	⊖

Key ✓ **Fully addressed** ⊖ **Partially addressed** ! **Not addressed**

* There is a total of 24 agencies reporting on the status of recommendations from 2022. One of the 25 agencies reported on last year, Resilience NSW, was abolished in December 2022.

2. Internal control trends

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

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

This chapter outlines the overall trends for agency controls and governance issues, including the number of audit findings, the degree of risk those deficiencies pose to the agency, and a summary of the most common deficiencies found across agencies.

For consistency and comparability, we have adjusted the 2022 results to incorporate additional audit findings that were reported after the date of the Internal controls and governance 2022 report. Therefore, the 2022 figures will not necessarily align with those reported in our 2022 report.

Section highlights

- The Audit Office identified 12 high-risk findings, compared to 23 last year, with eight repeated from last year. Eleven of the high-risk findings related to financial controls while one related to other (governance) controls.
- The proportion of repeat deficiencies has decreased from 48% in 2021–22 to 38% in 2022–23.

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.

The Audit Office of NSW (the Audit Office) rates 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 decreased from last year

The Audit Office identified 12 high-risk findings out of a total of 268 audit findings this year, compared to 23 high-risk findings out of a total of 279 audit findings in 2021–22. As a proportion of total audit findings, high-risk findings have also decreased from 8.2% to 4.5%.

Of concern were eight high-risk findings that were repeat deficiencies reported in the previous year (ten repeat high-risk findings in 2022). Eleven of the high-risk deficiencies related to financial controls while one related to other (governance) controls.

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

High-risk finding	Implication	Further reporting
Repeated high-risk findings		
Deficiencies were identified in the Department of Communities and Justice's payment system controls, whereby users are able to circumvent the department's controls and made unauthorised payments. This deficiency was first reported in 2013–14.	The system limitations, if not appropriately mitigated, increase the risk of invalid payments and public monies being misappropriated.	Agency: Department of Communities and Justice Further detail on this issue is included in the Report on Stronger Communities, which was tabled in November 2023.
The Department of Planning and Environment did not finalise the reporting exemption assessment for both 2021–22 and 2022–23 relating to a group of agencies that are controlled by the State. As a result, these agencies have not prepared and submitted annual financial statements for audit in both years, and did not comply with the *Government Sector Finance Act 2018* (GSF Act).	Non-compliance with the financial reporting obligations of the GSF Act. Lack of reliable financial data for these agencies presents difficulties in consolidating the total state sector accounts.	Agency: Department of Planning and Environment Further detail on this issue is included in the Report on Planning and Environment, which will be tabled in December 2023.
The Department of Planning and Environment should intervene to provide a regulatory response on local councils that have qualified audit reports relating to non-recognition of rural fire-fighting equipment. The financial statements of the NSW Total State Sector and the NSW Rural Fire Service do not recognise rural firefighting equipment, as the State is of the view that rural fire-fighting equipment, vested to local councils under section 119(2) of the *Rural Fires Act 1997*, is not controlled by the State.	The department is not fulfilling its role in addressing councils' non-compliance with legislative responsibilities, standards and guidelines.	Agency: Department of Planning and Environment Further detail on this issue is included in the Report on Planning and Environment, which will be tabled in December 2023.
Deficiencies exist in the Department of Planning and Environment's management and accounting of Crown land, including inadequate recording and reconciliation between the Crown land register and general ledger systems, incorrect data, and outstanding work orders and anomalies in the register. Some of these issues were first reported in 2017.	Control deficiencies in the completeness and accuracy of data can increase the risk of material misstatements in the financial statements. The department may also not be fulfilling its responsibilities under applicable legislation.	Agency: Department of Planning and Environment Further detail on this issue is included in the Report on Planning and Environment, which will be tabled in December 2023.
The forced processing of timesheets that have not been reviewed and approved in time for each pay cycle remains an ongoing issue for the Ministry of Health. Our audits identified that following the pay run, there was no subsequent review of the unapproved time records to confirm their validity, accuracy and completeness.	Timesheets may not reflect actual hours worked and may result in over/underpayment of staff. The lack of prior approval or subsequent review increases the risk of errors, retrospective pay adjustments and material misstatement in the financial statements.	Agency: Ministry of Health Further detail on this issue is included in the Report on Health, which will be tabled in December 2023.

High-risk finding	Implication	Further reporting
The Treasury's financial statements and supporting evidence submitted for audit included deficiencies that indicated a lack of quality review of information prior to its submission. This was a repeat high-risk finding from 2020–21.	A lack of quality review increases the risk of material misstatements and disclosure deficiencies in the financial statements.	Agency: NSW Treasury Further detail on this issue is included in the Report on Treasury, which will be tabled in December 2023.
NSW Treasury did not approve the final costings and funding sources of some grant programs before funds were withdrawn from administered bank accounts.	The absence of delegated approval of administration costs, prior to these being deducted, could lead to significant breaches of legislation and grant funding agreements.	Agency: NSW Treasury Further detail on this issue is included in the Report on Treasury, which will be tabled in December 2023.
Significant control deficiencies were identified with Service NSW's administration and financial reporting of grant programs.	The agency did not meet its performance obligations by obtaining the necessary approvals prior to recognising administration revenue. This may result in a breach of legislation and material misstatement in the financial statements.	Agency: Service NSW Further detail on this issue is included in the Report on Customer Service, which was tabled in November 2023.
New high-risk findings		
The Department of Enterprise, Investment and Trade overstated grants relating to the Jobs Plus Program at 30 June 2023. Deficiencies were noted in management's assessment to support the provision.	This increases the risk of material misstatement in the financial statements.	Agency: Department of Enterprise, Investment and Trade Further detail on this issue is included in the Report on Enterprise, Investment and Trade, which was tabled in November 2023.
The NSW Reconstruction Authority administered the temporary homes program in response to the 2022 Northern Rivers and Central West flood events, but did not assess the accounting implications arising from contractual agreements associated with the program.	There is an increased risk of material misstatements in the financial statements, as well as incomplete recording of asset and liabilities related to the agreements.	Agency: NSW Reconstruction Authority Further detail on this issue is included in the Report on Planning and Environment, which will be tabled in December 2023.
NSW Treasury did not have appropriate controls to identify and monitor the number and amount of payments made in relation to the Restart NSW Fund.	Lack of oversight and records of the payments being made out of the fund increases the risk of duplicate or inappropriate payments, and non-compliance with record-keeping responsibilities under the GSF Act.	Agency: NSW Treasury Further detail on this issue is included in the Report on Treasury, which will be tabled in December 2023.
Sydney Metro needs to improve how they manage contractors and conflicts of interest.	Insufficient controls to identify and manage conflicts of interest could cause serious financial and reputational damage to Sydney Metro.	Agency: Sydney Metro Further detail on this issue is included in the Report on Transport, which will be tabled in December 2023.

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

2.2 Common findings

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

The Audit Office classified the 268 internal control deficiencies that were identified in 2022–23 into common categories as follows:

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

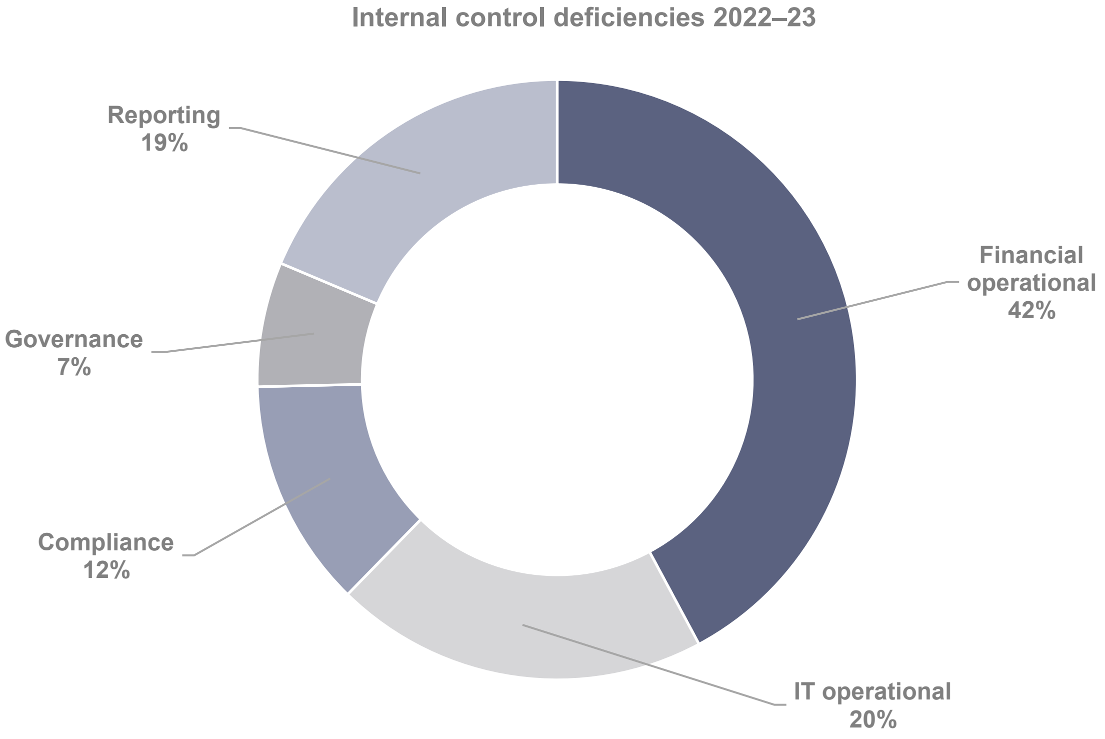


Exhibit 2.

Source: Audit Office of NSW findings.

The graph above shows that 62% of the deficiencies (67% in 2021–22) were financial or IT operational deficiencies, with the remainder split among compliance deficiencies (12% compared to 19% in 2021–22), governance deficiencies (seven per cent compared to six per cent in 2021–22), and reporting deficiencies (19% compared to eight per cent in 2021–22).

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

Operational (167)	New Issues	Repeat issues
❗ **High**:	1	6
⊖ **Moderate**:	49	43
✓ **Low**:	52	16

Common issue	Findings/implications	Lessons for agencies
Fixed assets	A number of internal control deficiencies across many agencies were identified, including: • delays in capitalisation of completed capital work-in progress or other asset additions • inaccurate and/or incomplete data in asset registers • inadequate review over the appropriateness of asset capitalisation threshold • lack of review over long outstanding work-in-progress balances.	Agencies should: • capitalise asset additions or capital work-in-progress when the asset meets the requirements of capitalisation per AASB 116 • regularly review data quality in asset registers • review asset capitalisation threshold policy and determine if it is in line with the NSW Treasury guidance TPP 06-06 • review work-in-progress balances periodically for indicators of impairment, indexation or other adjustments as required.
Payroll controls	Several internal control deficiencies were identified, including: • untimely processing of employee terminations • non-recoupment of overpaid salaries • poor management of timesheet/record-keeping, overtime claims, and leave requests • lack of evidence of review of payroll reports and checklists.	Agencies should ensure staff are trained in their obligations in relation to payroll controls and segregation of duties. Any changes made to payroll data must be authorised and reviewed within appropriate timeframes, and stricter controls for payroll should be implemented to prevent over-payments, and payments to terminated staff.
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.
Reconciliations	Key account reconciliations were not prepared or were not reviewed in a timely manner. Reconciliations contained unresolved variances, long outstanding transactions, and other unusual items.	Policies and procedures should require reconciliations be prepared and reviewed as part of month-end processes. Management should ensure this key control is performed. Reconciling differences should be resolved in a timely manner.
Quality and timeliness of financial information	Issues were noted with the quality and timeliness of workpapers supporting the financial statements provided for audit, resulting in delays and additional costs.	Agencies should ensure sufficient quality review is undertaken in preparing the financial statements and supporting documentation.

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 (33)	New Issues	Repeat issues
! **High**:	1	2
– **Moderate**:	8	7
✓ **Low**:	6	9

Common issue	Findings/implications	Lessons for agencies
Non-compliance with legislation	Non-compliance with legislation, Treasurer's Directions, and internal policies was identified.	Agencies should ensure central registers capture all key legislation and assign responsibility.
Financial delegations	Agencies did not incur expenditure in accordance with delegation instruments. System workflow settings for approval of expenditure were inconsistent with approved delegations.	Agencies should ensure that an appropriate delegation framework is in place for all forms of expenditure and review system settings for compliance.
Conflicts of interest	Control deficiencies were noted, including: • lack of documentation of conflict declarations • undisclosed conflicts • lack of review of declared conflicts.	Agencies should have registers to capture staff disclosures to ensure compliance with legislation and policies. Conflict of interest policies should specify the process and timeframes for review and resolution of declared conflicts.

Source: Audit Office findings.

Governance (18)	New Issues	Repeat issues
! **High**:	1	0
– **Moderate**:	3	6
✓ **Low**:	3	5

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.
Outdated or lack of formal 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.

Reporting (50)	New Issues	Repeat issues
❗ **High**:	1	0
⊖ **Moderate**:	18	7
✓ **Low**:	23	1

Common issue	Findings/implications	Lessons for agencies
Employee leave liabilities	From 1 October 2022 a new parental leave policy for NSW public sector employees was enacted. Agencies had not evaluated the change to the paid parental scheme for any financial statement related impacts.	Agencies should ensure any changes to employee entitlements are assessed for their potential financial statements impact under the relevant Australian Accounting Standards.
Accounting standard application	Application of accounting standards continues to challenge agencies. Issues were identified, including but not limited to: • revenue recognition • accounting for leases • accounting estimates for provisions.	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.
Fair value assessment and revaluation of property, plant and equipment	Agencies engaging valuers did not conduct their own assessments as to the reasonableness of the valuations, or review the valuation reports for errors and discrepancies. Agencies did not apply appropriate indices to asset values as part of the annual fair value assessment.	Agencies should ensure they comply with applicable Australian Accounting Standards and mandated Treasury guidance. Agencies continue to be responsible for the revaluation process and should: • assess the appropriateness of the methodology, key assumptions and judgements adopted in the valuation and impairment of plant and equipment • test key inputs and mathematical calculation of fair value and impairment assessments.

Source: Audit Office findings.

2.3 Trends in findings

The Audit Office assesses trends in agency controls by measuring the number of internal control findings that emerged from our financial audits. Three measures are used:

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

Our 2022–23 audits identified 268 internal control deficiencies, comprising:

- 186 financial related control deficiencies
- 57 IT related control deficiencies
- 25 other control deficiencies.

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

Deficiencies in financial and other 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.

IT control deficiencies are detailed further in the next chapter.

The number of internal control deficiencies decreased by four per cent from last year

There were 11 fewer control deficiencies identified in 2022–23. The composition of the findings showed a 24% decrease in IT findings and a three per cent increase in financial and other control findings.

The Audit Office found control deficiencies in all agencies this year (96% in 2021–22).

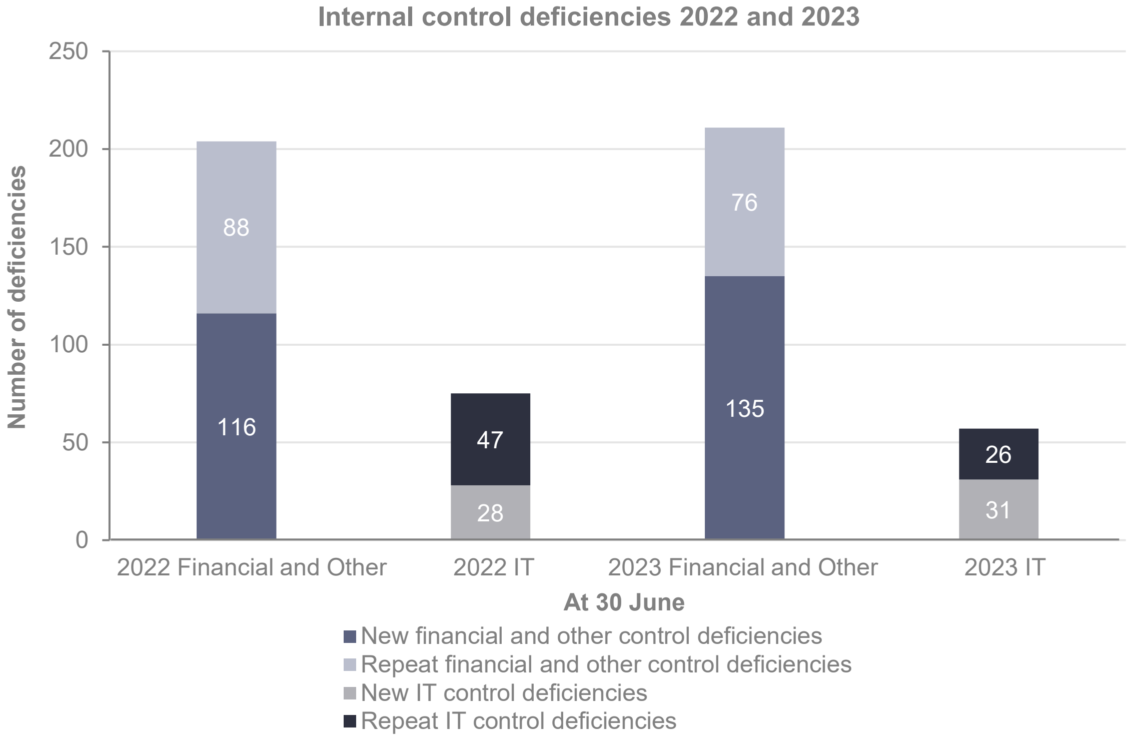


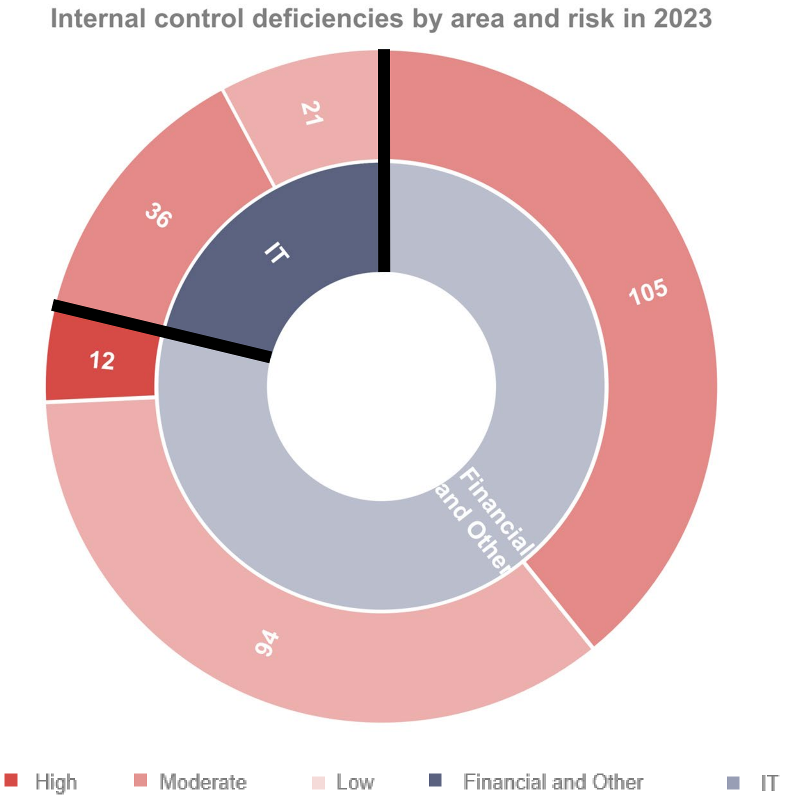
Exhibit 3.

Source: Audit Office findings.

Risk levels of IT related findings have decreased

Risk levels of IT related control findings have decreased from 2022 to 2023. For Financial and Other control findings, there has not been a noticeable difference in risk levels from last year.

The graph below shows the risk ratings of reported control deficiencies.



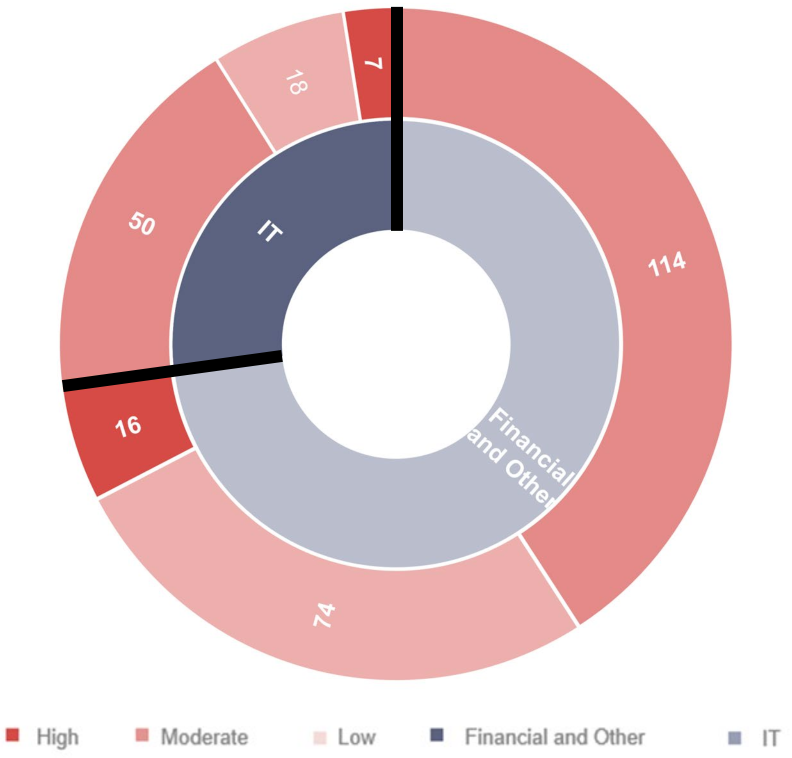


Exhibit 4.

Source: Audit Office findings.

Repeat findings have reduced from 48% to 38% of all findings

As a percentage of total internal control deficiencies, unresolved deficiencies from prior years now represent 38% of all internal control deficiencies identified (48% in 2021–22).

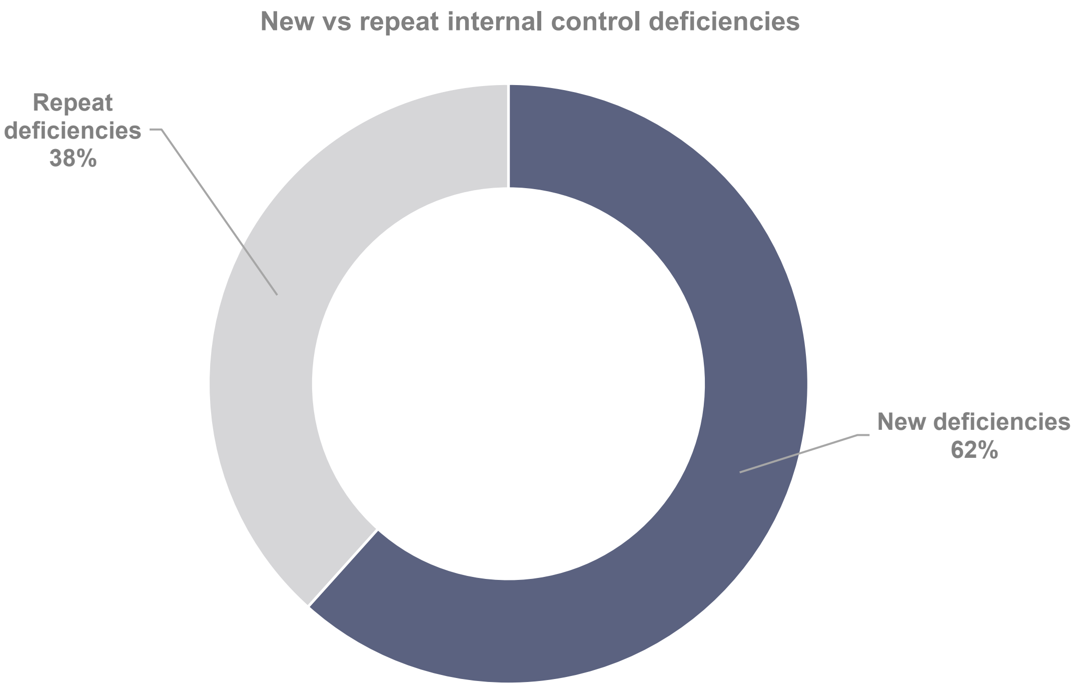


Exhibit 5.

Source: Audit Office findings.

At least 11 repeat findings reported in 2022–23 had been repeated since 2018. These need to be resolved by the relevant agencies as a priority.

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.

3. Information technology controls

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

Section highlights

- Over half of the agencies reviewed have deficiencies in managing user access.
- Thirty-six per cent of agencies had deficiencies in their controls over privileged accounts.
- Weaknesses were identified in how agencies manage service providers or other organisations which have access to their systems and data.
- Inadequate records were kept to demonstrate approvals for key system implementation milestones, including successful data migration testing and approval for go-live.
- Thirty-two per cent of agencies had not implemented segregations of duties over key payroll functions.

3.1 Background

Agencies rely on information technology (IT) systems to prepare their financial statements and deliver services to the public. The use of IT introduces risks to the integrity of information used in financial reporting, and to agency service delivery operations.

Risks to the integrity of information used for financial reporting include:

- unauthorised access to data that may result in destruction of data or improper modifications
- unauthorised changes to IT applications or other aspects of the IT environment that may undermine the integrity of processing or reporting of transactions
- inappropriate manual intervention that bypasses established checks and reviews
- potential loss of data or inability to access data as required.

Operational risks include:

- inability to continue operations or to deliver services, for example due to system outages or denial of service attacks
- theft of data, such as through ransomware attacks
- fraudulent transactions or payments made through IT systems
- failing to protect the security of personal or sensitive information
- non-compliance with laws and regulations.

Although operational risks are not the primary focus of an audit over financial statements, a failure to manage operational risks can lead to material financial impact.

IT controls are the policies and processes which mitigate these risks arising from the use of IT. Effective and robust controls are both the most effective way to mitigate these risks, and are required by legislation for government agencies.

Agencies are required, under the *Government Sector Finance Act 2018*, to establish, maintain and keep under review each of the following:

> (i) effective systems for risk management, internal control and assurance (including by means of internal audits) that are appropriate systems for the agency,
>
> (ii) arrangements for protecting the integrity of financial and performance information.

Source: *GSF Act 2018* s3.6 (1)b.

This section provides a summary of observations across common financial system IT controls evaluated or tested as part of our financial statement audits for the 25 agencies in scope for this report. While not naming the relevant agencies that form the findings, risks and recommendations in this report, those agencies have been separately informed. Agencies not in scope for this report can use this information to improve the management of their overall control environments.

Organisation of IT services in large NSW agencies

NSW government departments and agencies are grouped into portfolios of agencies. This has centralised some corporate services such as IT and cyber security.

The IT functions across the reported 25 agencies have the following relationships:

- 11 have their own unique IT environment
- 14 agencies are either fully (four agencies) or partly (ten agencies) relying on one of the lead agencies.

Following is a relational chart for the 25 agencies in this report. It shows the relational dependencies for IT services that support financial IT systems. The financial IT systems process financial information and are relevant to the preparation of the financial statements.

Relational chart of IT services in large NSW agencies

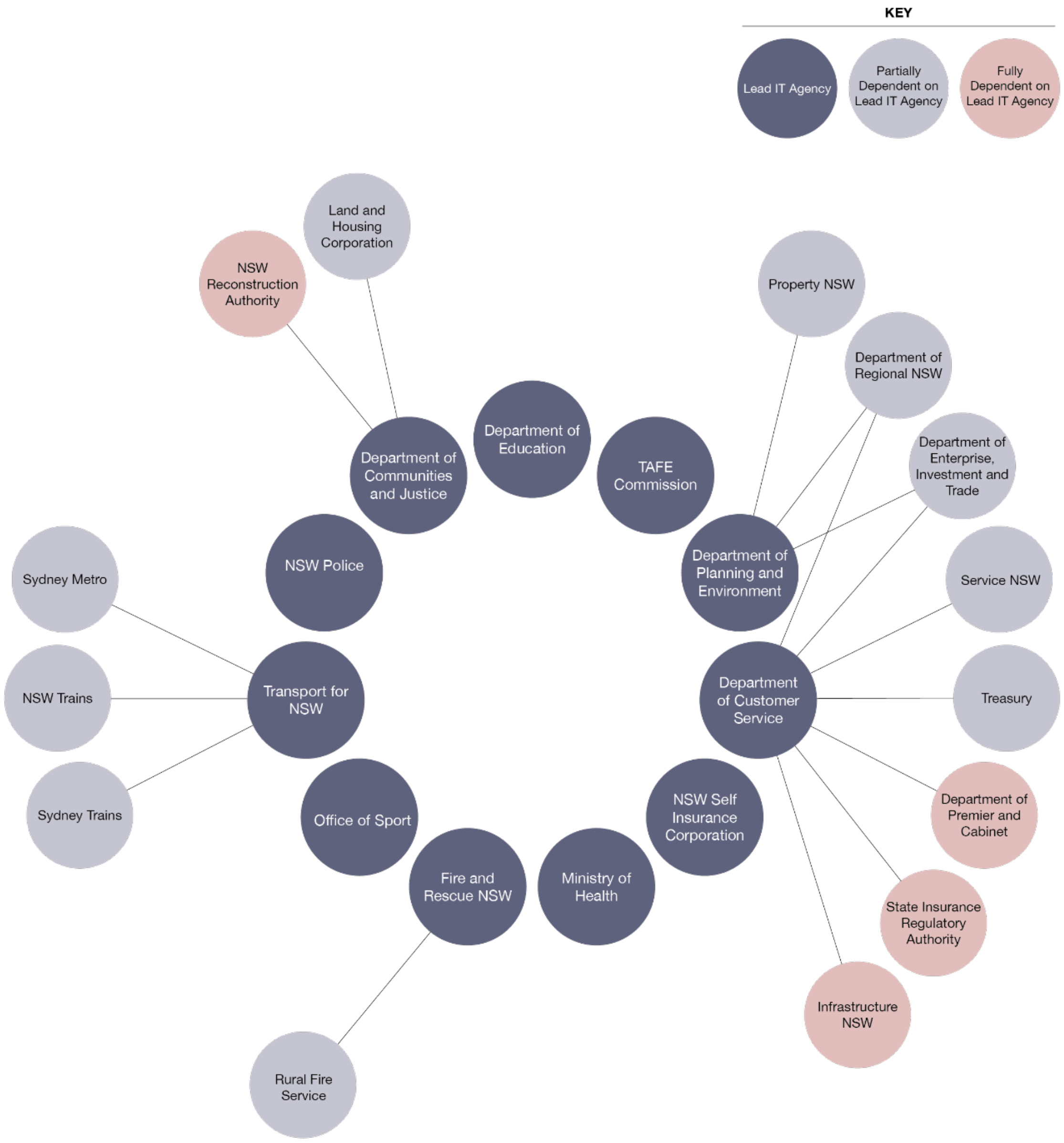

KEY
Lead IT Agency
Partially Dependent on Lead IT Agency
Fully Dependent on Lead IT Agency
Land and Housing Corporation
NSW Reconstruction Authority
Department of Communities and Justice
Department of Education
TAFE Commission
Property NSW
Department of Regional NSW
Department of Enterprise, Investment and Trade
Department of Planning and Environment
Service NSW
Sydney Metro
NSW Police
NSW Trains
Transport for NSW
Department of Customer Service
Treasury
Sydney Trains
Office of Sport
NSW Self Insurance Corporation
Department of Premier and Cabinet
Fire and Rescue NSW
Ministry of Health
State Insurance Regulatory Authority
Infrastructure NSW
Rural Fire Service

Exhibit 6.

Note: The diagram reflects the names of agencies at 30 June 2023 and the relationships for the provision of IT services for the majority of the year. Relationships for some lead and dependent IT services changed for part of the year to 30 June 2023 which are not reflected in this diagram. Changes to agencies and structures after 30 June 2023 from Machinery of Government and Administrative Orders outlined in section 1.1 are also not reflected in this diagram.

Source: Audit Office analysis of IT services and dependencies.

It is common for small or medium organisations to use shared service providers for IT systems and finance processes. In the NSW public sector, there are five agencies that operate IT shared services for more than 80 agencies. Where services are performed by another party, the agencies themselves remain accountable to ensure those services provided meet their requirements, and that the shared service provider maintains an appropriate level of controls within the systems to protect the integrity and confidentiality of data to which they have access.

Advantages of relying on other agencies for these functions include:

- economies of scale and reduced cost per person or transaction through centralisation of common processes for agencies with a similar culture, risk and industry
- reduced duplication of functions and processes across agencies
- potential for reduced disruption from some Machinery of Government changes.

The risks of interagency service reliance include:

- issues and problems could become pervasive across the set of agencies. This occurred with the Department of Customer Service in 2022 and was reported in our Customer Service 2022 report
- generalisation and loss of specialist and specific agency knowledge
- lack of clarity for what services are provided and service levels for customers
- lack of visibility over control deficiencies or incidents that occur at the shared service provider but impact the data belonging to the (customer) agency
- lack of clarity of responsibilities between providers and customers
- gaps or duplication of processes, checks and controls between provider and customer
- additional governance, accountability and assurance processes are required to ensure delivery of high performing services
- uncertainty of governance and accountability when agencies are reorganised due to Machinery of Government changes as previously reported in Machinery of government changes.

3.2 IT governance

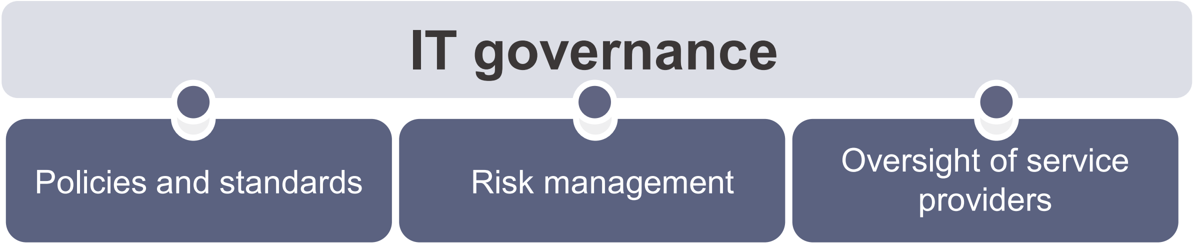


Exhibit 7.

IT governance provides a framework for accountability and transparency in how IT is managed in alignment with the agency's objectives.

We evaluated the following as part of all audits for the agencies in this report:

- policies and standards are defined and are current over all key areas of IT
- IT management identify and document risks, and report significant risks to senior management of the agency
- management obtains independent assurance that service providers maintain an appropriate level of control over their environment, proportionate to the reliance placed on that service provider.

From the audit work performed, the following themes were identified.

Four agencies did not have current IT policies and standards in place

Sixteen per cent of agencies had IT policies or standards which were either not formalised, not current or not complete. This has reduced compared to previous years (33% in 2021–22 and 24% in 2020–21), but improvement is still needed.

Risk

Failure to implement and maintain current policies and standards increases the risk of:

- not effectively managing new and evolving IT risks or changes in the environment
- inconsistent processes which do not meet operational goals
- non-compliance with laws and regulations
- lack of clarity on employees' roles and responsibilities in relation to IT.

Agencies should ensure IT policies remain relevant and current, especially after agency administrative changes (also known as Machinery of Government changes). These changes can abolish or create agencies, transfer policy, programs and service delivery to other agencies.

Supporting policies and standards do not always keep up with the transfer, and agencies need to evaluate where supporting IT functions and risks change and need updating. Machinery of Government changes have impacted ten of the 25 agencies since March 2023.

IT risks are identified and reported to senior management

All 25 agencies maintained a register of IT risks, and reported major risks to senior management outside the IT function.

Risk

Failure to identify and report significant risks and incidents reduces transparency and may lead to agencies unintentionally accepting risks that are outside their appetite.

Weaknesses in third-party IT service providers

Twelve per cent of agencies have deficiencies in their oversight of IT service providers or other organisations that are able to access their data. Gaps include failing to:

- review independent audit reports on the effectiveness of controls of a service provider
- apply information security to a service provider that handles sensitive personal data
- perform a risk assessment over all service providers used for IT services
- hold third parties accountable to meet their security obligations under agreements.

Risk

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

- interruption 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.

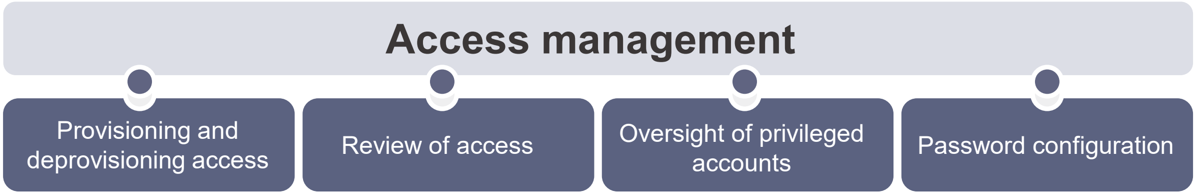
These risks can also arise from organisations not directly engaged by the agency, but which provide services to the third parties they work with. This concept is sometimes referred to as ‘fourth party risk’, reflecting that incidents at one organisation may have effects on others further up the supply chain.

Agencies should be aware of the risks arising from engaging a third party to provide services, or allowing third parties to access or store their data. Agencies should ensure that third parties are:

- obliged to maintain effective controls over their own environments
- provide a level of protection over data comparable to that if the agency still held the data
- are held accountable to meet their obligations
- applying adequate oversight to mitigate the risk of service providers to their third parties (sometimes called 'fourth party risk').

Third parties subject to a high level of oversight provide agencies with an independent assurance report detailing the effectiveness of controls over the reporting period. Agencies should ensure that weaknesses or incidents identified in these reports are responded to appropriately.

3.3 Access management



Access management

Provisioning and deprovisioning access

Review of access

Oversight of privileged accounts

Password configuration

Exhibit 8.

IT access management ensures that transactions and changes made to data are performed in the normal course of business by authorised staff.

We evaluated the following as part of the audits of all agencies in this report:

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

From the audit work performed, the following themes were identified.

Eight agencies failed to effectively restrict user access to current and approved staff

Thirty-two per cent of agencies had ineffective processes to ensure that access was approved before it was provided to users, and that access was removed promptly when no longer needed. Four lead IT agencies had ineffective processes, and two of these agencies separately manage the financial systems for another four agencies. These agencies were unable to show evidence of approval for the access provided to some users and had failed to disable all access once users had left the organisation.

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.

Agencies should ensure that access is approved before being provided and that evidence of approvals is retained.

Twelve agencies failed to effectively review and revalidate user access

Forty-eight per cent of agencies had deficiencies in their review and revalidation of user access. These gaps included:

- not keeping sufficient records to indicate the purpose or approach of the review
- only reviewing access for terminated staff accounts, but not revalidating that access was appropriate for other accounts
- commencing a process to revalidate user access, but the process remained incomplete as not all business areas had responded to confirm access remained appropriate
- not reviewing access for all key systems or for all accounts on those systems, or performing only informal, undocumented reviews
- performing reviews that did not identify access permissions in excess of requirements.

This deficiency is down from 56% in 2022 and 60% in 2021.

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
- compromising data integrity and confidentiality
- increasing the risk of unauthorised and invalid transactions.

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

Agencies are not effectively restricting and monitoring privileged users' access

Thirty-six per cent of agencies had deficiencies in their controls over privileged users' accounts. Eight lead agencies had these deficiencies, with one agency managing the system for another agency. This is unchanged from the 36% we observed in 2022.

Deficiencies included:

- using generic accounts with full system access
- failing to restrict privileged user access only to those users who require that level of access
- failing to monitor or review activity performed using privileged user accounts.

Risk

The absence of periodic reviews of privileged user accounts increases the risk that inappropriate and unauthorised activities within the system are not undetected.

Privileged user accounts may be misused 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.

Agencies should restrict the privileged user accounts, granting that level of access only on an 'as needs' basis. Agencies should regularly monitor or review activity by privileged users.

Agencies have improved compliance with their own password policies

This year, only one agency (four per cent) (28% in 2022) had not implemented password parameters in line with their own policies through system configuration.

The deficiencies repeated from prior year are:

- minimum and maximum password age not applied (such as prompting the periodic change of passwords), and no formal periodic process to manually require password changes
- use of default and generic passwords.

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 and non-financial information.

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

3.4 Change management

Change management
Testing
Authorisation
Segregating duties

Exhibit 9.

Management of IT changes ensures that changes to how programs work are in line with requirements, that unintended or unauthorised changes are not made. These management checks and reviews should be designed and enforced so they cannot be avoided, even when there is excessive access to both make and implement changes.

We evaluated the following as part of all audits for the agencies in the report:

- changes are appropriately tested before implementation to validate that systems operate as intended
- changes are authorised to ensure they are in line with business requirements and expectations, and have been adequately documented and reviewed
- duties are segregated to prevent people from making changes and then implementing them without independent approval.

From the audit work performed, the following themes were identified.

Agencies can still improve controls to better manage program changes

Twelve per cent of agencies did not segregate the developer access from the access to migrate the change into the production system. A lack of segregation allows changes to be made without an independent check, and could allow unauthorised changes to enter the production system. Where agencies allow these practices due to the small size of their specialist teams, additional governance and monitoring processes have not been implemented to reduce the risk.

This issue has improved on prior years, down from 20% in 2022 and 32% in 2021.

Risk

IT Change Management controls address the risk of unauthorised or inappropriate changes being made that undermine the integrity of financial processing or reporting.

Agencies should ensure that IT changes are appropriately tested, changes are authorised and there is a segregation of duties between those who can make changes and those who can implement changes.

Two agencies did not keep sufficient records of system implementation authorisations

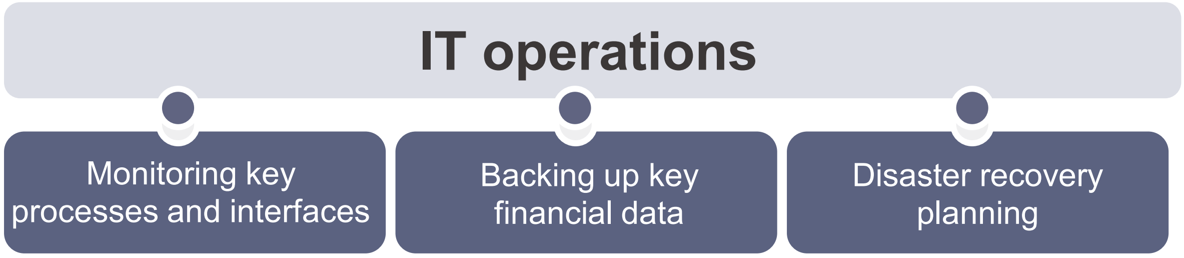
We reviewed two system implementations in the year, and in both cases, there were inadequate records to demonstrate achievement of key milestones, including successful data migration testing and approval for go-live.

Risk

> Failure to document key decisions undermines controls intended to ensure systems work as intended, and data is transferred accurately and completely.

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

3.5 IT operations



IT operations

Monitoring key processes and interfaces

Backing up key financial data

Disaster recovery planning

Exhibit 10.

Management of IT operations ensures that key IT processes operate as expected, and that interfaces between systems are complete and accurate, so there is integrity of the data and information transferred.

We evaluated the following as part of all audits for the agencies in the report:

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

From the audit work performed, the following themes were identified.

One agency needed to improve monitoring of key interfaces between finance systems

One agency did not have a control to ensure completeness and accuracy of an interface between finance systems. Our testing found discrepancies between the systems, which ought to have been synchronised if the interface was working correctly.

Monitoring is used to identify when key interfaces or batch jobs are interrupted or incomplete, and to ensure no data or transactions are missed. Interfaces and batch jobs allow for the correct calculation, reporting and processing of financial information to management, customers and suppliers.

The agency has committed to resolving this weakness by October 2023.

Risk

> Weaknesses in management and oversight of processing and interfaces risks data or transactions being unrecorded or unreported.

Four agencies do not have current disaster recovery plans (DRPs) or have not tested those plans

Sixteen per cent of agencies have deficiencies in their planning for recovering from disasters. Gaps included:

- three agencies have not tested one or more DRPs for a key finance system
- one agency does not have a DRP for a key system.

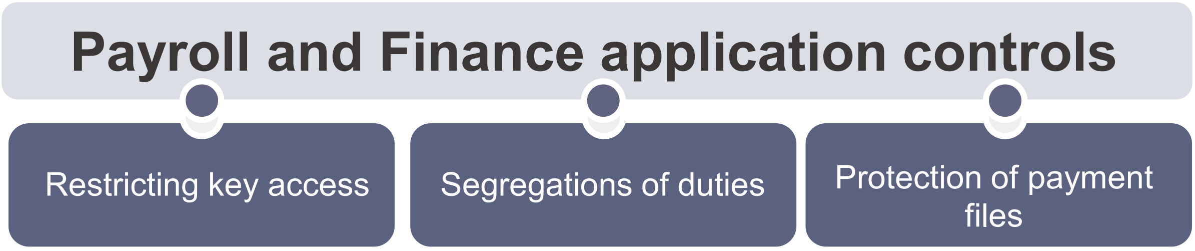
A disaster recovery plan helps agencies maintain IT services in the event of a service disruption, or restore IT systems and infrastructure in the event of a disaster or similar scenario.

Risk

Failure to effectively plan for recovery can lead to extended system outages and lost data in the event of a disaster.

Agencies should document plans to recover key systems and data in the event of a disaster, and test these plans.

3.6 Payroll and Finance application controls



Payroll and Finance application controls

Restricting key access

Segregations of duties

Protection of payment files

Exhibit 11.

There are key controls over purchasing and payroll systems that are common across most organisations.

These controls reduce the risk of unauthorised transactions or payments through those applications.

We evaluated the following as part of all audits for the agencies in this report:

- key transactions such as generating payment files are restricted to staff in appropriate roles
- segregation of duties is enforced, such as separating maintenance of masterfile data (for example, vendor bank details) and entering/approving invoices
- payment files are encrypted.

From the audit work performed, the following themes were identified.

Access is not effectively restricted for all sensitive payroll and finance system functions

Twenty-four per cent of agencies had not effectively restricted access to sensitive payroll functions only to staff who require this access to perform their role. Deficiencies at one of these agencies (a lead IT agency) impacts three other agencies. Another agency had not effectively restricted access to key transactions in its finance system only to those staff who require that level of access to perform their role.

Examples of inappropriate or excessive access include user accounts that can change rates of pay and bank account details, even though this access is not required in their roles.

Risk

Accounts with excessive access are able to perform actions that are not required for their role, and which may be inappropriate. This includes actions such as modifying bank details for employees or vendors, and raising or approving invoices.

Agencies should ensure that access to perform higher risk activities in finance systems is restricted only to users who require that level of access to perform their role.

Agencies should define what segregations of duties are required in their business processes

Twenty-four per cent of agencies have not defined the duties that should be segregated in their financial transaction processing. These six agencies comprise four lead IT agencies, with one of these agencies processing financial transactions on behalf of two dependent agencies.

Major finance applications allow for the enforcement of access rights in such a way that no single user can perform all the steps required to process certain transactions or other high-risk activities, reducing the risk of undetected fraud.

These can be configured when implementing the system, and should be based on commonly known risks as well as business-specific requirements.

Two agencies have not defined their own requirements, and have either configured segregations directly in the system without first documenting them, or have adopted the default settings in the system without considering their suitability for their business processes and risks.

We noted two agencies did not restrict all basic segregation of duties in their financial system for vendor master changes. Agencies need to review their procedures and roles so they can appropriately monitor and correct changes.

Some agencies have not implemented segregation of duties in their payroll system

Thirty-two per cent of agencies had not implemented segregations of duties over key payroll functions, with one further agency implementing due to a change in their payroll system part way through the year (but not in effect for most of the year). One of these lead IT agencies manages the payroll for three other agencies. System enforced segregation of duties in payroll can reduce the potential for fraud and error in payroll transactions by preventing errors and irregularities in the process. Enforcing this through the IT systems ensures a consistent and efficient management of this risk. Some agencies choose not to implement system-based segregation of duties, but then require additional controls to identify errors and irregularities, and corrective controls to address the errors when they are identified.

One agency had users with inappropriate access to edit the employee master file. The inappropriate users included accountants and reporting analysts who do not require access to update and edit personnel information as part of their role.

Risk

Failing to define or enforce segregations of duties can allow a single user account to perform all the steps required to process fraudulent transactions.

Agencies should define the segregations of duties applicable to their business processes, including payroll functions, and ensure these are configured so they are enforced by the finance and payroll systems.

Most agencies use encryption to ensure secure pay instructions are not modified

Twelve per cent of agencies did not encrypt payment files after being generated. One agency processes payroll on behalf of itself and two other dependent agencies covered by this report.

Files are protected by encryption while being transmitted to the bank, but before transmission, they are stored on agency systems in an unencrypted format. Banks recommend that payment files are encrypted upon generation. This reduces opportunities for the data to be changed, and also protects the confidentiality of the personal sensitive data that may be contained in those files.

One agency does encrypt some of its payment files, but not all due to technical incompatibility between the various technologies in use. They rely on reconciliations to detect any unauthorised changes, which might detect monetary changes, but is unlikely to detect changes in key fields such as account numbers.

Risk

Unencrypted payment files are more vulnerable to modification, such as fraudulently changing bank details for payees. These files also contain sensitive personal details such as rates of pay and bank details, which should be confidential.

Agencies should encrypt payment files where it is feasible to do so.

4. Cyber security

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

Section highlights

- Eighty-three per cent of maturity assessments have reported one or more Mandatory Requirements below level three, which is the level at which the requirement is self-assessed and considered to be practiced on a consistent and regular basis.
- Essential Eight maturity levels have remained unchanged or have declined, and may not be suitable for the level of risk agencies face.
- All 25 agencies reviewed have a cyber incident response plan and all but two newly created agencies tested their plan.
- Systems to detect cyber incidents across agencies could improve.
- There is a risk of under reporting cyber incidents at six agencies that kept insufficient records to support their cyber incident classifications.
- Overall, agencies need to increase their focus and prioritise efforts to ensure effective cyber security and resilience measures are in place.

4.1 Background

The threat from cyber attacks continues to rise. The Australian Cyber Security Centre (ACSC) in its Annual Cyber Threat Report (2022–23) noted 94,000 cybercrime reports, an increase of 23% on 2021–22. The average cost of each reported cybercrime has also increased, by 14% on 2021–22. That report noted that 12.9% of incidents reported to the ACSC related to State, Territory and Local Government agencies. The top 25 agencies included in this report have recognised cyber security as one of the top three risks in their enterprise risk register.

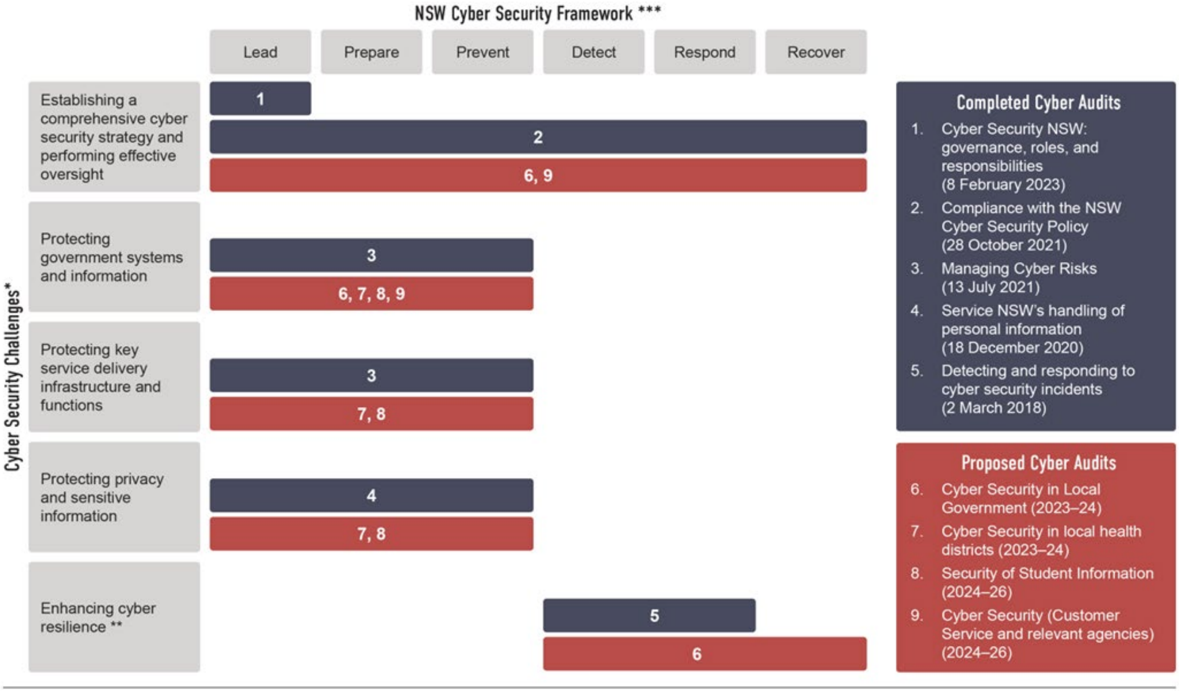
Cyber security involves using technology, processes and controls that are designed to protect IT systems and sensitive data from cyber attacks.

Cyber Security NSW (CSNSW), part of the Department of Customer Service, aims to provide the NSW Government with an integrated approach to preventing and responding to cyber security threats and attacks. CSNSW sets the policy requirements in the NSW Cyber Security Policy. The NSW Cyber Security Policy sets out 20 mandatory requirements for agencies, including implementation of the ACSC Essential Eight Strategies to Mitigate Cyber Security Incidents.

Our focus on cyber security

Our audit focus on cyber security, as explained in our Annual Work Program 2023–26, aims to provide insights into how agencies are progressing in implementing CSNSW's guidance, and how well agencies are mitigating key cyber security challenges faced by government as summarised in the following graphic.

Cyber Security Challenges guiding the focus of our Annual Work Program


NSW Cyber Security Framework ***
Lead
Prepare
Prevent
Detect
Respond
Recover
Cyber Security Challenges*
Establishing a comprehensive cyber security strategy and performing effective oversight
1
2
6, 9
Protecting government systems and information
3
6, 7, 8, 9
Protecting key service delivery infrastructure and functions
3
7, 8
Protecting privacy and sensitive information
4
7, 8
Enhancing cyber resilience **
5
6

Completed Cyber Audits

1. Cyber Security NSW: governance, roles, and responsibilities (8 February 2023)
2. Compliance with the NSW Cyber Security Policy (28 October 2021)
3. Managing Cyber Risks (13 July 2021)
4. Service NSW's handling of personal information (18 December 2020)
5. Detecting and responding to cyber security incidents (2 March 2018)

Proposed Cyber Audits

6. Cyber Security in Local Government (2023–24)
7. Cyber Security in local health districts (2023–24)
8. Security of Student Information (2024–26)
9. Cyber Security (Customer Service and relevant agencies) (2024–26)

Exhibit 12.

* Our Cyber Security Challenges have been adapted from those presented by the United States Government Accountability Office (GAO) — Cybersecurity | U.S. GAO to highlight challenges we have identified in the NSW public sector from our Financial and Performance Audits.

** When we refer to Cyber Resilience, we are aligning with the NSW Government Cyber Security Policy definition, where resilience includes incident detection, response and recovery.

*** Audits provide insights as to agencies' progress against the six Focus Areas of the NSW Cyber Security Framework, but not assurance in relation to all aspects of the framework.

Source: Audit Office Annual Work Program 2023–26, Audit Office of NSW; 17 August 2023.

Our performance audit report on Cyber Security NSW: governance, roles and responsibilities was tabled on 8 February 2023. That report found that Cyber Security NSW:

- has a clear purpose that is in line with wider government policy and objectives. However, it does not clearly and consistently communicate its key objectives, with too few reliable and meaningful ways of measuring progress toward those objectives
- does not provide adequate assurance of the cyber security maturity self-assessments performed by NSW government agencies. Department heads are accountable for ensuring their agency's compliance with NSW government policy
- has a remit to assist local government to improve cyber resilience. However, it cannot mandate action and does not have a strategic approach guiding its efforts.

The report made four recommendations. By 30 June 2023 the Department of Customer Service should:

1. implement an approach that provides reasonable assurance that NSW government agencies are assessing and reporting their compliance with the NSW Government Cyber Security Policy in a manner that is consistent and accurate
2. ensure that Cyber Security NSW has a strategic plan that clearly demonstrates how the functions and services provided by Cyber Security NSW contribute to meeting its purpose and achieving NSW government outcomes
3. ensure that Cyber Security NSW has a detailed, complete and accessible catalogue of services available to agencies and councils
4. develop a comprehensive engagement strategy and plan for the local government sector, including councils, government bodies, and other relevant stakeholders.

The Department of Customer Service accepted all four recommendations and has progressed several initiatives to fulfil them.

This report focuses on cyber security risks identified in our financial audits. Our financial audits consider cyber security planning and governance (with a focus in the current year on the detect and respond components of the NSW Cyber Security Policy), and the potential impact of incidents on the financial statements we audit.

4.2 Policy framework

The NSW Cyber Security Policy 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 NSW Cyber Security Policy is subject to annual review, which includes agency feedback. The current version of the NSW Cyber Security Policy was issued in January 2022.

The purpose of the policy is defined as:

> This Policy outlines the mandatory requirements to which all NSW Government departments and Public Service agencies must adhere to ensure cyber security risks to their information and systems are appropriately managed.

Source: NSW Cyber Security Policy, updated January 2022 ; Policy Statement | Digital.NSW.

The NSW Cyber Security Policy requires agencies to self-assess their maturity against 20 listed measures, which are named 'Mandatory Requirements', and to report this self-assessment to CSNSW. It also requires agencies to self-assess maturity against the Essential Eight and report this to CSNSW.

Under the current policy there is no assurance framework providing independent assessments of cyber security maturity.

In our Compliance with the NSW Cyber Security Policy report in 2021, we found that:

- the NSW Cyber Security Policy does not specify a minimum level for agencies to achieve in implementing the 'Mandatory Requirements' or the Essential Eight
- 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.

We recommended in that report that CSNSW monitor and report compliance with the NSW Cyber Security Policy, requiring agencies to resolve inaccurate or anomalous self-assessments where these are apparent.

The update of the NSW Cyber Security Policy is delayed

The latest policy revision for the 2023–24 reporting period was scheduled for July 2023, but has been delayed.

CSNSW advise that:

- the updated NSW Cyber Security Policy is now expected to be released by 31 December 2023
- an assurance methodology will be implemented for the FY2023–24 policy reporting period.

4.3 Maturity of cyber security

Agency cyber security maturity self-assessments for the year to June 2023 were required to be submitted to CSNSW by 31 October 2023. One hundred and ten assessments were submitted, with six agencies not submitting by the due date. One agency received an approved extension.

The six agencies who did not submit reports by 9 November 2023 were not part of the top 25 agencies as listed in the introduction. They are not included in any of the analysis for this chapter.

Maturity against Mandatory Requirements

This section of the report on maturity assessments covers all NSW government agencies that are required to report their self-assessed maturity ratings in implementing the NSW Cyber Security Policy mandatory requirements for the 2023 financial year. Detailed assessment criteria is provided in the NSW Cyber Security Policy's maturity model in relation to each requirement. The Policy's maturity model for the mandatory requirements uses the following scale:

NSW Cyber Security Policy Maturity scale

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

Note: Some requirements will vary slightly from the above maturity level principles and so it is important to reference the maturity model for specific details of each Mandatory Requirement.

Source: NSW Cyber Security Policy Maturity Model Guidance – 2022–23 Reporting Period.

Not every maturity assessment relates to a single agency:

- 7 maturity assessments are identified as aggregated, and cover more than one agency
- some requirements are performed by a lead agency on behalf of another dependent agency. Nine agencies have submitted maturity assessments as 'not applicable' where the lead agency performs or manages that requirement on their behalf. Other dependent agencies have noted that the maturity rating is inherited from the lead agency and duplicated that rating in their maturity assessment.

Agencies have not consistently implemented the Mandatory Requirements

Eighty-three per cent of maturity assessments have reported one or more Mandatory Requirements below level three, which is the level at which the requirement is self-assessed and considered to be practiced on a consistent and regular basis.

Below this level, requirements are either not performed (maturity level one), or performed only on an ad-hoc basis, or do not completely cover the scope of the requirement (maturity level two).

The only requirement reported to have been met at level three by all maturity assessments is the first requirement '1.1 Allocate roles and responsibilities as detailed in this policy'.

The requirements least often implemented above an ad-hoc level are:

- 40% of maturity assessments report level two or below for requirement 1.5 'Be accountable for the cyber risks of their ICT service providers with access to or holding of government information and systems and ensure these providers understand and comply with the cyber security requirements of the contract,' and
- 60% of maturity assessments report level two or below for requirement 3.5 'Ensure audit trail and activity logging records are determined, documented, implemented and reviewed for new ICT systems and enhancements'.

Inadequate oversight of third parties has contributed to some major Australian cyber incidents in the past year, with malicious actors exploiting control deficiencies at service providers, and using that to gain access to systems and data. The ACSC Cyber Threat Report (2022–23) states the increasingly complex ICT supply chains and advances in fields like artificial intelligence require a positive cyber security culture across business and the community. The ACSC recommends a focus on cyber supply chain risk management.

> Cyber supply chain risk management can be achieved by identifying the cyber supply chain, understanding cyber supply chain risk, setting cyber security expectations, auditing for compliance, and monitoring and improving cyber supply chain security practices.

Source: ACSC Cyber Supply Chain Risk Management updates May 2023 : PROTECT - Cyber Supply Chain Risk Management (May 2023).pdf.

The ACSC also identifies audit trails and logs as essential in helping Australian organisations contain, remediate and recover from cyber security incidents. This not only protects organisations but the ACSC sees it as crucial in helping protect others from cyber threats.

The charts below summarise the results across whole of government. This is based on agencies' own assessment of their maturity.

1. Planning and governance

Agencies must implement the NSW Cyber Security Policy mandatory requirements for cyber security planning and governance. The requirements are to: allocate cyber security roles and responsibilities; ensure there is a governance committee; develop, implement and maintain an approved cyber security plan; include cyber security in agency risk management frameworks; and be accountable for cyber risks at related ICT service providers.

The chart below details the self-assessed maturity ratings of these policy requirements on cyber security planning and governance. Maturity levels to the left of the solid vertical 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 line indicate that the requirement is practiced in at least a consistent and documented manner.

Maturity of Policy requirements

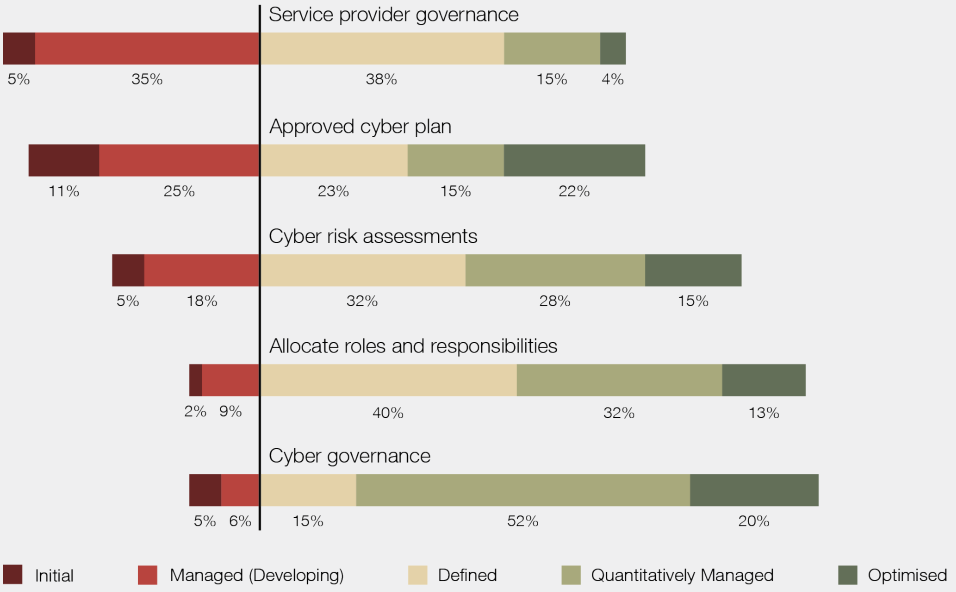


Exhibit 13.

Maturity assessments reported with a 'not applicable' maturity rating have been removed from the table and were under six per cent of returns.

Source: Individual self-assessed maturity returns against the NSW Cyber Security Policy (unaudited).

Our management letters and the NSW Cyber Security Policy Maturity Model Guidance detail the weaknesses and deliverables required to improve maturity ratings. The two most deficient measures were the same as those identified in 2022.

Forty per cent of maturity assessments were below level three (solid vertical line) for the requirement of cyber security service provider governance. Maturity levels below three are characterised by one or more of the following:

- lacked consideration for cyber security matters in procurement and contractual requirements for new and existing service providers
- had not obligated providers to report suspected or actual cyber security incidents
- had no processes to identify, assess and manage the risks of ICT service providers.

Thirty-six per cent of maturity assessments were below level three (solid vertical line) for the requirement of an approved cyber security plan that is integrated with business continuity arrangements. Maturity levels below three are characterised by one or more of the following:

- plans which were not reviewed or current
- plans did not have the appropriate level of approval by a governance committee
- plans had not identified key threats, risks and vulnerabilities
- agencies lack a capability uplift program.

2. Cyber security culture

Agencies must build and support a cyber security culture across their agency and NSW Government more broadly. The requirements are to: implement regular cyber security awareness training for all employees, contractors and outsourced ICT service providers; increase awareness and reporting of cyber security risks across all staff; foster a culture where cyber security risk management is understood, applied and drives decisions; control access for privileged access or access to sensitive or classified information; and share intelligence on security threats.

Maturity of Policy requirements

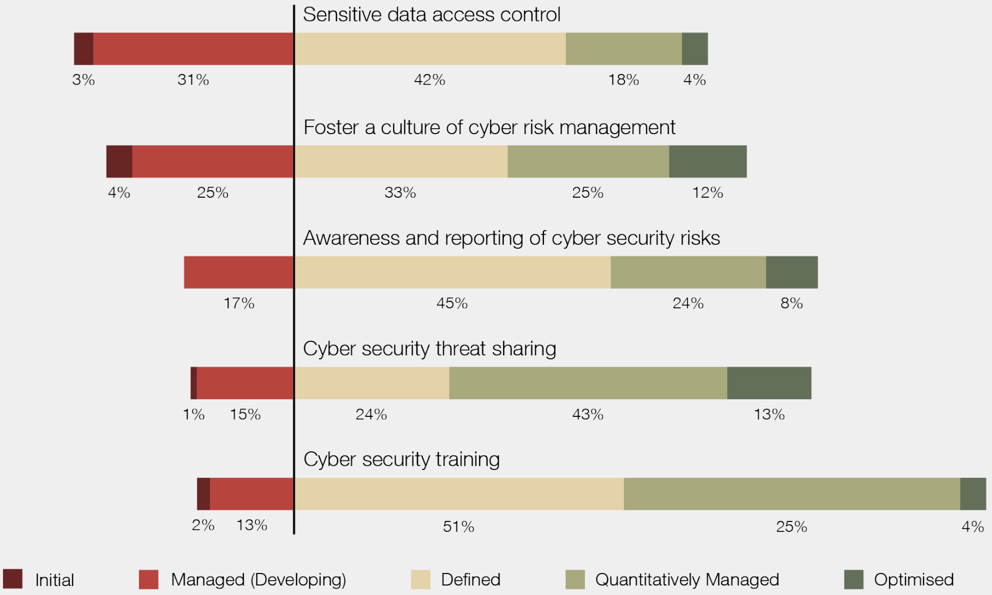


Exhibit 14.

Maturity assessments reported with a 'not applicable' maturity rating have been removed from the table and were under six per cent of returns.

Source: Individual self-assessed maturity returns against the NSW Cyber Security Policy (unaudited).

Our management letters and the Cyber Security NSW Policy Maturity Model Guidance detail the weaknesses and deliverables to improve maturity ratings. The two most deficient measures are the same as those identified in 2022.

Thirty-four per cent of maturity assessments were below level three (solid vertical line) for the requirement ensuring appropriate access controls and security screening processes are in place for people with privileged access or access to sensitive or classified information. Maturity levels below three are characterised by one or more of the following:

- no or limited ability to identify and correctly classify sensitive information
- incorrectly configured privileged access and access to sensitive information
- limited or no audit or deactivation of access as soon as operational tasks were completed.

Twenty-nine per cent of maturity assessments were below level three (solid vertical line) for the requirement to foster a culture where cyber risk management is a demonstrable factor in decision making and where cyber security management processes are understood and applied. Maturity levels below three are characterised by one or more of the following:

- limited cyber security risk assessment and analysis to IT and not the greater business
- lacked cross agency collaboration on cyber risk identification, assessment and mitigation
- lacked processes and communication for significant security incidents and issues to senior management and information owners
- did not integrate enterprise risk management and cyber security risk management.

3. Manage cyber security risks

Agencies must manage cyber security risks to safeguard and secure their information and systems, including data related to NSW citizens. The requirements are to: implement an Information Security Management System, Cyber Security Management System or Cyber Security Framework; implement the ACSC Essential Eight; classify information and systems according to their business value; ensure cyber security requirements are built into procurement and projects; and implement and review audit trail and activity logs.

Maturity of Policy requirements

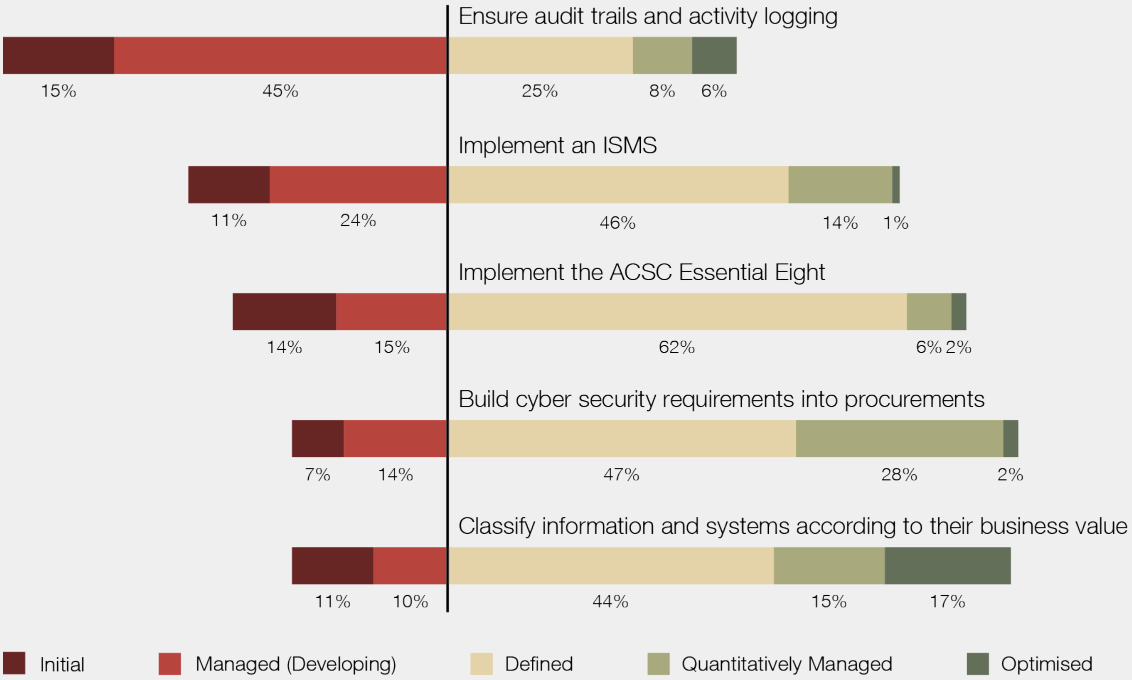


Exhibit 15.

Maturity assessments reported with a 'not applicable' maturity rating have been removed from the table and were under five per cent of returns.

Source: Individual self-assessed maturity returns against the NSW Cyber Security Policy (unaudited).

Our management letters and the Cyber Security NSW Policy Maturity Model Guidance detail the weaknesses and deliverables to improve maturity ratings. The two most deficient measures are the same as those identified in 2022.

Sixty per cent of maturity assessments were below level three (solid vertical line) for the requirement ensuring audit trails and activity logging are determined, documented, implemented and reviewed for new ICT systems and enhancements. Maturity levels below three are characterised by one or more of the following:

- limited or lack of auditing and logging of security devices, infrastructure and critical 'crown jewel' systems; and/or
- no process and defined rationale for reviewing and identifying unusual activity.

Thirty-five per cent of maturity assessments were below level three (solid vertical line) for the requirement to implement an Information Security Management System (ISMS) or Cyber Security Framework (CSF). Maturity levels below three are characterised by one or more of the following:

- the lack a documented ISMS or CSF
- the ISMS or CSF had was limited in scope and only covered the critical 'crown jewel' systems/assets
- agency risk appetite was not defined
- cyber security controls were not defined, implemented, assessed, documented or reviewed.

4. Resilience

Agencies must improve their resilience, including their ability to rapidly detect cyber incidents and respond appropriately, including to ensure critical services for NSW citizens are safeguarded. The requirements are to: have a cyber incident response plan integrated into agency incident and government cyber incident plans; exercise their cyber incident response plan annually; monitor cyber security events on ICT systems and assets; report cyber security incidents to CSNSW; and participate in whole-of-government cyber security exercises as required.

CSNSW did not perform a whole-of-government exercise for 2023. Our Cyber Resilience section expands on this later in this report.

Maturity of Policy requirements

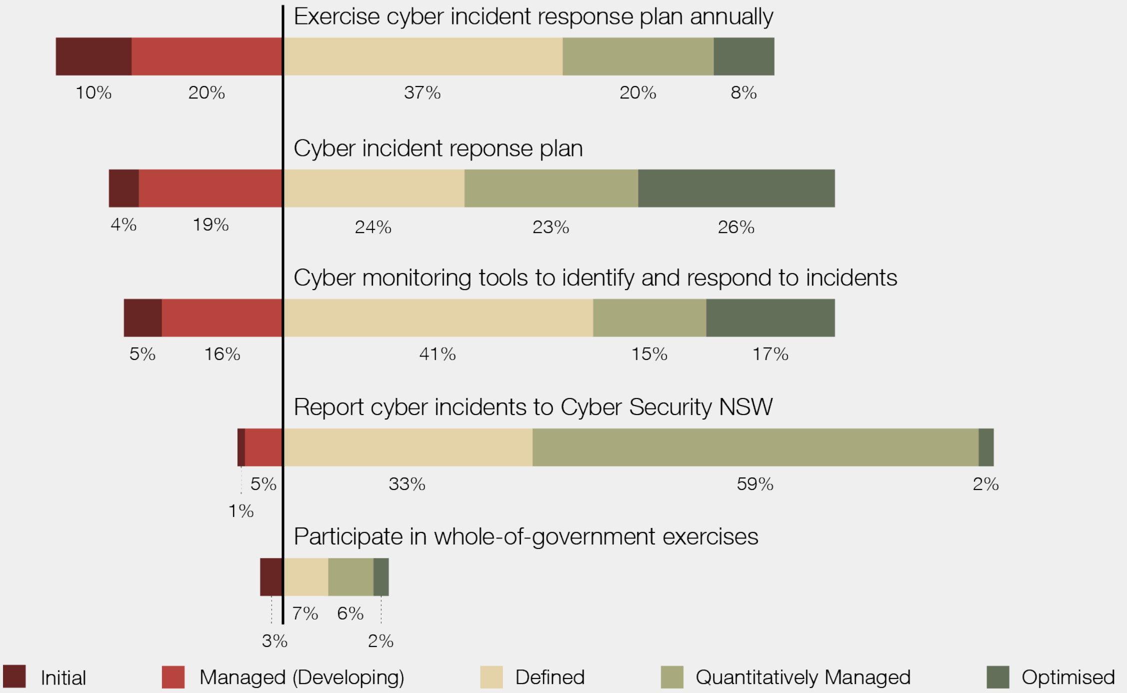


Exhibit 16.

Maturity assessments reported with a 'not applicable' maturity rating have been removed from the table. The 'not applicable' ratings were under six per cent of returns except for the participation in the whole-of government exercises.

Source: Individual self-assessed maturity returns against the NSW Cyber Security Policy (unaudited).

Our management letters and the Cyber Security NSW Policy Maturity Model Guidance detail the weaknesses and deliverables to improve maturity ratings. The two most deficient measures are the same as those identified in 2022.

Thirty per cent of maturity assessments were below level three (solid vertical line) for the requirement to exercise their cyber incident response plan at least every year. Maturity levels below three are characterised by one or more of the following:

- the lack of cyber incident response testing
- limited testing with only IT and not the business or senior management.

Twenty-three per cent of maturity assessments were below level three (solid vertical line) for the requirement to have a current cyber incident response plan that integrates with the agency incident management process and the NSW Cyber Incident Response Plan. Maturity levels below three are characterised by one or more of the following:

- no formal cyber incident response plans
- lack of integration with the enterprise incident management plans
- no analysis or reporting of cyber security events or incidents to senior management.

Maturity against Essential Eight

Cyber is a ubiquitous risk. Responding to cyber risk is challenging for agencies as the environment is highly dynamic. A pragmatic and proportional response to the risk each agency faces is required, given the most appropriate strategies, controls and safeguards are constantly evolving. This needs to be kept in mind when considering the following reporting on the Essential Eight. The Essential Eight Maturity Model itself keeps changing, introducing new requirements, and changing or dropping others. Therefore, reporting on maturity and the setting of target maturities has its limitations. However, at an aggregate level, the following information is insightful as to how the sector is responding to the risk of cyber.

The Australian Cyber Security Centre (ACSC) periodically updates the Essential Eight maturity model in response to the observed techniques in use by malicious actors.

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

Essential Eight Maturity Model

- 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.

Source: Summary of ACSC Essential Eight Maturity Model, November 2023 | Cyber.gov.au.

The ACSC suggests that:

> Generally, Maturity Level One may be suitable for small to medium enterprises, Maturity Level Two may be suitable for large enterprises, and Maturity Level Three may be suitable for critical infrastructure providers and other organisations that operate in high threat environments.

Source : ACSC Essential 8 Maturity Model FAQ, 21 September 2023 Essential Eight Maturity Model FAQ | Cyber.gov.au.

Essential Eight controls were reported to CSNSW on outdated requirements

New South Wales agencies were required to assess their cyber maturity at 30 June 2023 against the October 2021 version of the ACSC Essential Eight maturity model, though it has been superseded. Six of the eight Maturity requirements remained unchanged in the November 2022 update. CSNSW advise that an assessment against the former model allows direct comparability with previous years and visibility on year-on-year trends.

The ACSC however, strongly encourage organisations to use the latest version:

> legacy versions of the E8MM will often no longer be fit for purpose due to the continual evolution of tradecraft used by malicious actors.

Source : ACSC Essential 8 Maturity Model FAQ, 21 September 2023 Essential Eight Maturity Model FAQ | Cyber.gov.au.

The NSW Cyber Security Policy recognises the ACSC's Essential Eight has regular updates as a baseline of mitigation strategies and encourages agencies to refer to the latest version. CSNSW advise they are in discussion with the ACSC and will update the NSW Cyber Security Policy in consideration of the current and future Essential Eight models, its limitations and how to set the best minimum standards for agencies.

Recommendation

Agencies’ Essential Eight maturity reporting to CSNSW should be measured against the latest version of the ACSC Essential Eight Maturity model.

Essential Eight maturity levels have remained unchanged or have declined

The median reported maturity shows no improvement in agencies' implementation of the Essential Eight controls since the introduction of the reporting requirement, and there has been a decrease in median maturity reported for patching operating systems and restricting administrative privileges.

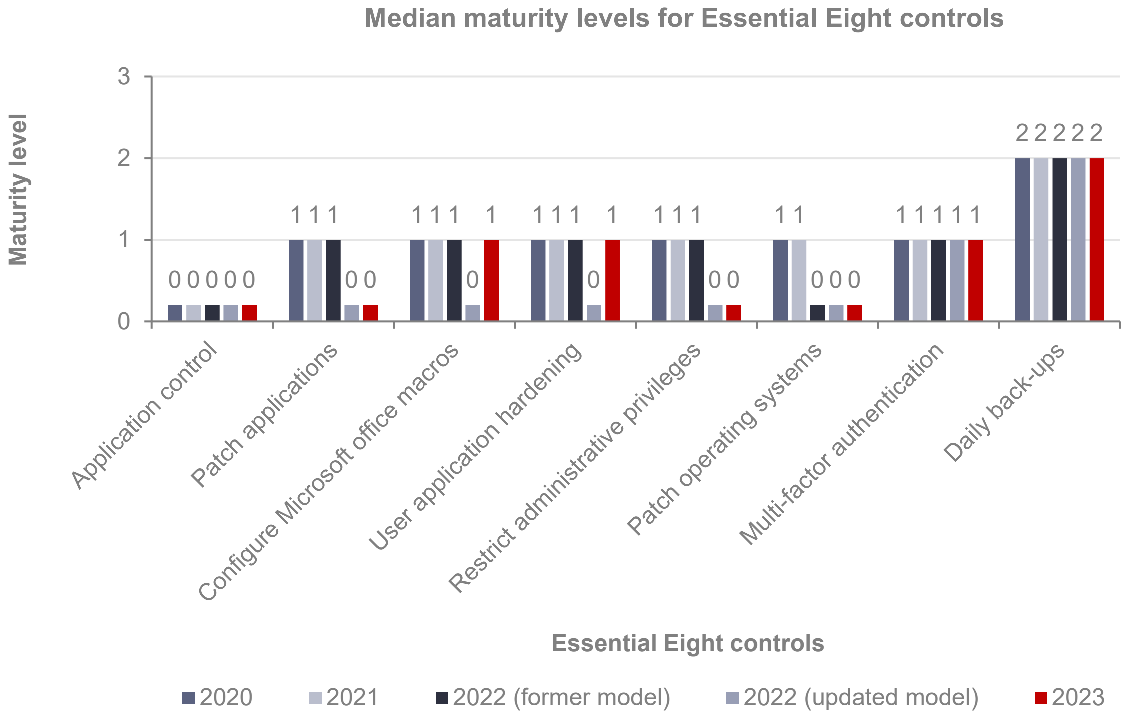


Exhibit 17.

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

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

Maturity against some Essential Eight strategies has decreased

The table below reports the maturity levels of NSW government agencies reported in implementing the former model of the Essential Eight cyber risk mitigation controls, using the previously mentioned scale from zero to three. The movement indicator shows whether there has been an overall increase or decrease in maturity levels from 2022 based on the relative percentages of self-assessments in each maturity level.

Number of self-assessments for 2023

Essential Eight controls	Maturity level zero	Maturity level one	Maturity level two	Maturity level three	Total*	Movement indicator compared to 2022**
Application control	56	36	10	4	**106**	▲
Patch applications	68	26	7	7	**108**	▼
Configure Microsoft Office macros	51	27	24	4	**106**	▲
User application hardening	51	45	8	2	**106**	▼
Restrict administrative privileges	63	35	7	2	**107**	▼
Patch operating systems	65	26	11	5	**107**	▼
Multi-factor authentication	44	44	15	4	**107**	▲
Daily back ups	19	27	40	22	**108**	▲

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

** Movement indicator shows an increase if the relative proportion of total self-assessments in Levels Two and Three have increased in 2023 compared to 2022. The indicator shows a decrease if the relative proportion of total self-assessments in Levels Two and Three have decreased in 2023 compared to 2022.

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

There has not been a consistent improvement in maturity across agencies, with half of the controls showing only small improvements, while half have decreased. Decreased maturity was reported for patching, application hardening and managing administrative privileges. As highlighted in section 3.3 above, we continue to report control deficiencies in restricting and monitoring privileged access at agencies, and these findings need to be addressed by the agencies as a priority.

Recommendation

As reported in both 2021 and 2022, agencies need to prioritise improvements against the NSW Cyber Security Policy as a matter of urgency.

Essential Eight maturity may not be suitable for the level of risk agencies face

Eighty-five per cent of maturity assessments have not reached level one maturity across each of the Essential Eight. Maturity level one is recommended by the ACSC for small to medium enterprises to address threat actors with low sophistication and using commonly available tools.

Maturity level one

The focus of this maturity level is malicious actors who are content to simply leverage commodity tradecraft that is widely available in order to gain access to, and likely control of, a system. For example, malicious actors opportunistically using a publicly-available exploit for a vulnerability in an internet-facing service that has not been patched, or authenticating to an internet-facing service using credentials that were stolen, reused, brute-forced or guessed.

Generally, malicious actors are looking for any victim rather than a specific victim and will opportunistically seek common weaknesses in many targets rather than investing heavily in gaining access to a specific target. Malicious actors will employ common social engineering techniques to trick users into weakening the security of a system and launch malicious applications. If the accounts compromised by malicious actors have special privileges, they will exploit them. Depending on their intent, malicious actors may also destroy data (including backups).

Source: ACSC Essential Eight Assessment Process Guide, 14 August 2023 Essential Eight Assessment Process Guide | Cyber.gov.au.

Ninety-four per cent of maturity assessments have not reached level two maturity across each of the Essential Eight. Maturity level two is recommended for large enterprises to address more capable threat actors using common techniques. We consider large departments, particularly those involved in service delivery to NSW citizens and those that hold data related to NSW citizens to be large enterprises.

Maturity level two

The focus of this maturity level is malicious actors operating with a modest step-up in capability from the previous maturity level. These malicious actors are willing to invest more time in a target and, perhaps more importantly, in the effectiveness of their tools. For example, these malicious actors will likely employ well-known tradecraft in order to better attempt to bypass controls implemented by a target and evade detection. This includes actively targeting credentials using phishing and employing technical and social engineering techniques to circumvent weaker methods of multi-factor authentication.

Generally, malicious actors are likely to be more selective in their targeting but still somewhat conservative in the time, money and effort they may invest in a target. Malicious actors will likely invest time to ensure their phishing is effective and employ common social engineering techniques to trick users into weakening the security of a system and launch malicious applications. If accounts compromised by malicious actors have special privileges, they will exploit them, otherwise they will seek accounts with special privileges. Depending on their intent, malicious actors may also destroy all data (including backups) accessible to an account with special privileges

Source: ACSC Essential Eight Assessment Process Guide, 14 August 2023 Essential Eight Assessment Process Guide | Cyber.gov.au.

Just one assessment of the 110 has reported that it has implemented all of the Essential Eight at level three. This maturity level is recommended for organisations that operate in a high threat environment, and is appropriate to address more sophisticated and targeted attacks from well funded and organised groups. This is an agency with fewer than 50 staff and an ICT budget under $300,000.

Target maturity across government

In 2022, agencies reported their target maturity for 2023 against the Mandatory Requirements and the Essential Eight, along with their assessed maturity level.

Agencies are targeting low levels of maturity

Target maturity for June 2024 remains low for many agencies. Of the 110 maturity assessments:

- 45 agencies (41%) have a target of below three for one or more Mandatory Requirements (this was 36% in 2022)
- 26 agencies (24%) have a target of zero for one or more Essential Eight (this was also 24% in 2022)
- 72 agencies (65%) have a target of below two for one or more of the Essential Eight (this was 64% in 2022).

Target maturity for the largest agencies

Due to changes in Machinery of Government and other changes in how agencies report, as well as the limited applicability of the Essential Eight for some types of systems, not all in-scope agencies have comparable data across 2022 and 2023. We identified 23 agencies that have reported comparable data for the Mandatory Requirements, and 21 agencies that have comparable data for the Essential Eight.

We compared the 30 June 2023 targets reported in 2022 with the current maturity reported in 2023 for these agencies.

No agency met all their June 2023 Mandatory Requirement maturity targets

Of the 23 agencies with comparable data, none of them reported meeting all their targets for 2023, as reported in 2022, against all the Mandatory Requirements.

All agencies had met their target for at least one of the requirements, and on average agencies reported 11.5 of the 20 requirements (57%) at or above the target they set for 2023, with 8.5 requirements (43%) below target.

No agency met all their June 2023 maturity targets for the Essential Eight

Of the 21 agencies with comparable data, none reported their current 2023 maturity at or above the target set in 2022, against all of the Essential Eight.

Three agencies (14%) had not met their 2023 target for any of the Essential Eight, and 18 had met their target for at least one of the Essential Eight.

On average, agencies reported 3.4 of the eight requirements (42%) at or above their reported 2023 target, with 4.6 requirements (58%) below target.

As reported in 2022, 92% of the 25 in-scope agencies had approved plans and 88% of agencies had approved budgets to meet these targets.

Recommendation

Agencies need to do more to ensure their uplift plans deliver measurable improvements in cyber security.

4.4 Cyber resilience

Importance of cyber resilience

Consistent with contemporary audit practices, our audits are increasingly considering cyber security as part of our financial statement audits, recognising that cyber incidents have the potential to have material financial impacts, as well as the importance of protecting delivery of public services to NSW citizens, and the sensitive data agencies hold.

An important aim of cyber security is to minimise the likelihood that systems will be compromised. However, even organisations with highly developed and mature cyber controls cannot eliminate the risk from sophisticated and well resourced attackers.

According to the ACSC:

> Australian organisations are frequently targeted by malicious cyber adversaries. The ACSC's assessment is that malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, and sophistication. As adversaries become more adept, the likelihood and severity of cyber attacks is also increasing due to the inter connectivity and availability of information technology platforms, devices and systems exposed to the internet.
>
> … While many of the incidents reported to the ACSC could have been avoided or mitigated by good cyber security practices, such as implementation of ASD's Essential Eight security controls, risks will still remain when organisations operate online.

Source: Cyber Incident Response Plan | Cyber.gov.au sourced online on 3 September 2023.

Therefore organisations must be prepared to identify when a cyber incident occurs, and be able to respond to cyber incidents to contain any compromises and minimise the impact. This preparedness to respond to cyber incidents can be described as cyber resilience.

This is even more important for organisations with low levels of maturity in their preventative cyber security controls, including many of the agencies covered by this report.

The following sections of this report focus on the cyber resilience component in the NSW Cyber Security Policy, which describes five 'Mandatory Requirements':

LEAD PREPARE PREVENT DETECT RESPOND RECOVER

4	Agencies must improve their **resilience** including their ability to rapidly detect cyber incidents and respond appropriately. Agencies must:
4.1	Have a current cyber incident response plan that integrates with the agency incident management process and the *NSW Government Cyber Incident Response Plan*.
4.2	Exercise their cyber incident response plan at least every year.
4.3	Ensure that ICT systems and assets are monitored to identify cyber security events and verify the effectiveness of protective measures.
4.4	Report cyber security incidents to their cluster CISO and/or Cyber Security NSW according to the *NSW Cyber Security Response Plan.* If relevant, ensure incident reporting is compliant with Federal reporting requirements.
4.5	Participate in whole-of-government cyber security exercises as required.

Exhibit 18.
Source: NSW Cyber Security Policy.

Cyber Incident Response Plans

The NSW Cyber Security Policy states that agencies must have a current cyber incident response plan, which integrates with the agency incident management process and the NSW Government Cyber Incident Response Plan. These plans should prepare agencies to identify and respond to cyber incidents when they occur, and minimise the impact to the agency and its stakeholders.

One agency has not developed their own Cyber Incident Response Plan

All 25 agencies have a cyber incident response plan.

One agency relies on the NSW Cyber Incident Plan and did not tailor this plan for their own agency. However, they use the Plan as a framework and tailored their supporting incident responses. Apart from this agency, the remaining 24 agencies integrated their agency incident management plans with the NSW Government Cyber Incident Response Plan.

The use of the standard NSW Cyber Incident Plan may not meet the operating requirements, risk appetite and threats specific to each agency. This could affect the scope and ability for an agency to adequately respond to an incident.

Some plans do not consider vendors in their Cyber Incident Response Plan

Twelve per cent of cyber incident response plans did not specify vendors in the response to cyber incidents.

Excluding vendors out of the incident response may weaken containment objectives and increase the outage of business operations. Vendors may include IT service providers and business suppliers, both within government and from the private sector.

Agencies should specifically include vendors in their cyber incident response plans.

Three agencies have documented incident responses for only one cyber security scenario

We noted 12% of agencies have detailed incident procedures and responses for only a ransomware scenario in their playbook. Playbooks are documented incident responses that are tailored to address plausible cyber security incidents, and support the cyber incident response plans. Playbooks could cover scenarios such as (but not limited to) denial of service attacks, website defacement, compromise by an external attack, phishing and data breaches. Cyber security playbooks allow agencies to have a planned and standardised approach for responding to these plausible cyber security scenarios.

Agencies without a broad range of playbooks may need to identify key stakeholders, IT systems and networks, and establish their response, containment and recovery processes during an incident, potentially delaying the response and increasing the severity of the incident.

Testing or exercising Cyber Incident Response Plans

The NSW Cyber Security Policy requires that agencies exercise their cyber incident response plan at least every year. Performing a cyber incident response exercise increases stakeholder familiarity with the plan, and validates that the plan will operate. It also gives an opportunity to identify gaps or deficiencies in the plan which can be remediated.

Testing of Cyber Incident Response Plans is key to identifying improvement areas

Testing or activation of the Cyber Incident Response Plan varied across the 21 agencies during 2022–23.

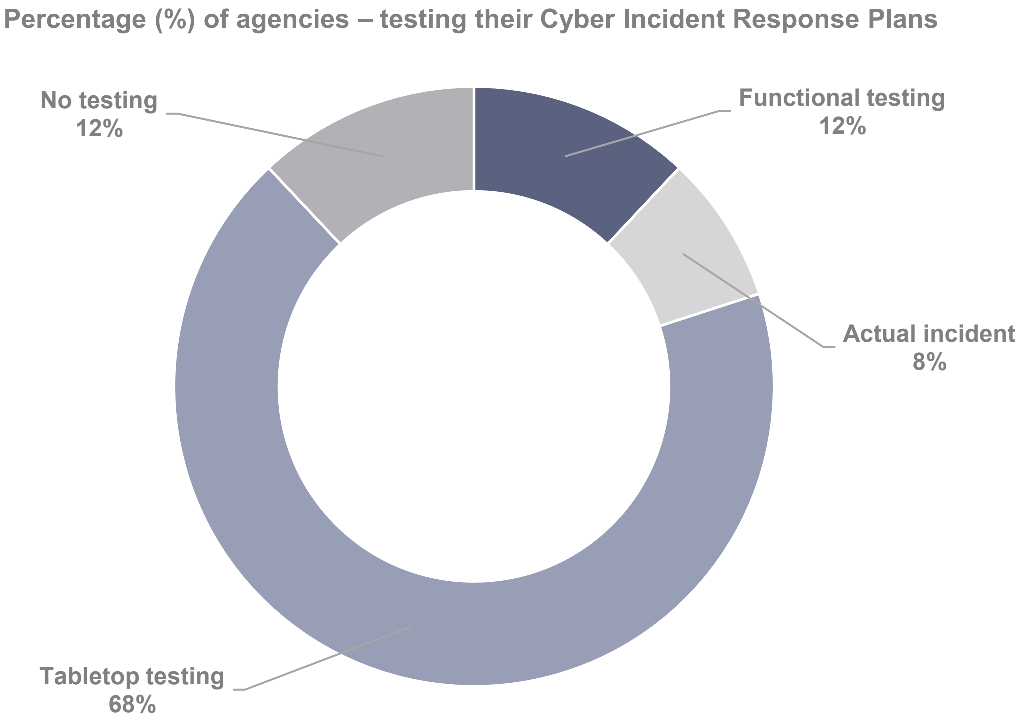


Exhibit 19.

Source: Audit Office analysis.

Tabletop testing is where key personnel meet to discuss and talk through a scenario and test plan details. Functional testing for the sampled clients included interactive exercises on a simulated IT environment with investigation of data, analysis and output of communications.

The two agencies that did not exercise or test their cyber incident response plans advised they were newly formed or had a new team. Both agencies intend to test their plan by 2024.

We noted 23 agencies that tested or activated their plans had identified potential improvements, and had documented their learnings from the exercises. Two of these agencies identified significant gaps:

- One of the tabletop test exercises had major failings in responsibility definition, protocols for forensic engagement and had not defined restoration timeframes. This exercise involved two participating agencies.
- The other agency had significant failings when testing their Cyber Incident Response Plan. Their test noted an inadequate plan, where the team deferred to draft or ad hoc processes. This resulted in confusion and several decision stalemates. This agency revised and updated their plan after the test.

Recommendations

All agencies need to:

- **regularly test their cyber incident response plans**
- **use tests that challenge the completeness and useability of the plan, the capability of agency response teams and supporting third-party providers**
- **maximise the identification of learnings and potential plan improvements through the testing exercise.**

No whole-of-government exercise was performed in 2022–23

Our 2023 report on Cyber Security NSW: governance, roles, and responsibilities reported that:

The foundations of Cyber Security NSW stem from the appointment of the Government Chief Information Security Officer in March 2017, which served the same high-level purpose of supporting government online service delivery. This role had four high-level 'pillars' to guide activity:

- coordinating the annual cyber security exercise program
- implementing the NSW Cyber Security Policy
- expanding the cyber security intelligence capability of the State
- cultural uplift and awareness raising.

The first pillar was the conduct of an annual cyber security exercise. The last whole-of-government exercise was conducted in two parts, in April and September 2021.

CSNSW advise that no exercise was performed due to the caretaker period and changes to government, and reviews of the State Emergency Management Plan and the State Emergency Sub Plan.

For policies to be effective they should be implemented as prescribed for good governance.

Monitoring systems to identify cyber incidents

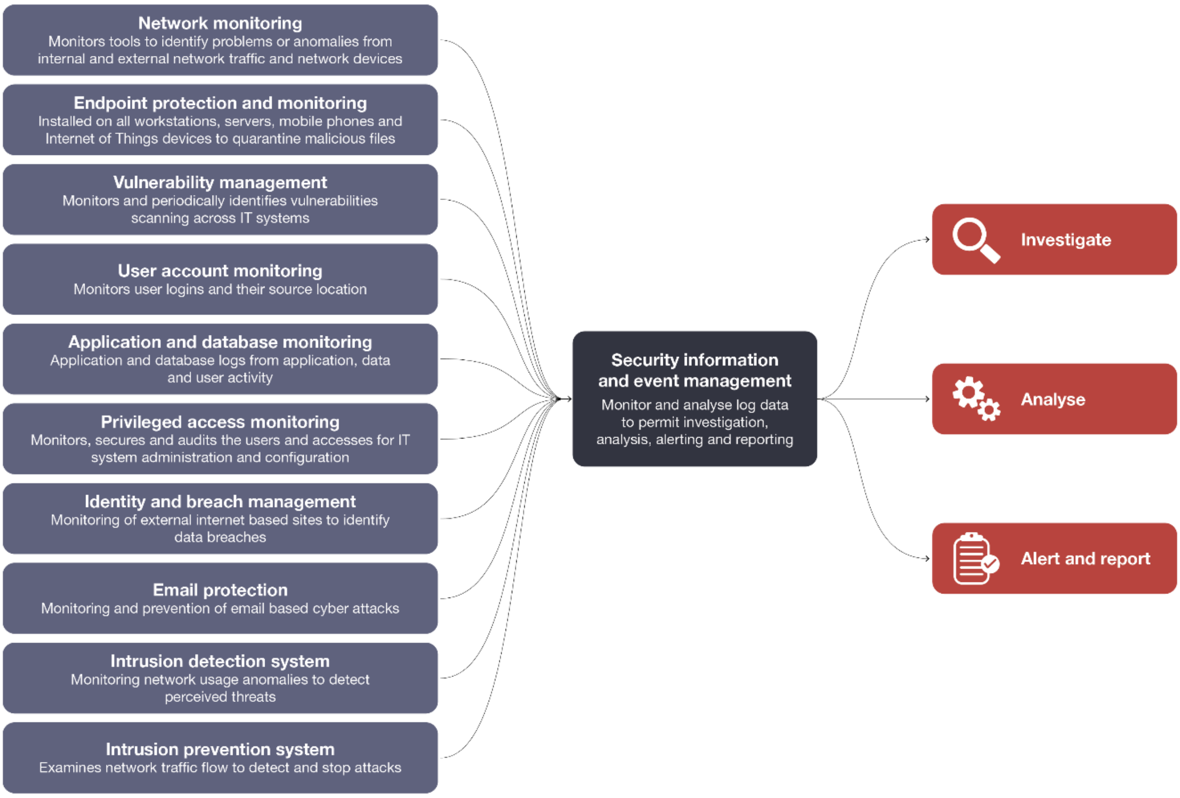
Agencies use monitoring systems to detect cyber security issues. These monitoring systems may monitor events, threats and vulnerabilities across IT systems, networks and users.

The NSW Cyber Security Policy requires that agencies ensure that ICT systems and assets are monitored to identify cyber security events and verify the effectiveness of protective measures. There is no specific direction or requirement on what monitoring should be in place.

Without effective monitoring systems, agencies are at greater risk of not identifying all cyber incidents, and maybe unable to respond adequately to minimise the impact of cyber incidents.

Observed cyber security event monitoring systems

Below is a flowchart of the typical monitoring systems we have observed in use by some agencies and what their purpose is. It shows the flow of different types of data collected across the IT systems, how they work together and the information and analysis that cyber security teams may obtain from their cyber security monitoring systems.



Network monitoring
Monitors tools to identify problems or anomalies from internal and external network traffic and network devices
Endpoint protection and monitoring
Installed on all workstations, servers, mobile phones and Internet of Things devices to quarantine malicious files
Vulnerability management
Monitors and periodically identifies vulnerabilities scanning across IT systems
User account monitoring
Monitors user logins and their source location
Application and database monitoring
Application and database logs from application, data and user activity
Privileged access monitoring
Monitors, secures and audits the users and accesses for IT system administration and configuration
Identity and breach management
Monitoring of external internet based sites to identify data breaches
Email protection
Monitoring and prevention of email based cyber attacks
Intrusion detection system
Monitoring network usage anomalies to detect perceived threats
Intrusion prevention system
Examines network traffic flow to detect and stop attacks
Security information and event management
Monitor and analyse log data to permit investigation, analysis, alerting and reporting
Investigate
Analyse
Alert and report

Exhibit 20.

Source: Audit Office analysis.

System monitoring for cyber incidents is varied across agencies

All 25 agencies have automated monitoring systems deployed to detect cyber security events. Agencies use multiple systems to monitor and evaluate these security events.

The scope of monitoring systems in place varies:

- some agencies cover their email account usage, server activity and network traffic with one suite of monitoring tools
- other agencies monitor all servers, workstations and mobile devices using multiple tools.

Agencies have increased the types of activities being monitored, and the number of systems being monitored during the year.

There is a varied capability to identify, triage and follow up incidents. Automation is being used to identify cyber security events. Events are being logged in industry standard systems, usually with artificial intelligence to feed into manual analysis, and interfaced incident escalation from externally managed security providers where relevant. One agency has automated their triaging for approved and standard cyber security events, which closes low priority incidents. Agencies retain internal security operations to analyse and triage moderate and high-risk incidents, sometimes in combination with their managed security service providers (MSSP).

The varied range in agencies' monitoring capability should reflect different risks, systems, and information held by individual agencies.

Risk

Limitations in coverage and capability of monitoring systems increases the likelihood that an intrusion or other cyber incident will go undetected, and therefore will not be contained. Timely identification of cyber incidents is critical to limiting the opportunity for loss of sensitive data and disruption to services.

Agencies should continue to expand the monitoring systems and type of activities being monitored.

Integration and performance issues with service providers can hinder effective cyber incident detection and response

The ability to build cyber security capability has been limited by a shortage of expertise that affects the cyber security industry, in both public and private sectors. Agencies utilise different resourcing models to enable this capability, and all agencies have internal security functions, with some supported by external providers.

Seventy-two per cent of agencies use managed security service providers (MSSP) to supplement their internal security operations teams. Integration between internal security operations and MSSPs varies, with some having interfaced incident management and some manually logging significant MSSP incidents into their internal systems. One agency assessed that their needs could be better achieved by establishing an internal function to replace a MSSP, highlighting the challenges that agencies can face in establishing an effective resourcing model.

Integration and performance issues can reduce the ability of agencies to identify, contain and respond to cyber security incidents in a timely and appropriate manner.

Risk

Workforce and capability gaps can reduce the effectiveness of detecting and responding to cyber incidents. Inadequate management of or integration with a third-party provider can also create gaps or misaligned expectations, resulting in less effective detection and response to cyber incidents.

Agencies should ensure they have the appropriate level of resources and capability, supported by robust and reliable processes across internal and external teams.

Three agencies have only recently implemented monitoring systems on key operational systems

NSW government agencies provide a number of essential services for NSW citizens, many of which depend on IT systems which were designed before cyber security became a significant concern or are not compatible with industry standard monitoring tools.

We noted three agencies only recently established cyber security monitoring on IT systems for their main operations even though those IT systems have been in place for several years:

- One agency only established their cyber security operations centre for their operational systems in early 2023. The delay was due to contractual gaps identified between the agency and the service provider. This required 18 months to design and establish the security architecture, monitoring systems and resource the security operations team.
- The second agency only setup the monitoring systems in 2022 and was still implementing them across the operational systems. Delays were caused by the need to update the security architecture and shift IT systems to current industry standard platforms.
- The third agency is still establishing monitoring systems to cover their key operational system.

Failure to adequately monitor these operational systems for cyber incidents could leave these IT systems vulnerable to attacks and outages. This could severely hinder or interrupt business operations or the provision of essential services.

Agencies should focus resources on supporting cyber security coverage on operational systems despite the complexities of dated systems.

Identifying incidents and activating the Cyber Incident Response Plans

The NSW Cyber Security Policy defines a cyber incident as:

> An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.

Criteria has been provided to classify incidents, and this has been adopted by all of the agencies in scope for this report. While there is some subjectivity in applying the criteria, examples are also provided to assist agencies correctly classify incidents.

Insufficient records kept to support incident classifications at six agencies

Twenty-four per cent of agencies have not kept records to show how they have determined classifications for potential cyber incidents. These agencies had detected events through their monitoring tools, which appeared to match the examples of cyber incidents in the classification criteria. From the records available it was not possible to determine why these had not been regarded as incidents. Examples identified included malware found to be spreading in an agency's IT environment, and a case of ransomware activated on an employee computer. Since these were not classified as incidents, the cyber incident response plans were not activated or followed.

One agency failed to identify any cyber incidents during the year despite having a well resourced cyber security function and extensive monitoring tools deployed. Failing to correctly identify a cyber incident increases the risk of under reporting cyber incidents and could limits the opportunity to respond appropriately to minimise the impact of those incidents.

Recommendations

Agencies should keep sufficient records to demonstrate that they are applying their cyber incident classification criteria in a consistent way.

There is a varied capability for agencies to follow their incident management plans for user identified cyber security events

Sixteen per cent of agencies had not followed their cyber incident response plans when analysing and responding to user identified cyber security events. User identified security events are incidents that are identified manually by personnel and raised as cyber security event.

Issues identified included:

- an incorrect low-risk rating on a compromised user account
- no root cause analysis for a compromised user account
- inadequate investigation and documentation of phishing incidents before resolving and closing tickets
- an agency did not close the incident tickets for four of the five sampled cyber security events, although there was timely resolution and remediation of the event
- a ransomware incident that was closed without investigation.

Agencies not following the cyber incident response plans may expose systems and data to cyber threats without appropriate analysis. This could result in unknown breaches and the unnecessary spread of cyber threats and attacks within the agencies' IT environment.

Agencies need to ensure cyber security events are identified, analysed and have appropriate responses.

5. Governance framework

Governance in the context of the NSW public service refers to the structures, processes, and mechanisms by which government departments and agencies are held to account when they make decisions and implement policies and programs in the service of the public interest. It also includes the principles and practices that guide how these agencies work together.

This chapter outlines our audit observations, conclusions and recommendations from our review of agencies' governance frameworks and practices, with consideration of NSW Treasury issued policies and best practices. It focuses on two key areas: governance arrangements and risk management.

Section highlights

- Whilst agencies have generally adopted governance and risk management frameworks that align with Treasury issued policies and best practices, we noted deficiencies, including:
  - 20% of governing boards operated without a board charter
  - 16% of agencies had risk management policies that were beyond their scheduled review date
  - 16% of agencies did not have a risk appetite statement
  - 28% of agency internal audit functions have not been externally evaluated in the last five years.
- Agencies should perform periodic assessments/reviews of their risk maturity and implement action plans where required.

5.1 Governance arrangements

The NSW public sector is divided into ten portfolios (groups of agencies), each overseen by a Secretary. Section 1.1 above lists the agencies included in this report by portfolio. The Cabinet Office NSW publishes a Governance Chart of the NSW portfolio arrangements.

Governing boards

Twenty per cent of governing boards operate without a board charter or terms of reference

Agencies operate under varied governance structures, with 40% of agencies having governing boards, while the remainder operate directly under their department executive.

Our review of the board arrangements noted the following:

Percentage (%) of boards	
20	operate without a board charter or terms of reference
25	of charters did not explicitly state the responsibilities of the board (with regard to decision-making) compared to responsibilities of management
30	do not periodically evaluate their performance against defined criteria
40	were not chaired by an independent member

Source: Audit Office analysis.

A board charter is an important policy document that describes the objectives, functions and governance of the board, including how it interacts with management. The charter is essential to ensuring smooth operation of the board and should incorporate a requirement for the board's performance to be periodically evaluated.

Remuneration committees

Most agencies do not have remuneration committees

Only two agencies had remuneration committees, with most agencies operating under industrial award agreements.

Remuneration committees are used to independently oversee and make decisions with regards to salaries and allowances for executives and senior management. Our review of the remuneration committees noted they were comprised of two to three members who were independent, including the Chair.

Organisational structures and capability frameworks

Twenty-eight per cent of agencies' organisational structures do not disclose gaps in personnel such as vacancies

Organisational structures provide a framework on how an agency is organised to achieve its objectives. The structure defines the hierarchy of staff within the agency and their roles and responsibilities within the overall structure. At a granular level, staff capability frameworks outline the responsibilities of individual roles.

Our review noted the following:

Percentage (%) of agencies	
100	have implemented a staff capability or equivalent framework that outlines employee roles and responsibilities. In most cases, agencies have adopted the NSW Public Service Capability framework
100	have developed an organisational structure
28	of organisational structures did not outline known gaps in personnel, such as vacancies
30	of agencies do not regularly report gaps in personnel to those charged with governance

Source: Audit Office analysis.

Periodic reporting of known gaps in personnel to those charged with governance is essential to ensuring key decision-makers are able to address critical gaps. An adaptable organisational structure is one tool that can be used to supplement such reporting.

Code of ethics and conduct

All agencies have established a code of ethics and conduct; some were deficient

Our review noted all agencies implement a code of conduct (code) to provide clear guidelines and rules to staff and to set the ethical, integrity and professional standards within the agency. While all staff are required to sign the code upon induction, we noted the following:

Percentage (%) of agencies	
28	did not require ongoing annual reviews and confirmation of adherence to the code
16	did not include third-party vendors within the code or in their statement of business ethics
20	had not reviewed their code by the schedule review date

Source: Audit Office analysis.

Agencies should ensure their codes extend to contractors and third-party vendors as necessary and are reviewed and confirmed by all personnel on a periodic basis.

5.2 Risk management

Risk management is an integral part of effective corporate governance. It helps agencies to identify, assess and prioritise risks and in turn minimise, monitor and control the impact of unforeseen events. It can also allow agencies to better respond to opportunities that may emerge and improve their services and activities.

The Treasury Policy Paper TPP 20-08 Internal Audit and Risk Management Policy for the General Government Sector (TPP 20-08) is a mandatory policy issued by NSW Treasury to assist agencies to meet their legislative obligations under the *Government Sector Finance Act 2018* (GSF Act), and outlines minimum standards for risk management, internal audit and Audit and Risk Committees. The policy's core requirements are founded on Australian Standard AS ISO 31000: 2018 Risk Management Guidelines.

Risk management policies and frameworks

All agencies have developed risk management policies and frameworks, however three were beyond their scheduled review date

Our review of agencies' risk management policies and frameworks noted:

- whilst all agencies have developed risk management policies to comply with TPP 20-08, four were beyond their scheduled review date
- all agencies have developed risk management frameworks (or equivalent) to comply with TPP 20-08
- 1 agency is yet to evaluate the structure and effectiveness of its risk management arrangements against the requirements of TPP 20-08 as it has only existed in its current form for less than 12 months. Two agencies have not assessed their arrangements within the last two years
- all but one agency adopted the 'three lines model' as outlined in TPP 20-08
- all but one agency completed annual attestations stating compliance with TPP 20-08 in the last 12 months.

Risk management policies and frameworks are critical to supporting organisations in their dealings with risks. A strong framework enables agencies to identify and assess key risks and enables decision makers to respond to these risks in a timely manner.

Risk maturity

NSW Treasury developed TPP 20-06 Treasury Risk Maturity Assessment Tool Guidance Paper (TPP 20-06) to support the improvement of risk management, culture and capability across the NSW public sector.

The Treasury Risk Maturity Assessment Tool (the Tool) is designed to support the improvement of risk management, culture and capability across the NSW public sector and provides key benefits including:

- helping agencies to assess their own maturity level
- identifying specific areas to improve risk culture and capability
- supporting whole of government improvements to risk management through a uniform tool
- allowing agencies to compare their results over time.

Over 70% of agencies self-assessed their risk maturity as having a 'repeatable' maturity level of risk management, and can be improved

Fifty-six per cent of agencies have completed a risk maturity assessment using the NSW Treasury’s risk maturity assessment tool, with some performed as early as 2021.

On completion of the self-evaluation, agencies determined an overall maturity level, between fundamental and advanced. The majority of agencies rated themselves as having 'repeatable' levels of maturity, indicating there is room for further improvement.

The table below shows how agencies have rated themselves:

Percentage (%) of agencies	Maturity level	Definition of maturity level as per TPP20-06
--	5 – Advanced	A continuously improving process, where risk management is optimised, delivers to stretch objectives and is subject to continuous improvement.
7	4 – Embedded	A predictable process, where risk management is formally defined, predictable, consistently delivered and meets defined objectives.
7	3 – Systematic	A standard, consistent process, where risk management is proactively managed, supported by defined process and is stable and measurable.
79	2 – Repeatable	A disciplined process where risk management is established and repeatable, documentation is limited and continued reliance on individuals.
7	1 – Fundamental	An un-coordinated process, where risk management is ad-hoc, unpredictable and highly dependent on individuals.

Source: Agencies' self-assessed risk maturity levels (unaudited).

All agencies who performed the assessment have advised they have developed action plans to address identified gaps.

Recommendation

Agencies should perform periodic assessments and reviews of their risk maturity and implement action plans. The results of the assessments should be reported to the agency's audit and risk committee for review and to track the effectiveness of action plans over time.

Risk registers

All but one agency maintained a corporate or enterprise risk registers, some were deficient

All but one agency maintained a corporate or enterprise risk register that aligned with their strategic plans. We noted the following deficiencies:

Percentage (%) of agencies	Observation on corporate/enterprise risk registers
4	did not contain risk mitigation strategies
20	lacked a timeline for implementation of mitigation strategies
32	did not define the residual risks post mitigation
4	did not assign responsibilities for identified risks

Source: Audit Office analysis.

Corporate/enterprise risk registers are a vital tool for agencies to track their key risks and to plan how to adequately address the risks to acceptable levels over time.

The following table shows agencies' top three risks as noted in their risk registers.

Percentage (%) of agencies	Top risks identified
60	Cyber security
32	Financial sustainability
36	Workforce planning
24	Health and safety

Source: Agencies' enterprise risk registers (unaudited).

With increasing severity and frequency, it is notable that cyber security risks are present in the top three risks raised by most agencies. All but one agency included cyber security within their risk registers. Refer to section 4 of this report for further details on how agencies manage their cyber maturity and resilience.

Risk appetite statements

Sixteen per cent of agencies do not have a risk appetite statement

Of the agencies that did, 29% did not have measurable risk tolerance levels included.

Risk appetite statements provide a formal expression of an agency's tolerances when dealing with risk and can lead to improved decision making, better prioritising of risk and ensuring risk management is aligned with the agency's objectives.

Shared governance arrangements

Our review noted 60% of agencies had one or more shared governance arrangements. These arrangements consisted of:

Percentage (%) of agencies	Shared governance arrangement
52	Audit and risk committee
44	Chief audit executive
52	Internal audit
40	No shared arrangements

Source: Audit Office analysis.

Shared governance arrangements can provide benefits and opportunities, including cost savings through shared resources. Agencies can also leverage the expertise of audit and risk committee members, internal audit and chief audit executives and benefit from a more holistic approach to risk that spans multiple and interconnected agencies, such as those that are within the same portfolio.

Shared governance arrangements may also have drawbacks, such as the need to:

- ensure sensitive information of each participating entity is kept confidential
- ensure arrangements align with the objectives of each participating agency and address the risks within each agency
- allow sufficient time for the audit and risk committee to address governance matters within each agency.

Internal audit function

Twenty-eight per cent of internal audit functions have not been subject to an external evaluation

All agencies operate an internal audit function as required under TPP 20-08 Internal Audit and Risk Management Policy for the General Government Sector as part of its core requirements. Under the policy, the internal audit function is to provide timely and useful information to management on:

- the adequacy of and compliance with the system of internal control
- whether agency results are consistent with established objectives
- whether operations or programs are being carried out as planned.

Internal audit functions are generally performed via a combination of internal staff and external service providers as noted below:

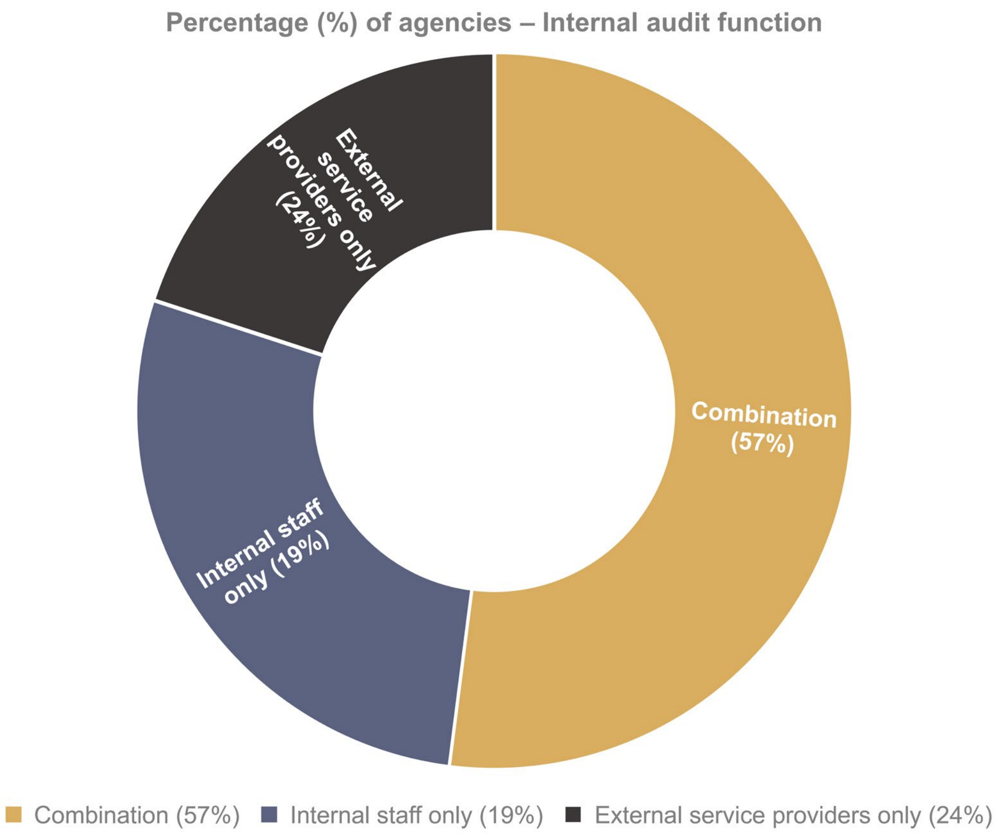


Exhibit 21.

Source: Audit Office analysis.

Our review of agencies' internal audit functions noted the following:

- all reported to the audit and risk committee with many also reporting to the agency's chief executive/accountable authority
- all operated under an internal audit charter. With one exception, charters are required to be reviewed at least annually as per TPP 20-08
- all had an internal audit plan that was endorsed by the audit and risk committee and approved by the accountable authority
- all had current internal audit plans in place
- internal audits are selected with consideration of the corporate/enterprise risks
- 28% of agencies have not had an external assessment performed on their internal audit function.

As required by TPP 20-08, agencies should ensure an external assessment of the internal audit function is conducted by a qualified, independent assessor selected in consultation with the audit and risk committee at least once every five years.

Audit and risk committees

Not all audit and risk committees (ARCs) complied with the requirements of Treasury policy TPP 20-08

All agencies operate ARCs as required under TPP 20-08. The policy defines an ARC as a committee established in accordance with the policy, to monitor, review and provide advice and guidance about the agency's governance processes, risk management and internal control frameworks and external accountability obligations.

Our review noted:

- 3 ARCs performed a self-assessment of their performance against the ARC charter only once every three years, instead of annually as required under TPP 20-08
- 5 ARCs had not provided formal reporting to the accountable authority in the last 12 months as required under TPP 20-08
- all were led by independent chairs appointed through the NSW Prequalification Scheme
- all were comprised of between three to five independent members, and were generally selected from the NSW Prequalification Scheme as required under TPP 20-08, with one exception
- all members had completed a declaration of interests
- all operated under an ARC charter. However, two agencies' charters were not reviewed in the last 12 months as required under TPP 20-08.

As required under the TPP 20-08, ARCs should ensure they periodically review their practices against the ARC charter and also ensure the charter aligns with Treasury policy.

6. Managing payroll and work health and safety

This chapter outlines our audit observations, conclusions and recommendations arising from our review of agencies' payroll controls and management of work health and safety (WHS).

Section highlights

- Agencies should improve their controls around payroll masterfile maintenance, such as enforcing segregation of duties in system access levels and ensuring changes to data are reviewed by an independent officer.
- On average, overtime expenses represented three per cent of total salaries and wages in 2023 and have increased by 40.2% since 2020, compared to salaries and wages which increased by 16.3% over the same period.
- Five agencies have outdated WHS policies, which do not reflect changes to WHS regulations. Sixteen per cent of agencies have not included psychosocial hazards in their WHS procedures or risk assessment process.

6.1 Payroll controls

The NSW public sector employs over 430,000 people to deliver a wide range of services, and consequently, employee expenses is one of the largest expense categories. For the year ended 30 June 2023, the NSW total state sector recorded $51.2 billion in employee expenses (including superannuation expenses). Effective controls around the payroll function ensure that government agencies are paying the correct amount of employee entitlements to the right people and minimising risks of fraud and error.

Agencies need to improve their controls around payroll masterfile maintenance

The payroll masterfile or employee masterfile is a database that contains all employee records including personal information, position, salary/hourly rate, bank account details, entitlements and key employment dates. It is a key payroll control objective that access to either view or change the masterfile is restricted as it contains sensitive data. It is similarly important that changes to the masterfile are appropriately reviewed for completeness and accuracy.

Five agencies do not have appropriate segregation of duties for maintaining the payroll masterfile. Staff at these agencies have access to both edit the masterfile and run the payroll process and/or authorise payroll disbursements. For one of the agencies, only changes to bank accounts are reviewed by an independent officer who does not have access to run the payroll process or authorise disbursements. However, this does not fully mitigate the risk of other unauthorised changes to masterfile data such as changing an employee’s pay rate, work load (full-time or part-time rate), allowances, or other details.

All agencies periodically review changes to payroll masterfile data. However, 24% of agencies do not have this review performed by person independent of the process to access and edit the masterfile.

Similarly, while all agencies regularly review the list of user access to edit the payroll masterfile, 16% of agencies do not have this performed by person independent of the process access to edit the masterfile.

Having a reviewer who is independent of the editing function ensures that the reviewer cannot make further changes that escape review, promoting clear accountability for changes processed.

Agencies lack system controls to prevent payments to terminated employees

Twenty per cent of all agencies do not have system controls to prevent payroll payments being made to terminated employees after their last day of service.

When combined with other deficiencies, this increases the risk of unauthorised or fraudulent payments.

Other payroll control deficiencies noted include:

- payroll staff at two agencies have the ability to edit their own masterfile data
- where staff are paid based on their hours worked, two agencies do not ensure all timesheets are reviewed and approved by a delegated officer prior to each payrun
- five agencies do not perform regular reporting of current staff to line management/business units so they can identify any anomalies.

Inadequate reviews on payroll compliance with employment conditions may increase the risk of not detecting staff underpayments

Almost a third of agencies have not undertaken a review or assessment of payroll compliance with requirements of employee awards or enterprise agreements in the last twelve months. No agency has received correspondence from regulatory bodies, such as the Fair Work Ombudsman or Australian Taxation Office, of actual or possible cases of staff underpayment during the year ended 30 June 2023. However, relying on the absence of complaints does not mean there is a not risk that underpayments may be undetected. Preventative controls are preferable when dealing with underpayment. When incidents occur, they can result in damage to relations with employees and cause a loss of reputation for the employer. It is important for employers to analyse the causes of underpayment and investigate whether the same circumstances could apply to a larger cohort of individuals employed under similar terms and conditions.

In recent years, a growing number of organisations have been investigated or acknowledged cases of staff underpayment. In the university sector, complexity in enterprise agreements and inconsistent interpretation of the terms within those agreements has meant that for several years, universities have both over and underpaid certain staff. This was detailed in our financial audit report Universities 2022. In 2020, NSW Health was subject to a class action claim by junior medical officers for unpaid overtime[1] which is still an ongoing legal matter.

Agencies generally have more comprehensive and complete records on staff overpayments than underpayments. This is partly due to the nature of internal controls which are aimed more towards detecting overpayments, such as through checking validity and eligibility of expenses.

Agencies identified a combined total of $22 million in staff overpayments during the year ended 30 June 2023, and had recouped 58% of this amount. Only eight agencies recorded any staff underpayments during the year ended 30 June 2023, totalling $3.8 million.

[1] Junior Doctors Underpayment Class Action (nsw.gov.au)

6.2 Managing WHS and staff wellbeing

Overtime management

Agencies can improve their management of overtime

Forty per cent of agencies do not have a policy on managing overtime, or rules for when overtime is appropriate. The only guidelines for the use of overtime are through the employee award. While awards may outline delegations for authorising overtime and general eligibility criteria, these are often not specific enough to support effective workforce management. Interpreting award conditions relies on judgement, which can vary across individual managers.

Forty per cent of agencies do not monitor overtime hours at an organisational level for trend analysis, to inform resource planning and monitor risks such as staff welfare, or excessive use or misuse of overtime provisions.

Twenty per cent of agencies have neither a policy on use of overtime nor monitoring procedures of overtime hours.

Forty-four per cent of agencies do not require additional levels of authority to approve overtime; that is, a level above normal line management approving timesheets.

Without monitoring, reporting, or requiring additional approval, there is less transparency on the use of overtime at the executive and governance levels of the organisation. Some degree of overtime is normal and expected. However, agencies should review overtime usage in the context of their organisational strategy and risk management framework to avoid issues with unsustainable workloads, potential WHS issues with wellbeing of staff, and safety of customers and the public.

On average, overtime expenses represented three per cent of total salaries and wages in 2023

The 25 agencies in this report recorded a combined total of $1.2 billion in overtime expenses for the year ended 30 June 2023.

Total overtime expenses have grown at a higher rate than total salaries and wages in the four years from 2020 to 2023. The increase in overtime expenses from 2020 to 2023 was 40.2%, compared to the increase in total salaries and wages over the same period of 16.3%.

The graph below shows the cumulative growth rate of both overtime and salaries and wages expenses over the years ended 30 June 2020 to 2023.

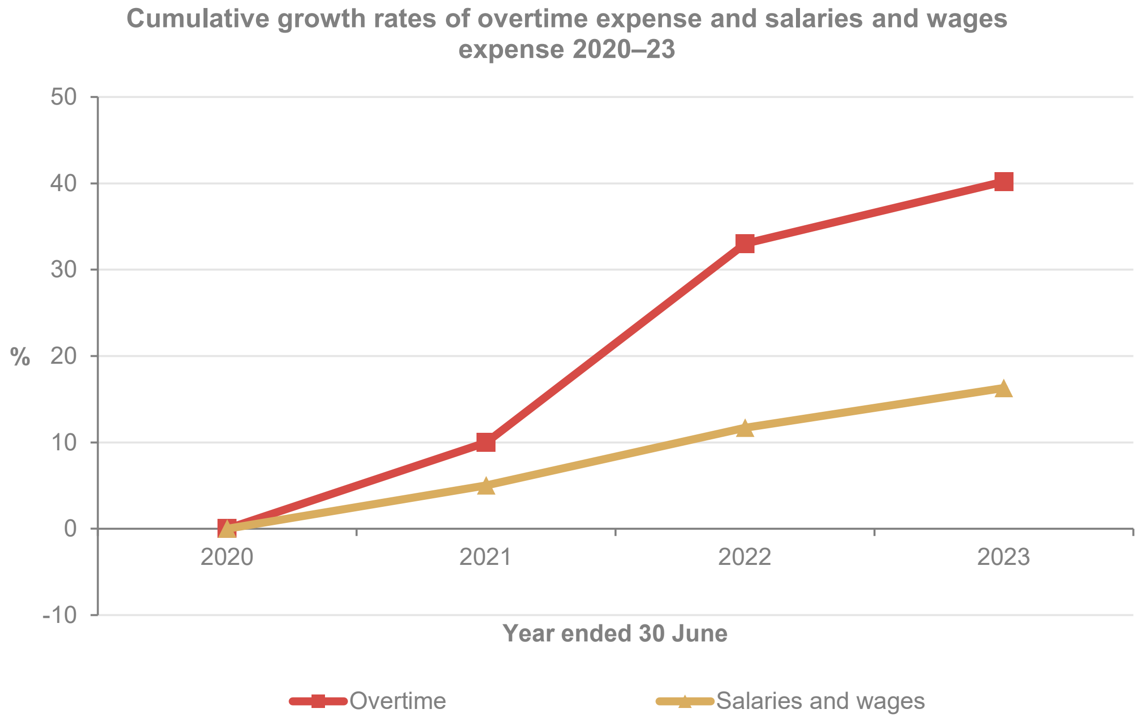


Exhibit 22.

Source: Audited financial statement information.

For three agencies (Sydney Trains, NSW Trains and Fire and Rescue NSW), overtime expenses represented over ten per cent of their total salaries and wages in 2023. The agencies advised these were generally driven by unplanned staff shortages at the operational level.

Ten agencies had at least one employee working overtime hours in excess of 50% of their standard hours

In 2023, the most overtime hours paid to an employee was 2,156 hours, which was 109% more than their standard hours. With overtime and standard hours combined, that employee may have worked the equivalent of 79 hours a week on average for a whole year. However, some awards and employment contracts provide for additional overtime hours be recorded over and above those actually worked, for example for the hour immediately preceding and following the overtime hours worked.

The table below lists the top five agencies with their top three employees with the highest number of recorded overtime hours in the year ended 30 June 2023.

Employee role	Overtime hours worked	Overtime hours as a percentage of standard hours^ (%)	Employer agency
Junior Medical Officer Trainee*	2,156	109.1	Ministry of Health
Correctional Officer	2,116	107.1	Department of Communities and Justice
Paramedic*	1,898	96.0	Ministry of Health
Team Lead Paramedic*	1,875	94.9	Ministry of Health
Senior Correctional Officer	1,536	77.7	Department of Communities and Justice
Senior ITSM Analyst	1,449	79.3	Transport for NSW
Station Officer	1,322	65.6	Fire and Rescue NSW
Correctional Officer	1,318	66.7	Department of Communities and Justice
Relieving Firefighter	1,309	64.9	Fire and Rescue NSW
Senior Software Engineer	1,202	65.8	Transport for NSW
Tow Truck Attendant	1,176	59.3	Transport for NSW
On Board Operations Supervisor	1,157	58.6	NSW Trains
Station Officer	1,138	56.4	Fire and Rescue NSW
On Board Operations Supervisor	1,104	55.9	NSW Trains
On Board Operations Supervisor	1,090	55.2	NSW Trains

^ Standard hours refers to the standard working hours as described in the respective employee's relevant award.

* The Ministry of Health only reports on overtime hours paid to the employee, which includes overtime factors such as time-and-a-half or double-time, in accordance with the relevant award, and does not necessarily represent actual overtime hours worked.

Source: Agencies provided overtime information (audited).

Most of the award conditions for overtime payment allow for overtime hours worked to be paid at time-and-a-half or double-time.

The employer agencies noted in the table above advised that the operational reasons for their employees' high levels of overtime were due to resourcing constraints, severe staff shortages, unfilled rosters, and increased activity demand due to a number of projects underway.

Of these five agencies, three do not have a specific policy on overtime management and two of the three also do not monitor overtime hours at an executive level.

Staff consistently working high hours of overtime may be at greater risk of poor mental and physical health. They may be more likely to suffer burn-out, stress related and other health conditions, and have an increased risk of occupational injury. These risks should be considered and managed through each agency's WHS policy framework and workforce strategy.

WHS management

Framework and structure

Five agencies have outdated WHS policies, which do not cover changes to WHS regulations

All agencies have a WHS policy that is aligned with WHS legislation: the *Work Health and Safety Act 2011* (WHS Act) and Work Health and Safety Regulation 2017 (WHS Regulation). However, five agencies' WHS policies are outdated as they have not incorporated updates to the WHS Regulation on managing psychosocial risks which were first introduced in NSW on 1 October 2022.

Four agencies also do not have psychosocial hazards in their WHS procedures.

Recommendation

Agencies should update their WHS policies and procedures to include current legislative requirements, including management of psychosocial risks.

All agencies' WHS policies:

- are generally aligned with the codes of practice from SafeWork NSW
- clearly allocate roles and responsibilities in accordance with the requirements of the WHS legislation
- extend responsibilities, as appropriate, to visitors and contractors.

Agencies have established appropriate WHS committees

WHS committees, or health and safety committees, allow organisations to work together with workers on health and safety matters. The functions of the WHS committee are to facilitate cooperation in developing and carrying out measures to improve the safety of workers, and help develop health and safety standards, rules and procedures.

All agencies except one have established a WHS committee, which is mandatory if requested by a health and safety representative in the organisation, or by five or more workers. The one agency without a WHS committee advised that it has not been requested to form a committee.

The compositions of other agencies’ WHS committees are in accordance with section 76 of the WHS Act, which requires at least half of the members to be nominated by workers.

Risk assessment and reporting

All agencies except one have included WHS risks in their corporate or enterprise risk registers. The one agency is renewing its risk register and framework to be implemented in late 2023, which is expected to include WHS risks. The risk ratings range from moderate to high. Eighty-eight per cent of agencies maintain a separate WHS risk register which contain more detailed, operational level risks. Of these, one agency does not have psychosocial risks in its WHS risk register.

Forty-five per cent of agencies with separate WHS risk registers have included psychosocial risks in their top three risks. These agencies tend to have more administrative operations than those agencies providing 'front line' services involving physical labour and use of heavy machinery and equipment.

Agencies assess WHS risks and hazards through a variety of methods, including:

- hazard reporting by workers
- workplace inspections
- consultation in various team meetings and WHS committees
- regular risk assessment processes, including review of incident reports
- investigations or audits.

However, the processes at eight per cent of agencies do not include assessment for psychosocial hazards.

Over 20% of agencies do not regularly report WHS matters to those charged with governance

Twenty-four per cent of agencies do not regularly report WHS matters to the board (or equivalent), and 20% do not report to the audit and risk committee. Twelve per cent of agencies report to neither the board nor the audit and risk committee. Whilst these agencies have reporting mechanisms to separate executive or management teams, the lack of oversight by those charged with governance may increase the risk of inadequate response to risks and/or incidents.

Officers, including those charged with governance, have duties of care under the WHS Act and it is important that they receive regular reporting to understand and be able to discharge their legal obligations for ensuring safe workplaces.

All agencies have reported notifiable incidents, as defined in the WHS Act, to SafeWork NSW, if any occurred during the year ended 30 June 2023. A notifiable incident is a death of a person, serious injury or illness of a person, or a dangerous incident. All agencies except two also communicated those reports of notifiable incidents to those charged with governance.

Three agencies did not demonstrate evidence that they reviewed and responded to complaints or whistle-blower reports regarding WHS in the year ended 30 June 2023.

WHS activities

Staff are required to complete WHS checklists for their home office at only 68% of agencies

Although all agencies have implemented flexible working arrangements, and the proportion of employees who regularly work from home ranges from five per cent to 100%, only 68% of agencies require employees to complete an annual WHS checklist on the safety of their home office where those employees do work from home. All agencies had completed WHS checklists for the agencies' work sites.

WHS training could be improved

Thirty-two per cent of agencies do not provide annual WHS refresher training for all employees. Of those that conduct mandatory WHS refresher training, the training completion rates range from 66% to 100%. The SafeWork NSW code of practice 'How to manage work health and safety risks' recommends providing up-to-date training to maintain competencies and ensure WHS control measures remain effective.

Twelve per cent of agencies do not carry out WHS induction training for contractors and visitors. Contractors and visitors are included in the scope of the WHS Act, as employers have a primary duty of care for the health and safety of all people in the workplace. In many circumstances, it is useful for contractors and some types of visitors (excluding customers, delivery people, etc) to receive a WHS induction the first time they are on-site.

Mental health

Under WHS laws, employers are responsible for managing risks to employees' mental health at work. Psychosocial hazards can harm mental health.

The most common psychosocial hazards that agencies have identified as relevant to their workers are listed in the chart below.

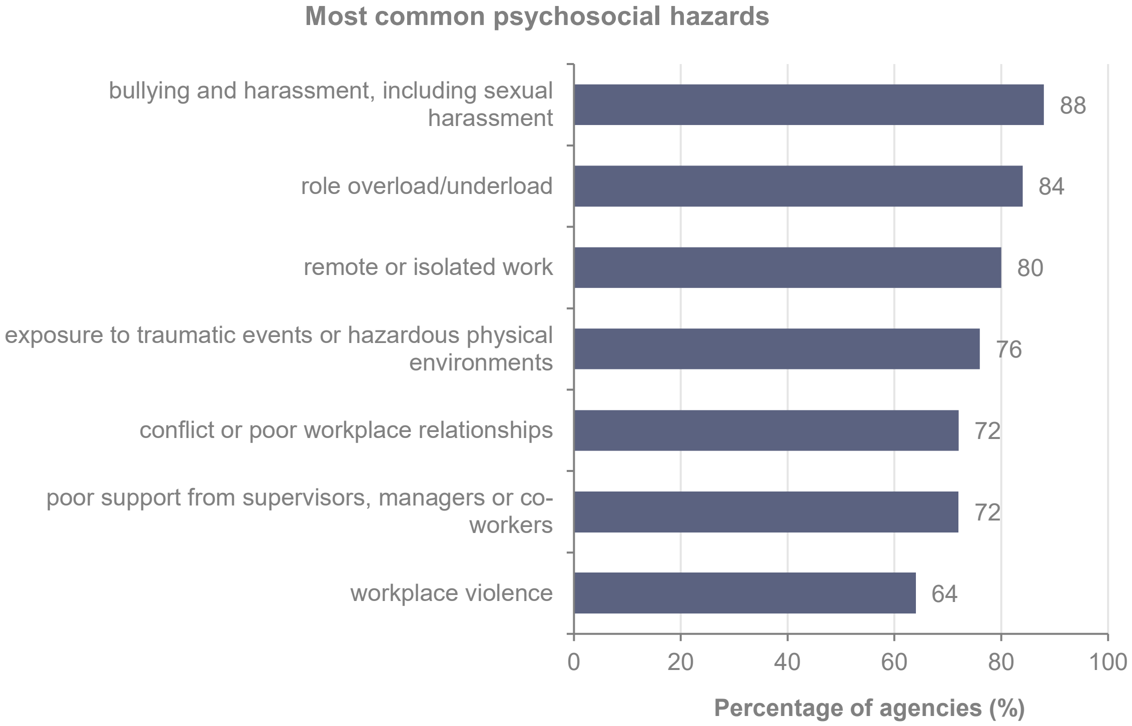


Exhibit 23.

Source: Agencies' identified risks (unaudited).

All except two agencies have reported psychosocial incidents during 2023, ranging from one to over 27,000 incidents. This is a broader category than psychological injury claims under WHS insurance, however 36% of agencies have not reported additional incidents compared to their number of psychological injury claims. This may indicate a lack of adequate reporting mechanisms for psychosocial incidents.

Psychological injury claims have grown in recent years and were the focus of a Parliamentary Standing Committee report, 2023 Review of Workers Compensation Scheme. The report made a number of recommendations for Insurance and Care NSW, the State Insurance Regulatory Authority and SafeWork NSW in relation to understanding the drivers of psychological claims and developing programs to identify, manage and respond to psychosocial hazards.

All agencies have conducted training during the 2023 year on bullying and harassment, as well as mental health first aid. Three agencies have not conducted training on stress management/burn-out risk, even though it is one of the top psychosocial hazards identified across the agencies (role overload).

One measure of identifying potential staff burn-out is whether employees are taking annual leave or long service leave. Taking regular periods of leave enables employees to maintain their physical and mental wellbeing and positively impacts on productivity in the workplace.

All agencies monitor excessive employee leave balances (usually those with over 30 days of annual leave, in accordance with Treasury Circular TC 16-03 'Managing Accrued Recreation Leave Balances') at least on a quarterly basis.

Employees at greater risk of burn-out are those who have not taken any annual leave or long service leave in the twelve months to 30 June 2023. The number of such employees range from nil to over 36,000. As a percentage of total staff (by headcount), this ranges up to 84.9%.

OUR VISION

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

OUR PURPOSE

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

OUR VALUES

Pride in purpose

Curious and open-minded

Valuing people

Contagious integrity

Courage (even when it's uncomfortable)

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

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

PHONE +61 2 9275 7100

mail@audit.nsw.gov.au

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

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au