FINANCIAL AUDIT

5 NOVEMBER 2019

Internal controls and governance

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 *Public Finance and 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 Total State Sector Accounts, a consolidation of all agencies' accounts.

Financial audits are designed to add credibility to financial statements, enhancing their value to end-users. Also, the existence of such audits provides a constant stimulus to entities to ensure sound financial management.

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

We also conduct performance audits. These examine whether an entity is carrying out its activities effectively and doing so economically and efficiently and in compliance with relevant laws. Audits may cover all or parts of an entity's operations, or consider particular issues across a number of entities.

As well as financial and performance audits, the Auditor-General carries out special reviews and compliance engagements.

Performance audits are reported separately, with all other audits included in one of the regular volumes of the Auditor-General's Reports to Parliament – Financial Audits.

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 *Public Finance and Audit Act 1983*, I present a report titled **'Internal controls and governance'**.

Margaret Crawford
Auditor-General
5 November 2019

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

contents

Internal controls and governance 2019

Section one – Internal controls and governance 2019

Section two – Appendices

Section one

Internal controls and governance 2019

This report analyses the internal controls and governance of 40 of the largest agencies in the NSW public sector for the year ended 30 June 2019.

Executive summary

This report analyses the internal controls and governance of 40 of the largest agencies in the NSW public sector for the year ended 30 June 2019.

1. Internal control trends

New, repeat and high risk findings

There was an increase in internal control deficiencies of 12 per cent compared to last year. The increase is predominately due to a 100 per cent increase in repeat financial and IT control deficiencies.

Some agencies attributed the delay in actioning repeat findings to the diversion of staff from their regular activities to implement and operationalise the recent Machinery of Government changes. As a result, actions to address audit recommendations have been deferred or re prioritised, as the changes are implemented.

Agencies need to ensure they are actively managing the risks associated with having these vulnerabilities in internal control systems unaddressed for extended periods of time.

Common findings

A number of findings were common to multiple agencies. These findings often related to areas that are fundamental to good internal control environments and effective organisational governance, such as:

- out of date policies or an absence of policies to guide appropriate decisions
- poor record keeping and document retention
- incomplete or inaccurate centralised registers or gaps in these registers
- policies, procedures or controls no longer suited to the current organisational structure or business activities.

2. Information technology controls

IT general controls

We examined information security controls over key financial systems that support the preparation of agency financial statements. We found:

- user access administration deficiencies at 58 per cent of agencies related to granting, review and removal of user access
- an absence of privileged user activity reviews at 35 per cent of agencies
- password controls that did not align to password policies at 20 per cent of agencies.

We also found 20 per cent of agencies had deficient IT program change controls, mainly related to segregation of duties in approval and authorisation processes, and user acceptance testing of program changes prior to deployment into production environments. User acceptance testing helps identify potential issues with software incompatibility, operational workflows, absent controls and software issues, as well as areas where training or user support may be required.

3. Gifts and benefits

Gifts and benefits registers

All agencies had a gifts and benefits policy and 90 per cent of agencies maintain a gifts and benefits register. However, 51 per cent of the gifts and benefits registers we examined contained incomplete declarations, such as missing details for the approving officer, value of the gift and/or benefit offered and reasons supporting the decision.

In some cases, gaps in recorded information meant the basis for decisions around gifts and benefits was not always clear, making it difficult to determine whether decisions in those instances were appropriate, compliant with policy and were not direct or indirect inducements to the recipients to favour suppliers or service providers.

Agencies should ensure their gifts and benefits register includes all key fields specified in the Public Service Commission's minimum standards for gifts and benefits. Agencies should also perform regular reviews of the register to ensure completeness and ensure any gift or benefit accepted by a staff member meets the public's expectations for ethical behaviour.

Managing gifts and benefits

We found opportunities to improve gifts and benefits processes and enhance transparency. For example, only three per cent of agencies publish their gifts and benefits registers on their websites.

Agencies can improve management of gifts and benefits by:

- ensuring agency policies comprehensively cover the elements necessary to make it effective in an operational environment, such as identifying risks specific to the agency and actions that will be taken in the event of a policy breach
- establishing and publishing a statement of business ethics on the agency's website to clearly communicate expected behaviours to clients, customers, suppliers and contractors
- providing on-going training, awareness activities and support to employees, not just at induction
- publishing their gifts and benefits registers on their websites to demonstrate a commitment to a transparently ethical environment.

Reporting and monitoring

Only 35 per cent of agencies reported trends in the number and nature of gifts and benefits recorded in their registers to the agency's senior executive management and/or a governance committee.

Agencies should regularly report to the agency executive or other governance committee on trends in the offer and acceptance of gifts and benefits.

4. Internal audit

Obtaining value from the internal audit function

Agencies have established and maintained internal audit functions to provide assurance on the effectiveness of agency controls and governance systems. However, we identified areas where agencies' internal audit functions could improve their processes to add greater value. For example, only 73 per cent of CAEs regularly attend meetings of the agency board or executive management committee.

Internal audit functions can add greater value by involving the CAE more extensively in executive forums as an observer.

Internal audit functions should also consider producing an annual report on internal audit. An annual report allows the internal audit function to report on their performance and add value by drawing to the attention of audit and risk committees and senior management strategic issues, thematic trends and emerging risks.

Role of the Chief Audit Executive

Forty-five per cent of agencies assigned responsibilities to the Chief Audit Executive (CAE) that were broader than internal audit, but 17 per cent of these had not documented safeguards to protect the independence of the CAE.

The reporting lines and status of the CAE at some agencies also needs review. At two agencies, the CAE reported to the CFO.

Agencies should ensure:

- the reporting lines for the CAE comply with the NSW Treasury policy, and the CAE does not report functionally or administratively to the finance function or other significant recipients of internal audit services
- the CAE's duties are compatible with preserving their independence and where threats to independence exist, safeguards are documented and approved.

Quality assurance and improvement program

Thirty-five per cent of agencies did not have a documented quality assurance and improvement program for its internal audit function.

The policy and the International Standards for the Professional Practice of Internal Auditing require agencies to have a documented quality assurance and improvement program. The results of this program should be reported annually.

Agencies should ensure there is a documented and operational Quality Assurance and Improvement Program for the internal audit function that covers both internal and external assessments.

5. Managing contingent labour

Obtaining value for money from contingent labour

According to NSW Procurement data, spend on contingent labour has increased by 75 per cent over the last five years, to $1.5 billion in 2018–19. Improvements in internal processes and a renewed focus on agency monitoring and oversight of contingent labour can help ensure agencies get the best value for money from their contingent workforces.

Agencies can improve their management of contingent labour by:

- preparing workforce plans to inform their resourcing strategy and ensure that engaging contingent labour aligns with the strategy and best meets business needs
- involving agency human resources units in decisions about engaging contingent labour
- regularly reporting on contingent labour use and tenure to agency executive teams
- strengthening on-boarding and off-boarding processes.

We also found 57 per cent of the 23 agencies we examined with contingent labour spend of more than $5 million in 2018–19 have implemented the government's vendor management system and service provider 'Contractor Central'.

6. Managing sensitive data

Identifying and assessing sensitive data

Sixty-eight per cent of agencies maintain an inventory of their sensitive data and where it resides. However, these inventories are not always complete and risks may be overlooked.

Agencies can improve processes to manage sensitive data by:

- identifying and maintaining an inventory of sensitive data through a comprehensive and structured process
- assessing the criticality and sensitivity of the data so that protection of high risk data can be prioritised.

Managing data breaches

Eighty-eight per cent of agencies have established policies to respond to potential data breaches when they are identified and 70 per cent of agencies maintain a register to record key information in relation to identified data breach incidents.

Agencies should maintain a data breach register to effectively manage the actions undertaken to contain, evaluate and remediate each data breach.

1. Introduction

This report covers the findings and recommendations from our 2018–19 financial audits that relate to internal controls and governance at 40 of the largest agencies (refer to Appendix three) in the NSW public sector. The 40 agencies selected for this volume constitute around 84 per cent of total expenditure for all NSW public sector agencies.

Although the report includes several agencies that have changed as a result of the Machinery of Government changes that were effective from 1 July 2019, its focus on sector wide issues and insights means that its findings remain relevant to NSW public sector agencies, including newly formed agencies that have assumed the functions of abolished agencies.

This report offers insights into internal controls and governance in the NSW public sector

This is the third report dedicated to internal controls and governance at NSW State Government agencies. The report provides insights into the effectiveness of controls and governance processes in the NSW public sector by:

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

Without strong governance systems and internal controls, agencies increase the risks associated with effectively managing their finances and delivering services to citizens. For example, if they do not have strong information technology controls, sensitive information may be at risk of unauthorised access and misuse.

Areas of specific focus of the report have changed since last year

Last year's report topics included transparency and performance reporting, management of purchasing cards and taxi use, and fraud and corruption control. We are reporting on new topics this year and re-visiting agency management of gifts and benefits, which we first covered in our 2017 report. Re-visiting topics from prior years provides a baseline to show the NSW public sectors' progress implementing appropriate internal controls and governance processes to mitigate existing, new and emerging risks in the public sector.

Our audits do not review all aspects of internal controls and governance every year. We select a range of measures and report on those that present heightened risks for agencies to mitigate. This year the report focusses on:

- internal control trends
- information technology controls, including access to agency systems
- protecting sensitive information held within agencies
- managing large and diverse workforces (controls around employing and managing contingent workers)
- maintaining an ethical culture (management of gifts and benefits)
- effectiveness of internal audit function and its oversight by Audit and Risk Committees.

The findings in this report should not be used to draw conclusions on the effectiveness of individual agency control environments and governance arrangements. Specific financial reporting, internal controls and audit observations are included in the individual 2019 cluster financial audit reports, which will be tabled in parliament from November to December 2019.

2. Internal control trends

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

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

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

Key conclusions and sector wide learnings

We identified four high risk findings, compared to six last year. None of the findings are common with those in the previous year. There was an overall increase of 12 per cent in the number of internal control deficiencies compared to last year. The increase is predominately due to a 100 per cent increase in the number of repeat financial and IT control deficiencies.

Some agencies attributed the delay in actioning repeat findings to the diversion of staff from their regular activities to implement and operationalise the recent Machinery of Government changes. As a result, actions to address audit recommendations have been deferred or re-prioritised, as the changes are implemented. Agencies need to ensure they are actively managing the risks associated with having these vulnerabilities in internal control systems unaddressed for extended periods of time.

We also identified a number of findings that were common to multiple agencies. These common findings often related to areas that are fundamental to good internal control environments and effective organisational governance. Examples include:

- out of date policies or an absence of policies to guide appropriate decisions
- poor record keeping and document retention
- incomplete or inaccurate centralised registers or gaps in these registers.

Policies, procedures and internal controls should be properly designed, be appropriate for the current organisational structure and its business activities, and work effectively.

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 may impact the reliability of its financial statements. This in turn, increases the risk that the audit opinion will be modified.

We rate the risk posed by each financial and IT 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

We identified four high risk findings, compared to six high risk findings in 2017–18. None of the high risk findings is a repeat deficiency from the previous year. Three of the four high risk deficiencies related to financial controls and one was related to IT controls.

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

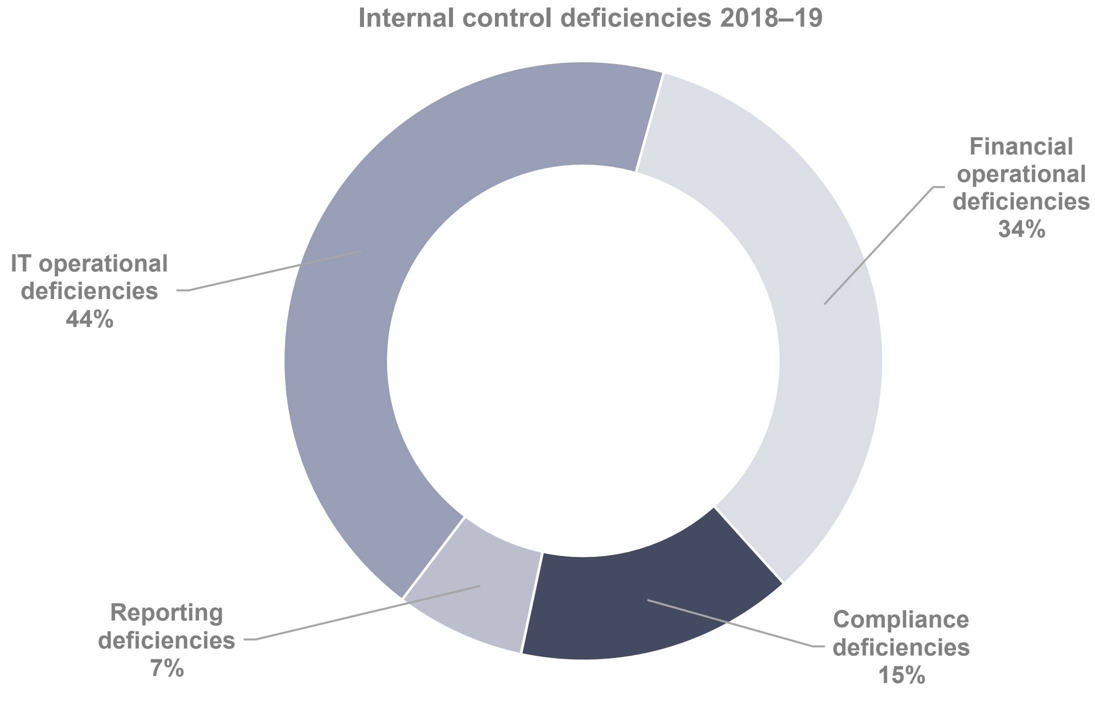
High risk finding	Implication
Deficiencies in controls to manage privileged user access administration and monitoring privileged user activities were noted on a key business system. Audit logs were not maintained or reviewed and generic privileged user accounts and privileged user accounts with unidentified users were identified.	Privileged users are able to access key systems and functions. They may also be able to remove records of their activity if programmed logging features are disabled. Inappropriate privileged user access exposes agencies to greater risk of unauthorised changes to systems and data by these users, or by cyber criminals using their logon details. The unauthorised changes may not be identified in a timely manner and/or be traceable to individual users.
We noted a high number of exceptions in underlying lease data maintained by an agency managing a high volume of leases. This included differences between data recorded in registers and key terms and conditions in the underlying contracts, including lease payments, lease terms and extension options.	Data quality issues could create a risk of material misstatement to the agency's financial statements, particularly on adoption of the new lease accounting standard, effective from 1 July 2019. The agency is also not complying with its records management requirements. Inaccurate data may render it unable to effectively manage its portfolio of leases.
We noted deficiencies in controls to manage inventories held for distribution, including: • policies that did not require all items in warehouses, stores and caches to be included in the annual stocktake • inventory movements were not reflected in the financial management system on a timely basis • warehouse records were unable to establish the dates when inventory items were despatched.	There is a risk that inventories are materially understated for financial reporting purposes because: • certain items are excluded from the stocktake • warehouse records are not able to establish despatch dates. There is an increased risk that theft will not be detected, or will not be detected on a timely basis. The agency has previously experienced fraud in this area.
An agency's preliminary assessment of the impact of new and updated Australian Accounting Standards issued but not effective **contained a number of deficiencies in the approach adopted.** The impact of the new standards is expected to be material to the agency.	Lack of robust and detailed documentation to support the application of steps and/or criteria in the Australian Accounting Standards and Treasury Guidance Papers may result in a material misstatement to the agency's financial statements.

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 many agencies. Where deficiencies relate to multiple agencies, central agencies can help ensure consistent, timely, efficient and effective responses to identified deficiencies.

We classified the 349 internal control deficiencies we identified in 2018–19 into common categories as follows:

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



Source: Audit Office management letters.

The graph above shows that 78 per cent of the deficiencies (79 per cent in 2017–18) were financial or IT operational deficiencies, with the remainder split between compliance deficiencies (15 per cent compared to 17 per cent in 2017–18) and reporting deficiencies (seven per cent compared to four per cent in 2017–18).

The table below describes the most common deficiencies across agencies, including their risk rating, the number of repeat deficiencies and the recommendations our management letters have communicated to agencies.

Operational

!	**High:**	2 new	0 repeat
⊖	**Moderate:**	84 new	80 repeat
✓	**Low:**	79 new	27 repeat

Common issue	Findings/implication	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. These issues increase the risk that outdated policies and procedures may be followed, that policies and procedures do not reflect better practice, or where practice is not documented, the agency is at risk from the loss of corporate knowledge when staff turnover.	Agencies should establish processes that assure its policies reflect current requirements, the organisation's current structure and delegations, and avoid duplication, contradictions or gaps.
Maintaining master files	Controls were not established to: • ensure sufficient segregation of duties over access to key master files • verify the validity, accuracy and/or completeness of changes to key master files, such as vendor and payroll tables.	Agencies should: • review controls established over access to key master files to prevent inappropriate access to, change or erasure of data • regularly review system access of business users to ensure incompatible duties are removed.
Use of purchase orders	Purchase orders were created and approved only after the goods and services were purchased.	Agencies should ensure staff are trained in their obligations to comply with proper procurement practices, policies and legislation.
Information technology	IT control deficiencies related to IT governance, user access administration, program change and computer operations.	Refer to Section 3 of this report for further details.

Compliance

❗	**High:**	0 new	0 repeat
⊖	**Moderate:**	24 new	11 repeat
✓	**Low:**	14 new	5 repeat

Common issue	Finding/implication	Lessons for agencies
Contract registers	Agencies have not established contract registers or have incomplete or inaccurate contract registers. These agencies may face challenges with: • complying with GIPA obligations • identifying contracts that are nearing completion, and commence procurement activity in a timely manner • effectively managing their contractual commitments • disclosing contractual commitments accurately in their financial statements.	Agencies should focus on establishing complete and accurate contract registers. This includes: • developing policies and procedures that govern the timely and accurate updating of the contracts register • monitoring the contracts register, including identifying contracts nearing completion so a new procurement can be commenced in a timely manner.
Document retention	Agencies do not always maintain documents to evidence performance of key control activities. Deficiencies reduce accountability and reduce compliance with State records legislation.	Agencies should educate staff in their responsibilities and retain documentary evidence that they have discharged those responsibilities. Agencies should ensure appropriate records management policies have been communicated to staff.
Central registers, such as those used to manage conflicts and gifts and benefits.	Central registers are not kept, or are not updated in a timely manner. Without a central register to capture such information, agencies may not have the visibility it needs to oversight whether management of conflicts and/or gifts and benefits complies with requirements and internal policies.	Agencies should ensure they have registers to capture staff disclosures in a way that complies with legislation and policies. Conflict of interest, gifts and benefits and other relevant policies should deal with the timeliness of how such registers are updated.

Reporting

❗	**High:**	2 new	0 repeat
⊖	**Moderate:**	7 new	5 repeat
✓	**Low:**	7 new	2 repeat

Common issue	Finding/implication	Lessons for agencies
Reconciliations	Key reconciliations were not prepared, or were not reviewed in a timely manner. Reconciliations of inter-agency balances were not performed. There were unconfirmed balances in reconciliations.	Reconciliations should be prepared and reviewed as part of month-end processes. Management policies and procedures should be observed and ensure this key control is performed. Inter-agency balances should be reconciled regularly. Reconciliation differences should be resolved in a timely manner.

2.3 New and repeat findings

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

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

Our 2018–19 audits identified 349 internal control deficiencies, comprising:

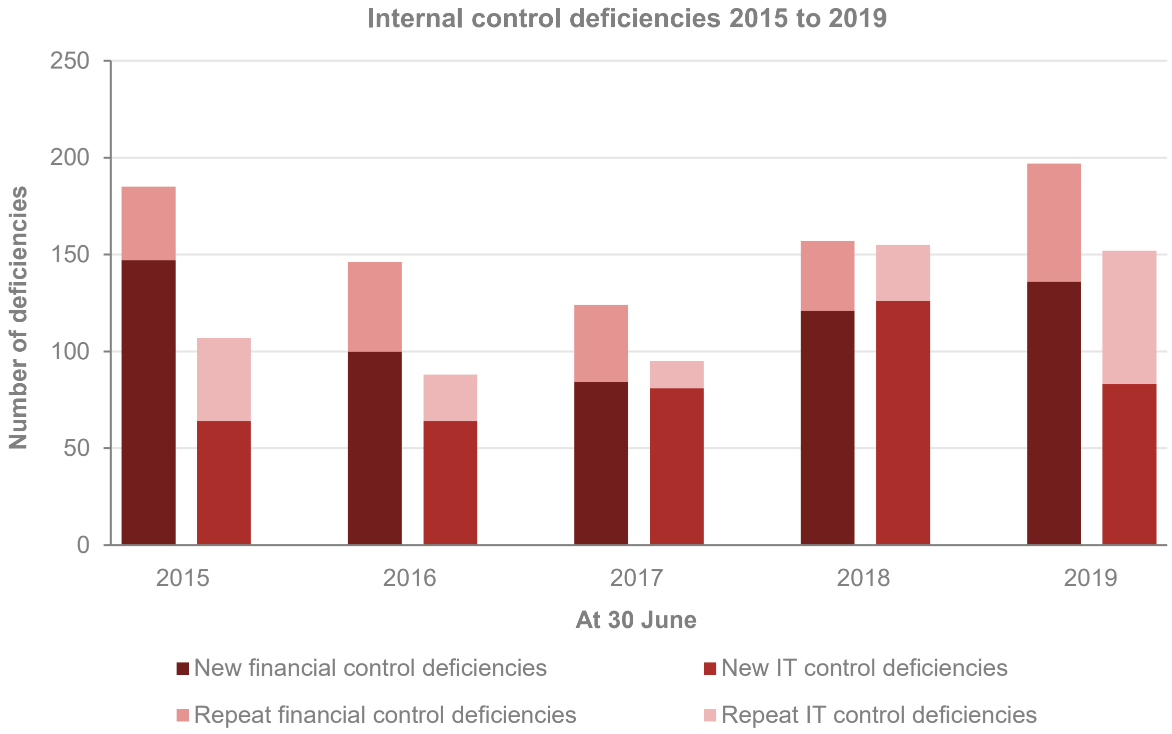
- 197 financial control deficiencies
- 152 IT control deficiencies.

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

The number of internal control deficiencies has increased by 12 per cent from last year

The 12 per cent increase in internal control deficiencies is predominately due to a 100 per cent increase in repeat internal control deficiencies and a 12 per cent increase in new financial control deficiencies. This follows an increase in internal control deficiencies of 42 per cent in 2017–18.

We explore the reasons for this increase later in this chapter.



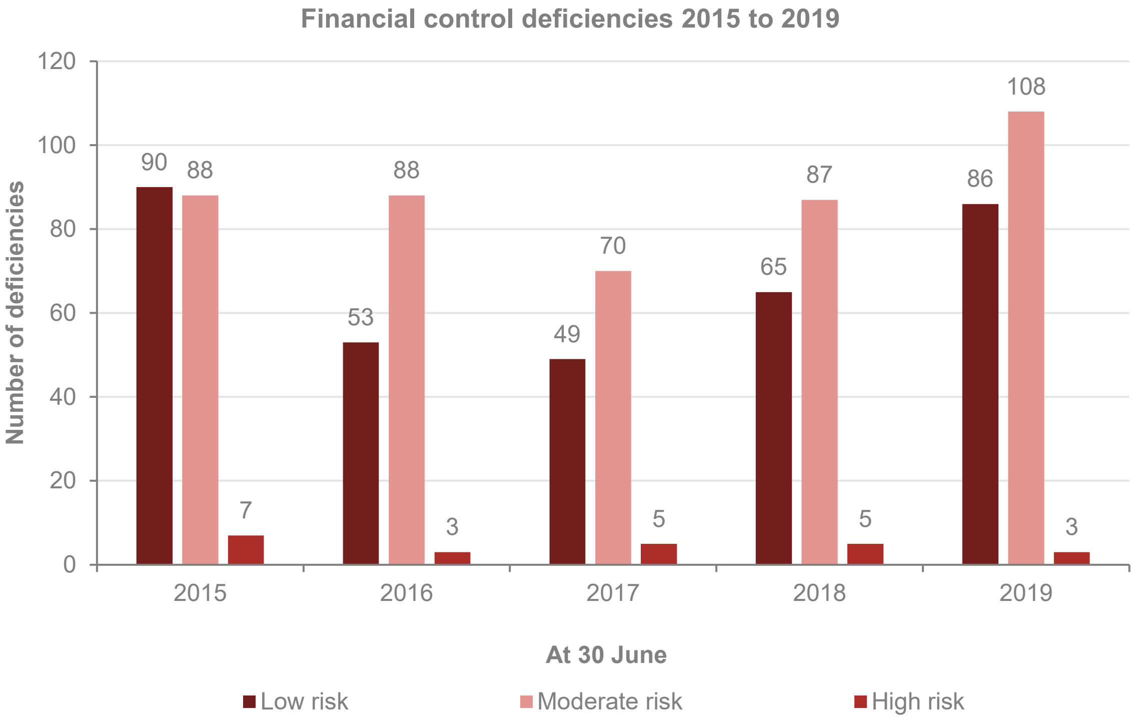
Source: Audit Office management letters.

The number of financial control deficiencies has increased by 25 per cent from last year

Over the last 12 months, the number of financial control deficiencies has increased by 25 per cent from last year, following an increase of 27 per cent noted in 2017–18. We found financial control deficiencies at 85 per cent of agencies (75 per cent in 2017–18) with new financial control deficiencies increasing by 12 per cent and repeat financial control deficiencies increasing by 69 per cent from 2017–18.

Deficiencies in internal controls increase the risk of intentional and accidental errors in processing information, producing management reports and generating financial statements. This can impair decision-making, affect service delivery and expose agencies to fraud, financial loss and reputational damage. Poor controls may also mean agency staff are less likely to follow internal policies, inadvertently causing the agency not to comply with legislation, regulation and central agency policies.

The graph below shows the risk rating of reported financial control deficiencies for the past five years.



Source: Audit Office management letters.

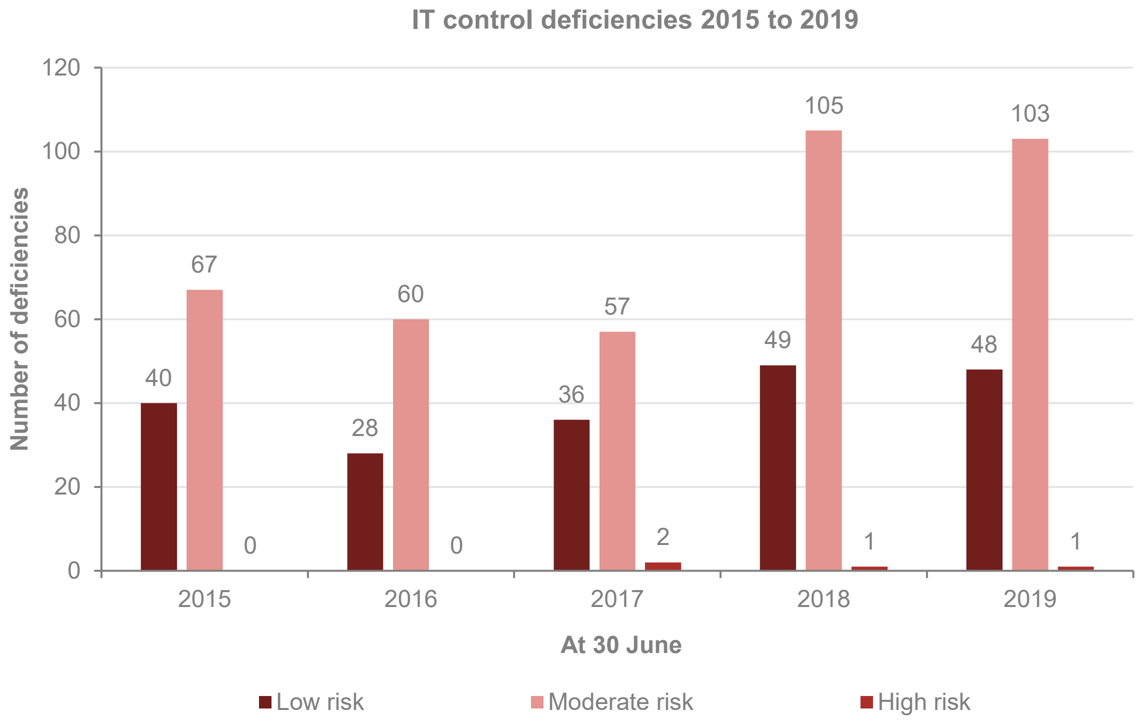
The number of IT control deficiencies has remained consistent with the previous year, following a 63 per cent increase in 2017–18

The number of reported IT control deficiencies has decreased slightly, by 1.9 per cent compared to last year, following a 63 per cent increase in 2017–18. This remains historically high compared to the three years prior to 2017–18. Overall, the number of IT control deficiencies has increased by 42 per cent compared to 2014–15.

The high number of IT control deficiencies in 2018–19 is largely due to unresolved IT control deficiencies. Repeat findings have increased by 138 per cent, from 29 in 2017–18 to 69 in 2018–19. Conversely, new IT control deficiencies have decreased by 34 per cent, from 126 in 2017–18 to 83 in 2018–19.

Good IT controls are an essential ingredient underpinning effective processes, policies and procedures for managing information systems, securing sensitive information, and ensuring the integrity of agency data. Poor IT controls increase risks to agencies, including unauthorised access, cyber security attacks, fraud, data manipulation, privacy breaches, non-compliance with laws and regulations and information theft. The longer a deficiency remains unaddressed, the greater the risk that the vulnerability will not only be exploited, but will be repeatedly exploited increasing the potential losses to the agency.

The graph below shows the risk rating of reported IT control deficiencies for the past five years.

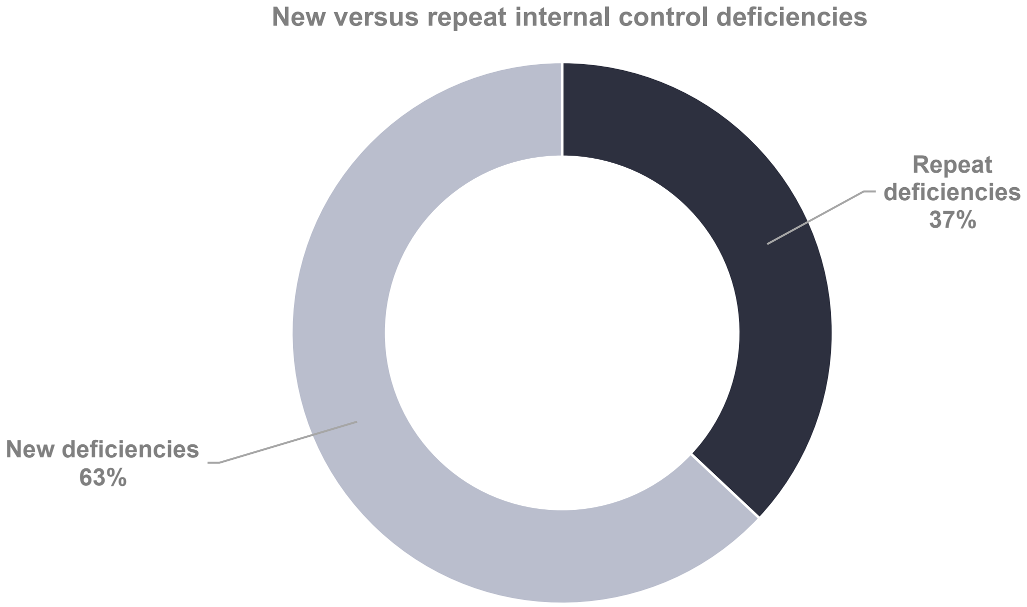


Source: Audit Office management letters.

Agencies need to further focus their attention on these issues and prioritise the rectification of IT weaknesses.

Repeat control deficiencies increased by 100 per cent from 2017–18

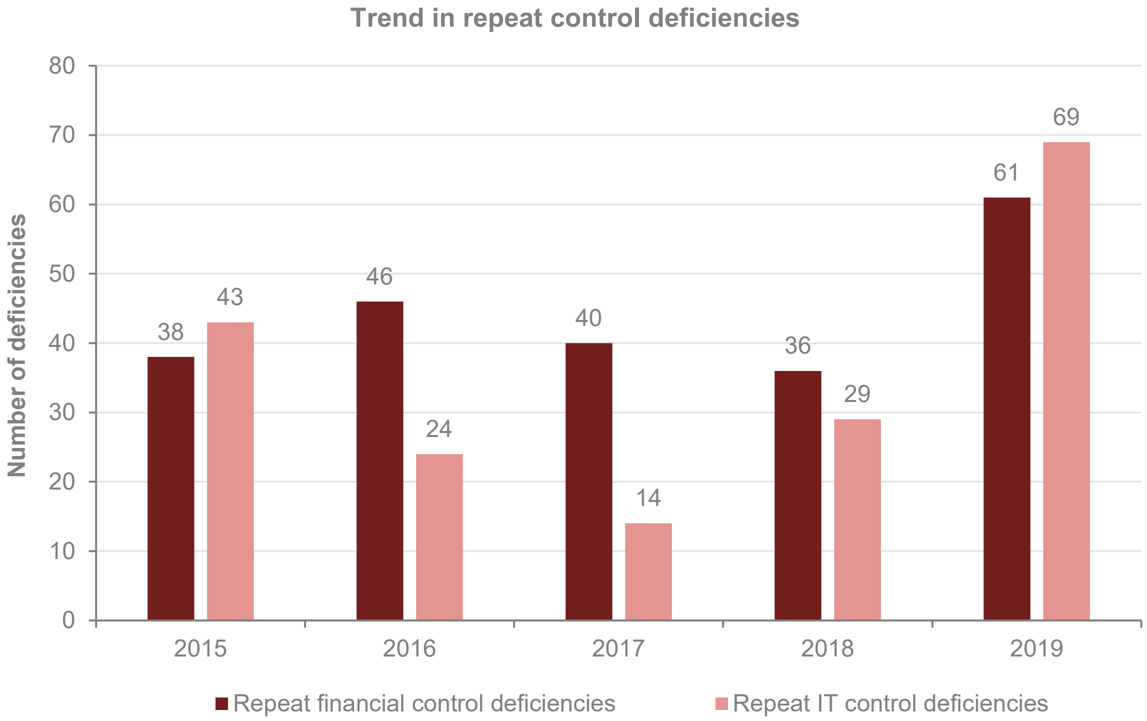
The number of repeat internal control deficiencies we identified has increased by 100 per cent from 2017–18. As a percentage of all internal control deficiencies, unresolved deficiencies from prior years now represent 37 per cent of all the internal control deficiencies we identified. This highlights a trend of agency delays in addressing control deficiencies.



Source: Audit Office management letters.

The graph below shows a rise in both repeat financial and IT control deficiencies in the current year. There was an increase of:

- 69 per cent in the number of repeat financial control deficiencies, following decreases in repeat financial control deficiencies between 2015–16 to 2017–18
- 138 per cent in IT control deficiencies, following a 107 per cent increase in 2017–18.



Source: Audit Office management letters.

The recent Machinery of Government changes have contributed to the increase in repeat internal control deficiencies. Some agencies attributed the delay in actioning repeat findings to the diversion of staff from their regular activities to implement and operationalise the Machinery of Government changes. As a result, actions to address audit recommendations have been deferred or re-prioritised.

Vulnerabilities in internal controls systems that can be exploited by internal and external parties 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 the above challenges by ensuring:

- there is clear ownership of recommendations arising from internal control deficiencies, with timeframes and actions plans for their implementation
- audit and risk committees and agency management monitor the implementation status regularly focussing 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.

Key conclusions and sector wide learnings

Government agencies' financial reporting is heavily reliant on information technology (IT). We continue to see a high number of deficiencies related to IT general controls, particularly those related to user access administration. These controls are key in adequately protecting IT systems from inappropriate access and misuse.

IT is also important to the delivery of agency services. These systems often provide the data to help monitor the efficiency and effectiveness of agency processes and services they deliver. Our financial audits do not review all agency IT systems. For example, IT systems used to support agency service delivery are generally outside the scope of our financial audit. However, agencies should also consider the relevance of our findings to these systems.

Agencies need to continue to focus on assessing the risks of inappropriate access and misuse and the implementation of controls to adequately protect their systems, focussing on the processes in place to grant, remove and monitor user access, particularly privileged user access.

3.1 IT general controls

IT governance

IT governance provides a structure to enable agencies to effectively manage their IT risks and ensure that associated activities are aligned to achieve their objectives to deliver services to the public.

Most agencies have implemented policies to manage their key IT systems

Ninety-five per cent of agencies have established IT policies to ensure key IT processes and functions are appropriately managed. However, ten per cent of these policies were not regularly reviewed, with one policy not reviewed since 2012. Regular review of IT policies ensure that the strategies and procedures agencies implement effectively manage the evolving IT risks affecting their IT environments. The implementation of IT policies ensures there are adequate processes in place for the on-going management of existing and new IT risks affecting agencies.

Agencies can improve monitoring over activities performed by third party service providers

During 2018–19, eight per cent of agencies have not implemented processes to monitor and assess the effectiveness of the processes and controls implemented by service providers to manage the IT infrastructure relied upon by agencies. Ineffective monitoring of processes and controls operated by the service providers increases the risk that controls deficiencies affecting agency operations will not be adequately addressed.

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

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

Information security

Information technology is often at the core of how agencies deliver services in every sector. While IT can improve service delivery, the growing dependency on technology and the government's larger digital footprint means agencies face risks if they do not adequately protect their IT systems from unauthorised access and misuse.

User access administration

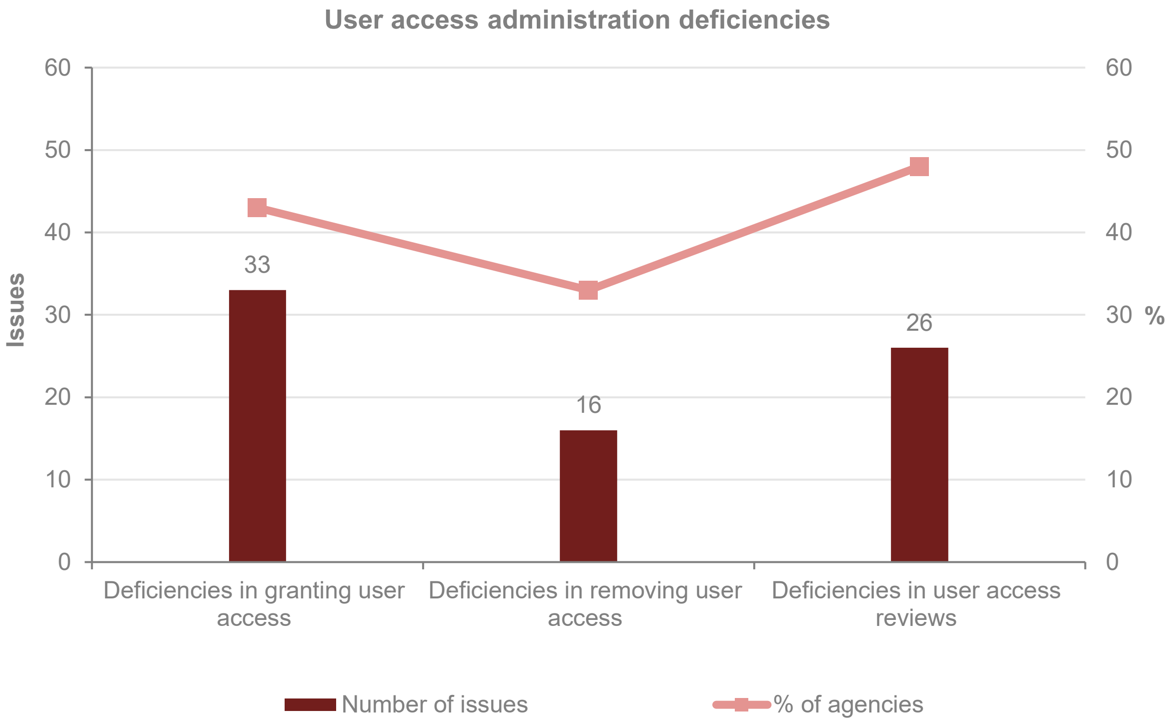
User access administration over IT systems needs to be improved

All agencies have implemented formal processes for user access creation and modification to IT systems. However, the graph below shows all aspects of user access management require improvement. We found:

- 33 issues related to granting user access across 43 per cent of agencies
- 16 issues related to removing user access across 33 per cent of agencies
- 26 issues related to periodic reviews of user access across 48 per cent of agencies.

Examples of deficiencies included:

- absence of periodic user access reviews performed to ensure access levels align with the user's role
- regular reviews of dormant user accounts not performed
- no process to periodically review third party user access and remove profiles when they are no longer required, on a timely basis
- weaknesses in processes to ensure staff access is changed to reflect new responsibilities, on a timely basis, and delays in removing the access of terminated staff
- no approval or no evidence of approval to support granting access to new users or changes to user access level.



Source: Audit Office management letters.

Poor management of user access:

- exposes agencies to the risk of fraud
- compromises data integrity and confidentiality
- increases the risk of unauthorised and invalid transactions
- increases the risk of dormant user profiles, particularly high level profiles, being used for cyber attacks or other illegal activity.

The NSW Cyber Security Policy mandates that agencies complete a self-attestation of compliance with the core requirements of the policy. This policy requires that agency information security management systems take account of the controls in ISO 27001 'Information technology - Security techniques - Information security management systems - Requirements'. This standard requires the regular review of users' access rights, and the removal or adjustment of access rights upon termination of employment or transferral.

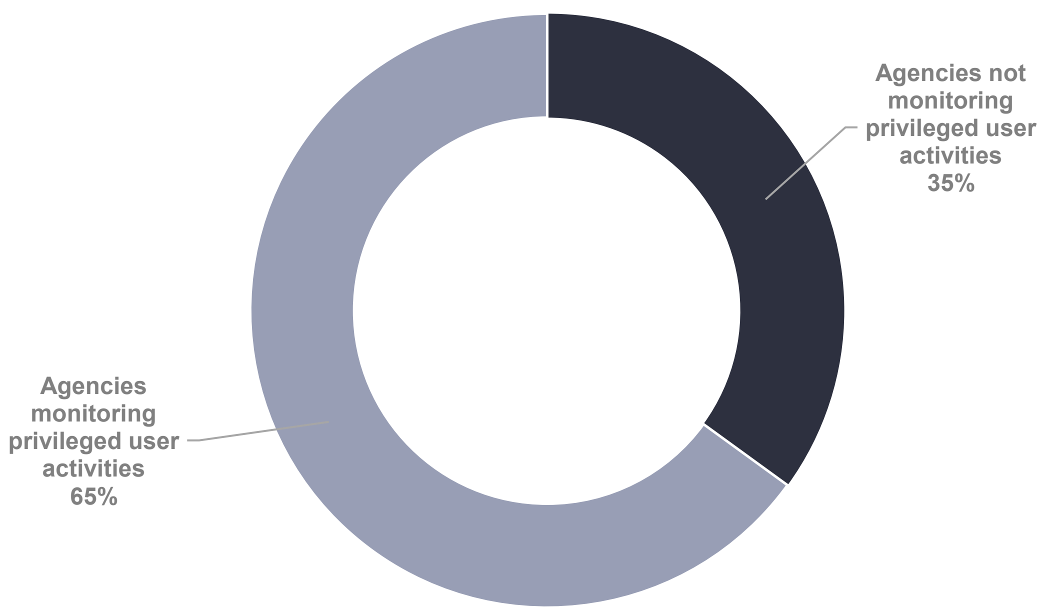
Privileged access

Monitoring of privileged user accounts needs to be strengthened

Agency staff often have access to sensitive data. If that access is not properly controlled and monitored it can increase the risk of a data leak, inappropriate access or use for a fraudulent or improper purpose. This is particularly true for those privileged users who are 'trusted insiders' such as employees, business partners, or third-party contractors.

Thirty-five per cent of agencies do not periodically review the activities of privileged users to identify suspicious or unauthorised activities.

Monitoring of privileged user activities



Source: Audit Office management letters.

Examples of deficiencies included:

- system audit logs not enabled to track user account activities
- no process to periodically review privileged user activities where system audit logs are enabled and maintained
- limited segregation of duties of staff with privileged IT user profiles from business operational responsibilities.

The absence of periodic reviews of privileged user accounts increases the risk that these accounts can 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.

Poor management of privileged access may also lead to breaches of Section 3.6 of the *Government Sector Finance Act 2018* and the NSW Cyber Security Policy. This policy requires that agency information and security management systems take account of ISO 27001. This standard requires that privileged access rights are controlled and restricted.

Agencies should review the number of privileged users and access granted to privileged users, and assess and document the risks associated with their activities. Based on this review agencies should:

- grant and restrict privileged user access only to staff who require that level of access to perform their role
- identify controls to address the risks associated with privileged user activity, including regular monitoring of activity logs.

Password controls

Management of password controls can be improved

Twenty per cent of agencies either did not comply with their own policy on password parameters or did not enforce the minimum expected standard. The deficiencies identified related to:

- passwords not meeting minimum password lengths
- passwords not meeting complexity requirements
- no limit on the number of failed login attempts enforced
- password history not enforced (i.e. the number of passwords remembered and restricting the recycling of recently used passwords)
- minimum and maximum password age is applied (i.e. prompting the change of passwords frequently).

Our audits also identified default and generic passwords were being used by agencies. Weak passwords increase the risk of unauthorised use of, and changes to, financial information. Weaknesses were identified across agency IT applications, databases and database servers.

Agencies should review IT password settings to ensure that they comply with minimum standards and the requirements of their password policies.

Program changes

Approval of changes to IT programs prior to implementation can be strengthened

All agencies have established IT change management policies to ensure the changes to IT programs and related infrastructure components are appropriately authorised, performed and tested prior to implementation. We found deficiencies in agency IT program change controls at 20 per cent of agencies. These deficiencies related to:

- inappropriate segregation of duties over developing and releasing IT program changes to the production environment
- inability to provide evidence for approval of IT program changes
- other issues, such as retaining evidence of approval provided to the service provider prior to releasing changes to production and deficiencies in IT change management policy.

Weak program change controls expose agencies to the risk of:

- unauthorised and/or inaccurate changes to systems or programs
- issues with data accuracy and integrity
- inappropriately accepting releases that come with upgrades.

Agencies should consistently perform user acceptance testing before system upgrades and program changes are deployed. Changes should not be made without appropriate approval and documentation to support the approval.

Computer operations

Management of computer operations is essential to an agency's IT environment as it ensures agencies have implemented appropriate policies and procedures to manage potential disasters and critical system failures. This includes developing business continuity plans and disaster recovery plans.

Some agencies have ineffective business continuity or disaster recovery plans

We found deficiencies in agency disaster recovery and/or business continuity processes at 20 per cent of agencies. These deficiencies related to:

- absence of business continuity or disaster recovery plans, including supporting business impact analysis
- regular review of business continuity plans
- not testing the business continuity or disaster recovery plans during the year.

Without detailed analysis and planning, agencies cannot predict the impact of disruption, identify maximum tolerable outages, or plan informed recovery strategies. They also risk:

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

While most agencies have business continuity and disaster recovery plans, the consequences for those that don’t can be very high were an event to occur. The NSW Cyber Security Policy requires agencies to develop, review and test their business continuity arrangements.

4. Gifts and benefits

This chapter outlines our audit observations, conclusions and recommendations, arising from our review of agency controls to manage gifts and benefits.

Key conclusions and sector wide learnings

We found most agencies have implemented the Public Service Commission's minimum standards for gifts and benefits. All agencies had a gifts and benefits policy and 90 per cent of agencies maintained a gifts and benefits register and provided some form of training to employees on the treatment of gifts and benefits.

Based on our analysis of agency registers, we found some areas where opportunities existed to make processes more effective. In some cases, gaps in recorded information meant the basis for decisions around gifts and benefits was not always clear, making it difficult to determine whether decisions in those instances were appropriate and compliant with policy. Fifty-one per cent of the gifts and benefits registers reviewed contained declarations where not all fields of information had been completed. Seventy-seven per cent of agencies that maintained a gifts and benefits register did not include all key fields suggested by the minimum standards.

Areas where agencies can improve their management of gifts and benefits include:

- ensuring agency policies comprehensively cover the elements necessary to make it effective in an operational environment, such as identifying risks specific to the agency and actions that will be taken in the event of a policy breach
- establishing and publishing a statement of business ethics on the agency's website to clearly communicate expected behaviours to clients, customers, suppliers and contractors
- updating gifts and benefits registers to include all key fields suggested by the minimum standards, as well as performing regular reviews of the register to ensure completeness
- providing on-going training, awareness activities and support to employees, not just at induction
- regularly reporting gifts and benefits to executive management and/or a governance committee such as the audit and risk committee, focussing on trends in the number and types of gifts and benefits offered to and accepted by agency staff
- publishing their gifts and benefits registers on their websites to demonstrate a commitment to a transparently ethical environment.

4.1 Background

The *Ethical Framework* under the *Government Sector Employment Act 2013* requires agencies to implement clear policies and practices to support ethical conduct within the organisation. A 2014 Public Service Commission Direction established minimum standards (the minimum standards) to help agencies effectively manage gifts and benefits received by or offered to public sector employees.

The minimum standards include:

- a policy for the management of gifts and benefits
- a gifts and benefits register
- training and support for employees.

These standards are important as gifts can be offered to agency staff with the intention of inducing them to favour a person or company for reasons other than merit. This can result in decisions that are neither in the agency's nor the public's interest. The minimum standards define gifts and benefits as:

> any item, service, prize, hospitality or travel, provided by a customer, client, applicant, supplier, potential supplier or external organisation, which has an intrinsic value and/or a value to the recipient, a member of their family, relation, friend or associate.

We have reviewed agency management of gifts and benefits in the past. The exhibit below details the results of our more recent audits.

Exhibit 1: Previous Audit Office reports on agency gifts and benefits management

Performance Audit Report on Managing Gifts and Benefits (published February 2013)

The report found that overall, the five audited entities were managing some aspects of gifts and benefits effectively, but other aspects required improvement. It found all five agencies:

- had gifts and benefits policies that addressed some but not all of the attributes of a sound policy
- had communicated their gifts and benefits policies to staff and external stakeholders
- had registers in place for recording the details regarding each gift and benefit. However, none of the registers included sufficient information to gauge whether the decisions regarding the treatment of each gift and benefit were appropriate.

The report also recommended that the Public Service Commission develop a set of minimum standards for gifts and benefits management, which were subsequently issued in 2014, as noted above.

Report on Internal Controls and Governance (published December 2017)

The report found that all 39 major agencies had a gifts and benefits policy, but there were gaps in the management of gifts and benefits by some agencies that increased the risk of unethical conduct.

Where relevant, we have included the results from our 2017 Report on Internal Controls and Governance below for comparison purposes.

Overview of gifts and benefits registers

The table below shows the number and value of gifts and benefits recorded in agency gifts and benefits registers for 2018–19 financial year.

We analysed agency gifts and benefits registers and reviewed items with a high value that were accepted by agencies. Accepting a high value gift or benefit is not necessarily a threat to the integrity of the recipient or the agency. Tickets to supplier hosted conferences or events, or invitations to educational courses may legitimately benefit both the recipient and their agency. However, in some cases it was difficult for us to make this determination because the gift register did not clearly record:

- that the acceptance of the gift or benefit had been approved by the approving officer
- the relationship with the gift provider (business or personal)
- a description of the context in which the gift was offered and/or received
- the rationale for the decision regarding the acceptance (or refusal, or disposal) of the gift.

We found the smaller an agency, in terms of its annual expenditure, the more likely it was to accept a gift or benefit from a supplier or potential supplier.

Gifts and benefits register

Agency expenditure (2018–19)

Description	$100 million to $500 million	$500 million to $1.0 billion	$1.0 billion to $5.0 billion	$5.0 billion +
Offers received				
Number of agencies	15	10	10	5
Highest value of offers	$8,000	$6,000	$30,000	$7,000
Lowest value of offers	$5	$1	$1	$1
Number of entries in the registers	728	310	502	522
Offers accepted				
Highest value offer accepted	$8,000	$6,000	$30,000	$3,799
Lowest value offer accepted	$5	$1	$1	$5
Percentage of offers accepted (including pending approval)	95%	94%	79%	67%
Offers declined				
Highest value offer declined	$2,000	$200	$1,200	$7,000
Lowest value offer declined	$10	$10	$3	$1
Percentage of offers declined	5%	6%	21%	33%

Source: Audit Office analysis of agency gifts and benefits registers (for the period 1 July 2018 to 31 March 2019).

Analysis of registers shows staff are accepting higher risk gifts and benefits

We examined agency gifts and benefits registers for offers that presented a higher risk to the agency, in that they could be perceived as an inducement for a staff member to act in a certain way. These offers were gifts and benefits, which had been accepted by an agency staff member and that are more likely to be, or perceived to be for the benefit of the staff member rather than their agency, such as offers of hospitality.

Agency staff need to have effective working relationships with contacts in the commercial sector, but agency policies and practices need to ensure these relationships do not result in, or cannot be perceived to result in preferential treatment for the supplier or business partner.

We were not always able to establish from the information in agency registers, the rationale for why the gift or benefit had been accepted, or what was the approximate value of the gift or benefit. Nor were we always able to establish how the agency had concluded that there was no actual or perceived ethical conflict.

On-going monitoring and oversight from agency executive management and/or governance committees would help to ensure decisions related to higher risk gifts and benefits are being appropriately and consistently made. We explore this further in Section 4.4 below, while the exhibit below provides examples of higher risk hospitality gifts and benefits accepted by agencies.

Exhibit 2: Examples of higher risk accepted gifts, benefits and hospitality

Our review of gifts and benefits registers identified instances of service providers, customers, consultants or suppliers that have offered hospitality, gifts and benefits, which were accepted by agency staff, such as:

- tickets to the Australian Open tennis in Melbourne as part of a two-day conference held by a service provider (value not estimated in the agency register)
- tickets to a corporate box at the Newcastle Jets soccer game valued at $75 offered by a customer
- dinner and theatre tickets valued at $200 offered by a service provider
- tickets to the 2019 Archibald, Wynne and Sulman Prizes Exhibition valued at approximately $200 offered by a service provider
- tickets to the Sydney Food Awards Events valued at $94 offered by a media partner
- dinner and tickets to the theatre valued at $180 offered by a consultant
- tickets to the 2018 Customer Experience Award Ceremony valued at $175 by a service provider
- tickets to a Michael Bublé concert valued at $150 offered by a consultant
- tickets to Care and Service Excellence (CASE) Awards valued at $185 offered by a service provider.

None of the agencies that accepted the above gifts, benefits or hospitality publicly reported their gifts and benefits register. Only half the agencies reported on activity in the gifts and benefits register to an executive management and/or a governance committee.

4.2 Policy framework

We reviewed the adequacy of the policies agencies have developed and implemented to support the minimum standards.

Agencies have established a policy for the management of gifts and benefits

Consistent with our 2017 Report on Internal Controls and Governance, all agencies have established policies and guidance to guide employees in their roles and responsibilities when they are offered or receive a gift. However, 20 per cent of agencies have not reviewed their gifts and benefits policies by the scheduled date and there are some key gaps in agency policies:

- 17 per cent of policies did not identify specific risks relevant to the agency or its business units
- 17 per cent of policies did not specify how breaches would be handled
- 27 per cent of agencies' policies did not specify that it applied to contingent workers.

Up to date and comprehensive policies help ensure there is appropriate management of gifts and benefits. Without appropriate guidance there is a risk that staff may unwittingly accept gifts that influence, or are perceived to have influenced their decisions.

The table below provides an overview of agencies' compliance with key policy components set out in the minimum standards.

Policy requirement per the minimum standard	Percentage of agencies complying with requirements (%)
State employees' obligations clearly	100
Outline an approval process	100
Address conflicts of interest	98
Define 'gifts and benefits'	98
Establish threshold, if appropriate	88
Specify how breaches will be handled	83
Identify specific risks	83

Source: Audit Office analysis.

Most policies clearly outlined employees' obligations in relation to gifts and benefits

All agencies' policies provided guidance outlining obligations for agency staff in relation to gifts and benefits. However, we found a small percentage of agencies' policies contained one or more gaps in their guidance.

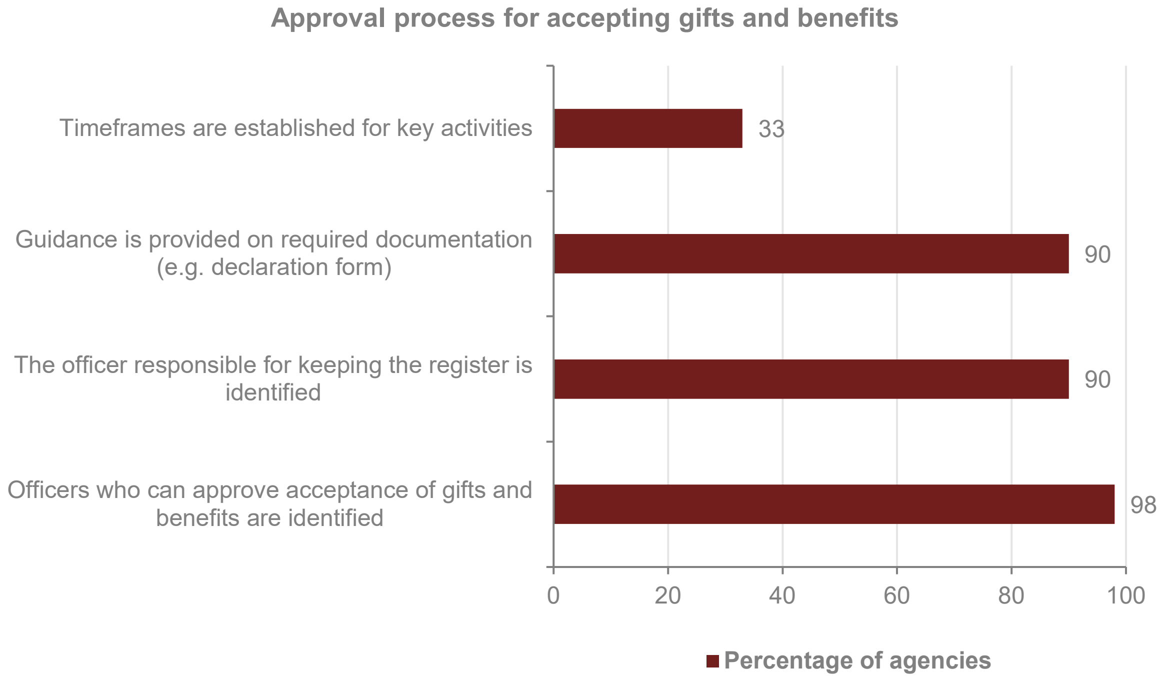
Employee's obligation, as set out in the minimum standards	Percentage of agencies providing guidance (%)
Not to solicit a gift or benefit	95
To decline a gift or benefit where the recipient is currently, or may in the future, exercise discretion in making a decision affecting the giver	95
To seek management approval to accept a gift and benefit that is allowed	95
To record gifts and benefits in the register promptly	95
To read, understand and comply with the gifts and benefits policy	93
To decline a gift or benefit that is not allowed	90
Not to accept a gift or benefit where it is to be provided to a family member, relation, friend or associate	88
Not to accept a gift or benefit where the recipient is unsure about whether the gift or benefit is permitted	88
To always decline, but register the offer of a gift of benefit where a conflict of interests exists (actual, potential or reasonably perceived)	87

Source: Audit Office analysis.

Approval processes for gifts and benefits could be improved by setting clear timeframes

All agencies have policies outlining the approval process for accepting gift and benefits that identify who can approve declarations and who maintains the agency gift register. However, only 33 per cent of the policies included timeframes for key activities required by the approval process, such as making a declaration following an offer, and having it assessed by a manager authorised to approve the offer. This increases the risk that actual or perceived conflicts of interest arising from offers of gifts or benefits will not be dealt with in a timely and appropriate manner.

The graph below summarises key aspects of the approval process specified in agency policies.



Source: Audit Office analysis.

4.3 Managing gifts and benefits

We reviewed the adequacy of agency gifts and benefits registers, and the training and awareness programs agencies have implemented to support adherence to the minimum standards.

Recommendation

Agencies should:

- **ensure their gifts and benefits register includes all key fields specified in the minimum standards, as well as performing regular reviews of the register to ensure completeness**
- **provide on-going training, awareness and support activities to employees, not just at induction**
- **establish an annual attestation process for senior management to attest compliance with gifts and benefits policies and procedures**
- **publish their gifts and benefits registers on their websites to demonstrate their commitment to a transparently ethical environment.**

Declaration process

Most agencies have implemented a standard process to declare gifts and benefits

Ninety-eight per cent of agencies have established a standard gift declaration form for staff to complete when making declarations about offers of gifts and benefits.

Ineffective declaration processes increase the risk that there will be an inadequate assessment over the decision to accept or decline the gift or benefit, the decision will not be authorised, or will not be made on a timely basis.

A standard declaration form ensures that all key information about the offer, and the agency's decision are captured and recorded in the gifts and benefits register.

Despite agencies having declaration procedures in place, only 75 per cent of the agencies require employees to immediately declare gifts and benefits at the point at which the offer is made.

Gifts and benefits register

Some agency gifts and benefits registers do not include key fields, or contain gaps in recorded information

While 90 per cent of agencies keep a centralised register for declarations of gifts and benefits, they do not contain all key fields suggested by the minimum standards, as set out in the table below. Fifty-one per cent of the gifts and benefits registers we reviewed contained declarations with at least one missing information field, such as details of the officer approving acceptance of the gift or benefit, the value of the gift or benefit and/or details of the reasons for the decision.

Gaps in agency gifts and benefits registers make it difficult to determine whether decisions regarding the treatment of each gift and benefit was appropriate in the circumstances and consistently applied. Gaps in information diminish the usefulness of reporting to agency executive teams and/or governance committees on trends in gifts and benefits. It also reduces the transparency of agency reporting, where agencies elect to make this information public.

The table below outlines whether agency gifts and benefits registers comply with key information requirements specified in the Direction's minimum standards.

Key information requirement for agency gifts and benefits registers (of the 90% of agencies with centralised registers)	Percentage of agencies requiring this information (%)
Date of receipt	100
Name and business unit of the receiver	100
Name and organisation of the giver	100
Description of the gift or benefit	100
Estimated value of the gift or benefit	100
Decision (e.g. accept and retain; accept and dispose; refuse)	94
Description of the context in which the gift or benefit was offered and/or received	89
Name of the approving manager or supervisor	86
Disclosure of any relationship–business or personal–between the giver and receiver	86
Reasons for the decision	74
Supporting evidence for the estimated value of the gift or benefit	31

Source: Audit Office analysis.

Gifts and benefits registers are not being made publicly available by agencies

Only three per cent of agencies have published their gifts and benefits register on their website. Publishing the gifts and benefits register demonstrates the agency's commitment to establishing a transparently ethical environment. Transparency and openness allows agencies to demonstrate to the public that appropriate decisions are being made in relation to acceptance of gifts, benefits and hospitality and how the agency manages actual or perceived conflicts of interest.

Statement of business ethics

Agencies did not always publish a statement of business ethics on their website

Only 60 per cent of agencies have established and published a statement of business ethics on their website. This compares unfavourably to the 2017 Report on Internal Controls and Governance, where we found 87 per cent of agencies had established and published a statement of business ethics. Not all of the agencies reviewed this year were reviewed in the previous year.

	2019 Report Percentage of agencies (%)	2017 Report Percentage of agencies (%)
Agencies that have established and published a statement of business ethics	60	87

Without a statement of business ethics, clients, customers, suppliers and contractors may not be aware of an agency's values, its probity processes and the standard of behaviour the agency expects when a customer, client, applicant, supplier, potential supplier or external organisation deals with the agency and its staff. It also makes it harder for agencies to hold those parties to account for conduct that breaches the ethical standards of the NSW public sector.

The exhibit below reinforces the importance of establishing a statement of business ethics.

Exhibit 3: ICAC Investigation into corrupt procurement practices at a public sector agency (August 2017)

> The ICAC investigated corrupt procurement practices at a public sector agency. In addition to making findings about procurement practices, the investigation identified that a number of public officials had engaged one of the agency's suppliers to perform minor works and renovations at their homes. In one case involving the construction of a swimming pool, a significant discount was given, which the Commission found to be a corrupt payment and created a significant corruption risk because the practice may constitute an actual or perceived corrupt payment. Additionally, a sense of obligation or friendship could arise between a contractor and a public official, resulting in the public official improperly favouring the supplier in the exercise of his or her public functions.

Training and support

Agencies do not always provide on-going training and support to staff on gifts and benefits

Ninety per cent of agencies provide training to new starters on their obligations in regards to gifts and benefits as part of the induction process. Eighty-eight per cent of agencies have designated a senior officer to advise employees on their obligations, but only 73 per cent of agencies provide on-going training to all staff.

While the overall results are positive, the results show that agencies could do more in providing on-going training and support to employees. On-going training and awareness programs allow agencies to communicate to all staff their responsibilities and obligations in relation to gifts and benefits offered or received. It also demonstrates the agency's commitment to maintaining an ethical environment and reduces the risk of inappropriate conduct by employees.

The minimum standards recommend that agencies remind staff of their obligations in managing gifts and benefits at least annually and that formal training is integrated into existing cyclical training or development activities, including performance development programs. The minimum standards also specify that the nature and type of awareness or training should take into account the risk and likelihood of receiving a gift or benefit based on the employee's role.

4.4 Reporting and monitoring

Recommendation

Agencies should regularly report to the agency executive or other governance committee on trends in the offer and acceptance of gifts and benefits.

Monitoring and reporting on gifts and benefits can be improved

Seventy-three per cent of agencies had a designated senior manager who reviewed entries in the gifts and benefits register and helped ensure actions taken complied with the policy. Thirty-five per cent of agencies reported trends in the number and nature of gifts and benefits recorded in their registers to the agency's senior executive management and/or governance committees, which was a decline since we last examined this area in our 2017 report.

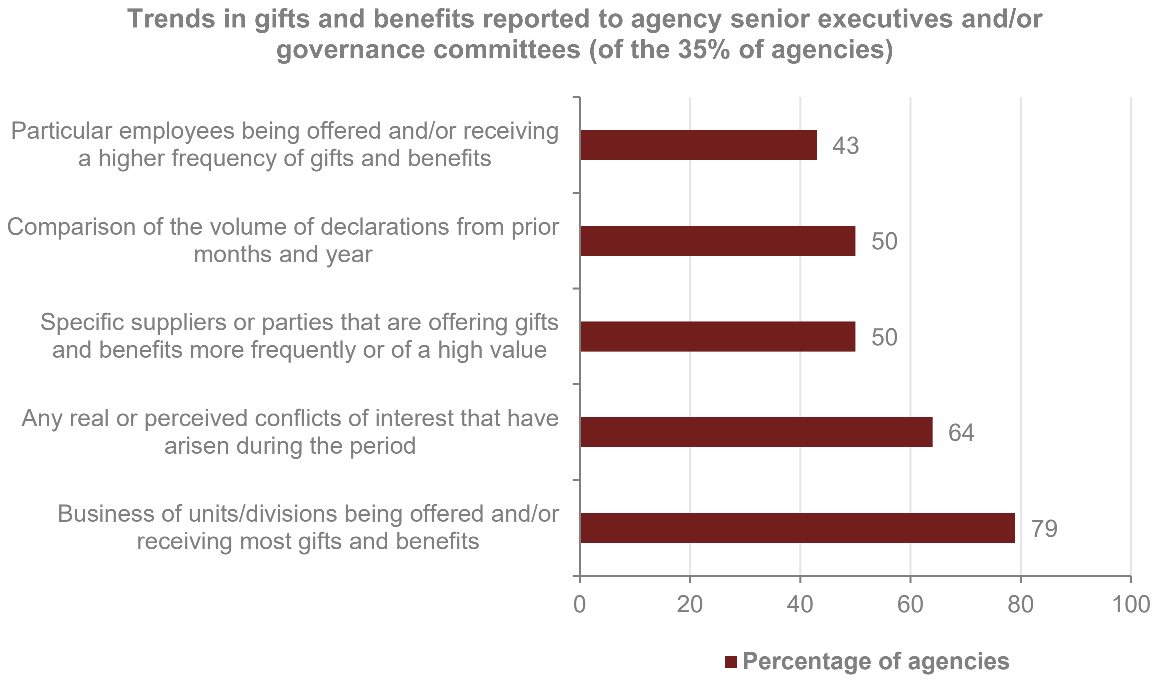
	Percentage of agencies reporting trends in 2019 (%)	**Percentage of agencies reporting trends in 2017 (%)**
Trends in the number and nature of gifts and benefits recorded in gifts and benefits complied and reported to the agency's senior executives and/or governance committee	35	67

Periodic review of the number, nature and trends in gifts and benefits registers by agency executive management and/or governance committees helps agencies support an ethical culture by:

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

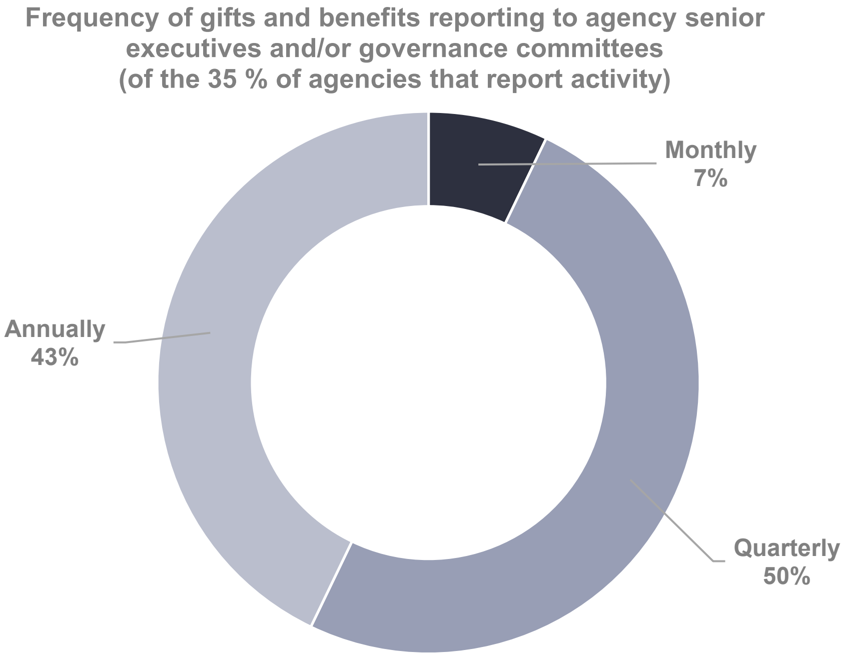
Reporting and monitoring of this nature also helps reinforce to staff the importance of complying with the agency's gifts and benefits policy.

Of those agencies that reported information on gifts and benefits to senior management and/or governance committees, the areas that were reported included the following:



Source: Audit Office analysis.

The graph below illustrates the frequency with which the information was reported to agency executive management and/or governance committees.



Source: Audit Office analysis.

5. Internal audit

This chapter outlines our audit observations, conclusions and recommendations, arising from our review of agency internal audit functions.

Key conclusions and sector wide learnings

We found agencies have established and maintained internal audit functions to provide assurance on the effectiveness of agency controls and governance systems as required by TPP15-03 'Internal Audit and Risk Management Policy for the NSW Public Sector'. However, we identified areas where agencies' internal audit functions could improve their processes to add greater value, including:

- documenting and implementing safeguards to address conflicting roles performed by the Chief Audit Executive (CAE)
- ensuring the reporting lines for the CAE comply with the NSW Treasury policy, and the CAE reports neither functionally or administratively to the finance function or other significant recipients of internal audit services
- involving the CAE more extensively in executive forums as an observer
- documenting a Quality Assurance and Improvement Program for the internal audit function and performing both internal and external performance assessments to identify opportunities for continuous improvement
- reporting against key performance indicators or a balanced scorecard and producing an annual report on internal audit to bring to the attention of the audit and risk committee and senior management strategic issues, thematic trends and emerging risks that may require further attention or resources.

5.1 Background

NSW Treasury's Policy Paper TPP15-03 Internal Audit and Risk Management Policy for the NSW Public Sector (the policy) sets out three core requirements for internal audit. These are for agencies to:

- establish and maintain an internal audit function
- operate an internal audit function that is consistent with the International Standards for the Professional Practice of Internal Auditing
- have an Internal Audit Charter that is consistent with the content of the 'model charter'.

The policy applies to most agencies within the scope of this report, except for State Owned Corporations. For these agencies, applying the policy is a matter of best practice.

Internal audit is a key component of an agency's internal control environment. NSW Treasury's policy adopts the Institute of Internal Auditors' definition of internal audit, which is:

> an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

A key principle of the policy is that an agency's internal audit function provides timely and useful information to management about:

- 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.

This chapter does not review compliance with all aspects of the policy, but considers how agencies have implemented some key policy requirements, as well as elements of better practice in internal auditing.

5.2 Resourcing

The policy requires agency heads to ensure there is an operational and adequately resourced internal audit function. Agencies may choose to deliver the function using:

- an 'in-house' model, whereby all, or predominantly all resources are the agency's own human resources
- an 'out-sourced' model, whereby services are provided exclusively by an appropriately qualified third party provider
- a ‘co-sourced’ model, whereby the agency provides and manages internal audit services through a combination of in-house resources and contracted services delivered by an appropriately qualified third party provider.

An agency may co-source or out-source their internal audit resources using a pooled arrangement through, for instance, their cluster.

Sourcing model

Most agencies have implemented a co-sourcing model

We found that all agencies have implemented an internal audit function, as required by the policy. The most commonly implemented model by agencies is a co-sourcing model, whereby internal audit services are provided and managed by a combination of in-house and contracted resources.

The table below sets out the internal audit sourcing model adopted by agencies in the scope of this report.

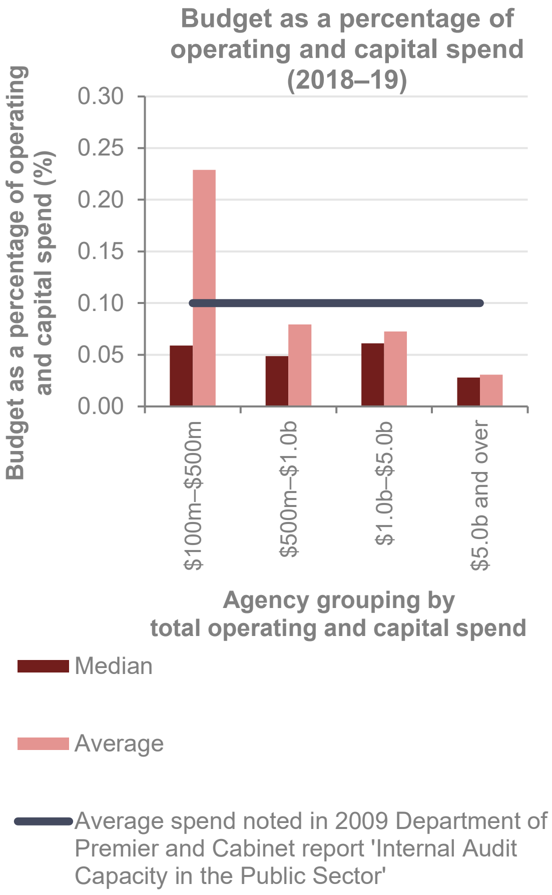
Internal audit sourcing model	Number of agencies
In-house	3
Co-sourced	20
Out-sourced	17

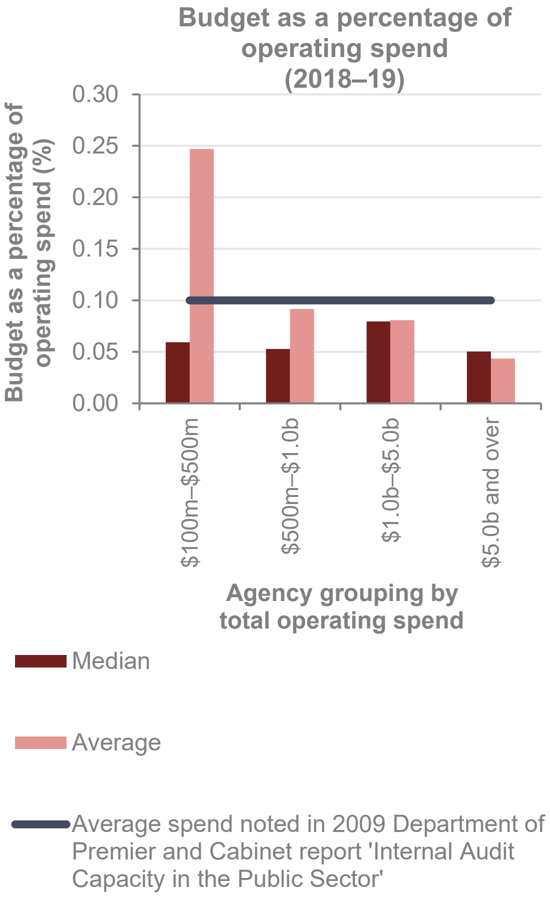
Source: Audit Office analysis.

Internal audit budgets

Both the size and complexity of an agency’s operations will impact the internal audit budget. Therefore, it is important that the complexity of an agency is also taken into account when assessing the adequacy of internal audit resources and not simply its size. For example, a recent Internal Audit Benchmarking Survey performed by the Institute of Internal Auditors found that there was little correlation between internal audit size and organisational turnover.

We grouped the 40 agencies into four ranges based on the size of their total operating and capital spend and calculated each agency’s internal audit budget as a percentage of this spend. In the graph below, we have included the median and average budget of agencies in each of the groupings as a percentage of total spend. This information will allow internal audit functions in the NSW public sector to compare its budget against similar sized agencies.





Source: Internal audit budgets provided by agencies (unaudited) and agency operating, and capital expenditure sourced from audited financial statements. For the purpose of this analysis agency operating expenditure excludes grants paid to cluster agencies.

In 2009, the Department of Premier and Cabinet released a report titled 'Internal Audit Capacity in the Public Sector'. The report noted that total spend on internal audit was on average 0.1 per cent of operating expenditure.

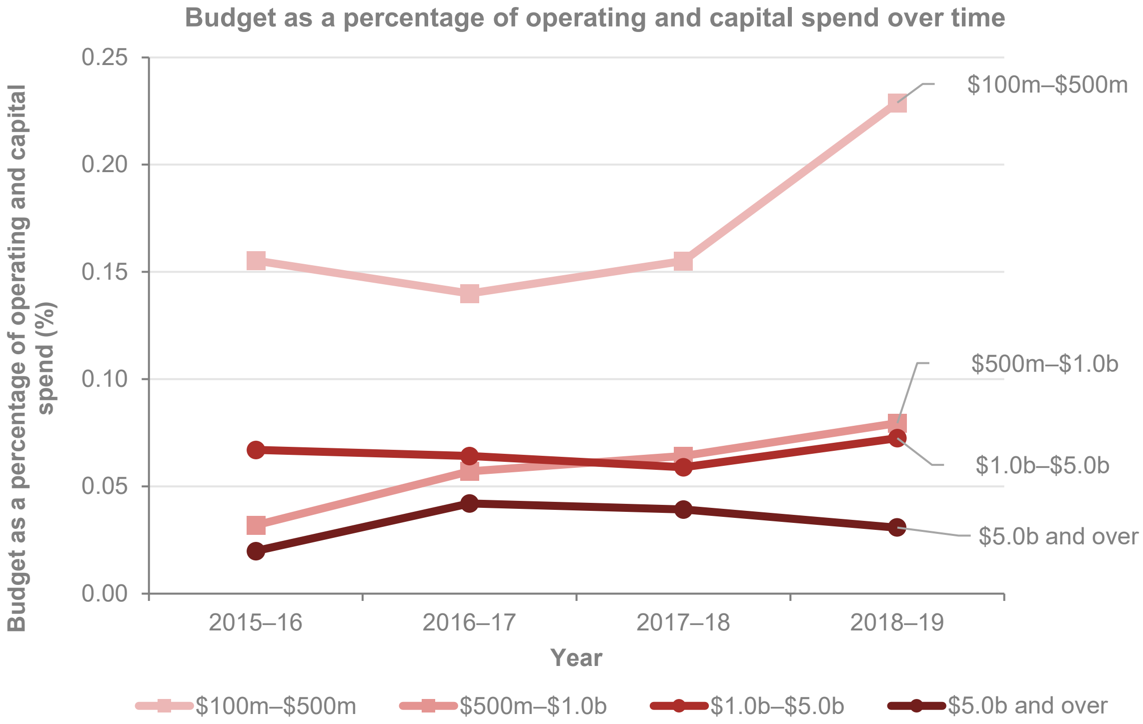
The median and average budget of agencies in each of the groupings is sitting below the amount noted in the report. Pressure on agencies to drive budget efficiencies and meet efficiency dividend targets can often impact the effectiveness of their risk management and control frameworks. However, this increases the importance of internal audit functions having the necessary resources to provide assurance to agencies on these aspects of their operations.

The policy requires agency heads to ensure that the internal audit function has a budget and access to skilled and capable resources that are sufficient relative to the risks and assurance needs of the agency. Audit and risk committees and agency heads should be seeking assurance from the Chief Audit Executive that the level of resourcing is appropriate to the agency, such that they can discharge their responsibilities under the policy.

Internal audit spend has generally remained proportionately stable over time

The graph below illustrates the change in average internal audit functions' budgets over time as a percentage of total operating and capital expenditure. Smaller agencies spend proportionally more than larger agencies.

Average internal audit budgets have remained stable as a proportion of total operating and capital spend over the last four years, with a small average increase across agencies in each of the groupings, except those with capital and operating expenditure exceeding $5.0 billion.



Source: Internal audit budgets provided by agencies (unaudited) and agency operating, and capital expenditure sourced from audited financial statements. For the purpose of this analysis agency operating expenditure excludes grants paid to cluster agencies.

5.3 Chief audit executive

Recommendation

Agencies should ensure:

- **the reporting lines for the CAE comply with the NSW Treasury policy, and the CAE does not report functionally or administratively to the finance function or other significant recipients of internal audit services**
- **the CAE's duties are compatible with preserving their independence and where threats to independence exist, safeguards are documented and approved.**

The chief audit executive (CAE) is the most senior officer responsible for the internal audit function. Although the CAE is part of the agency, the role must be operationally independent from management. To achieve this, internal audit has a dual reporting line. The policy advises that the CAE should report functionally to the audit and risk committee on completed audits and strategic matters, and administratively to the agency head on day to day matters.

Internal audit charter

All agencies have an internal audit charter in place

All agencies have an internal audit charter that is consistent with the 'model charter' in the policy. However, 37 per cent of agencies had not published the charter on the agency's intranet.

The purpose of the internal audit charter is to address the role, responsibilities, authority, activities and reporting lines of the internal audit function. Publishing the internal audit charter helps to raise awareness of the internal audit function, as well as ensuring that agency staff are aware of the authority and purpose of internal audit.

Roles and responsibilities

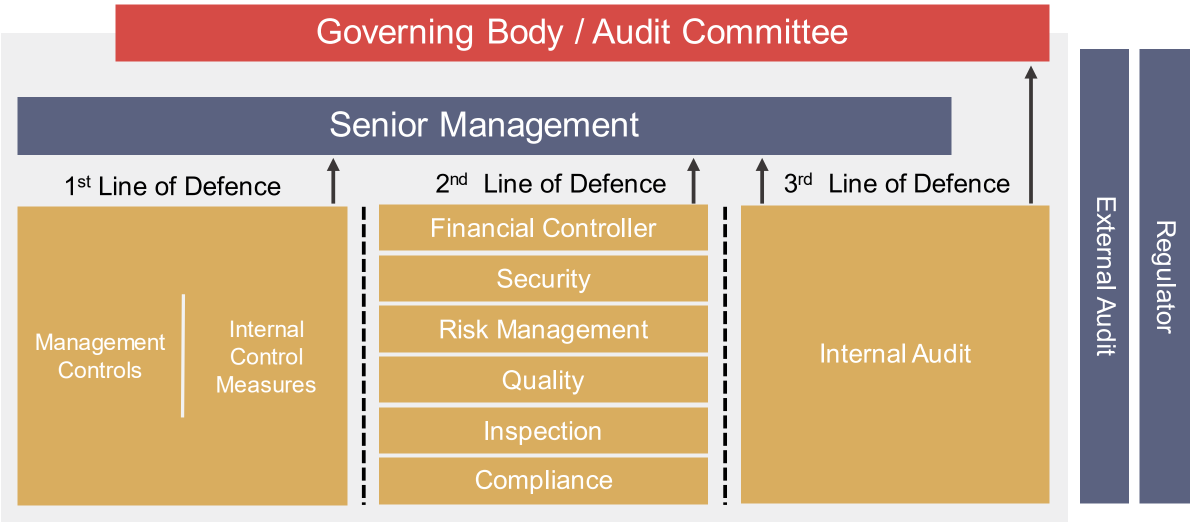
The policy requires the agency head to determine whether the CAE role will be a dedicated role within the agency. It specifies that this would generally be the case where the agency has more than one of the following factors:

- significant assets
- a high risk profile
- a high level of expenditure
- engages in complex transactions.

The responsibilities of the CAE are often broader than only internal audit

Forty-five per cent of agencies assigned responsibilities to the CAE that were broader than internal audit. As the analysis below demonstrates, smaller agencies are more likely to assign additional responsibilities to the CAE where the CAE role is not a full time equivalent position. Generally, these additional responsibilities are likely to be in relation to risk, compliance and/or investigation activities. However, in these circumstances, it is important that safeguards are considered to protect the independence of the CAE, which is explored further below.

The Institute of Internal Auditors endorse the three lines of defence model. Internal audit is the third line of defence, and without adequate safeguards, having internal audit perform level one or two responsibilities risks failure in an agency's lines of defence.



Source: Institute of Internal Auditors. Refer link.

The three lines of defence are:

First line of defence - functions that own and manage risk. These are the managers and staff who are responsible for identifying and managing risk as part of their accountability for achieving objectives.

Second line of defence - functions that oversee or who specialise in compliance or the management of risk. These are the policies, frameworks, tools, techniques and support to enable risk and compliance to be managed by those in the first line of defence.

Third line of defence - functions that provide independent assurance. This is provided by internal audit.

Of the 40 agencies whose functions we reviewed, 18 agencies had level one or two responsibilities assigned to their internal audit functions.

Total operating and capital spend	Level one responsibilities in the 'three lines of defence model' (number of agencies)	Level two responsibilities in the 'three lines of defence model' (number of agencies)
$100 million–$500 million	3	7
$500 million–$1 billion	--	5
$1.0 billion–$5.0 billion	--	2
$5.0 billion	--	1

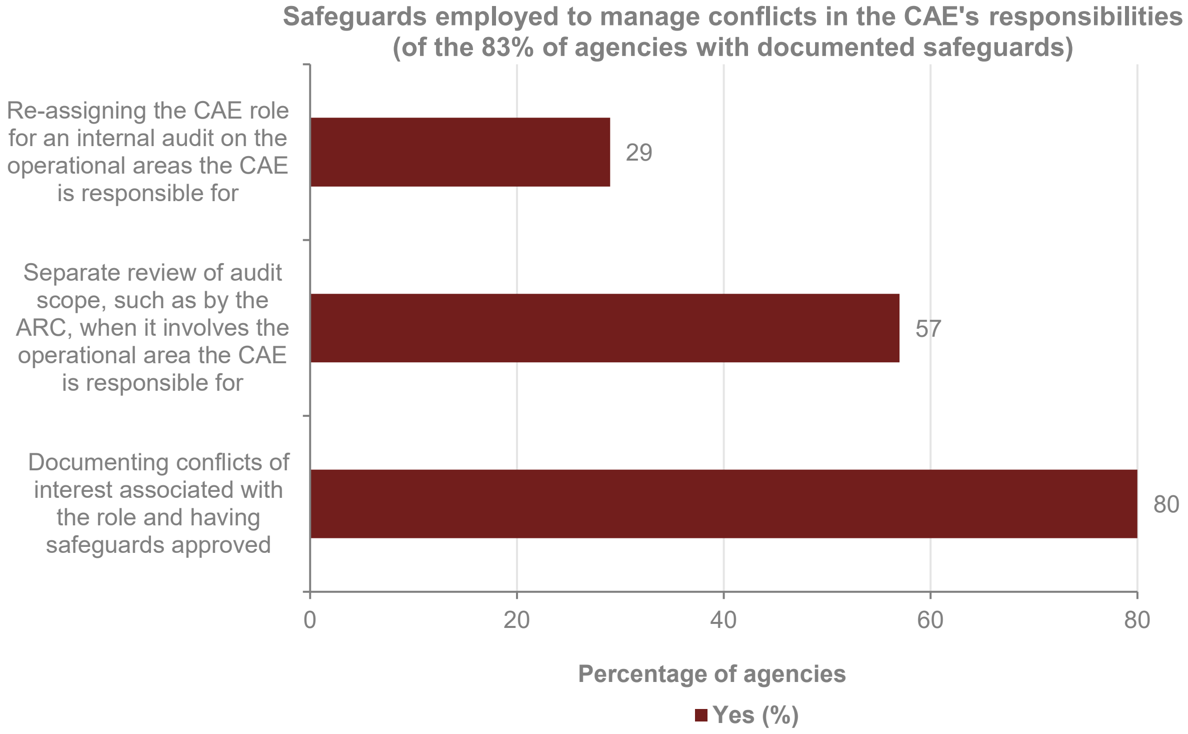
Source: Audit Office analysis.

Agencies have not always documented safeguards where the CAE has conflicting roles

Seventeen per cent of 18 agencies have not documented safeguards in circumstances where the responsibilities of the CAE are broader than overseeing the internal audit function.

Where the CAE's responsibilities extend beyond internal audit there is a possibility the CAE may perform an internal audit on an area they have operational responsibility over. Without safeguards to protect the independence of the internal audit function there is an increased risk that conflicts of interest will arise that impact the objectivity of internal audit findings.

The policy provides examples of safeguards that can be implemented. The types of safeguards implemented by the 83 per cent of agencies that have documented safeguards are presented below.



Source: Audit Office analysis.

Reporting lines

Most CAEs are positioned at a relatively senior level within the agency

Ninety-five per cent of CAEs either report directly to the agency head or report to a direct report of the agency head. Positioning the CAE at a senior level in the agency ensures that they can discuss and negotiate internal audit results with senior management on a reasonably equal footing. It also:

- reduces the risk of a conflict of interest arising in the reporting line (also see below)
- helps to ensure the CAE has direct access to the agency head to raise concerns and highlight emerging risks.

Our analysis below shows that the status of the CAE's position within agencies varied.

Number of reporting levels from the agency head	Departments	Statutory bodies	State Owned Corporations	Number of agencies
1 level (i.e. reports directly to the agency head)	12	10	2	24
2 levels	5	5	4	14
3 levels	1	1	--	2

Source: Audit Office analysis.

Two agencies CAEs reporting lines did not comply with the policy

The policy does not allow the CAE to report to the Chief Finance Officer (CFO) for administrative or functional matters. Reporting to a member of management who receives internal audit services can impair the independence of the CAE, create conflicts of interest that are difficult to safeguard against and undermine the effectiveness of the internal audit function.

We found two instances where the CAE's independence and the effectiveness of internal audit were potentially compromised by agency arrangements:

- a CAE reported administratively to the CFO. The agency's policy provided for direct access to the agency head at the CAE's discretion and where a potential conflict existed, but the agency had not obtained an exemption from the NSW Treasury policy
- an acting finance manager, who reports to the CFO, has also been acting in the CAE role for a year. The agency had determined that it was sufficient for the finance manager, in their capacity as CAE to have direct access to the Board, the CEO and the ARC. In the period that this arrangement has been in place, one internal audit has been performed on compliance with licensing outcomes, which is part of the CFO's responsibilities, but no specific reviews have been performed on the finance function.

In circumstances where the CAE does not report directly to the agency head, the CAE's reporting line should be to the next most independent member of management who is not a receiver of significant internal audit services.

CAEs could add value through greater involvement in executive forums

It is essential to the operation of an effective internal audit function that the CAE has direct access to the head of the agency and the audit and risk committee chair. We found this happened in the vast majority of cases:

- 95 per cent of CAEs meet regularly with the agency head
- 95 per cent of CAEs meet regularly with the audit and risk committee chair.

However, only 73 per cent of CAEs regularly attend meetings of the agency board or executive management committee. Attendance at these forums enables the CAE to keep abreast of strategic priorities, risks and issues impacting the agency, which can be considered in the internal audit planning process. The CAE can also add value to these forums by:

- providing senior management with updates on common findings and themes, emerging risks and the status of outstanding recommendations
- providing advice to the committee on relevant matters in a 'trusted advisor' capacity.

5.4 Internal audit planning

Developing and approving the internal audit plan

Some agencies' annual internal audit plans have not been approved by the agency head, and others have been approved late

All agencies have implemented an annual internal audit plan. Ninety-eight per cent of internal audit plans were endorsed by the audit and risk committee. Only 78 per cent of agencies could evidence approval by the agency head, of which 54 per cent were approved after the start of the 2018–19 financial year.

Timely approval of the internal audit plan by the agency head reduces the risk:

- the plan will not adequately address the strategic risks facing the agency
- the plan will not be delivered on time, as a result of delays in commencement of internal audit activity.

The policy requires agency heads to approve the annual internal audit plan. CAEs should make arrangements to have internal audit plans approved before the plan is due to commence.

Assurance maps are not always used to inform the development of internal audit plans

Sixty-two per cent of agencies do not use assurance maps to inform development of internal audit plans. An assurance map can help avoid duplication and identify gaps in assurance activities, and allow internal audit to direct resources to where they are most needed. It also provides audit and risk committees with a comprehensive view about the agency's internal control environment and identify where gaps may exist.

An assurance map documents the sources of assurance in place across key risks. Assurance can be obtained in a number of ways, including internal or external audit activity, other third party reviews, oversight committees and management review activities. An assurance map should be used to inform the internal audit plan in conjunction with other information sources, including:

- agency strategic plans, priorities and risk registers
- input from senior management and audit and risk committees
- external information, such as recent ICAC findings or reports from industry or other authoritative bodies
- internal audit topics from prior years.

Coverage of internal audit plans

There are opportunities for internal audit to increase focus on culture and continuous auditing

We identified some topics that are likely to be highly relevant to agencies in the current environment and considered how well agency internal audit plans address these matters. The results of our analysis are below.

Topic	Included in 2018–19 agency's internal audit plan %	Why is it important?
Continuous auditing	20	Continuous auditing enables internal audit to continuously gather from process data that supports auditing activities. This can involve interrogating key information technology systems on a regular and frequent basis to identify anomalies or transactions that are outside predetermined parameters. Continuous auditing can deliver greater value because it: • enables internal audit to shift its focus from cyclical and ad-hoc reviews to continuous, broader more proactive reviews • supports investigation or compliance review activities • acts as a general deterrent against fraud in the agency.
Organisational culture	28**	The recent Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry highlighted the importance of organisational culture. Even agencies with good governance processes can be undermined by a culture that condones poor behaviour and lax decision-making practices. Agencies need to monitor culture to ensure organisational values are reflected in operationally.
Project assurance or multi-stage	58	The NSW Government will invest $93.0 billion in infrastructure over the next four years*. Infrastructure investment projects of this scale often run over several years and create operational and financial risks. Agencies' project governance need to support the on time, on budget delivery of projects.

Topic	Included in 2018–19 agency's internal audit plan %	Why is it important?
Cyber or IT security	73	The NSW Government's digital footprint is expanding as it prioritises on-line interfaces with citizens, and the number of transactions conducted through digital channels increases. Agencies need to maintain secure digital environments that protect citizen interests, privacy, and autonomy.

* Budget Paper 'Infrastructure Statement 2019–20'.

** This includes agencies that performed internal audits that considered aspects of organisational culture, as part of a broader internal audit topic.

Source: Audit Office analysis.

5.5 Quality assurance and improvement and performance measurement and reporting

Quality assurance and improvement

Recommendation

Agencies should ensure there is a documented and operational Quality Assurance and Improvement Program for the internal audit function that covers both internal and external assessments.

Thirty-five per cent of agencies did not have a documented quality assurance and improvement program, as required by the policy and the International Standards for the Professional Practice of Internal Auditing (the standards).

A quality assurance and improvement program helps ensure conformance with the standards, assess the ongoing efficiency and effectiveness of internal audit activity and identify opportunities for improvement.

Agency internal audit policies and procedures should set out the quality assurance and improvement program. This should be established even if the agency adopts an outsourced internal audit model.

Not all agencies are performing internal and external assessments of internal audit activity

The analysis below shows the types of internal and external assessments performed by agencies.

Internal and external assessments of internal audit activity	Percentage of agencies (%)
Internal assessments	
Evaluation performed after completion of each internal audit	73
Evaluation completed annually by the audit and risk committee	63
Evaluation completed annually by senior management	45
Annual self-assessment performed against the standards and reported to audit and risk committee	63
External assessments	
External quality assessment performed in the last five years	80

Source: Audit Office analysis.

Performance measurement and reporting

On-going reporting

Only 43 per cent of agencies report on the performance of their internal audit functions against key performance indicators

All agencies perform some form of ongoing reporting to audit and risk committees, covering the status of the internal audit plan, completed audits and outstanding recommendations. However, 57 per cent of agencies have not implemented any form of reporting against key performance indicators (KPIs) or in a balanced scorecard reporting format. This makes it is difficult for audit and risk committees to objectively assess the performance of the internal audit function.

A balanced scorecard is a common method of measuring and managing performance of the internal audit function. Examples of KPIs and other guidance on the use of balanced scorecard reporting can be found in the Institute of Internal Auditors Whitepaper Balanced Scorecard Reporting.

Annual reporting

Some agencies are starting to produce an annual report on internal audit

Forty-five per cent of agencies produce an annual report on internal audit, summarising the work of internal audit and achievements for the year. An annual report allows the internal audit function to report on their performance and add value by drawing to the audit and risk committees and senior management's attention strategic issues, thematic trends and emerging risks.

There is an increasing focus by audit and risk committees on thematic reporting and trends, as a means of identifying corrective actions with broader impact than addressing just a single issue.

The table below identifies some good practice areas that agencies could report on. This table also shows which of the 45 per cent of agencies that do produce and annual report on the internal audit function also report against these aspects of better practice.

Elements of performance included in annual reports on the internal audit function (of the 45% of agencies reporting on the internal audit function)	Percentage of agencies (%)
Highlight keys activities/achievements contributing to the achievement of goals and objectives	78
Provides a view on the state of the agency's governance, risk and control arrangements	67
Highlight opportunities for improvement and strategies to address them	72
Highlight the state of the agency's controls and culture	61
Includes the outcomes of annual performance surveys	50
Illustrates trends, and highlights emerging themes and systematic issues	56
Identifies the future focus areas for internal audit	50
Includes an update on the status of KPIs	44

Source: Audit Office analysis.

Outstanding recommendations

Agencies have good processes for reporting outstanding recommendations

All agencies have established a database to log and monitor the status of outstanding recommendations. Ninety-eight per cent of agencies also report on the status of outstanding recommendations to audit and risk committees. Eighty-eight per cent of agencies report to the relevant executive management committee on the status of outstanding recommendations.

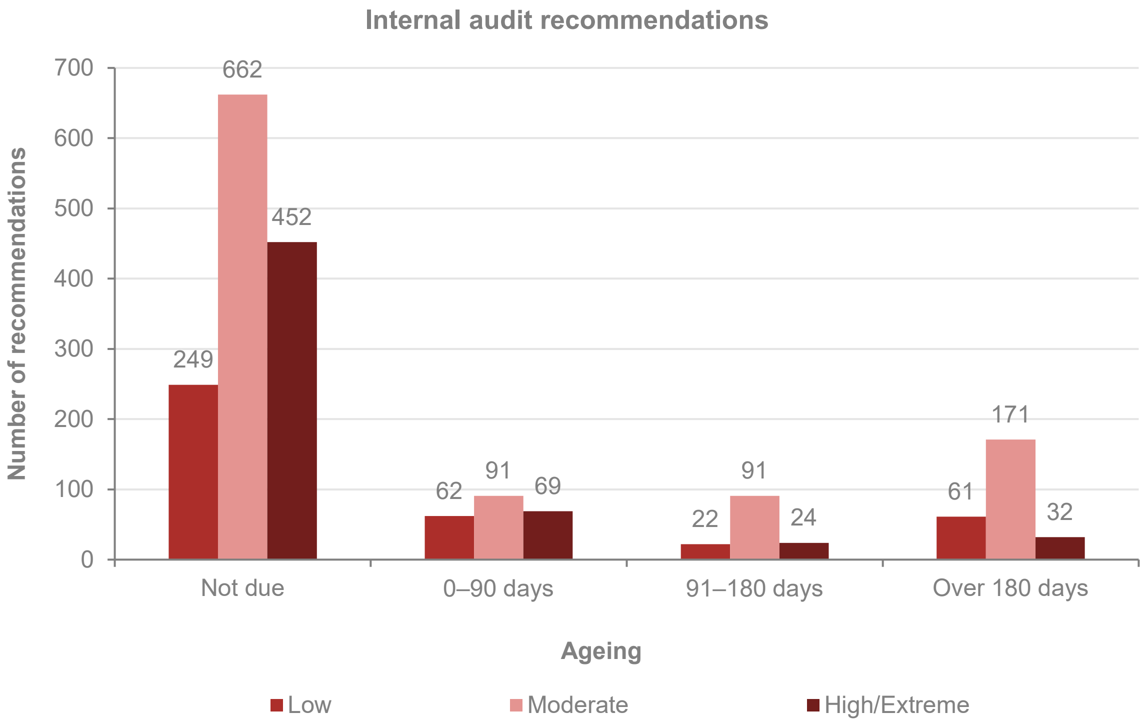
While all audit and risk committees receive reports on the status of outstanding recommendations, we found some opportunities to improve the quality of reporting, as detailed in the table below.

Elements of a status report on outstanding recommendations	Percentage of agencies (%)
Includes analysis on overdue recommendations, including identifying 'at risk' recommendations	95
Provides an opinion of management's commitment to addressing audit recommendations	69
Presents an analysis of trends (e.g. over the last 1–5 years) in recommendations opened, closed and overdue	44
Includes graphs or tables of overdue recommendations by:	
• risk rating (e.g. high, medium, low)	77
• business unit	72
• overdue ageing analysis	62

Source: Audit Office analysis.

Long over-due internal audit recommendations can indicate a culture of complacency at an agency. It can also expose an agency to an unacceptable level of financial, operational, strategic or compliance risk. Outstanding recommendations should be actively monitored and promptly escalated if they are not being addressed within agreed timeframes.

The graph below illustrates the ageing of open internal audit recommendations at 31 March 2019 across all 40 agencies. As an average, the number of overdue recommendations is relatively low. However, there are over 1,300 recommendations that are not yet past their due date, including over 400 high or extreme risk recommendations that agencies are in the process of addressing.



Source: Audit Office analysis.

The Institute of Internal Auditors Whitepaper Reporting on the Status of Audit Recommendations provides further guidance on this subject.

6. Managing contingent labour

This chapter outlines our audit observations, conclusions and recommendations, arising from our review of agency controls to on-board, manage and off-board contingent labour.

Key conclusions and sector wide learnings

Agencies have implemented controls to manage contingent labour and most agencies have some level of reporting and oversight of contingent labour at an executive level. However, the increasing trend in spend on contingent labour warrants a renewed focus on agency monitoring and oversight of their use of contingent labour. Over the last five years spend on contingent labour has increased by 75 per cent, to $1.5 billion in 2018–19.

There are also some key gaps that limit the ability of agencies to effectively manage contingent labour. Key areas where agencies can improve their management of contingent labour include:

- preparing workforce plans to inform their resourcing strategy, and confirm prior to engaging contingent labour, that this solution aligns with the strategy and best meets business needs
- involving agency human resources units in decisions about engaging contingent labour
- regularly reporting on contingent labour use to agency executive teams, particularly in terms of trends in agency spend, tenure and compliance with policies and procedures
- strengthening on-boarding and off-boarding processes, including establishing checklists to on-board and off-board contingent labour, making provisions for knowledge transfer, and assessing, documenting and capturing performance information.

6.1 Background

The Public Service Commission (PSC) issued the Contingent Workforce Management Guidelines (the PSC guidelines) in December 2014 to aid agencies on the use and management of contingent workers. The PSC guidelines, which set out best practice in contingent workforce management, define contingent labour as:

> people employed by a contingent labour supplier and hired from the supplier by a NSW Government agency to provide labour or services.

The Contingent Workforce Prequalification Scheme (the scheme) is overseen by NSW Procurement and is mandatory for NSW public sector agencies. The scheme establishes a list of approved contingent labour suppliers.

We reviewed agency contingent workforce management in 2017. The exhibit below details the results of that audit.

Exhibit 4: Previous Audit Office report on contingent workforce management

Performance Audit Report on Contingent Workforce - Management and Procurement
(published April 2017)

Our audit found that none of the three agencies reviewed was able to demonstrate that contingent labour was the best resourcing strategy to meet their agency's business needs or deliver value for money. This was because:

- the use of contingent labour was not informed by workforce planning at an agency level, with limited work undertaken in this area
- 2 of the three agencies had limited oversight of their contingent workforce. Information was not reliable or accurate, reports were onerous to produce, and there was limited reporting to the agency's executive
- none of the agencies routinely monitored and centrally documented the performance of contingent workers to ensure services are delivered as planned.

We also found:

- long tenure of contingent workers was an issue for agencies
- on and off-boarding processes could be strengthened
- there was a risk that agencies were being overcharged when engaging contingent labour
- there was no system in place to monitor the performance of contingent workers. At that time, the Department of Education was the only agency that had introduced Contractor Central, a software program with the capability to provide real-time reports on the contingent workforce.

This chapter focusses on only the 23 agencies within the scope of this report that have a contingent labour spend exceeding $5.0 million in 2018–19.

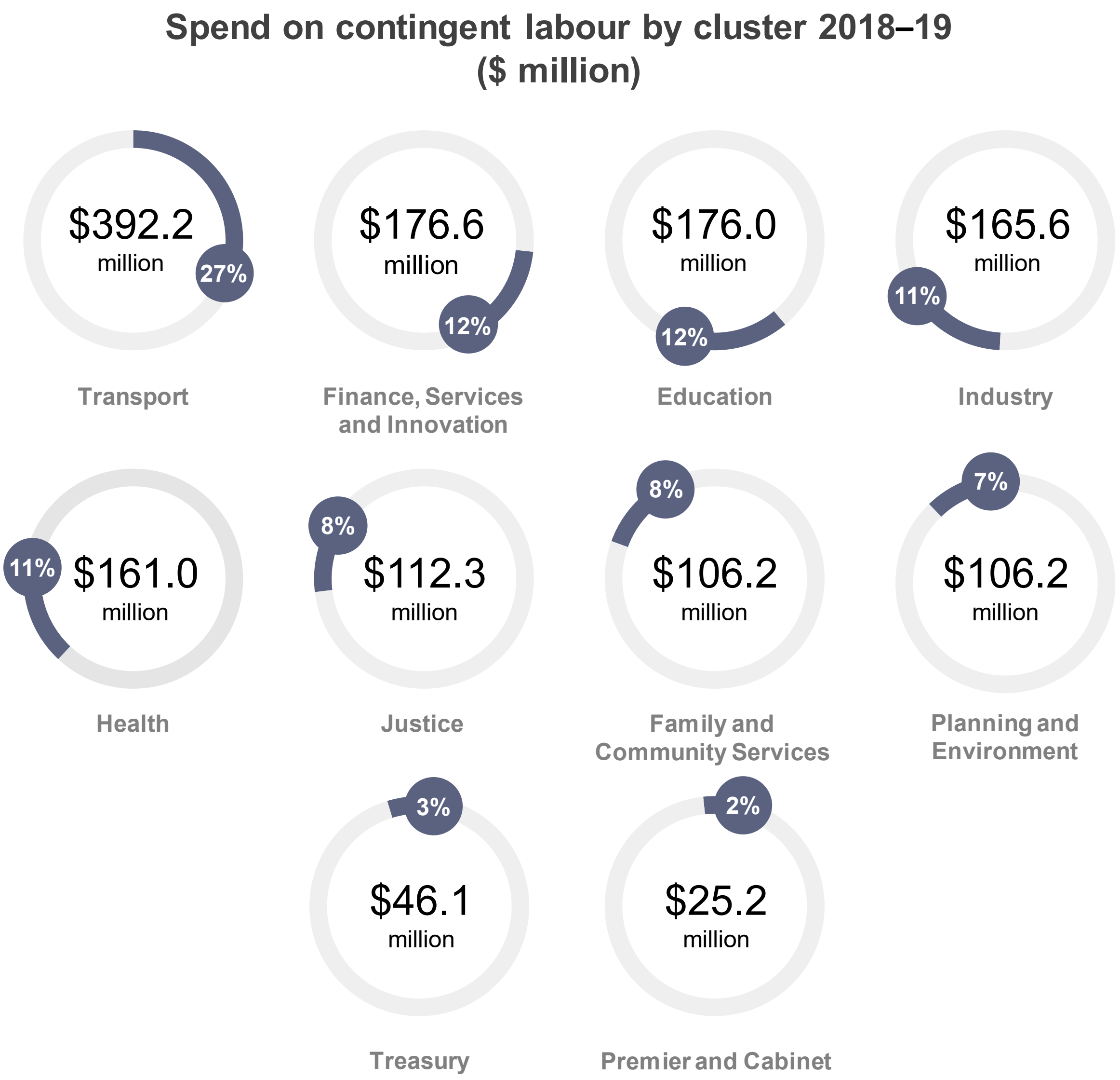
Contractor Central is widely used by agencies to manage contingent workers

Fifty-seven per cent of the 23 agencies we reviewed have now implemented a whole-of-government vendor management system and managed service provider solution to manage their contingent workforce. The scheme, vendor management system and managed service provider are collectively known as 'Contractor Central'.

Agencies are reliant on contingent workers to meet business needs

According to reporting from NSW Procurement, NSW Government agencies collectively spent $1.5 billion on contingent labour in 2018–19 ($840 million in 2014–15). This represents an increase of $627 million over the last five years, or 75 per cent. The significant and growing spend on contingent labour highlights the importance of agencies having controls to manage the risks and opportunities that arise from the use of contingent labour.

The chart below shows a breakdown of spend by cluster in 2018–19.



Source: NSW Procurement report titled 'Prequalification Scheme Contingent Workforce Government Expenditure Report – June 2019' (unaudited). The report states that it is possible some contractor information has been duplicated.

6.2 Hiring contingent labour

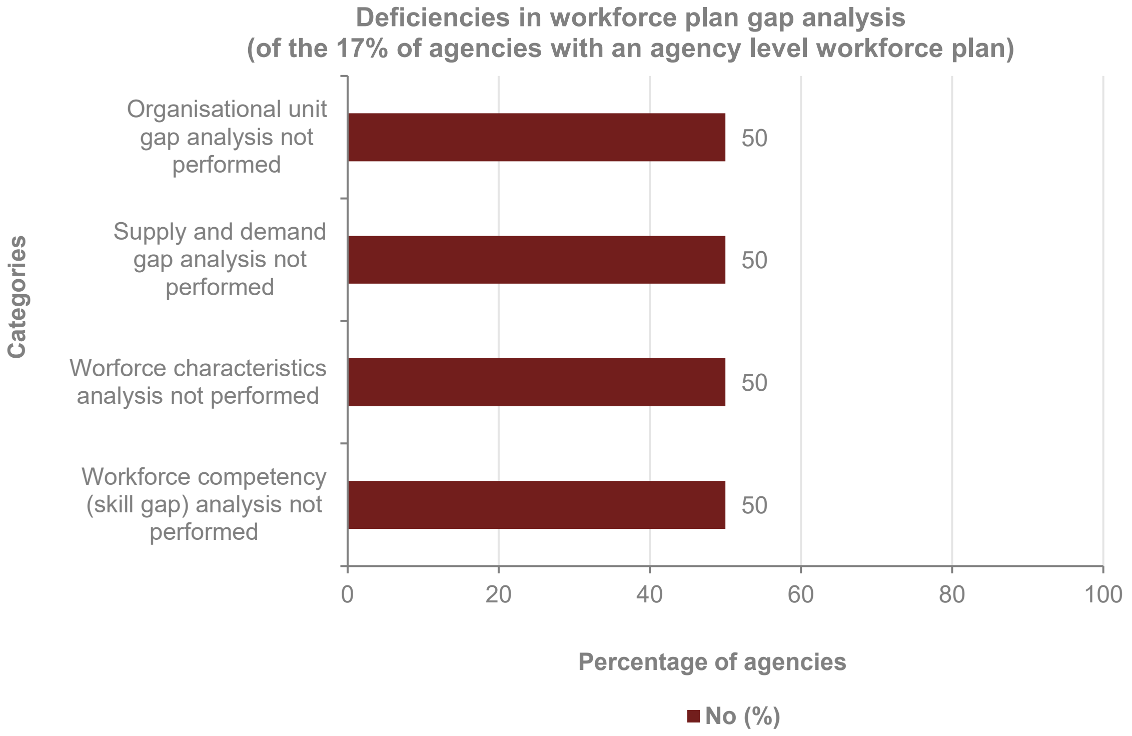
Workforce planning

Only 17 per cent of agencies had established an agency level workforce plan

A workforce plan helps hiring managers make decisions on the best resourcing strategy to meet the business need, which is important because a broad range of supply options should be considered prior to engaging contingent labour. The PSC guidelines provide some examples of supply strategies, including:

- activating talent pools within an agency or cluster
- redesigning roles to meet future needs and undertaking regular role reviews
- designing stronger recruitment campaigns
- advertising temporary or casual employment opportunities.

More broadly, a workforce plan should take into account an agency's workforce strategy and identify how it plans to manage workforce risks. The development of the strategies and initiatives to manage workforce risks should be informed by workforce analysis, including workforce segmentation, supply and demand analysis and skills capability gap analysis. We found gaps in agency workforce plans and deficiencies in workforce planning processes.



Source: Audit Office analysis.

Of the agencies that had developed an agency workforce plan and performed workforce gap analysis, we found none had identified using contingent labour as a strategy to fill workforce supply or capability gaps. Yet engaging contingent workers is a significant and growing way agencies fill these gaps. Not acknowledging that engaging contingent workers is part of their workforce plan makes it less likely the agency will:

- make appropriate decisions for the efficient and effective engagement of contingent labour
- manage the risks associated with contingent workforces
- monitor their usage of contingent labour.

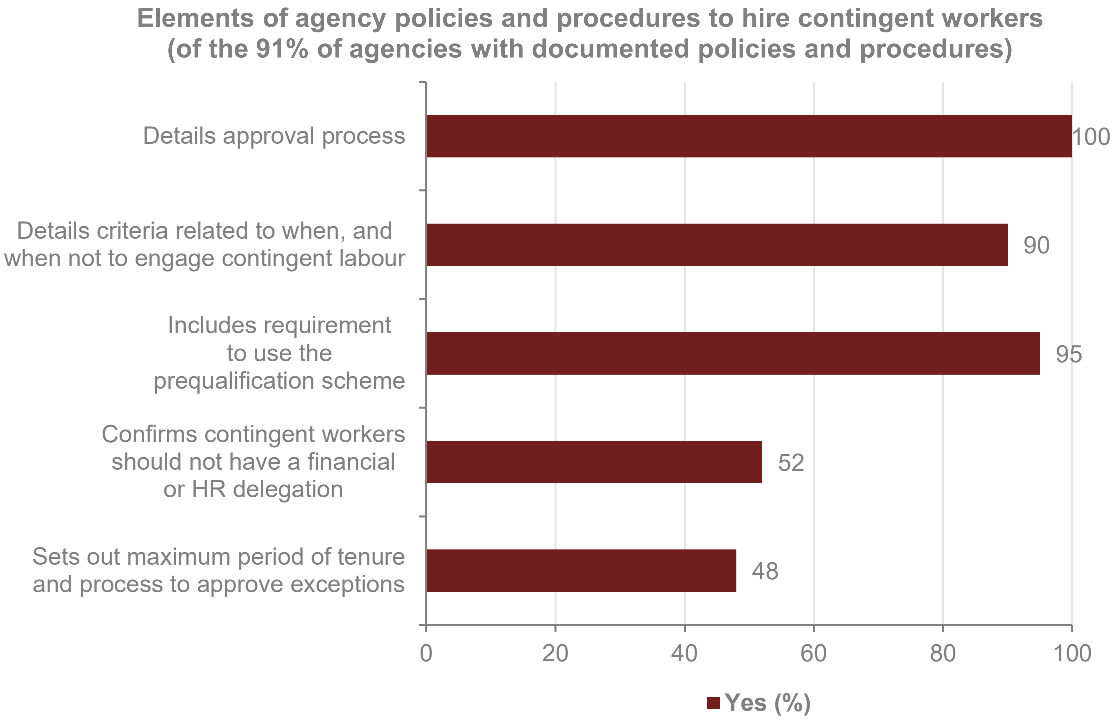
Hiring policies

Agencies have policies and procedures to help hiring managers on-board contingent labour

Ninety-one per cent of agencies have policies, procedures or other guidelines in place to on-board contingent labour. However, opportunities exist to make this guidance more comprehensive. For example, only 48 per cent of agencies prescribe a maximum period of tenure and specify a process to approve extensions to this period. This increases the risk that contingent labour will be engaged on a long-term basis or without on-going re-evaluation or that the agency's recruitment and competitive selection processes will be bypassed.

The PSC guidelines suggest, as a guide, that contingent labour should not be engaged on an ongoing basis for more than six months. In our 2017 audit, we found contingent workers employed on that basis for up to 20 years. We have revisited agency processes to monitor the tenure of contingent labour and the results are reported later in this chapter.

The graph below shows areas where agency policies, procedures and guidelines related to hiring contingent labour could be more comprehensive.



Source: Audit Office analysis.

Human resources staff are not always involved in decisions to hire contingent labour

Thirty per cent of agencies do not have a process to ensure hiring managers obtain the advice of human resources before engaging a contingent worker. Without the involvement of human resources staff there is an increased risk that:

- hiring decisions are not consistent with agency policy
- other recruitment options are not explored
- excess capacity in the agency, the cluster or the broader public sector is not utilised
- the decision adopted does not align with the agency's workforce plan
- value for money is not achieved or cannot be demonstrated
- screening procedures, such as reference and police checks are bypassed.

Human resources staff are often best placed to provide advice on the above matters.

Preventative and detective controls

Some agencies do not have employment screening policies for contingent labour

Thirty per cent of agencies do not have policies that require screening for contingent labour hires. As a result, there is an increased risk that agencies will:

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

The exhibit below further highlights the risk of poor screening practices.

Exhibit 5: ICAC Investigation into the Conduct of a Department of Finance, Services and Innovation (DFSI) ICT Project Manager (January 2019)

The investigation concerned allegations that a DFSI ICT Project Manager had dishonestly and partially exercised his public official functions in exchange for a financial benefit. The report contained a number of findings and recommendations, including that:

- it was unlikely the ICT Project Manager would have been hired had the history of prior misconduct been detected
- a failure to engage in adequate employment screening appeared to have arisen from a lack of awareness among DFSI officers of the risks associated with contracting an ICT project manager
- if DFSI had an employment screening framework it would be more readily available to conduct risk appropriate employment screening on labour hire contractors.

Agencies provide induction programs to contingent workers, but this could be more comprehensive

Eighty-three per cent of agencies provide an induction program to contingent labour hires. The table below shows where some agencies could improve their induction programs.

Scope of induction programs (of the 83% of agencies with induction programs)	Percentage of agencies (%)
Code of conduct, including acknowledgement of the agency code of conduct	84
Agency requirements regarding confidential information, intellectual property and responsibilities in handling government information	74
Appropriate use of email and internet	74
Use of key information systems	47

Source: Audit Office analysis.

Contingent workers are not subject to individual performance agreements, but in many agencies, they make an important contribution to achieving an agency's business objectives and service delivery outcomes. A comprehensive induction program clearly sets out the contingent worker's roles and responsibilities, provides training that addresses operational and compliance risks relevant to their responsibilities, and clearly communicates the agency's expected standard of ethical behaviour.

Agencies have implemented controls to approve contingent labour hire and timesheets

We reviewed controls over the timesheet approval processes for contingent workers. We found that contingent labour hires had been approved in accordance with agency delegations and timesheets had been approved in line with the signed contract.

These controls help to ensure that contingent labour is only engaged where a business need exists, and that agencies are not being over-charged for contingent labour by paying above the agreed rate of pay.

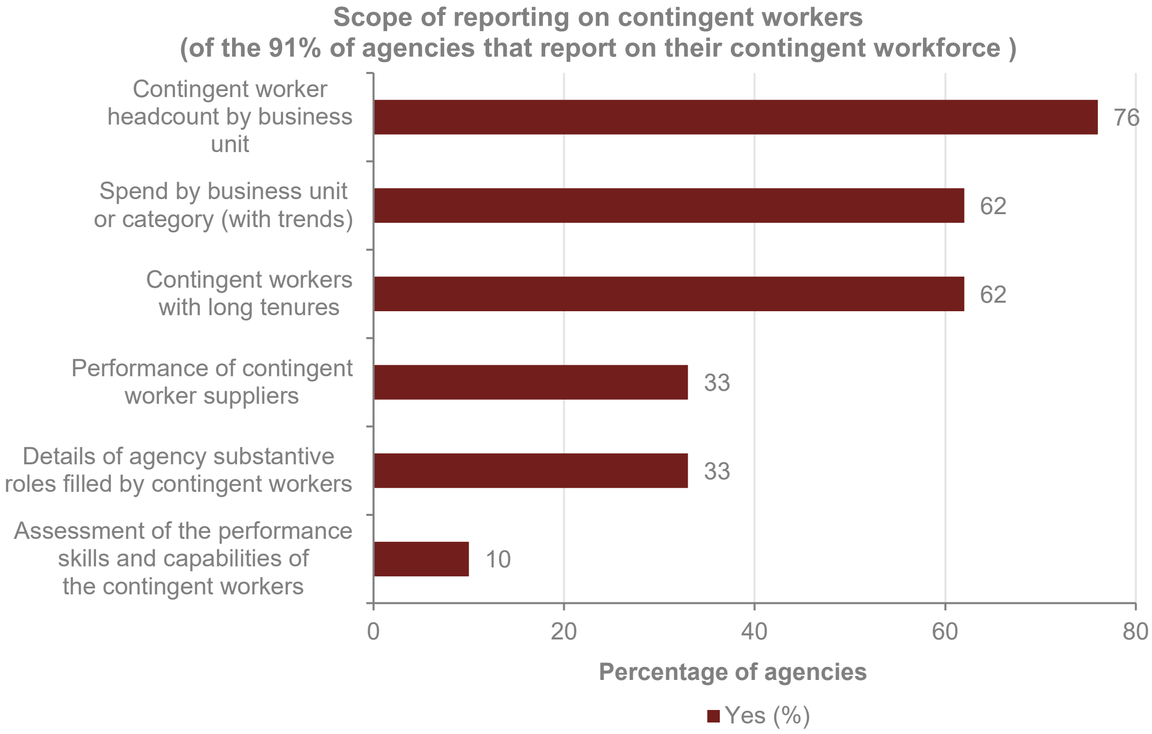
6.3 Monitoring the use of contingent labour

Agency reporting on the use of contingent labour is limited or is not performed

Ninety-one per cent of agencies report some information to their executive committee (or other relevant governance committee) on the use of contingent labour. The level of reporting varied across the agencies. For example, at some agencies reporting on contingent labour was limited to reporting head count data only. We identified opportunities for agencies to improve the information they report to their executive and governance committees.

The growing spend on contingent labour across the NSW public sector means on-going monitoring, review and oversight of the use of contingent labour by agency executive teams is required to reduce the risk that contingent labour is not meeting agency business needs.

The graph below shows some gaps in agency reporting on the use of contingent labour.



Source: Audit Office analysis.

Reporting on contingent labour can provide invaluable insights to an agency executive or governance committee, including:

- identifying trends in use of contingent labour across business units, highlighting possible over-reliance and/or cost saving opportunities
- cost and charge-out rate comparisons above set thresholds
- identifying contingent workers with long tenures and the sufficiency of action taken to address this, such as commencing recruitment action or plans to off-board the contingent worker
- highlighting contingent worker and/or supplier performance issues and actions taken to mitigate risks arising
- highlighting compliance issues and where targeted intervention, such as training and awareness activities are required.

Limited oversight may contribute to long tenure of contingent workers across agencies

Agencies are engaging contingent labour to perform long term engagements. In some cases, the complexity of some projects, such as information technology implementations justifies the long tenure of specialised staff. In other instances, the reasons for the long tenure of some contingent workers are not documented.

The table below shows contingent labour average and maximum tenure across agencies.

	Agency expenditure (2018–19)				
Tenure data (at 31 March 2019)	**$100 million to $500 million**	**$500 million to $1.0 billion**	**$1.0 billion to $5.0 billion**	**$5.0 billion**	**All in scope agencies**
Number of agencies	3	6	9	5	23
Average tenure (across all in scope agencies)					
Average tenure (calendar days)	282	331	421	384	375
Agency with highest average tenure (calendar days)	379	618	548	515	618
Agency with lowest average tenure (calendar days)	185	191	219	241	185
Maximum tenure (across all in scope agencies)					
Average maximum tenure (calendar days)	1,381 (Approx. 3.8 years)	1,739 (Approx. 4.8 years)	3,391 (Approx. 9.3 years)	4,433 (Approx. 12.2 years)	2,985 (Approx. 8.2 years)
Maximum tenure (highest across all in scope agencies) (calendar days)	1,885 (Approx. 5.2 years)	3,241 (Approx. 8.9 years)	8,233 (Approx. 22.6 years)	9,834 (Approx. 26.9 years)	9,834 (Approx. 26.9 years)
Lowest maximum tenure (lowest across all in scope agencies) (calendar days)	877 (Approx. 2.4 years)	623 (Approx. 1.7 years)	881 (Approx. 2.4 years)	1,734 (Approx. 4.8 years)	623 (Approx. 1.7 years)

Source: Agency data (unaudited).

Long tenures highlight a risk that contingent labour is being inappropriately used in an agency. Contingent workers are often engaged on non-standard arrangements, which may specify higher rates of pay or other terms and conditions that are not offered to staff employed on a permanent or temporary basis.

Better reporting to and oversight by agency executive teams would help to ensure that use of contingent labour across the agencies is suited to the type of services required, does not duplicate skills already in the organisation and represents value for money.

6.4 Off-boarding contingent labour

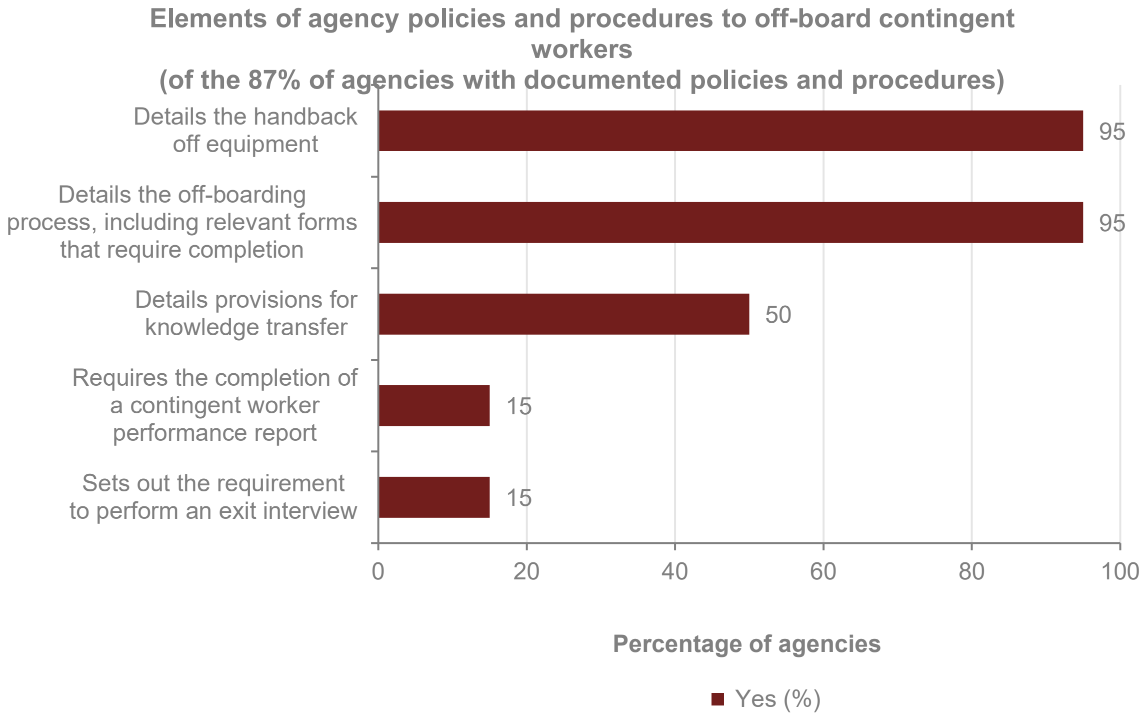
Off-boarding policies

Guidance to off-board contingent workers could be strengthened

Eighty-seven per cent of agencies have policies, procedures or other guidelines in place to off-board contingent labour. However, there are key gaps in this guidance associated with capturing knowledge transfer and assessing and documenting contingent worker performance. This limits the effectiveness of this guidance.

Often contingent workers are engaged to fill a knowledge or capability gap in the agency. Without a process to prompt or assist the agency capture this knowledge there is a risk of knowledge loss. Assessing and documenting contingent worker performance also provides valuable knowledge in assessing the worker for any future roles at the agency or within the cluster.

The graph below shows where agency policies, procedures and guidelines related to off-boarding contingent labour promote the elements of better practice.



Elements of agency policies and procedures to off-board contingent workers
(of the 87% of agencies with documented policies and procedures)

Source: Audit Office analysis.

Agencies should ensure processes are documented, and arrangements are in place to help transfer knowledge from contingent workers to agency staff through coaching, training and/or support to help those staff perform new tasks.

Data on contingent workers' skills, capability and performance should be captured in a central database for future reference.

Preventative and detective controls

Some agencies do not use an off-boarding checklist to manage the off-boarding process

We reviewed the implementation of contingent labour off-boarding processes. Forty-three per cent of agencies did not use an off-boarding checklist to manage this process. This increases the risk that steps will be missed in the off-boarding process and:

- equipment is not returned
- security passes and clearances are not revoked
- physical and system access are not removed on a timely basis.

We also found processes to off-board contingent workers addressed some, but not all elements of better practice. The findings are detailed in the table below.

Step included in the off-boarding process (of the 57% of agencies)	Percentage of agencies (%)
Exit checklist used to ensure all key off-boarding tasks performed	57
Knowledge transfer documented	30
Performance report prepared on contingent worker	22
Performance rating assigned to supplier	13
Exit interview conducted	9

Source: Audit Office analysis.

7. Managing sensitive data

This chapter outlines our audit observations, conclusions and recommendations, arising from our review of governance and processes in relation to the management of sensitive data.

Key conclusions and sector wide learnings

Information technology risks are rapidly increasing. More interfaces between agencies and greater connectivity means the amounts of data agencies generate, access, store and share continue to increase. Some of this information is sensitive information, which is protected by the *Privacy Act 1988*.

It is important that agencies understand what sensitive data they hold, the risks associated with the inadvertent release of this information and how they are mitigating those risks. We found that agencies need to continue to identify and record their sensitive data, as well as expand the methods they use to identify sensitive data. This includes data held in unstructured repositories, such as network shared drives and by agency service providers.

Eighty-eight per cent of agencies have established policies to respond to potential data breaches when they are identified and 70 per cent of agencies maintain a register to record key information in relation to identified data breach incidents.

Key areas where agencies can improve their management of sensitive data include:

- identifying sensitive data, based on a comprehensive and structured process and maintaining an inventory of the data
- assessing the criticality and sensitivity of the data so that the protection of high risk data can be prioritised
- developing comprehensive data breach management policies to ensure data breaches are appropriately managed
- maintaining a data breach incident register to record key information in relation to identified data breaches incidents, including the estimated cost of the breach
- providing on-going training and awareness activities to employees in relation to sensitive data and managing data breaches.

7.1 Background

The Information Management Framework outlines the shared direction of information management within the NSW Public Sector. The framework outlines the key elements of data management including identifying core information assets and systems and performing risk assessments of the high value information systems and assets an agency holds.

Good data management helps agencies deal with, and limit the impact of cyber attacks and other unauthorised access to the systems that hold that data. All agencies hold and manage sensitive data as part of their operations. Sensitive information includes employee personal details, credit information, medical records, patient personal details, drivers licence information, criminal records, young offenders' records, biometric information and other personal details. The management of risks associated with the inadvertent release of sensitive information is crucial to agency operations.

The loss of sensitive data can result in:

- fraudulent use of an individual's personal data
- financial loss to the agency and the individuals affected
- reputational damage and loss of public trust in the agency responsible for its safekeeping.

This chapter focusses on what agencies have done to identify and assess their sensitive data and to manage data breaches.

Risks posed by sensitive data can be easily overlooked or not identified

It is important for government agencies to know what sensitive data is, and how it is being controlled. Agencies should ask:

- How does sensitive data enter the agency?
- Where does it reside?
- How, and under what circumstances does it leave the agency?

These are simple questions, but without this understanding the risks posed by sensitive data can be easily overlooked or not identified. Our audits are focussed on agencies' key financial systems and not necessarily those systems that store sensitive personal data. However, over the years we have identified and reported gaps in relation to managing sensitive data. The examples below, as well as a multitude of highly publicised cases demonstrate how simple it can be for an agency to be exposed to data breaches, particularly if they are not assessing and actively managing the risks that arise from holding sensitive data.

Exhibit 6: Examples of gaps identified in relation to managing sensitive data

Test databases

Unencrypted sensitive business data was copied to development and test environments where the information could have been copied on to USB devices. Various users had access to this data, including contracted developers.

Printers

Policies or procedures were not in place to cover the erasure of data on common printers accessed by external parties for support or repairs.

Access restrictions

A large number of database administrators at the agency and their service provider had access to modify and extract unencrypted sensitive data, without activity audit logging controls in place.

Data migrations

The security risks posed by a data migration project were not adequately managed. For example, there was:

- no policy of framework in place that dealt with user access security, data governance and physical and network security
- no risk assessment performed over the sensitive data to identify data masking requirements during migration and user acceptance testing
- no restrictions or process to ensure secure disposal of data and removal of user access from the migration environment.

Backups

Daily system backups of employee records were saved to a network drive in clear text format.

Source: Audit Office management letters (2017 to 2019).

7.2 Identifying and assessing sensitive data

We reviewed the adequacy of agency processes to identify sensitive data and assess its risk.

Agencies are not proactively identifying sensitive data held and where it resides

An agency's ability to appropriately protect sensitive data is limited without a comprehensive understanding of all sensitive data held and where it is stored. Sixty-eight per cent of agencies maintain an inventory of their sensitive data. However, this may not be a complete inventory because, of these agencies:

- 11 per cent had not captured data held in unstructured data repositories, such as shared network drives and email servers
- 29 per cent of agencies had not considered data held by their service providers.

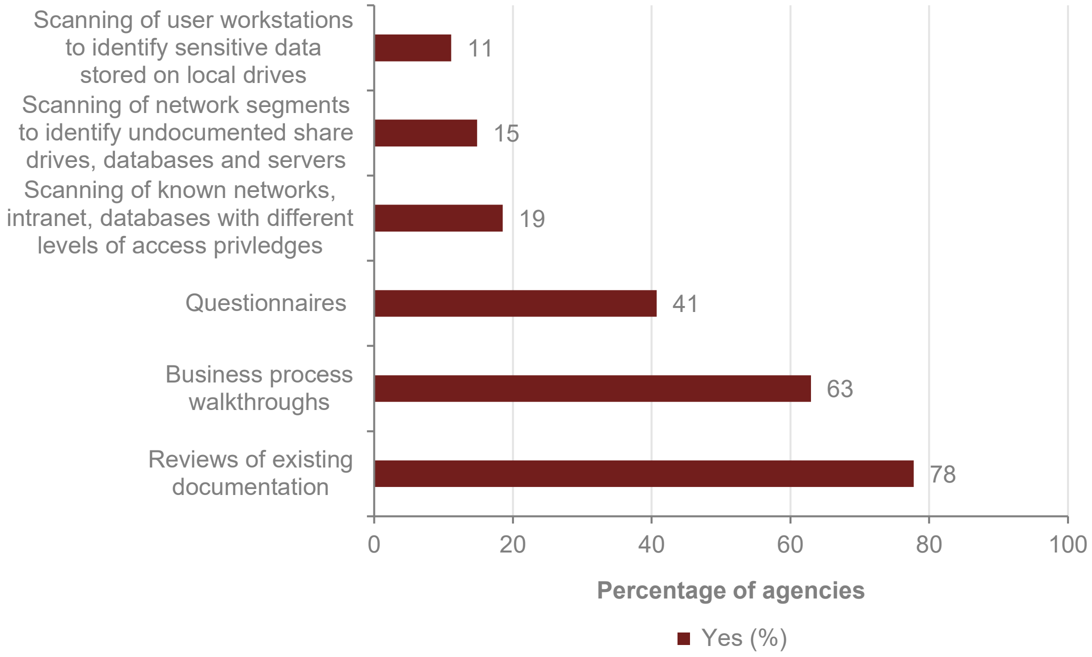
We also found that the process whereby agencies identified their sensitive data was not always comprehensive. Generally, agencies relied on common processes such as reviewing existing documentation (e.g. data flow diagrams) and business process walkthroughs to identify sensitive data. Other processes were less commonly used, such as:

- using questionnaires sent to key officers, such as business process owners and database administrators
- scanning network shared drives, intranet sites and databases
- scanning network segments to identify undocumented shared drives, databases and servers
- scanning user workstations to identify sensitive data stored on local drives.

The use of common processes to identify where sensitive data is held increases the risk that not all sensitive data will be identified, meaning it may not be adequately protected.

The graph below shows the processes used by agencies to identify where their sensitive data is located within their IT infrastructure.

Identification processes for the location of sensitive data (of the 68% of agencies that had conducted an exercise)



Source: Audit Office analysis.

Agency processes to identify whether data is sensitive needs to improve

Only 74 per cent of the agencies performed a risk assessment as part of their sensitive data identification process to determine the data's criticality and sensitivity. Of these agencies, only 81 per cent had performed another level of review to assess the potential impact of the data loss to the agency. For example, impact assessments should consider:

- regulatory implications
- extent of financial impact
- level of business disruption
- magnitude of reputational damage.

Without a comprehensive risk assessment, data sensitivity may be inappropriately classified and resources may not be allocated to the highest risk data. Risk assessment procedures enable agencies to identify their high-risk data and prioritise its protection.

Not all agencies have developed data classification and labelling policies or guidelines

Eighty-five per cent of the agencies have established data classification policies or guidelines to define the classification of data. Inconsistent methods of classification and labelling increase the risk that sensitive information will be mishandled and not adequately protected.

The NSW Government Information Classification, Labelling and Handling Guidelines helps agencies identify the confidentiality requirements of information assets and apply suitable protective markings.

7.3 Managing data breaches

We reviewed the adequacy of agency policies and processes to adequately respond to data breaches.

Most agencies have developed a data breach management policy

Eighty-eight per cent of agencies have established policies to ensure all employees are aware of their roles and responsibilities when a potential data breach is identified. However, 14 per cent of agencies have not reviewed their data breach management policies by the scheduled date and, as noted in the table below, opportunities exist to make agency policies more comprehensive.

Maintaining up-to-date policies ensures all potential data breaches are appropriately managed by agencies and their staff and service providers. Without adequate guidance there is an increased risk data breaches go unreported and are not effectively managed. In addition, appropriate strategies would not be developed to prevent the reoccurrence of similar breaches in the future.

The table below highlights elements of agency data breach management and the percentage of agencies that include those elements in their policies.

Key elements of an agency data breach management (of the 88% of agencies with policies to manage data breaches)	Percentage of agencies (%)
Detailed approach (step by step) of how the agency will respond to a data breach incident	94
Instructions of the first response on how to contain the data breach	94
A process to evaluate a data breach is set out	94
Processes for how the agency will assess the root cause of the incident and plan any prevent future breaches	94
Guidance on how the agency will assess the risk associated with the incident	91
Detail on roles, responsibilities and accountabilities for handling data breaches	89
Notification procedures to inform internal and external stakeholders	80
Requirements on what, when and how to report data breaches and how they have been handled to those charged with governance	57

Source: Audit Office analysis.

Not all agencies maintain a data breach/incident register or measure the cost of data breaches

Seventy per cent of agencies maintain a register to record key information in relation to identified data breach incidents. This enables agencies to assess the circumstances and impact of the breach, and implement appropriate remedial actions. However, registers did not always contain all key fields, as set out in the table below.

The absence of a data breach register makes it difficult to determine whether the actions taken regarding the containment, evaluation and remediation actions of each data breach were appropriate. A register also enables agencies to develop effective preventative strategies, based on the type and seriousness of the breach.

The table below outlines better practice elements of data breach registers and the percentage of agencies whose registers contain those elements.

Key fields in data breach registers (of the 70% of agencies that maintain registers)	Percentage of agencies (%)
Date of incident	100
Description/nature of incident	100
Description of how the incident was contained	75
Details of how the data breach was evaluated	68
Details of assessment of the risk from data breach	61
Details of notified related parties and authorities	54
Details of applied preventative controls for future events	50
Estimated cost of data breach*	11

* While 11 per cent of agencies include this field in their incident register, none have recorded the cost of any recorded data breaches.

Source: Audit Office analysis.

As at 31 March 2019, agencies had recorded 3,324 data incidents, while no costs were recorded against these incidents. Although, we would expect agency investment decisions in data breach prevention and detection to be based on broader considerations, such as reputational and legal obligations, the cost of data breaches can be a relevant input in determining if investment is adequate. The exhibit below provides an indication of the cost of data breaches and significant steps required to resolve it.

Exhibit 7: 2018 Cost of Data Breach Study: Global Overview issued by IBM Security and Ponemon Institute

The report highlighted that the cost of data breaches continues to increase, and more consumer records are being lost or stolen, year after year. The report estimated an average cost of:

- $148 per lost or stolen record
- $3.86 million per data breach.

The methodology applied in the report to estimate the cost to resolve data breaches was categorised into the following categories:

Detection and escalation

Activities to enable the detection and reporting of breaches to appropriate personnel within an appropriate timeframe. This includes:

- forensic and investigation activities
- assessment and audit activities
- crisis team management
- communication to the executive management and board of directors.

Notification

Activities to notify individuals who had data compromised in the breach as regulatory activities and communications. This includes:

- emails, letters, outbound telephone calls or general notice that personal information was lost or stolen
- communication with regulators, determination of all regulatory requirements and engagement of external experts.

Post data breach response

This relates to processes to assist affected individuals and customers of the data breach as well as costs associated to compensate the affected individuals and regulatory implications. This includes:

- help desk activities and inbound communications
- legal expenditures
- regulatory fines
- product discounts.

Lost business costs

These costs are associated with the cost of lost business such as business disruption, system downtime and customer churn. This includes:

- cost of business disruption and revenue loss during system downtime
- cost of lost customers and acquiring new customers
- reputation losses.

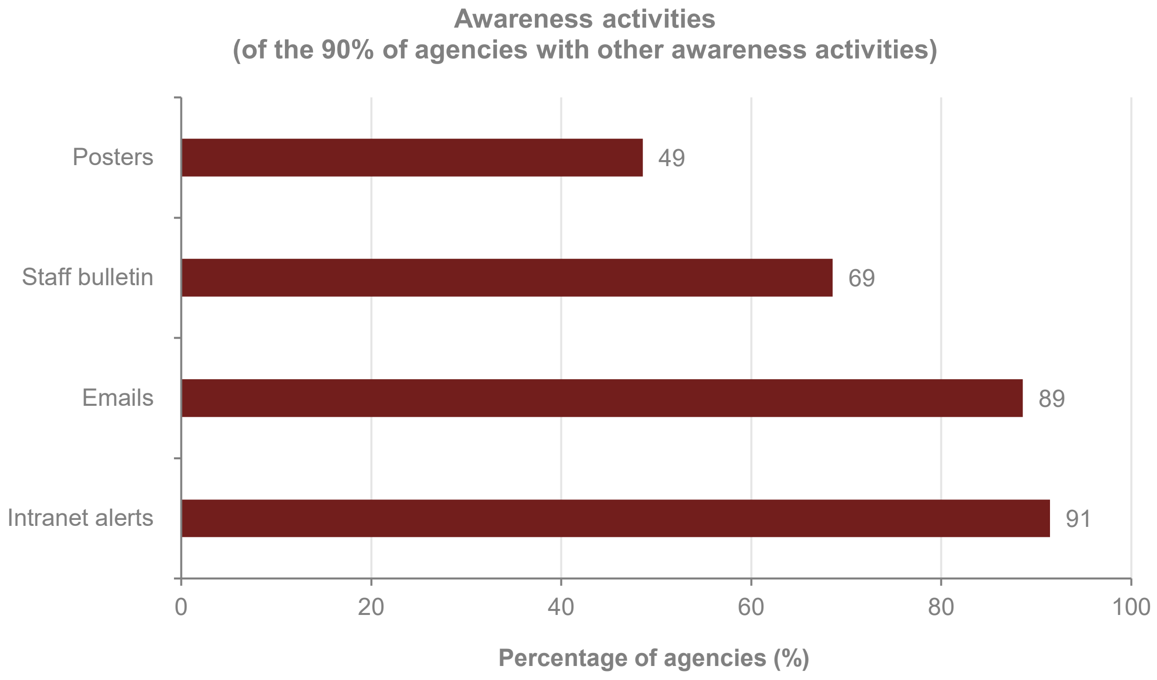
Agencies should continue to provide training and awareness to help manage data breaches

Seventy per cent of agencies have provided training to employees in relation to data protection and breach management, with a specific focus on new starters. Eighty-one per cent of these agencies continue to provide on-going training to staff.

Data breach management awareness training helps agencies reduce the risk of data breaches occurring due to human error, and increase the detection of data breaches. Training ensures employees:

- understand the risks to the agency (both financial and reputational)
- are aware of policies and procedures for data breach management
- have the ability to identify potential breaches when they occur
- understand the importance of de-identifying sensitive data where release of certain information is required or appropriate
- consider contextual information, which may still allow individuals to be identified, even after the data is de-identified
- report potential breaches in a timely manner.

The graph below details the different methods agencies use to create awareness of data breaches.



Source: Audit Office analysis.

Section two

Appendices

Appendix one – List of 2019 recommendations

The table below lists the recommendations made in this report.

1. Gifts and benefits

1.1 Managing gifts and benefits

Agencies should: ⊖

- ensure their gifts and benefits register includes all key fields specified in the minimum standards, as well as performing regular reviews of the register to ensure completeness
- provide on-going training, awareness and support activities to employees, not just at induction
- establish an annual attestation process for senior management to attest compliance with gifts and benefits policies and procedures
- publish their gifts and benefits registers on their websites to demonstrate their commitment to a transparently ethical environment.

1.2 Reporting and monitoring

Agencies should regularly report to the agency executive or other governance committee on trends in the offer and acceptance of gifts and benefits. ⊖

2. Internal audit

2.1 Chief Audit Executive

Agencies should ensure: ⊖

- the reporting lines for the CAE comply with the NSW Treasury policy, and the CAE does not report functionally or administratively to the finance function or other significant recipients of internal audit services
- the CAE's duties are compatible with preserving their independence and where threats to independence exist, safeguards are documented and approved.

2.2 Quality assurance and improvement and performance measurement and reporting

Agencies should ensure there is a documented and operational Quality Assurance and Improvement Program for the internal audit function that covers both internal and external assessments. ⊖

Key ✓ **Low risk** ⊖ **Medium risks** ! **High risks**

Appendix two – Status of 2018 recommendations

Recommendation	Current status	
Internal control trends		
Agencies should reduce risk by addressing high risk internal control deficiencies as a priority.	All high risk internal control deficiencies identified last year have been rectified.	✓
Agencies should reduce IT risks by: • assigning ownership of recommendations to address IT control deficiencies, with timeframes and actions plans for implementation • ensuring audit and risk committees and agency management regularly monitor the implementation status of recommendations.	All agencies are assigning ownership of recommendations and timeframes for completion. Ninety-eight per cent of agencies are reporting on the status of outstanding recommendations to their audit and risk committee, while eighty-eight per cent of agencies are reporting to the relevant executive management committee.	✓
Information technology		
Agencies should ensure their contract registers are complete and accurate so they can more effectively govern contracts and manage compliance obligations.	The completeness and accuracy of contract registers remains an issue at agencies.	⊖
Agencies should strengthen the administration of user access to prevent inappropriate access to key systems.	User access administration remains an issue at agencies. Refer to Section 3.1 for further details.	❗
Agencies should: • review the number of, and access granted to privileged users, and assess and document the risks associated with their activities • monitor user access to address risks from unauthorised activity.	The use and monitoring of privileged users remains an issue at agencies. Refer to Section 3.1 for further details.	❗
Agencies should ensure IT password settings comply with their password policies.	Password controls remains an issue at agencies. Refer to Section 3.1 for further details.	❗
Agencies should maintain appropriate segregation of duties in their IT functions and test system changes before they are deployed.	Program change controls remains an issue at agencies. Refer to Section 3.1 for further details.	⊖
Transparency and performance reporting		
Agencies should comply with the annual reports regulation and report on all mandatory fields, including significant cost overruns and delays, for their major works in progress.	Of the 14 agencies, ten have implemented the recommendation.	⊖

Recommendation	Current status	
Management of purchasing cards and taxis		
Agencies should mitigate the risks associated with increased purchasing card use by ensuring policies and purchasing card frameworks remain current and compliant with the core requirements of TPP 17-09 'Use and Management of NSW Government Purchasing Cards'.	Of the six agencies with purchasing card policies past its scheduled review date: • 2 agencies had updated and finalised new policies. • 4 agencies policies were under review or there was an updated purchasing card policy in draft.	⊖

Key ✓ Fully addressed ⊖ Partially addressed ! Not addressed

Appendix three – In-scope agencies

NSW public sector agencies by cluster selected for this volume include:

Stronger Communities
Department of Family and Community Services[*]
Department of Justice[*]
Fire and Rescue NSW
Legal Aid Commission of New South Wales
NSW Police Force
Office of Sport
Office of the Director of Public Prosecutions
Office of the NSW Rural Fire Service

[*] Department of Family and Community Services and Department of Justice were abolished under the Administrative Arrangements (Administrative Changes - Public Service Agencies) Order 2019 and their functions transferred to other agencies.

Customer Service
Department of Finance, Services and Innovation[*]
Long Service Corporation
Service NSW
State Insurance Regulatory Authority

[*] Abolished under the Administrative Arrangements (Administrative Changes - Public Service Agencies) Order 2019 and its functions transferred to other agencies.

Education
Department of Education
TAFE Commission

Planning, Industry and Environment
Department of Planning and Environment[1]
Department of Industry[1]
Essential Energy
Environment Protection Authority
Forestry Corporation of New South Wales
Hunter Water Corporation
Landcom
Office of Environment and Heritage[1]

Planning, Industry and Environment
Office of Local Government[1]
Property NSW
Sydney Opera House Trust
Sydney Water Corporation
Water NSW

[1] Abolished under the Administrative Arrangements (Administrative Changes - Public Service Agencies) Order 2019 and their functions transferred to the Department of Planning, Industry and Environment.

Health
Ministry of Health

Premier and Cabinet
Department of Premier and Cabinet
Infrastructure NSW
UrbanGrowth NSW Development Corporation*

* Abolished under the *State Revenue and Other Legislation Amendment Act 2019* and its functions transferred to Infrastructure NSW.

Transport
NSW Trains
Roads and Maritime Services
State Transit Authority of New South Wales
Sydney Trains
Transport for NSW

Treasury
Insurance and Care NSW
New South Wales Treasury Corporation
The Treasury
Destination NSW

Professional people with purpose

OUR VISION

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

OUR PURPOSE

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

OUR VALUES

Pride in purpose

Curious and open-minded

Valuing people

Contagious integrity

Courage (even when it's uncomfortable)

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

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

PHONE +61 2 9275 7100
FAX +61 2 9275 7200

mail@audit.nsw.gov.au

Office hours: 8.30am-5.00pm

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au