

# Internal Controls and Governance 2018

30 OCTOBER 2018



NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

FINANCIAL AUDIT

# 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.



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 52 of the *Public Finance and Audit Act 1983*, I present a report titled '**Internal Controls and Governance 2018**'.

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

**Margaret Crawford**

Auditor-General  
30 October 2018

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

# contents

---

## Internal controls and governance 2018

### **Section one – Internal controls and governance 2018**

Executive summary	1
Introduction	6
Internal control trends	7
Information technology	17
Transparency and performance reporting	29
Management of purchasing cards and taxi use	35
Fraud and corruption control	46

### **Section two – Appendices**

Appendix one – List of 2018 recommendations	57
Appendix two – Status of 2017 recommendations	58
Appendix three – Cluster agencies	61

# **Section one**

## **Internal controls and governance 2018**

This report analyses the internal controls and governance of the 40 largest agencies in the NSW public sector for the year ended 30 June 2018.



# Executive summary

This report analyses the internal controls and governance of the 40 largest agencies in the NSW public sector for the year ended 30 June 2018.



## 1. Internal control trends

### New, repeat and high risk findings

We found 42 per cent more internal control deficiencies than last year, including six high risk findings (seven in 2016–17), one of which was repeated from both last year and 2015–16. The current year's increase reversed a trend of declining numbers of internal control deficiencies over the previous four years.

Deficiencies relating to information technology (IT) increased by 63 per cent since last year, largely driven by the government's increasing digital footprint as its on-line interfaces with citizens are prioritised, and skilled IT and finance staff are redirected to complex IT projects and systems implementations.

A number of findings were common to multiple agencies. Central agencies or the lead agency in a cluster can play a lead role in helping ensure agency responses to common findings are consistent, timely, efficient and effective.

**Recommendation:** Agencies should reduce risks by:

- addressing high risk internal control deficiencies as a priority
- 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.



## 2. Information technology (IT), including IT vendor management

### Management of IT vendors

We examined 30 IT vendor contracts to see how well agencies manage their service providers.

#### Contract risk and performance management

Forty-one per cent of agencies did not use contract management plans or assess contract risks. Half of the agencies that did assess contract risks had not updated their risk assessments since the commencement of the contract.

Eighty-six per cent of agencies meet with vendors to discuss performance. Only 24 per cent of agencies sought assurance about the accuracy of vendor reporting against KPIs, yet sixty-seven per cent of the IT contracts allow agencies to determine performance based payments and/or penalise underperformance.

**Conclusion:** Agencies are monitoring IT vendor performance, but could improve outcomes and more effectively manage under-performance by:

- a more active, rigorous approach to both risk and performance management
- checking the accuracy of vendor reporting against KPIs and where appropriate seeking assurance over their accuracy
- invoking performance based payments clauses in contracts when performance falls below agreed standards.

## IT general controls

### Transitioning services

Forty-three per cent of the IT vendor contracts did not contain transitioning-out provisions. Where IT vendor contracts do make provision for transitioning-out, only 28 per cent of agencies have developed a transitioning-out plan with their IT vendor.

**Conclusion:** Contract transition/phase out clauses and plans can mitigate risks to service disruption, ensure internal controls remain in place, avoid unnecessary costs and reduce the risk of 'vendor lock-in'.

### Contract registers

Contract registers help agencies manage their compliance obligations under the *Government Information (Public Access) Act 2009* (the GIPA Act). They also help agencies' central procurement teams better govern their portfolio of contracts, monitor contract end dates or contract extensions, and commence new procurements in a timely manner. Eleven out of forty agencies did not have contract registers, or had registers that were not accurate and/or complete.

**Recommendation:** Agencies should ensure their contract registers are complete and accurate so they can more effectively govern contracts and manage compliance obligations.

### Access controls

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

- user access administration deficiencies at 65 per cent of agencies related to granting, review and removal of user access
- absence of privileged user activity reviews at 40 per cent of agencies
- password controls did not align to password policies at 23 per cent of agencies.

**Recommendation:** Agencies should:

- strengthen the administration of user access to prevent inappropriate access to key systems:
- 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
- ensure IT password settings comply with their password policies.

### Program change controls

Fifteen 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.

**Recommendation:** Agencies should maintain appropriate segregation of duties in their IT functions and test system changes before they are deployed.



### 3. Transparency and performance reporting

#### Reporting on performance

We reviewed how transparent agencies are in their performance reporting. We reviewed key performance metrics in agencies' 2016–17 annual reports. While agency financial statements are audited, performance information in annual reports is not.

Fifty-seven per cent of agencies clearly linked reporting on performance against their strategic objectives, but the use of targets and trends over time was limited, and applied inconsistently. These findings are consistent with previous performance audits, which have also noted issues related to the collection of performance information.

**Conclusion:** There is significant disparity in the quality and consistency of how agencies report on their performance in their annual reports. This limits the reliability and transparency of reported performance information.

#### Reporting on projects

##### Major works in progress

The annual reports regulation requires agencies to report on major works. However, we found 47 per cent of agencies did not report on costs to date and estimated completion dates for major works in progress. Of the 47 per cent of agencies that reported on major works, only one agency reported detail about significant cost overruns, delays, amendments, deferments or cancellations.

NSW Treasury produce an [annual report checklist](#) to help agencies comply with their annual report obligations.

**Recommendation:** 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.

##### Completed major works

The annual reports regulation does not require agencies to report on completed works (only works in progress). Fifty-three per cent of agencies voluntarily reported some information on completed major works.

**Conclusion:** Agencies could improve their transparency if they reported, or were required to report:

- on both works in progress and projects completed during the year
- actual costs and completion dates, and forecast completion dates for major works, against original and revised budgets and original expected completion dates
- explanations for significant cost overruns, delays and key project performance metrics.



### 4. Management of purchasing cards and taxis

#### Management of purchasing cards

##### Policy framework

Agencies increasingly use purchasing cards to reduce bureaucratic processes and allow operational staff to make required purchases in dispersed procurement environments. We found all agencies that used purchasing cards had a policy in place. However, 26 per cent of agencies had not reviewed their purchasing card policy by the scheduled date, or had not scheduled a revision date for their policy.

**Recommendation:** 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'.

## Management of taxis

### Preventative controls

All agencies have designed and implemented some preventative controls to deter the potential misuse of purchasing cards. However, only 32 per cent of agencies apply merchant blocks and only 37 per cent apply geographic restrictions on purchasing cards.

**Conclusion:** Further opportunities exist for agencies to better control the use of purchasing cards, such as:

- updating purchasing card registers to contain all mandatory fields required by TPP17–09
- appointing a program administrator for the agency's purchasing card framework and defining their role and responsibility for the function
- strengthening preventive controls to prevent misuse.

### Detective controls

Agencies have designed and implemented some detective controls aimed at identifying misuse of purchasing cards. However, data analytics was used at only 29 per cent of agencies, and independent spot checks were used at only 49 per cent of agencies.

**Conclusion:** More effective monitoring using purchasing card data can provide better visibility over spending activity and can be used to:

- detect misuse and investigate exceptions
- analyse trends to highlight cost saving opportunities.

Most agencies have a policy for managing taxi use, but 41 per cent are past their scheduled review date, or do not have a scheduled revision date. More than half of all agencies' policies do not offer alternative, lower cost travel options. For example, only 36 per cent of policies promoted the use of general Opal cards.

**Conclusion:** Agencies can promote savings and provide more options to staff where their taxi use policies:

- limit the circumstances where taxi use is appropriate
- offer alternate, lower cost options to using taxis, such as general Opal cards and rideshare.



## 5. Fraud and corruption control

### Prevention systems

Commissioning, outsourcing of services, and the advancement of digital technology is changing government agencies' fraud and corruption risks. Despite this, we found 23 per cent of agencies were not performing regular fraud risk assessments. Consequently, some agencies' fraud risk assessments may not be as robust and comprehensive as they could be.

Only 54 per cent of agencies have an employment screening policy. All agencies have IT security policies, but gaps in IT security controls undermines the effectiveness of these policies. Deficiencies in internal controls, which increased by 42 per cent this year, also create a fraud vulnerability that increases the longer the deficiency is unaddressed.

**Conclusion:** Poor IT security along with other gaps in agency prevention systems, such as employment screening practices heightens the risk of fraud and inappropriate use of data. Agencies' systems of internal controls may be less effective where new and emerging fraud risks have been overlooked, or known weaknesses have not been rectified.

## Detection systems

Thirty-eight per cent of agencies had implemented a data monitoring program. Several more reported they were in the process of developing a program. Data monitoring, whereby entire populations of transactional data are analysed for indicators of fraudulent activities, is one of the most effective methods of early detection. Early detection decreases the duration a fraud remains undetected thereby limiting the extent of losses.

**Conclusion:** Data monitoring is an effective tool for early detection of fraud and is more effective when informed by a comprehensive fraud risk assessment.

## Notification systems

All agencies have notification systems for reporting actual or suspected fraud and corruption. Most agencies provide multiple reporting lines, provide training and publicise options for staff to report actual or suspected fraud and corruption.

**Conclusion:** Training staff about their obligations and the use of fraud notification systems promotes a fraud-aware culture.



# 1. Introduction

---

This report covers the findings and recommendations from our 2017–18 financial audits that relate to internal controls and governance at the 40 largest agencies (refer to Appendix three) in the NSW public sector.

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

This is our second 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. The way agencies deliver services increasingly relies on contracts and partnerships with the private sector. Many of these arrangements deliver front line services, but others provide less visible back office support. For example, an agency may rely on an IT service provider to manage a key system used to provide services to the community. The contract and service level agreements are only truly effective where they are actively managed to reduce risks to continuous quality service delivery, such as interruptions caused by system outages, cyber security attacks and data security breaches.

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 report divides these into the following five areas:

1. Internal control trends
2. Information technology (IT), including IT vendor management
3. Transparency and performance reporting
4. Management of purchasing cards and taxis
5. Fraud and corruption control.

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, controls and service delivery comments are included in the individual 2018 cluster financial audit reports, which will be tabled in Parliament from November to December 2018.

## **The focus of the report has changed since last year**

Last year's report topics included asset management, ethics and conduct, and risk management. We are reporting on new topics this year. We plan to introduce new topics and re-visit our previous topics in subsequent reports on a cyclical basis. This will provide a baseline against which to measure the NSW public sectors' progress in implementing appropriate internal controls and governance processes to mitigate existing, new and emerging risks in the public sector.

## **Agencies selected for the volume account for 95 per cent of the state's expenditure**

While we have covered only 40 agencies in this report, those selected are a large enough group to identify common issues and insights. They represent about 95 per cent of total expenditure for all NSW public sector agencies.



## 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 findings, level of risk and the most common deficiencies we found across agencies. The rest of this volume presents this year's controls and governance findings in more detail.

Observation	Conclusions and recommendations
<b>2.1 High risk findings</b>	
We found six high risk findings (seven in 2016–17), one of which was repeated from both last year and 2015–16.	<b>Recommendation:</b> Agencies should reduce risk by addressing high risk internal control deficiencies as a priority.
<b>2.2 Common findings</b>	
We found several internal controls and governance findings common to multiple agencies.	<b>Conclusion:</b> Central agencies or the lead agency in a cluster can play a lead role in helping ensure agency responses to common findings are consistent, timely, efficient and effective.
<b>2.3 New and repeat findings</b>	
Although internal control deficiencies decreased over the last four years, this year has seen a 42 per cent increase in internal control deficiencies.  IT control deficiencies feature in this increase, having risen by 63 per cent since last year. The number of repeat IT control deficiencies has doubled and is driven by the increasing digital footprint left by agencies as government prioritises on-line interfaces with citizens, and the number of transactions conducted through digital channels increases.	The increase in new IT control deficiencies and repeat IT control deficiencies signifies an emerging risk for agencies.  <b>Recommendation:</b> Agencies should reduce IT risks by: <ul style="list-style-type: none"><li>• assigning ownership of recommendations to address IT control deficiencies, with timeframes and actions plans for implementation</li><li>• ensuring audit and risk committees and agency management regularly monitor the implementation status of recommendations.</li></ul>

## 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. Rectifying high risk findings should be prioritised.

### We found six high risk findings, including one repeat high risk deficiency

The number of high risk internal control deficiencies has fallen from seven in 2016–17 to six this year. Five of the six high risk deficiencies related to financial controls and one to IT controls. One high risk deficiency was reported last year and in 2015–16.

Agencies should prioritise rectifying these high risk internal control deficiencies.

Finding	Implication
A high proportion of purchase orders were created and approved only after the goods and services were purchased (repeat issue).	There is an increased risk of: <ul style="list-style-type: none"><li>• purchases that have no business requirement and/or are outside of financial delegation</li><li>• disputes with vendors over the goods received/services performed</li><li>• double payments to vendors</li><li>• delays in payments to vendors</li><li>• reduced ability to monitor commitments and manage cashflows.</li></ul>
Financial delegations in the agency's HR system are not aligned to its organisational structure or delegations manual. Instances of non-compliance with the delegation policy were identified for committed purchases.	There is an increased risk of: <ul style="list-style-type: none"><li>• purchases being made outside of financial delegations</li><li>• purchases for which there no business requirement</li><li>• non-compliance with the <i>Public Finance and Audit Act 1983</i>.</li></ul>
There is no requirement to independently validate and verify vendor requests for changes to electronic payee/payment details, and verify changes to supplier bank account details when making changes to payment instructions in the vendor master file.	There is an increased risk of unauthorised changes being made to vendor bank account details resulting in financial loss to the agency as a result of fraud, phishing scams or error.
Instances were noted where staff did not follow the agency's procurement policy, including: <ul style="list-style-type: none"><li>• single source procurement where a competitive process may have been more appropriate</li><li>• approval of contract variations outside of financial delegations</li><li>• non-observance of contract management processes.</li></ul>	There is a risk the agency isn't achieving value for money from its procurement or contract management activities.
Employee leave entitlement data contains errors as a result of data migration issues following a system implementation several years ago. The data migration did not include all records relating to leave taken in service and other breaks in employment. Appropriate strategies to identify and rectify the data migration issues have not been put in place.	There is an increased risk of incorrect leave liability balances being reported in the financial statements. However, the true extent of the error cannot be reliably calculated without manually investigating each employee's records.

Finding	Implication
Absence of controls to monitor privileged user activities over several key systems.	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. This exposes agencies to greater risk of unauthorised changes to systems and data by these users, or by cyber criminals using their logon details. The absence of activity logs increases the risk that unauthorised changes may not be identified in a timely manner and/or be traceable to individual users.

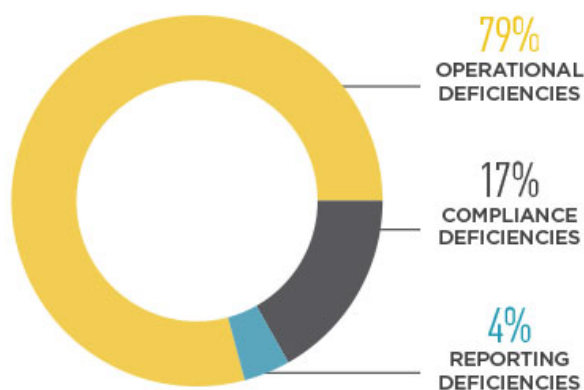
## 2.2 Common findings

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 or the lead agency in a cluster can help ensure consistent, timely, efficient and effective responses to identified deficiencies.

We classified the 312 internal control deficiencies we identified in 2017–18 into three groups:

- operational deficiencies
- compliance deficiencies
- reporting deficiencies.




### INTERNAL CONTROL DEFICIENCIES 2017-18



SOURCE: Audit Office management letters.

The graph above shows that 79 per cent of deficiencies (80 per cent in 2016–17) were operational, with the rest split between compliance deficiencies (17 per cent compared to 13 per cent in 2016–17) and reporting deficiencies (four per cent compared to seven per cent in 2016–17).




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, 3 repeat
	Moderate	113 new, 36 repeat
	Low	81 new, 11 repeat



  

Common issue	Findings/implication	Recommendations
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 of loss of corporate knowledge, that outdated policies and procedures may be followed, or that policies and procedures do not reflect better practice.	Agencies should establish processes that assure its policies reflect current requirements, reflect the organisation's current structure and delegations, and avoid both duplication and gaps.
Maintaining master files	Controls were not established to: <ul style="list-style-type: none"> <li>ensure sufficient segregation of duties over access to key master files</li> <li>verify the validity, accuracy and/or completeness of changes to key master files, such as vendor and payroll tables.</li> </ul>	Agencies should: <ul style="list-style-type: none"> <li>review controls established over access to key master files to prevent inappropriate access to, change or erasure of data</li> <li>regularly review system access of business users to ensure incompatible duties are removed.</li> </ul>
Purchase orders	Purchase orders were created and approved only after the goods and services were purchased. At one agency, this practice was so pervasive it was rated as high risk (see section 2.1).	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	1 new, 0 repeat
	Moderate	31 new, 4 repeat
	Low	14 new, 4 repeat

Common issue	Finding/implication	Lessons for agencies
Contract registers	<p>Agencies have not established contract registers or have incomplete or inaccurate contract registers. These agencies face challenges with:</p> <ul style="list-style-type: none"> <li>• complying with GIPA obligations</li> <li>• identifying contracts that are nearing completion, and commencing procurement activity in a timely manner</li> <li>• effectively managing their contractual commitments</li> <li>• disclosing contractual commitments accurately in their financial statements (where applicable).</li> </ul>	<p>Agencies should focus on establishing complete and accurate contract registers. This includes:</p> <ul style="list-style-type: none"> <li>• developing policies and procedures that govern the timely and accurate updating of the contracts register</li> <li>• monitoring the contracts register, including identifying contracts nearing completion so a new procurement can be commenced in a timely manner.</li> </ul>
Document retention	<p>Agencies do not always maintain documents to evidence performance of key control activities. This reduces accountability and increases the risk of non-compliance with State records legislation.</p>	<p>Control owners should be trained in their responsibilities to retain documents. Agencies should ensure appropriate records management policies have been communicated to staff.</p>
Central registers, such as those used to manage conflicts and gifts and benefits.	<p>Central registers are not kept, or are not updated in a timely manner.</p> <p>Without a central register to capture such information, agencies may not have the visibility it needs to oversight whether the management of conflicts and gifts and benefits complies with legislation and internal policies and is dealt with consistently.</p>	<p>Agencies should ensure they have registers to capture staff disclosures in a way that complies with legislation and policies.</p> <p>Conflicts of interest, gifts and benefits and other relevant policies should deal with the timeliness of how such registers are updated.</p>

Reporting		
	Moderate	5 new, 3 repeat
	Low	0 new, 4 repeat

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

Additional matters related to IT vendor management, fraud and corruption control and management of purchasing cards and taxis are detailed in later chapters of this report.

## 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 2017–18 audits identified 312 internal control deficiencies, comprising:

- 157 financial control deficiencies
- 155 IT control deficiencies.

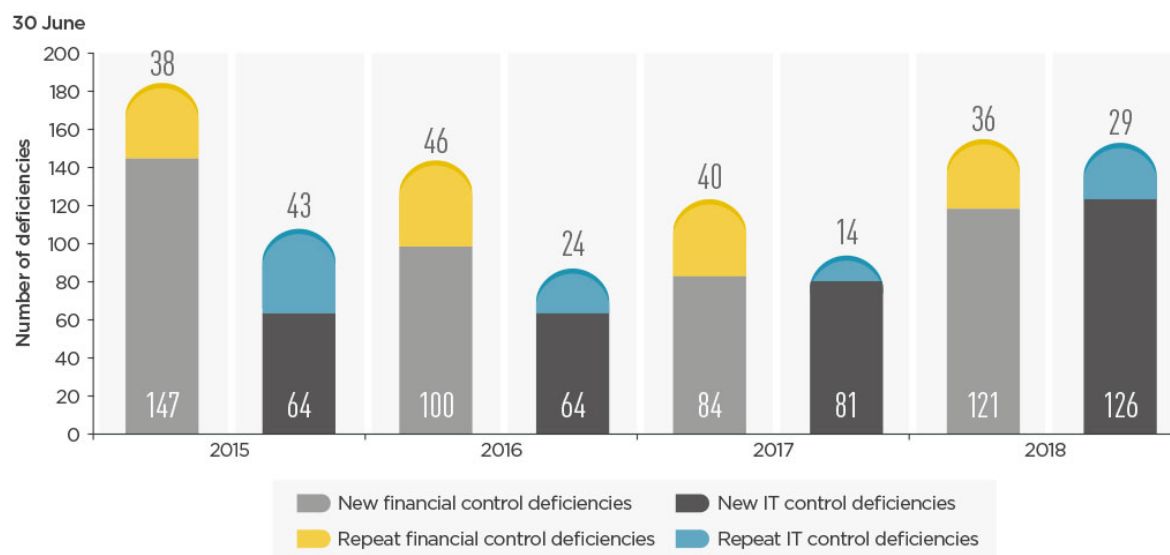
We reported these deficiencies to agency management and those responsible for governance at agencies, such as audit and risk committees and cluster secretaries. Our management letters outline each audit finding, assess its implications, rate the level of risk and make recommendations.

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](#).

## We have identified 42 per cent more internal control deficiencies than last year, many related to IT

The increase is predominately due to an increase in IT control deficiencies. Last year, we identified several emerging IT risks for agencies to prioritise. Accordingly, this year we focused our audits on how agencies had addressed the issues we identified. Our 2017–18 audits indicate that agencies need to further focus their attention on these issues.

### INTERNAL CONTROL DEFICIENCIES 2015-18



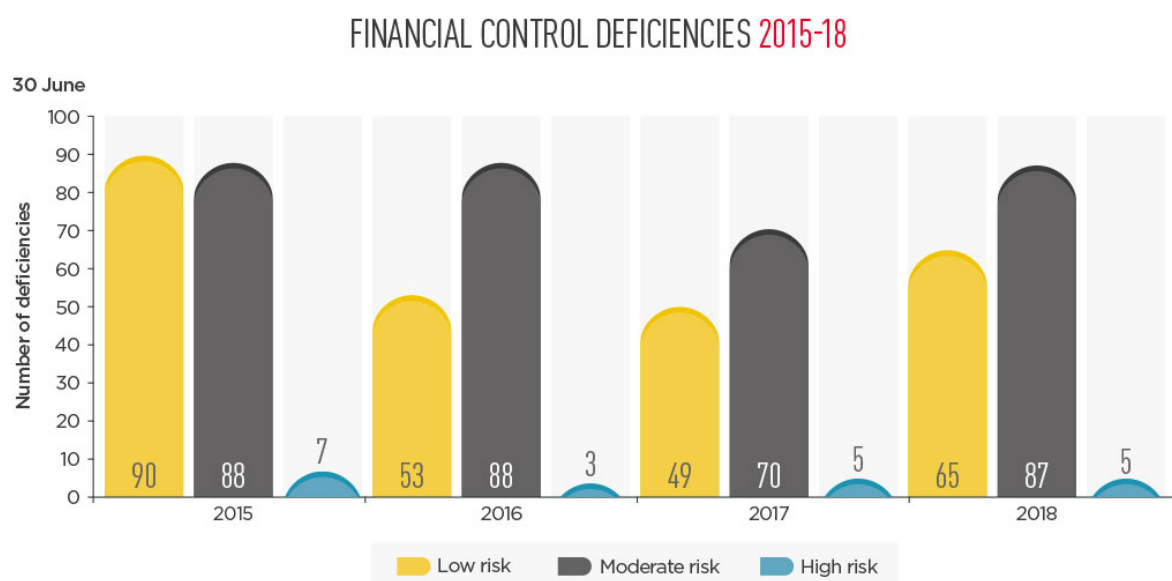
SOURCE: Audit Office management letters.

## The number of financial control deficiencies we identified rose for the first time in four years

Over the last 12 months financial control deficiencies increased by 27 per cent, after having declined by 33 per cent over the previous three years. However, the 157 deficiencies we found in 2017–18 is still lower than the 185 we found in 2014–15. We found financial control deficiencies at 75 per cent of agencies, a decrease from 79 per cent in 2016–17.

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 four years.



### **We identified 63 per cent more IT control deficiencies than last year**

The number of reported IT control deficiencies increased by 45 per cent over the last four years, from 107 in 2014–15 to 155 in 2017–18. This year, we found IT control deficiencies at 75 per cent of agencies, an increase from 63 per cent last year. We also found:

- new IT control deficiencies increased 56 per cent, from 81 in 2016–17 to 126 in 2017–18
- moderate risk deficiencies increased by 84 per cent, from 57 in 2016–17 to 105 in 2017–18
- high risk deficiencies decreased from two in 2017–18 to one in 2017–18.

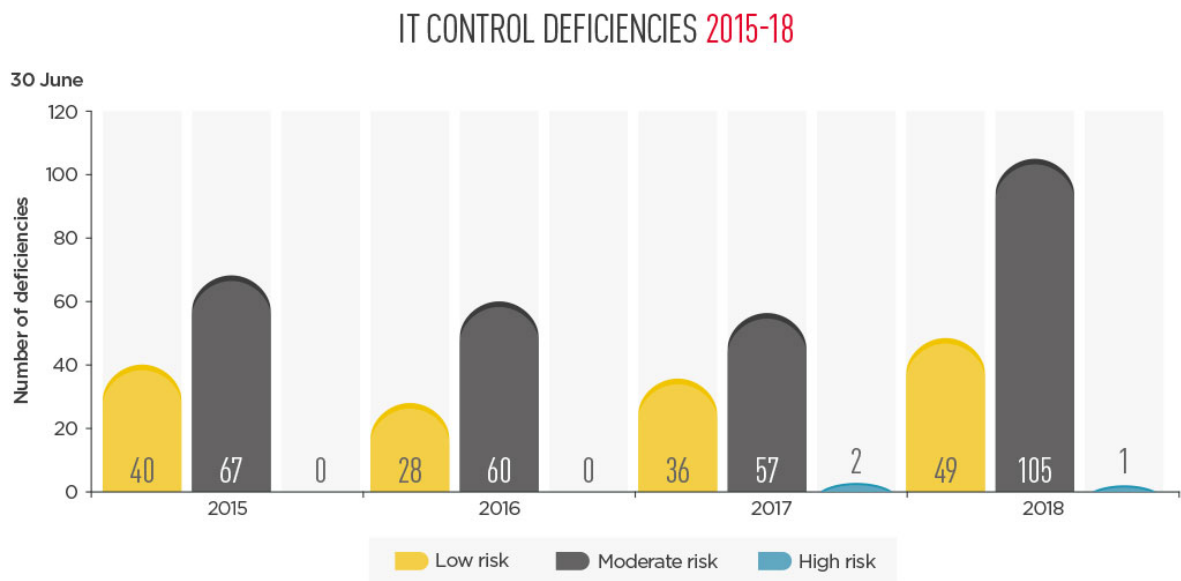
The increase in IT control deficiencies is driven by:

- the government's increasing digital footprint as it prioritises on-line interfaces with citizens, and the number of transactions conducted through digital channels increases
- re-direction of IT staff from business as usual activities to implement complex IT projects and systems
- absence of formal risk assessments over privileged user access, including high level access granted to third parties
- continued transition of services to outsourced service providers and shared service arrangements, which can 'blur' lines of responsibility.

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



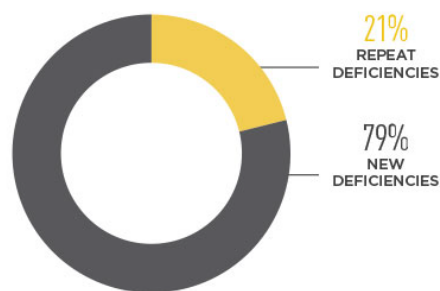
SOURCE: Audit Office management letters.

The increase in the number of control deficiencies we found this year, suggest agencies need to prioritise rectifying IT weaknesses in the year ahead.

#### Nearly a quarter of all control deficiencies have been unaddressed for more than 12 months

The number of repeat internal control deficiencies we identified has increased. As a percentage of all internal control deficiencies, it continues to represent nearly a quarter of all the internal control deficiencies we identified.

### NEW VERSUS REPEAT INTERNAL CONTROL DEFICIENCIES

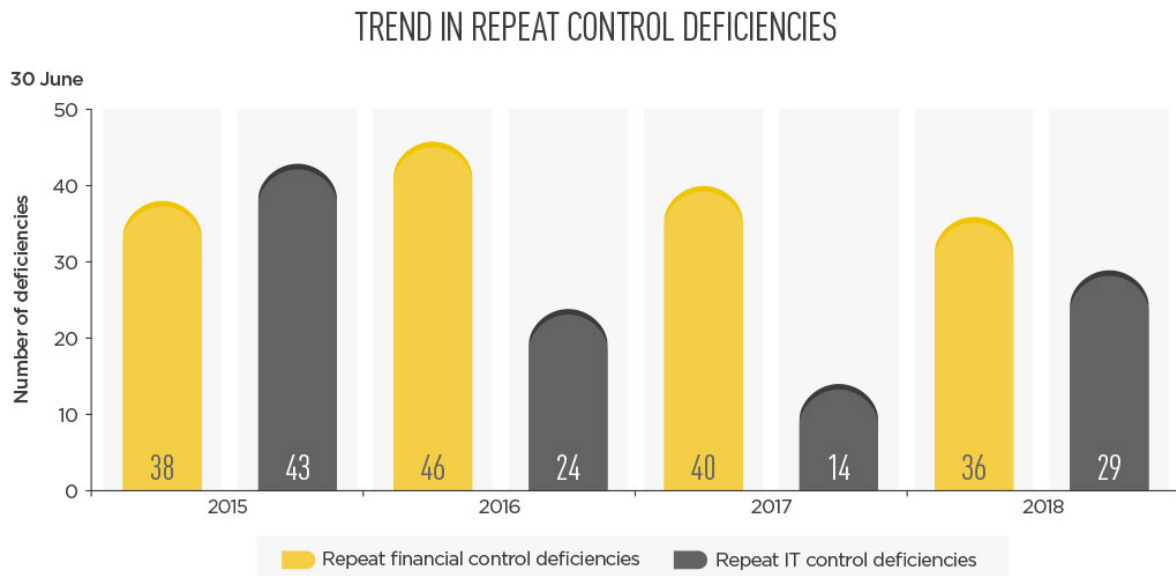


SOURCE: Audit Office management letters.

Of concern is the increase in repeat IT control deficiencies, up four percentage points from last year to 19 per cent of total IT control deficiencies.

### Repeat IT control deficiencies signify an emerging risk to agencies

Rectifying certain IT deficiencies can take longer than rectifying other control deficiencies. IT fixes may require program changes, system testing and interruptions to services. However, until they are addressed vulnerabilities that can be exploited by internal and external parties pose a threat to agencies. The graph below shows a spike in repeat IT control deficiencies in the current year.



SOURCE: Audit Office management letters.

Good IT controls underpin the effectiveness of processes and controls and protect the sensitive data agencies hold. Agencies need to address the above challenges by ensuring:

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

Proper controls should be maintained through any change process and considered as part of the design and implementation of a new system and the transition from a legacy system.



## 3. Information technology

Government agencies' financial reporting is now heavily reliant on information technology (IT). IT is also increasingly 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 audits reviewed whether agencies have effective controls in place to manage both key financial systems and IT service contracts.

### Observation

### Conclusions and recommendations

#### 3.1 Management of IT vendors

##### Contract management framework

Although 87 per cent of agencies have a contract management policy to manage IT vendors, one fifth require review.

**Conclusion:** Agencies can more effectively manage IT vendor contracts by developing policies and procedures to ensure vendor management frameworks are kept up to date, plans are in place to manage vendor performance and risk, and compliance with the framework is monitored by:

- internal audit focusing on key contracting activities
- experienced officers who are independent of contract administration performing spot checks or peer reviews
- targeted analysis of data in contract registers.

##### Contract risk management

Forty-one per cent of agencies are not using contract management plans and do not assess contract risks. Half of the agencies that did assess contract risks, had not updated the risk assessments since the commencement of the contract.

**Conclusion:** Instead of applying a 'set and forget' approach in relation to management of contract risks, agencies should assess risk regularly and develop a plan to actively manage identified risks throughout the contract lifecycle - from negotiation and commencement, to termination.

##### Performance management

Eighty-six per cent of agencies meet with vendors to discuss performance.

Only 24 per cent of agencies sought assurance about the accuracy of vendor reporting against KPIs, yet sixty-seven per cent of the IT contracts allow agencies to determine performance based payments and/or penalise underperformance.

**Conclusion:** Agencies are monitoring IT vendor performance, but could improve outcomes and more effectively manage under-performance by:

- a more active, rigorous approach to both risk and performance management
- checking the accuracy of vendor reporting against those KPIs and where appropriate seeking assurance over their accuracy
- invoking performance based payments clauses in contracts when performance falls below agreed standards.

##### Transitioning services

Forty-three per cent of the IT vendor contracts did not contain transitioning-out provisions.

Where IT vendor contracts do make provision for transitioning-out, only 28 per cent of agencies have developed a transitioning-out plan with their IT vendor.

**Conclusion:** Contract transition/phase out clauses and plans can mitigate risks to service disruption, ensure internal controls remain in place, avoid unnecessary costs and reduce the risk of 'vendor lock-in'.

## Observation

## Conclusions and recommendations

### Contract Registers

Eleven out of forty agencies did not have a contract register, or have registers that are not accurate and/or complete.

**Conclusion:** A contract register helps to manage an agency's compliance obligations under the *Government Information (Public Access) Act 2009* (the GIPA Act). However, it also helps agencies more effectively manage IT vendors by:

- monitoring contract end dates and contract extensions, and commence new procurements through their central procurement teams in a timely manner
- managing their contractual commitments, budgeting and cash flow requirements.

**Recommendation:** Agencies should ensure their contract registers are complete and accurate so they can more effectively govern contracts and manage compliance obligations.

## 3.2 IT general controls

### Governance

Ninety-five per cent of agencies have established policies to manage key IT processes and functions within the agency, with ten per cent of those due for review.

**Conclusion:** Regular review of IT policies ensures risks are considered and appropriate strategies and procedures are implemented to manage these risks on a consistent basis. An absence of policies can lead to ad-hoc responses to risks, and failure to consider emerging IT risks and changes to agency IT environments.

### User access administration

Seventy-two deficiencies were identified related to user access administration, including:

- thirty issues related to granting user access across 43 per cent of agencies
- sixteen issues related to removing user access across 30 per cent of agencies
- twenty-six issues related to periodic reviews of user access across 50 per cent of agencies.

**Recommendation:** Agencies should strengthen the administration of user access to prevent inappropriate access to key systems.

### Privileged access

Forty per cent of agencies do not periodically review logs of the activities of privileged users to identify suspicious or unauthorised activities.

**Recommendation:** 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.

### Password controls

Twenty-three per cent of agencies did not comply with their own policy on password parameters.

**Recommendation:** Agencies should ensure IT password settings comply with their password policies.

### Program changes

Fifteen per cent of agencies had deficient IT program change controls mainly related to segregation of duties and authorisation and testing of IT program changes prior to deployment.

**Recommendation:** Agencies should maintain appropriate segregation of duties in their IT functions and test system changes before they are deployed.

## 3.1 Management of IT vendors

Agencies increasingly contract delivery of key IT services to private sector vendors. There is good reason for this. IT systems are increasingly complex, and the risks are often best mitigated by seeking specialist skills to augment the agency's capability and capacity. However, even when the service is outsourced, the agency remains accountable for risks, including:

- 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.

We examined 30 IT vendor contracts to see how well agencies manage their service providers. We focussed on contracts that had a significant value and/or provided key services to the agency, such as software and infrastructure services, network, security, internet and telecommunications services.

### Contract management framework

#### **Most agencies have policies to manage IT vendors, but some require review**

Eighty-seven per cent of agencies have established contract management policies, but 19 per cent of those policies are past their scheduled review date. This increases the risk that outdated policies and procedures may be followed or that policies and procedures do not reflect current best practice.

The way agencies manage their IT vendors depends on their dependency on their IT vendors and the significance of the contract. Agencies can manage their IT vendors within their broader procurement framework, by using an IT vendor framework, or through an IT vendor contract specific framework.

We consider the robustness of agency contract management practices later in this report.

## Exhibit 1 – The importance of an effective contract management framework

### Lessons from the Learning Management and Business Reform Program

Our 2014 performance audit report on the [Learning and Management Business Reform Program](#) identified opportunities to improve the Department of Education's (the Department's) contract management framework.

The performance audit report found cost increases and delays might have been avoided by better program management, and contract management controls and processes. Procurement and contract management guidance should have been in place at the start of the program to address:

- competitive market testing
- documented vendor and contract reviews
- managing contract variations or contract extensions
- processes to verify invoices against work performed.

At the time of that audit, we also identified that:

- vendor and contract management processes help to ensure the quality, completeness and accuracy of work is consistently checked before invoices are paid
- the potential impact of risks and the contingency required to support the program were not reassessed when a new contract was negotiated. The new contract shifted risks from the vendor to the Department undetected.

Following the 2014 performance audit, the Department advises contract management processes have been improved by:

- recording contract details through the Department's contract register to support management of change requests, variations, on-going and new requirements
- transitioning all Learning and Management Business Reform contracts through the new Vendor Management System information to ensure rates and tenure are closely monitored and managed
- requiring the Learning and Management Business Reform Program to comply with the Department's financial and procurement delegations and working closely with Procurement Solutions Directorate and Legal Services to ensure compliance.

## Contract risk management

### Agencies are not using contract management plans or assessing contract risks

Contract management plans were not implemented for 41 per cent of the contracts we selected. A contract management plan should provide a framework whereby agencies:

- track how both parties to the contract are meeting their commercial and contractual commitments
- regularly monitor their service provider's performance
- can manage transition-in and out processes to ensure service delivery is uninterrupted and that appropriate controls remain in place throughout the transition
- assign appropriate resources to manage contracts, and provide clarity over their roles and responsibilities
- track and report on the realisation of benefits.

Poor contract management increases the risks associated with an IT vendor contract. Yet we also found that:

- risk assessments had not been performed on 41 per cent of contracts
- where a risk assessment had been performed, only 56 per cent of risk assessments had been updated during the lifecycle of the contract.

Contracting services from IT vendors allows agencies to access a larger pool of talent and leverage the investments others have made in technology. However, failure to assess and mitigate contract risks can have adverse consequences. The table below details some common risks and the proportion of agencies that identified the risk, where the agency had performed a contract risk assessment.

<b>Risk</b>	<b>Agencies that identified the risk (%)</b>	<b>Possible consequences</b>
<b>Dependence on a single supplier</b>	13	<ul style="list-style-type: none"> <li>• Use of single source procurement strategy limiting value for money or extension of contract without a value for money assessment.</li> <li>• Inability to transition from the vendor, even when underperforming.</li> <li>• Loss of internal knowledge and expertise impacting on ability to monitor performance or transition service back in-house.</li> </ul>
<b>Poor performance</b>	83	<ul style="list-style-type: none"> <li>• Service disruption/loss of business continuity.</li> <li>• Reputational damage.</li> </ul>
<b>Vendor insolvency</b>	28	<ul style="list-style-type: none"> <li>• Service disruption/loss of business continuity.</li> <li>• Financial losses.</li> </ul>
<b>Transitioning services</b>	24	<ul style="list-style-type: none"> <li>• Fraudulent conduct and/or information security breaches related to breakdowns in internal controls.</li> <li>• Service disruption/loss of business continuity.</li> </ul>
<b>Non-compliance with contractual terms (vendor or agency)</b>	72	<ul style="list-style-type: none"> <li>• Penalties and/or disputes.</li> <li>• Breaches of legislative requirements not detected, such as privacy legislation.</li> <li>• Breaches of key terms, such as insurance requirements, causing financial losses.</li> <li>• Information not provided causing an inability to monitor performance or enforce performance based penalties.</li> </ul>

Source: Audit Office analysis.

It is important that agencies don't apply a 'set and forget' approach in relation to management of contract risks. Risks should be assessed regularly and a plan put in place to manage the risks identified as the contract moves through its lifecycle, from negotiation and commencement to termination. Where a risk is identified, responsibilities can be established across the agency and IT vendor to mitigate the risk.

NSW Procurement publish a standard contract management plan on their website that agencies can access.

## Performance management

### Most agencies monitor IT vendor performance, but don't seek assurance over the accuracy of reported performance

Accurate reporting and active management of performance gains importance when the IT vendor's contract is strategically important, of high value, or the reported performance is used to enforce penalties or determine performance based payments.

Eighty-seven per cent of the contracts selected had service level arrangements (SLAs). Those SLAs specified KPIs for the vendor, and the frequency with which they were to be reported. Management received reports and met regularly with the IT service provider to discuss their performance in 86 per cent of cases. However, only 24 per cent of agencies have engaged their internal audit function or an independent auditor to obtain comfort that the reported KPIs used to assess performance are accurate. This is despite 67 per cent of the selected contracts containing clauses to impose penalties for underperformance or determine performance based payments.

These results are not dissimilar from one of the findings from our 2017 Report on [Sydney Roads Maintenance Contracts](#). The report found that Roads and Maritime Services had established a contract management framework, which includes most elements of good practice. However, it had not done enough to assure itself that the contractor provided performance and financial data was correct. This was important because this data was used to measure performance and calculate contractor payments.

The performance of strategically important IT contracts is best managed where monitoring processes, including the process undertaken to obtain comfort over the accuracy of reported KPIs is set out in a contract management plan. Agencies can further enhance their management of strategically important contracts by seeking assurance over the accuracy of reported service performance information.

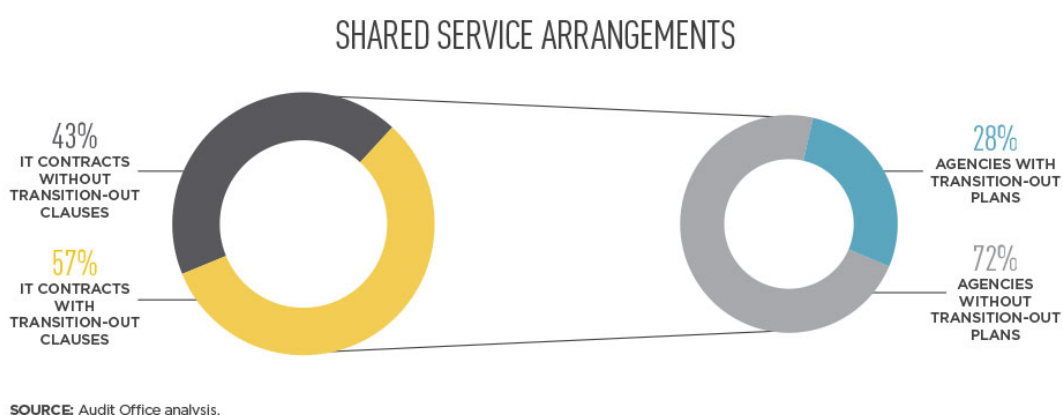
## Transitioning services

### Agencies can improve transition out arrangements with IT vendors

Agencies can mitigate their IT vendor dependency and transition risks by ensuring contracts contain clauses that:

- require the vendor to assist with the transition-out on contract termination
- require the vendor to develop and have approved a transition plan.

The following chart details the transition-out arrangements in place with IT vendors.



Fifty-seven per cent of the IT vendor contracts had clauses that required the vendor to provide assistance on transition and/or develop a transition/phase out plan. However, only 28 per cent of agencies have actually developed a transition/phase out plan with the IT vendor. While agencies may plan to implement a plan, it is better practice to do this early in the contract life, as the transition may need to occur before the expected contract end date.

Ineffective contract transition/phase out processes could result in service disruption, breakdowns in controls, unnecessary costs and an increased risk of 'vendor lock-in'. This risk is compounded where the contract is silent on the IT vendors' obligation to help with the transition/phase out.

### **Agencies could make better use of their contract registers to manage IT contracts**

Contract registers are an important tool from a financial management, legislative and contract management perspective. A contract register helps to manage an agency's compliance obligations under the *Government Information (Public Access) Act 2009* (the GIPA Act). The contract register also:

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

Our report on [Government agencies compliance with the GIPA Act](#) from 2016 found exceptions around the completeness and accuracy of agency contract registers. In our 2017–18 audits, we identified exceptions at 11 agencies because they did not have a contract register, or had registers that were not accurate and/or complete. This increases the risk of non-compliance with the GIPA Act, and sub-optimal procurement and contract management outcomes.

The GIPA Act allows for government information to be available to the public and includes establishing and maintaining a register of contracts with the Private Sector with a value of \$150,000 or more. The register is required to be published on the Government's Tenders website or on the agency website.

## **3.2 IT general controls**

Our audits reviewed IT general controls related to key financial systems that support the preparation of agency financial statements. IT general controls relate to the policies, procedures and activities put in place by an agency to ensure the confidentiality, integrity and availability of its ICT systems and data. These systems underpin the integrity of financial statement data.

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 consider the relevance of our findings below to these systems.

### **IT Governance**

IT governance provides a framework that ensures agencies' IT infrastructure supports and enables them to operate effectively and achieve its objective to deliver services to the public.

#### **Most agencies have policies for their key IT functions, but some require review**

Ninety-five per cent of agencies have established IT policies to manage key IT processes and functions within the agency. However, ten per cent of these policies are not regularly reviewed with one policy not reviewed since 2013. Regular review of IT policies ensures risks are considered and appropriate strategies and procedures are implemented to manage these risks on a consistent basis. An absence of policies can lead to ad-hoc responses to risks, and failure to consider emerging IT risks and changes to agency IT environments.

## Agencies can improve governance over new system implementations

During 2017–18, eight per cent of agencies implemented new IT systems that were within the scope of our financial audits. We found that agencies':

- project management plans did not articulate accountabilities, dependencies with other projects, responsibilities and timelines
- formal risk assessment activities were not performed to identify and manage risks associated with data migration
- security management plans did not deal with:
  - management and monitoring of user access related to project staff and contractors who had been granted system access to complete project activities
  - removal of user access from the migration environments after the data had been migrated
  - preventing copying of potentially sensitive data
  - data governance, including securing disposal of data and data masking requirements during migration and user acceptance testing phases
- training was not provided to all system users.

Deficiencies in project governance over new system implementations increase the risk of:

- the new system failing to meet the needs of the business or users and consequently the benefits of the project not being realised
- delays in delivery and cost overruns
- information security and data privacy breaches.

## 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 means agencies face risks if they do not adequately protect their IT systems from unauthorised access and misuse.

### User access administration

#### Agencies can improve user access administration over IT systems

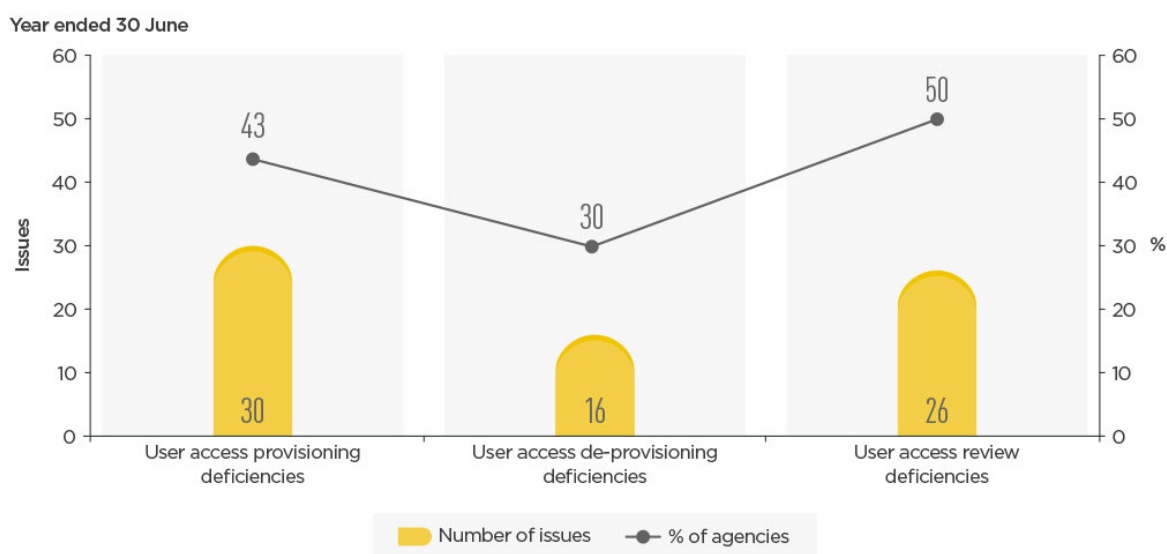
All agencies have implemented formal processes for user access creation and modification to IT systems. However, the graph below shows all aspects of user access management require improvement. We found:

- thirty issues related to granting user access across 43 per cent of agencies
- sixteen issues related to removing user access across 30 per cent of agencies
- twenty-six issues related to periodic reviews of user access across 50 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 and remove access of third party users
- weaknesses in the process to ensure staff access is removed on a timely basis and delays in removing the access of terminated staff
- no approval or no evidence of approval to support granting of access to new users or changes to user access level.

## USER ACCESS ADMINISTRATION DEFICIENCIES



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 those user profiles being used for cyber attacks.

The [NSW Government Digital Information Security Policy](#) mandates that agencies (except State Owned Corporations and universities) 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.

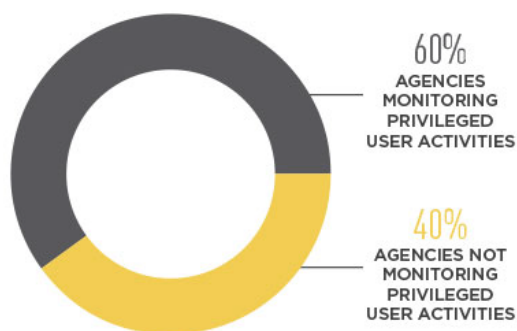
Agencies need to strengthen user access administration to prevent inappropriate access to sensitive systems.

## Privileged access

### Some agencies are not monitoring activities of privileged account users

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 or fraud. This is particularly true for those privileged users that are 'trusted insiders' who can be employees, business partners, or third-party contractors.

#### MONITORING OF PRIVILEGED USER ACTIVITIES



SOURCE: Audit Office management letters.

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

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 IT privileged users 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
- 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 11 of the *Public, Finance and Audit Act* and the [NSW Government Digital Information 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 to only staff that 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

### Agencies can improve their password controls

Twenty-three per cent of agencies did not comply with their own policy on password parameters. The deficiencies identified were 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 not applied (i.e. prompting the change of password frequently).

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

Agencies should review IT password settings to ensure that they are complying with the requirements of their password policies.

## Program changes

### Some agencies are not approving changes to IT programs prior to implementation

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 15 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 failure of a service provider to obtain approval before releasing changes to production and deficiency in IT change management policy.

At one agency, we noted that inappropriate changes were made to the finance system during the year. This caused a \$3.0 million understatement in annual leave expense every month, and manual calculations and journals were required each month to correct the expense. This issue highlights the importance of performing adequate user acceptance testing before IT program changes are moved to a production environment.

Weak program change control exposes agencies to the risk of:

- unauthorised and/or inaccurate changes to systems or programs
- issues with data accuracy and integrity
- inappropriately accepting contractual terms and 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 agencies' IT environments as it ensures appropriate policies and procedures to manage potential disasters and critical system failures have been implemented. This includes developing business continuity plans and disaster recovery plans.

### **Some agencies have not developed business continuity plans and disaster recovery plans**

We found deficiencies in agency disaster recovery and/or business continuity processes at 13 per cent of agencies. These deficiencies related to:

- absence of business continuity or disaster recovery plans, including supporting business impact analysis
- 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 Government Digital Information Security Policy](#) requires agencies to develop, review and test their disaster recovery plans.



## 4. Transparency and performance reporting

This chapter outlines our audit observations, conclusions and recommendations from our review of how agencies reported their performance in their 2016–17 annual reports. The Annual Reports (Statutory Bodies) Regulation 2015 and Annual Reports (Departments) Regulation 2015 (annual reports regulation) currently prescribes the minimum requirements for agency annual reports.

Observation	Conclusion or recommendation
<b>4.1 Reporting on performance</b>	
<p>Only 57 per cent of agencies linked reporting on performance to their strategic objectives.</p> <p>The use of targets and reporting performance over time was limited and applied inconsistently.</p>	<p><b>Conclusion:</b> There is significant disparity in the quality and consistency of how agencies report on their performance in their annual reports. This limits the reliability and transparency of reported performance information.</p> <p>Agencies could improve performance reporting by clearly linking strategic objectives to reported outcomes, and reporting on performance against targets over time. NSW Treasury may need to provide more guidance to agencies to support consistent and high-quality performance reporting in annual reports.</p>
<p>There is no independent assurance that the performance metrics agencies report in their annual reports are accurate.</p> <p>Prior performance audits have noted issues related to the collection of performance information. For example, our 2016 <a href="#">Report on Red Tape Reduction</a> highlighted inaccuracies in how the dollar-value of red tape reduction had been reported.</p>	<p><b>Conclusion:</b> The ability of Parliament and the public to rely on reported information as a relevant and accurate reflection of an agency's performance is limited.</p> <p>The relevance and accuracy of performance information is enhanced when:</p> <ul style="list-style-type: none"><li>• policies and guidance support the consistent and accurate collection of data</li><li>• internal review processes and management oversight are effective</li><li>• independent review processes are established to provide effective challenge to the assumptions, judgements and methodology used to collect the reported performance information.</li></ul>

Observation	Conclusion or recommendation
<b>4.2 Reporting on projects</b>	
<p>Agency reporting on major projects does not meet the requirements of the annual reports regulation.</p> <p>Forty-seven per cent of agencies did not report on costs to date and estimated completion dates for major works in progress. Of the 47 per cent of agencies that reported on major works, only one agency reported detail about significant cost overruns, delays, amendments, deferrals or cancellations.</p> <p>The information the annual reports regulation requires agencies to report deals only with major works in progress. There is no requirement to report on completed works.</p> <p>Sixteen of 30 agencies reported some information on completed major works.</p>	<p>NSW Treasury produce an <a href="#">annual report checklist</a> to help agencies comply with their annual report obligations.</p> <p><b>Recommendation:</b> 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.</p> <p><b>Conclusion:</b> Agencies could improve their transparency if they reported, or were required to report:</p> <ul style="list-style-type: none"> <li>• on both works in progress and projects completed during the year</li> <li>• actual costs and completion dates, and forecast completion dates for major works, against original and revised budgets and original expected completion dates</li> <li>• explanations for significant cost overruns, delays and key project performance metrics.</li> </ul>

## 4.1 Reporting on performance

Annual reporting is one of the 17 key elements of our [governance lighthouse](#). Making timely and balanced disclosures helps ensure agencies are transparent and accountable for their performance. Inadequate external performance reporting limits accountability and reduces transparency, which makes it hard for Parliament and the public to assess whether agencies are doing a good job.

We reviewed how transparent agencies are in how they report on performance. This involved reviewing key performance metrics reported in agency 2016–17 annual reports.

### Requirements and guidance about what agencies should report on performance in annual reports is limited

NSW Treasury provides limited guidance to support better practice performance reporting in agency annual reports. Annual reports legislation requires agencies to report on the nature and range of activities and, only if practicable, qualitative and quantitative performance measures showing efficiency and effectiveness. However, the guidance does not specifically require agencies to report:

- outcomes against stated objectives
- performance over time
- against set targets and baselines
- other information, such as the performance measurement methodology and any limitations or changes to adopted targets or performance measures between years.

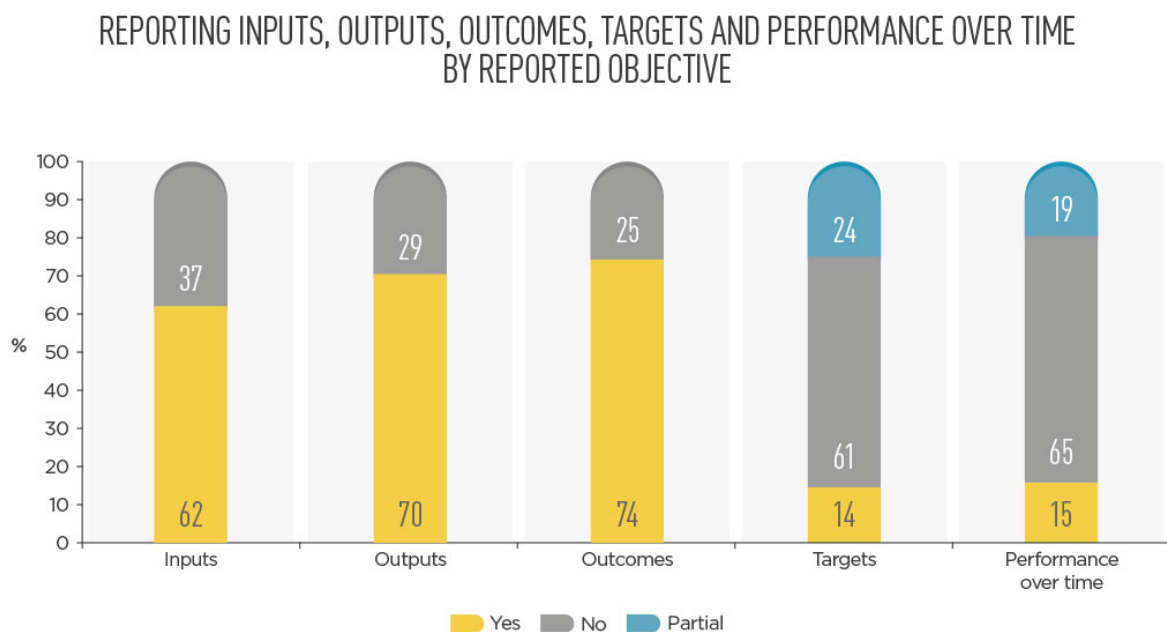
In the absence of comprehensive requirements and guidance, inconsistent practices and significant disparities in the quality, consistency, relevance and usefulness of performance reporting have emerged (see below for further details).

Some other jurisdictions' performance reporting frameworks establish clear links between the jurisdictional budget, agency corporate or strategic plans and annual reporting. For instance, the Commonwealth Government's enhanced Commonwealth performance framework nominates the corporate plan, annual performance statements, the Portfolio Budget Statements and annual reports, as key publications of government agencies. The framework prescribes the minimum matters to be included in agency corporate plans, annual reports and annual performance statements.

Improved guidance would help NSW agencies provide more relevant and reliable information to Parliament and the public.

### Linking objectives to outcomes, and reporting performance against targets enhances transparency

Only 57 per cent of agencies clearly referenced their performance reporting to their strategic objectives. For each of these reported objectives, we reviewed the nature of the performance metrics reported and whether this is accompanied by reporting on performance over time and set targets. We found the area of greatest relative weakness for agencies was reporting their performance against targets consistently over time. The results are detailed below.



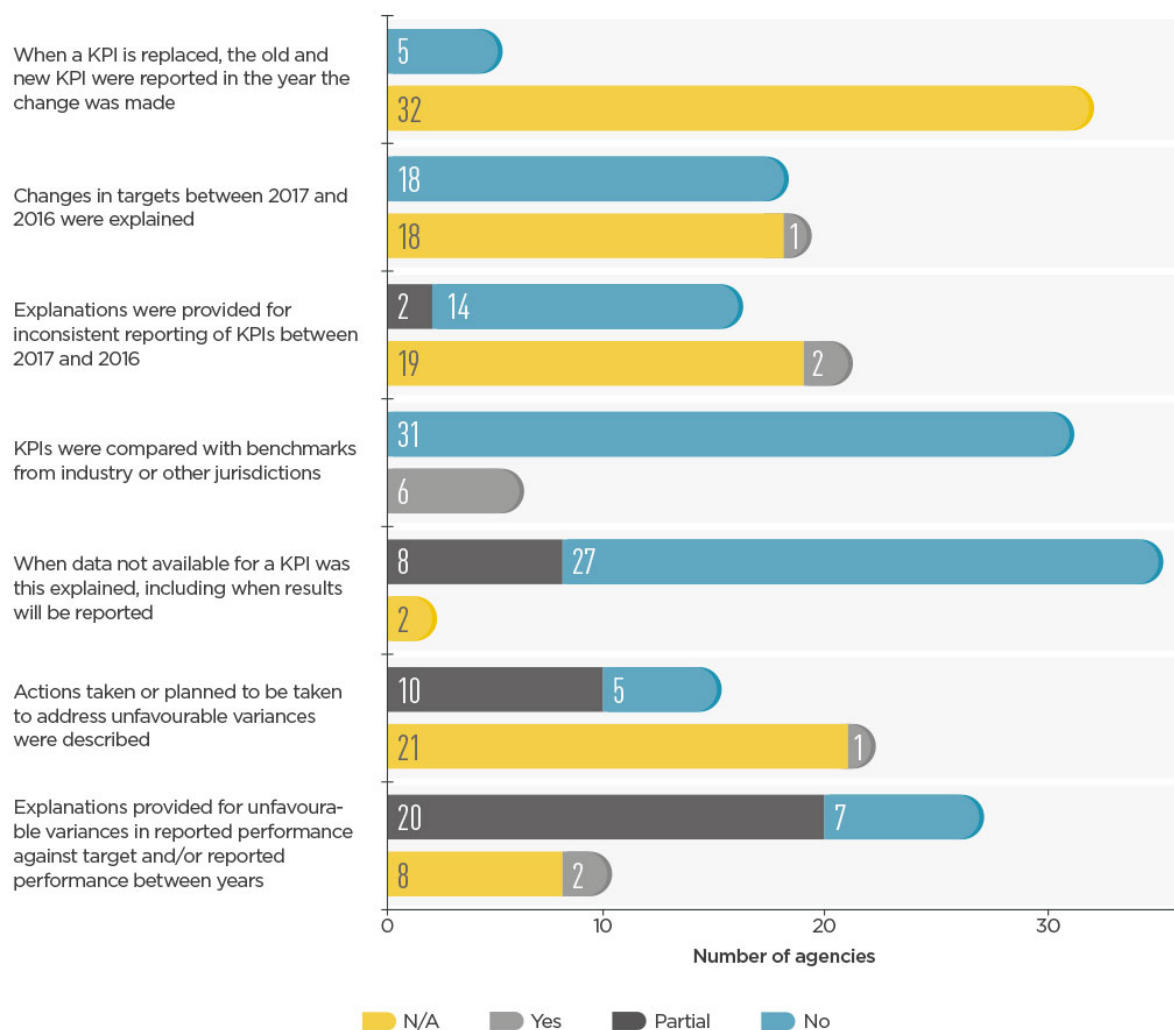
**SOURCE:** Audit Office analysis of agency 2016–17 annual reports.

\*A partial rating has been assigned when reporting targets or performance over time has been reported inconsistently against a given objective.

We also found that some other common principles of performance reporting were not in place, as illustrated in the graph below. Significantly, the areas where agencies' reporting was the least informative were:

- explaining variances between reported performance and target and/or reported performance consistently over time
- explaining why a target has changed between years
- comparing performance against benchmarks from industry or other jurisdictions.

## COMPARISON AGAINST COMMON PERFORMANCE REPORTING PRINCIPLES



SOURCE: Audit Office analysis of agency 2016-17 annual reports. \*A partial rating has been assigned when the above principles have been adopted inconsistently. N/A - Assigned where the principle was not relevant to the agencies 2016-17 annual report.

More generally, our analysis of annual reports showed agencies tend to report and focus on positive achievements, with limited acknowledgement where improvement is required.

### There is no independent assurance about the accuracy of reported performance metrics

Agencies are solely responsible for the accuracy of the performance metrics reported in their own annual reports. No independent assurance is required or sought that an agency's performance information is accurate. This limits the credence Parliament and the public might place on reported information as a relevant and accurate reflection of an agency's performance.

Prior performance audits have noted issues related to the collection of performance information. For example, our 2016 [Report on Red Tape Reduction](#) highlighted inaccuracies in how the dollar-value of red tape reduction had been reported. Estimates of the savings were in some cases based on unverified or unsubstantiated assumptions, cost-transfers, or pre-implementation projections that had not yet been achieved. Our 2018 report on [Progress and measurement of the Premier's Priorities](#) assessed the effectiveness of the approach undertaken by the Premier's Implementation Unit to measure and report on progress towards the Premier's Priorities performance targets. The report highlighted that the data used to measure progress of the Premier's Priorities came from a variety of government and external datasets, some which have inherent limitations that were not made clear when reported to the public.

For the purposes of this report, we did not look in detail at the systems and processes agencies have implemented to produce their performance metrics. The quality, reliability accuracy and consistency of reported information is enhanced by:

- developing policies and guidance aimed at improving the consistency and accuracy of data, related to collection, manipulation and presentation
- assigning responsibilities for management oversight of processes
- having effective internal review processes
- establishing independent review processes to provide effective challenge to the methodology used to collect the performance data, assumptions adopted, benchmarks applied and key judgements made.

## 4.2 Reporting on projects

The NSW Government's [2018–19 Infrastructure Statement](#) forecasts an \$87.2 billion investment program over four years to 2021–22. Transparent reporting on the progress of major projects is essential to ensure agencies are held accountable for the performance of projects they manage and realisation of benefits.

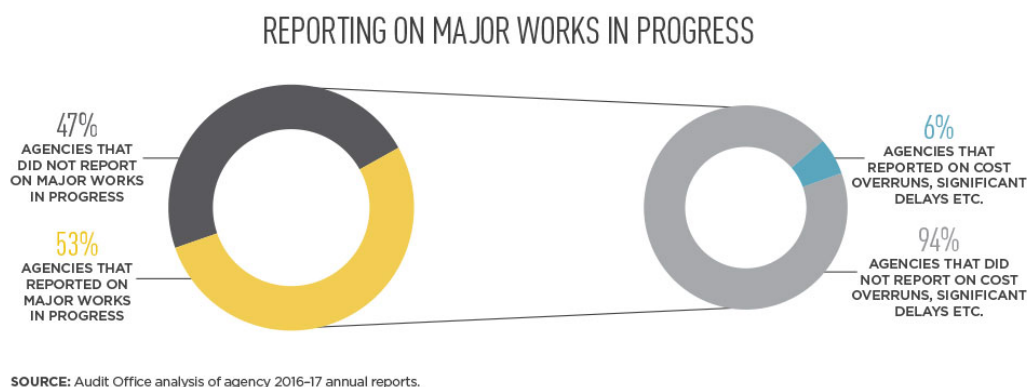
The annual reports regulation requires agencies to report the following information in their annual reports:

- details, lists or tables of major works in progress, the cost of those works to date and the estimated dates of completion, together with particulars of significant cost overruns in major works or programs
- the reasons for any significant delays to, or amendment, deferment or cancellation of, major works or programs.

We assessed the transparency of agency reporting on major works in progress by reviewing whether the above information was reported in agency 2016–17 annual reports. We also considered whether agencies added other important information on their major projects, such as original and revised budgets and key project metrics, even though there is no legislative requirement to report this information.

### Agency reporting on major works in progress does not comply with annual report regulation

Fourteen of 30 agencies that should have reported on major works in progress in their annual report had not done so. In addition, of the 16 agencies that did report on major works in progress only one reported any detail around significant cost overruns, significant delays, amendments, deferrals or cancellations of major works, as detailed in the graph below.



As there are known delays in several projects being delivered by agencies within the scope of this report, it appears unlikely that such reporting was not relevant for the agencies concerned.

The annual reports regulation does not define 'major works in progress'. However, the Budget Papers refer to 'major works'. Each year each approved major work is described with its allocated funding. For context, the table below shows the value of the major works, as detailed in the 2016–17 Budget Papers, of the 14 agencies that did not report on their major works programs in their annual reports.

Major works program (range of values)	Number of agencies
Nil-\$1,000,000	1
\$1,000,001-\$10,000,000	4
\$10,000,001-\$50,000,000	2
\$50,000,001-\$100,000,000	3
\$100,000,000+	4

Source: 2016–17 Budget Papers and Audit Office analysis.

Some agencies expressed the view that since the annual reports regulation does not define what constitutes a 'major work', they had excluded their smaller major works programs. They did not believe their omission was material to their annual reporting.

Notwithstanding the above, the NSW Budget Papers do include details of major works in progress, the cost of those works to date and the estimated dates of completion, but the NSW Budget Papers do not include any of the other information required by the annual reports regulation, such as details of significant cost overruns and delays.

NSW Treasury produce an [annual report checklist](#) to assist agencies with their annual report compliance obligations. Agencies can use this checklist to improve the completeness and consistency of their annual reporting.

### **Agencies are not required to publicly report on completed major projects**

There is no legislative requirement for agencies to report on completed major works. While 16 of the 30 agencies did report on completed major works, there was no reporting of actual costs and completion dates against original and revised budgets, or the original expected date of completion.

Without this information, it is difficult to draw meaningful conclusions about the performance of a project or program. In addition, Parliament and the public have limited comfort that public resources have been used efficiently and effectively.

Overall, reporting on major projects and programs could be improved if:

- agencies report on both works in progress and projects completed during the year
- actual costs, completion dates and forecast completion dates (for works in progress) are reported against original and revised budget and original expected completion date
- the above is supported by qualitative information explaining the reasons for significant cost overruns, delays or other information, such as key performance metrics relevant to the project.



## 5. Management of purchasing cards and taxi use

This chapter outlines our audit observations, conclusions and recommendations, arising from our review of agency preventative and detective controls over purchasing card and taxi use for 2017–18.

Observation	Conclusion or recommendation
<b>5.1 Management of purchasing cards</b>	
<b>Volume of credit card spend</b> Purchasing card expenditure has increased by 76 per cent over the last four years in response to a government review into the cost savings possible from using purchasing cards for low value, high volume procurement.	<b>Conclusion:</b> The increasing use of purchasing cards highlights the importance of an effective framework for the use and management of purchasing cards.
<b>Policy framework</b> We found all agencies that held purchasing cards had a policy in place, but 26 per cent of agencies have not reviewed their purchasing card policy by the scheduled date, or do not have a scheduled revision date stated within their policy.	<b>Recommendation:</b> 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'.
<b>Preventative controls</b> We found that: <ul style="list-style-type: none"><li>• all agencies maintained purchasing card registers</li><li>• seventy-six per cent provided training to cardholders prior to being issued with a card</li><li>• eighty-nine per cent appointed a program administrator, but only half of these had clearly defined roles and responsibilities</li><li>• thirty-two per cent of agencies place merchant blocks on purchasing cards</li><li>• forty-seven per cent of agencies place geographic restrictions on purchasing cards.</li></ul>	<p>Agencies have designed and implemented preventative controls aimed at deterring the potential misuse of purchasing cards.</p> <p><b>Conclusion:</b> Further opportunities exist for agencies to better control the use of purchasing cards, such as:</p> <ul style="list-style-type: none"><li>• updating purchasing card registers to contain all mandatory fields required by TPP17–09</li><li>• appointing a program administrator for the agency's purchasing card framework and defining their role and responsibility for the function</li><li>• strengthening preventive controls to prevent misuse.</li></ul>

Observation	Conclusion or recommendation
<p><b>Detective controls</b></p> <p>Ninety-two per cent of agencies have designed and implemented at least one control to monitor purchasing card activity.</p> <p>Major reviews, such as data analytics (29 per cent of agencies) and independent spot checks (49 per cent of agencies) are not widely used.</p>	<p>Agencies have designed and implemented detective controls aimed at identifying potential misuse of purchasing cards.</p> <p><b>Conclusion:</b> More effective monitoring using purchasing card data can provide better visibility over spending activity and can be used to:</p> <ul style="list-style-type: none"> <li>• detect misuse and investigate exceptions</li> <li>• analyse trends to highlight cost saving opportunities.</li> </ul>
<p><b>5.2 Management of taxis</b></p>	
<p><b>Policy framework</b></p> <p>Thirteen per cent of agencies have not developed and implemented a policy to manage taxi use. In addition:</p> <ul style="list-style-type: none"> <li>• a further 41 per cent of agencies have not reviewed their policies by the scheduled revision date, or do not have a scheduled revision date</li> <li>• more than half of all agencies' policies do not offer alternative travel options. For example, only 36 per cent of policies promoted the use of general Opal cards.</li> </ul>	<p><b>Conclusion:</b> Agencies can promote savings and provide more options to staff where their taxi use policies:</p> <ul style="list-style-type: none"> <li>• limit the circumstances where taxi use is appropriate</li> <li>• offer alternate, lower cost options to using taxis, such as general Opal cards and rideshare.</li> </ul>
<p><b>Detective controls</b></p> <p>All agencies approve taxi expenditure by expense reimbursement, purchasing card and Cabcharge, and have implemented controls around this approval process. However, beyond this there is minimal monitoring and review activity, such as data monitoring, independent spot checks or internal audit reviews.</p>	<p><b>Conclusion:</b> Taxi spend at agencies is not significant in terms of its dollar value, but it is significant from a probity perspective. Agencies can better address the probity risk by incorporating taxi use into a broader purchasing card or fraud monitoring program.</p>

## 5.1 Management of purchasing cards

In 2015, the Department of Finance, Services and Innovation released [DFSI-2015-02 Efficient Electronic Payment Methods](#), which superseded Treasury Circular TC11–15 'Use of Purchasing Cards and Electronic Payment Methods'.

DFSI–2015–02 requires relevant agencies to use purchasing cards for all procurement related expenditure of \$5,000 or less for specified expenditure categories, unless there is a more cost effective electronic alternative. Supporting this policy is NSW Treasury's TPP [17-09 Use and Management of NSW Government Purchasing Cards](#), which helps agencies manage the use and administration of purchasing cards. This policy does not apply to State Owned Corporations and universities.

When effectively controlled, purchasing cards are a cost-effective payment method for low value, high volume procurement of goods and services. We assessed the policies, procedures and controls agencies have in place to ensure purchasing cards effectively manage the risk of:

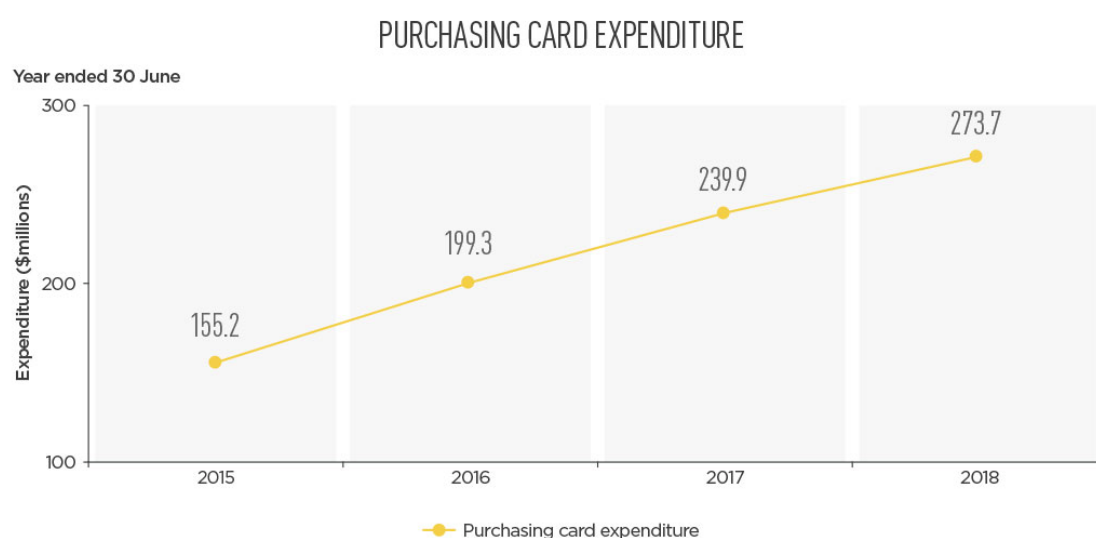
- inappropriate use and waste
- the potential for transactional and/or accounting error (e.g. duplication of payments)
- the application of inappropriate purchase method (e.g. indirectly purchasing an item or service on a purchasing card rather than seeking to negotiate contract terms and conditions).

## Volume of credit card spend

### Agencies are transitioning to purchasing cards for low value, high volume procurement

A government review in 2011 estimated that using purchasing cards and EFTs in the NSW public sector could achieve gross savings of around \$127.4 million over six years, based on a minimum transaction threshold of \$3,000 or less. The review also projected recurrent gross annual savings of \$33.0 million from year six onwards. It pointed out additional savings could be achieved by using better information to improve procurement sourcing.

TC11–15, and subsequently DSFI–2015–02 were issued in response to this review. The primary objective was to increase the uptake of purchasing cards across agencies. This report has not set out to confirm whether the uptake of purchasing cards met relevant targets, if the expected benefits have been realised, or whether the desired effect of increasing the use of purchasing cards had been achieved. The graph below highlights the increased use of purchasing cards over the last four years across the agencies we reviewed.



SOURCE: Audit Office analysis.

\*This analysis excludes three agencies, as we were unable to source purchasing card spend from prior years due to decommissioning and replacement of expense systems.

The 76 per cent rate of growth in purchasing card expenditure over the last four years means agencies should focus on developing effective frameworks for controlling and monitoring the use of purchasing cards.

## Policy framework

The establishment and implementation of a purchasing card policy is a core requirement under TPP 17–09.

We reviewed whether agencies had developed and implemented policies to control purchasing card use.

### All agencies have purchasing card policies in place

All agencies that held purchasing cards had policies in place. But 26 per cent of agencies have either not reviewed their purchasing card policies by the scheduled date, or have not specified a scheduled revision date for their policy.

TPP17–09 became effective from 1 April 2018. For those agencies that do not have a process for reviewing policies as pronouncements are made, or on a regular cyclical basis, there is a risk that their policies are not aligned to TPP17–09. Regular review of policies also ensures significant changes within the agency's structure, internal control environment, other regulatory requirements and better practice are reflected in agency policies on a timely basis.

## Preventative controls

Robust preventative controls at agencies is the foundation for a strong control environment to manage the use of purchasing cards.

We reviewed the adequacy of agency preventative controls.

### All agencies have established centralised registers of authorised cardholders

We found all agencies maintained a centralised register of authorised cardholders. TPP 17–09 requires agencies to maintain a purchasing card register and specifies several mandatory fields. However, we found purchasing card registers contained some, but not all required fields.

Fields included in agency purchasing card registers	Percentage of agencies (%)
Cardholder name included	100
Individual transaction limit and monthly limit specified	95
Last four digits of cardholder's card number included	89
Cancellation (where employee had changed roles or no longer employed) date specified	50*
Administrative conditions/restrictions attached to individual Pcards recorded	38
Confirmation the cardholder signed a Statement of Responsibility recorded	29

\* Generally, agencies removed the cardholder from the register when they ceased employment, rather than entering the card cancellation date.  
Source: Audit Office analysis.

A complete and accurate register helps manage the issue, use and cancellation of purchasing cards. It also helps ensure agencies manage card use within the overall limit approved under the *Public Authorities (Financial Arrangements) Act 1987*.

Agencies reported they did not comply with the TPP's core requirements because the information was being managed within multiple registers, or was contained within their expense management system. Agencies also advised that because cardholders could not obtain a purchasing card without signing a statement of responsibility, they did not believe that including the information in a register added any value.

### The roles and responsibilities of the program administrator were not adequately defined

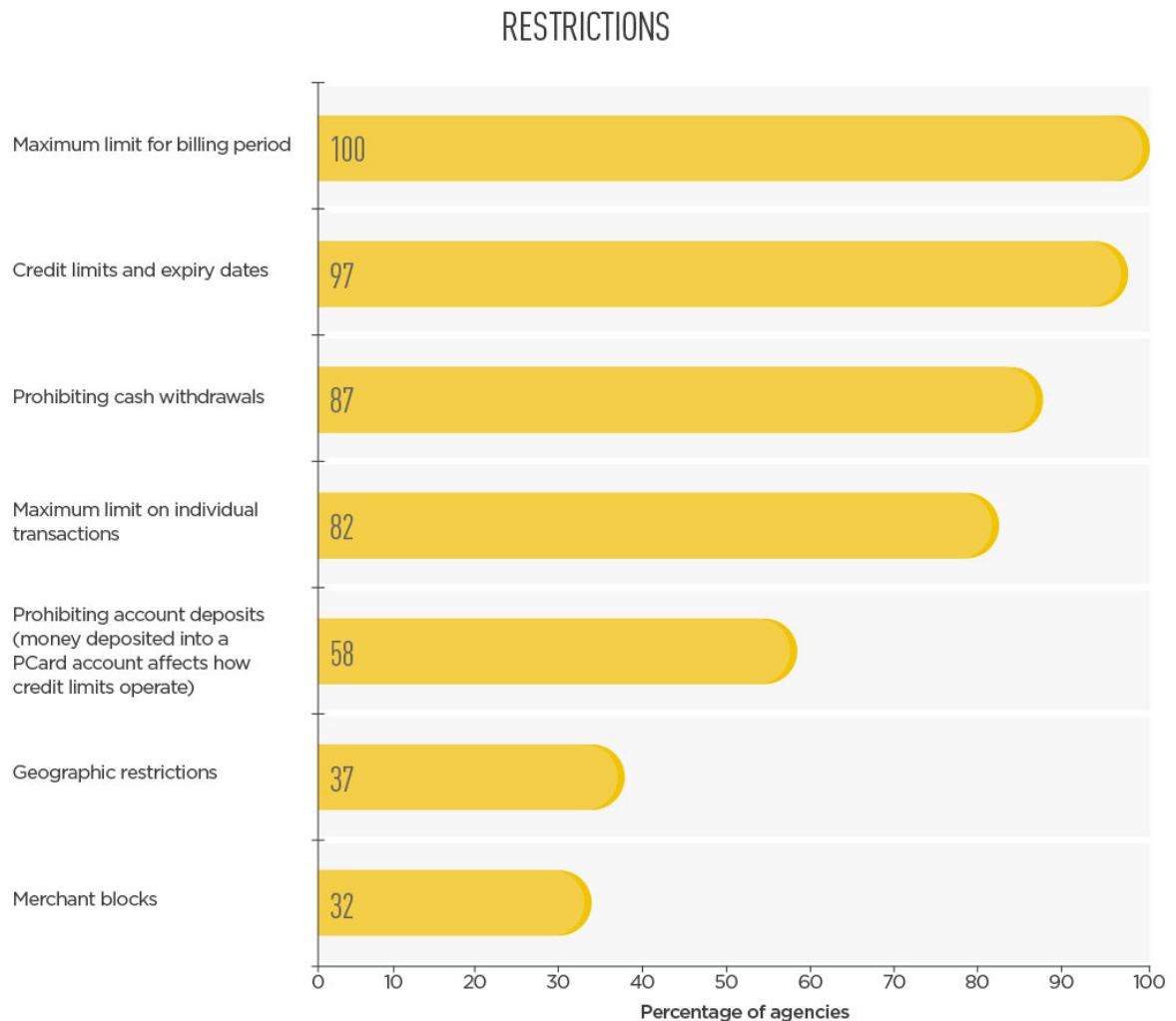
Eighty-nine per cent of agencies have appointed a program administrator or have an officer appointed to administer their frameworks for managing purchasing cards. But only 57 per cent of those agencies' purchasing card policies have clearly defined the roles and responsibilities of the program administrator.

Defining the roles and responsibilities of the program administrator ensures the expectations and obligations of the role are clearly communicated and known by all staff. It also establishes a central point of reference for staff when they need to clarify policy requirements, or when other issues arise such as a lost or stolen card.

Agencies should consider formally appointing a program administrator and updating their purchasing card policy to define the roles and responsibilities of the function.

### Only basic restrictions are applied to the use of purchasing cards

All agencies applied some restrictions on cardholders, mainly through applying credit limits and expiry dates, transaction limits and placing blocks on cash withdrawals. However, other restrictions, such as merchant blocks, geographic restrictions and prohibiting account deposits were less commonly used. The graph below shows the restrictions applied by agencies.



SOURCE: Audit Office analysis.

Agencies were more likely to use detective controls to highlight transactions with higher risk merchants, or from interstate or overseas locations. Wider use of cardholder restrictions is a more proactive control, which can also reduce the administrative costs of identifying and investigating suspicious transactions.

### Not all agencies provide training to staff on their cardholder responsibilities

Along with requiring staff to sign a statement of responsibility when issued with a purchasing card, 76 per cent of agencies also provide training to staff on their responsibilities and obligations.

Training can more effectively communicate key responsibilities and help cardholders understand their accountability for purchasing card use. It also demonstrates the agency's commitment to maintaining an effective purchasing card framework and minimising misuse.

## Detective controls

Detective controls are used by agencies to identify potential irregularities and misuse of purchasing cards. Detective controls further reduce the risk associated with the use of purchasing cards.

### All agencies reconcile their monthly purchasing card transactions

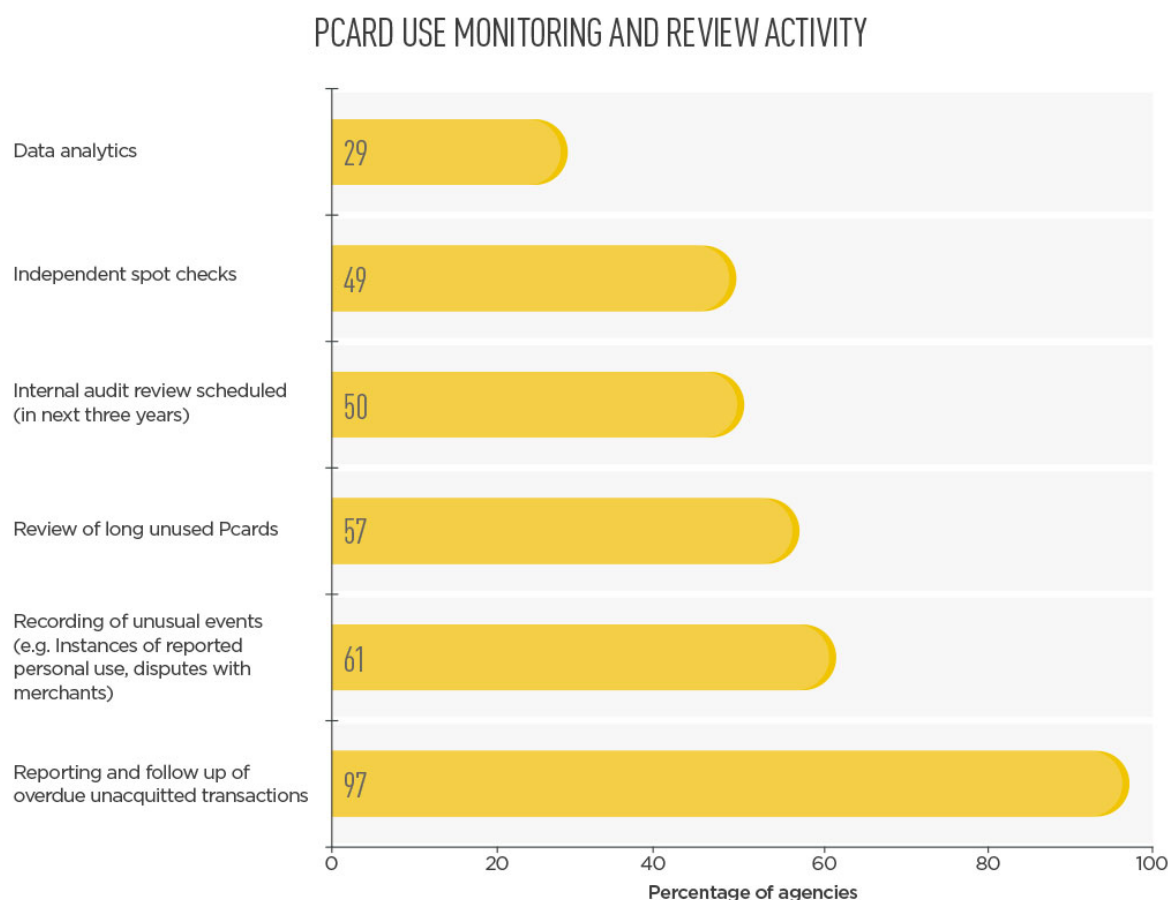
We found all agencies had controls in place to acquit monthly transactions, have the cardholder's direct manager review and approve purchasing card acquittals and to follow up on overdue unacquitted transactions.

A monthly purchasing card reconciliation process ensures that purchasing card transactions are valid, accurately coded and consistent with the agencies' purchasing card policy. It is the first line of defence in identifying fraudulent or erroneous transactions.

### Most agencies have some detective controls over purchasing card activity, but there are opportunities for improvement

Ninety-two per cent of agencies have designed and implemented at least one control to monitor and review purchasing card activity.

The extent of monitoring and review at each agency will depend on the significance of purchasing card activity, and the assessed risk of fraud and error associated with that activity. The graph below details the monitoring and review activity at agencies, while Exhibit 2 below, highlights some better practice examples from the agencies we reviewed.



SOURCE: Audit Office analysis.

Opportunities exist to improve monitoring and review activities by applying reviews, such as data analytics and independent spot-checks. The examples below show how some agencies use analysis to identify high risk patterns and anomalies in high volume transaction populations.

## Exhibit 2 - Better practice examples of purchasing card detection and monitoring controls

### Roads and Maritime Services

Roads and Maritime Services (RMS) operates a six-monthly purchasing card analytics program that focuses on the user's spending profile to identify potential misuse within the agency. The analysis identifies outliers (volume and value) and exceptions around common fraud and corruption indicators. Some information captured in the report includes:

- purchasing card activity summarised by volume and spend, by division and category, number of purchasing cards issued vs number of purchasing cards used, and average transaction amount by division
- spend by month and category (such as accommodation, travel, meals, taxis etc) identifying outlier transactions arising based on volume and value of transactions
- top ten purchasing card users
- details of exceptions arising from various tests, including potential personal use purchases, prohibited purchases, transactions made while an employee is on leave, transactions on weekends and public holidays, transactions made using a prohibited merchant, potential transaction splitting, overseas transactions and transactions made after an employee is terminated.

### Ministry of Health

The Ministry of Health's shared service agency, Healthshare has a continuous control monitoring program in place for purchasing cards. Tests are run daily to identify exceptions and these are investigated.

Tests include identification of excessive adjustments, credits or disputes, transactions made on Sundays, possible split transactions, duplicate transactions, employees whose credit cards are dormant for more than 30 days and transaction and descriptors with suspicious key words.

### Hunter Water Corporation

The purchasing card administrator performs random audits of employee purchasing card reconciliations for compliance with the agency's purchasing card policies. Departures from policy are followed up and corrective action taken, where appropriate.

### Department of Finance, Services and Innovation

The Department of Finance, Services and Innovation has implemented a monthly process to reconcile active purchasing card users to human resource establishment reports. This control helps to ensure that all terminated employees' purchasing cards are cancelled in a timely manner and reduces the risk that a terminated employee will misuse an uncanceled purchasing card.

## Most agencies report to senior management on purchasing card activity

Sixty-six per cent of agencies provide some level of reporting to senior management and/or those charged with governance on purchasing card activity. Management oversight helps to support the ongoing operation of a control environment, reinforces the importance of the control framework, and provides assurance the purchasing card framework is operating as intended.

At a minimum, agencies should be reporting to senior management on:

- cards in circulation, cancelled cards and inactive cards
- unacquitted transactions
- actions taken to address long overdue unacquitted transactions
- the results of monitoring activities
- outcomes from any investigations.

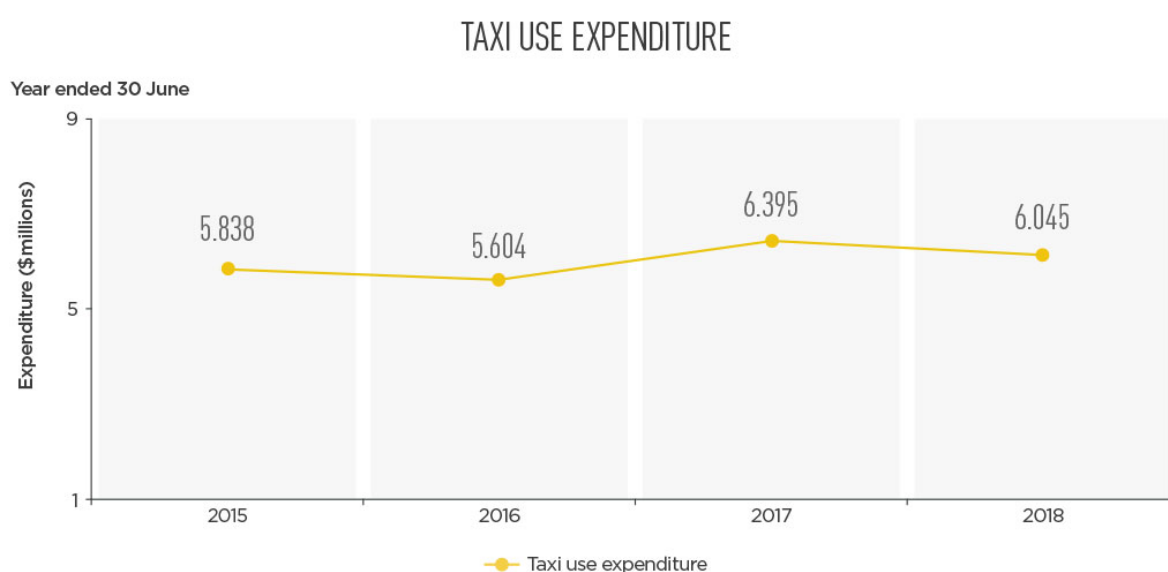
## 5.2 Management of taxis

Although the amount spent on taxis is not large in the context of agency operating budgets they are at higher risk of misuse. This risk needs to be managed effectively.

The NSW Government Travel and Transport Policy states 'taxi and ride-sharing options (e.g. Uber) should only be used when there is no appropriate and timely public transport option available'. We evaluated the policies, procedures and preventative and detective controls agencies have in place to comply with this policy. We focused on the following common payment methods; expenses claim forms, e-tickets, Cabcharge cards and purchasing cards (see section 5.1 above).

### Volume of taxi spend

Taxi use expenditure was approximately \$6.0 million across the in-scope agencies. The graph below shows the volume of spend on taxis over the last four years.



SOURCE: Audit Office analysis.

\*This analysis excludes seven agencies, as we were unable to source taxi use spend from prior years due to decommissioning and replacement of expense systems.

### Policy framework

We reviewed the adequacy of agency policies developed and implemented to support the NSW Government Travel and Transport Policy.

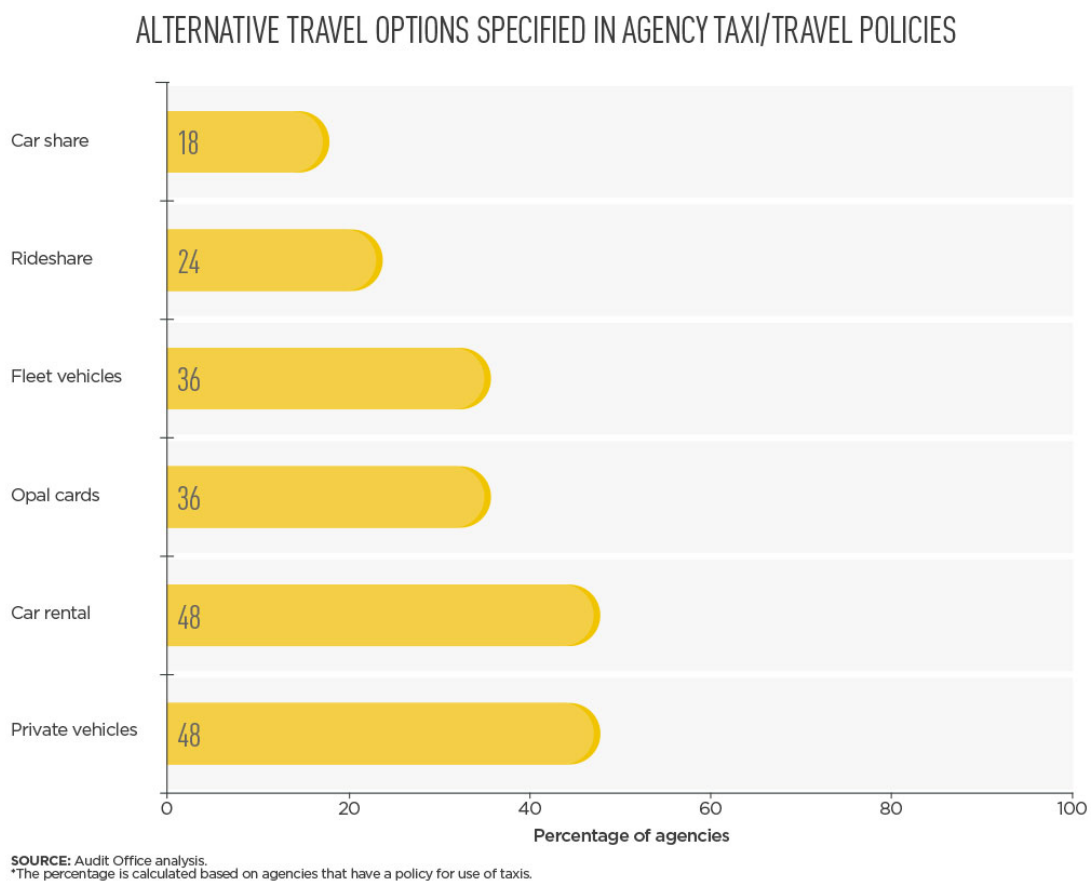
#### Some agencies have not developed policies for taxi use, or are applying outdated policies

Thirteen per cent of agencies have not developed and implemented a policy, either in a dedicated policy or broader travel policy, to manage taxi use. A further 41 per cent of agencies have not reviewed the policy by the scheduled revision date or do not have a scheduled revision date in the policy. The oldest policy dated back to 2009.

Failure to update policies by the scheduled review date increases the risk that outdated policies and procedures may be followed and that policies and procedures do not reflect current best practice. Specifically, for taxis, there is a risk that the policy does not reflect an agency's current preferred method for managing taxis and has not provided for the use of other more cost-effective travel options (see below).

## Most agency policies do not promote the use of cost saving travel options

The NSW Government Travel and Transport Policy encourages agencies to adopt alternative travel options such as ride-share and general Opal cards for use within Sydney metropolitan areas. The results of our analysis are presented below.



## Most policies deal only with common situations where taxis are used

Eighty-two per cent of the agencies have provided specific guidance in their policies related to typical and common situations when taxis can be used, however guidance could be more comprehensive to help reduce the risk of potential misuse. We found that some agencies' policies did not provide guidance around the following:

Guidance included in agency travel or taxi specific policies	Percentage of agencies (%)
Guidance on reporting lost or stolen cards	93
Travel to place of residence where personal safety is an issue (e.g. travel after 8pm)	87
Information on retention of supporting documentation for taxi claims	82
Guidance on return of unused e-tickets or Cabcharge cards	74
Travel to and from airports for official travel	60
Travel to and from official business functions	50
Prohibits entering into set fare arrangements with preferred drivers	6

Source: Audit Office analysis.

Seventy-seven per cent of agencies' policies specify the agency's preferred method to pay for taxis. By nominating a single preferred payment method, agencies are better able to monitor taxi use as there is one source of truth.

## Preventative controls

### Agencies have few preventative controls in place

Because taxi use is not considered a major expense stream, agencies are less focussed on implementing extensive preventative controls to reduce misuse. That said, 50 per cent of agencies using e-tickets require the staff member's direct supervisor to approve the request before the e-ticket is provided. Also, 72 per cent of agencies require Cabcharge card application forms to be completed before an employee is granted a card. This helps to ensure that only staff members with a business need are given the cards.

## Detective controls

We reviewed the adequacy of agency controls to monitor taxi use.

### Most agencies have implemented processes to approve taxi use expenditure

All agencies have implemented controls to approve taxi expenditure by expense reimbursement and purchasing card. However, we found 28 per cent of agencies did not require the supervising manager to review monthly Cabcharge card invoices to verify that the travel costs incurred on the card are valid before processing the invoice for payment.

### Registers help to manage the use of Cabcharge cards and e-tickets

The use of a centralised register ensures agencies are able to effectively monitor the use of Cabcharge cards and e-tickets, and prevent misuse by cancelling e-tickets and Cabcharge cards that are not required. We found:

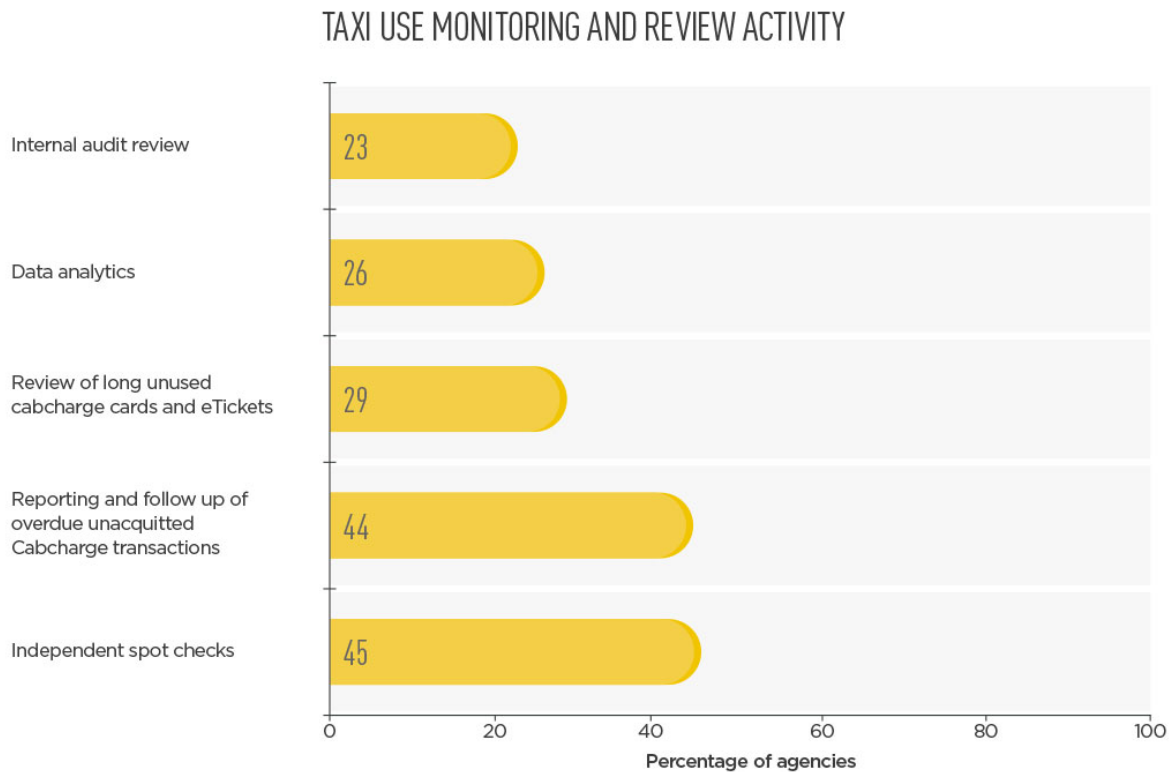
- eighty-seven per cent of agencies have established registers for issued e-tickets (either centralised or at a business unit level) within the agency. However, 33 per cent do not regularly review the register to ensure it remains up to date, and cancel unused e-tickets after a specified period (note: e-tickets expire automatically after 12 months)
- seventy-seven per cent of agencies maintain a register of issued Cabcharge cards.

Regular review of the registers helps to ensure:

- Cabcharge cards and e-tickets are only issued to active employees
- long outstanding e-tickets and unused Cabcharge cards are followed up and cancelled if necessary.

### Controls to monitor and review taxi use can be enhanced

Fifty-three per cent of agencies have not implemented controls, such as data analytics, spot checks and internal audit reviews to monitor and review taxi use. The graph below details the monitoring and review activity happening at the 47 per cent of agencies that have implemented controls to monitor and review taxi use.



SOURCE: Audit Office analysis.

The amount agencies spend on taxis is generally small in comparison to agency operating budgets. Agencies need to select and implement controls that balance the costs and benefits of their approach, but provide them with an appropriate level of assurance that taxi use complies with their policies. Some agencies may even find it more efficient to monitor taxi use as part of a broader purchasing card or fraud monitoring program.



## 6. Fraud and corruption control

---

Fraud and corruption control is one of the 17 key elements of our [governance lighthouse](#). Recent reports from ICAC into state agencies and local government councils highlight the need for effective fraud control and ethical frameworks. Effective frameworks can help protect an agency from events that risk serious reputational damage and financial loss.

Our 2016 [Fraud Survey](#) found the NSW Government agencies we surveyed reported 1,077 frauds over the three year period to 30 June 2015. For those frauds where an estimate of losses was made, the reported value exceeded \$10.0 million. The report also highlighted that the full extent of fraud in the NSW public sector could be higher than reported because:

- unreported frauds in organisations can be almost three times the number of reported frauds
- our 2015 survey did not include all NSW public sector agencies, nor did it include any NSW universities or local councils
- fraud committed by citizens such as fare evasion and fraudulent state tax self-assessments was not within the scope of our 2015 survey
- agencies did not estimate a value for 599 of the 1,077 (56 per cent) reported frauds.

Commissioning and outsourcing of services to the private sector and the advancement of digital technology are changing the fraud and corruption risks agencies face. Fraud risk assessments should be updated regularly and in particular where there are changes in agency business models. NSW Treasury Circular [TC18-02 NSW Fraud and Corruption Control Policy](#) now requires agencies develop, implement and maintain a fraud and corruption control framework, effective from 1 July 2018.

Our [Fraud Control Improvement Kit](#) provides guidance and practical advice to help organisations implement an effective fraud control framework. The kit is divided into ten attributes. Three key attributes have been assessed below; prevention, detection and notification systems.

This chapter outlines our audit observations, conclusions and recommendations, arising from our review of agency fraud and corruption controls for 2017–18.

## Observation

## Conclusion or recommendation

### 6.1 Prevention systems

#### Prevention systems

Ninety-two per cent of agencies have a fraud control plan in place, 81 per cent maintain a fraud database and 79 per cent report fraud and corruption matters as a standing item on audit and risk committee agendas.

Only 54 per cent of agencies have an employment screening policy and all agencies have IT security policies, but gaps in IT security controls could undermine their policies.

**Conclusion:** Most agencies have implemented fraud prevention systems to reduce the risk of fraud. However poor IT security along with other gaps in agency prevention systems, such as employment screening practices heightens the risk of fraud and inappropriate use of data. Agencies can improve their fraud prevention systems by:

- completing regular fraud risk assessments, embedding fraud risk assessment into their enterprise risk management process and reporting the results of the assessment to the audit and risk committee
- maintaining a fraud database and reviewing it regularly for systemic issues and reporting a redacted version of the database on the agency's website to inform corruption prevention networks
- developing policies and procedures for employee screening and benchmarking their current processes against ICAC's publication 'Strengthening Employment Screening Practices in the NSW Public Sector'
- developing and maintaining up to date IT security policies and monitoring compliance with the policy.

Twenty-three per cent of agencies were not performing fraud risk assessments and some agency fraud risk assessments may not be as robust as they could be.

**Conclusion:** Agencies' systems of internal controls may be less effective where new and emerging fraud risks have been overlooked, or known weaknesses have not been rectified.

### 6.2 Detection systems

#### Detection systems

Several agencies reported they were developing a data monitoring program, but only 38 per cent of agencies had already implemented a program.

Studies have shown data monitoring, whereby entire populations of transactional data are analysed for indicators of fraudulent activity, is one of the most effective methods of early detection. Early detection decreases the duration a fraud remains undetected thereby limiting the extent of losses.

**Conclusion:** Data monitoring is an effective tool for early detection of fraud and is more effective when informed by a comprehensive fraud risk assessment.

### 6.3 Notification systems

#### Notification system

All agencies have notification systems for reporting actual or suspected fraud and corruption. Most agencies provide multiple reporting lines, provide training and publicise options for staff to report actual or suspected fraud and corruption.

**Conclusion:** Training staff about their obligations and the use of fraud notification systems promotes a fraud-aware culture.

## 6.1 Prevention systems

Fraud prevention systems are the most cost-effective way to minimise fraud in an agency. Prevention strategies should be proportionate to the fraud risks identified by the agency.

We reviewed the adequacy of agency fraud prevention systems.

### **Most agencies have fraud control plans in place**

Ninety-two per cent of agencies have implemented fraud control plans. A fraud control plan sets out key fraud control activities, responsibilities and timeframes. The fraud control plan should be linked to fraud risk assessments and other key fraud control activities.

The effectiveness of some agencies' fraud control plans is impacted by the absence of regular fraud risk assessments (see below).

### **Some agencies are not documenting or regularly reviewing their fraud risks**

Fraud risk assessments are a key component of an agencies' fraud and corruption control plan. Despite this we found that 23 per cent of agencies were not performing fraud risk assessments. Fraud risk assessments should be integrated into the enterprise risk management process and performed at a sufficiently granular level so that it is given proper attention at an operational level. For example, at one agency, the 'Risk of fraud and corruption' was identified in the corporate risk register, but not cascaded through operational risk registers and therefore did not meaningfully address the agency's key fraud and corruption risks.

Agencies that do not perform fraud risk assessments or do not perform them at a sufficiently granular level are less likely to have mitigated the risk by implementing appropriate prevention or detection controls that target areas of high or emerging fraud risk.

The Fraud and Corruption Control Standard AS8001-2008 and our [Fraud Control Improvement Kit](#) suggests fraud risk assessments should be performed at least every two years.

### **A fraud database helps agencies analyse, report and monitor trends in suspected and actual frauds**

Nineteen per cent of agencies did not maintain a fraud control database. Without a database, agencies may not identify systemic fraud and corruption issues that indicate additional preventative or detective control measures may be required.

AS8001–2008 suggests a fraud control database contain:

- the date and time of the report
- how it was identified
- nature of the incident
- value of any loss
- action taken in response to the incident.

Systemic issues identified from review of an agency's fraud database should feed into fraud control plans.

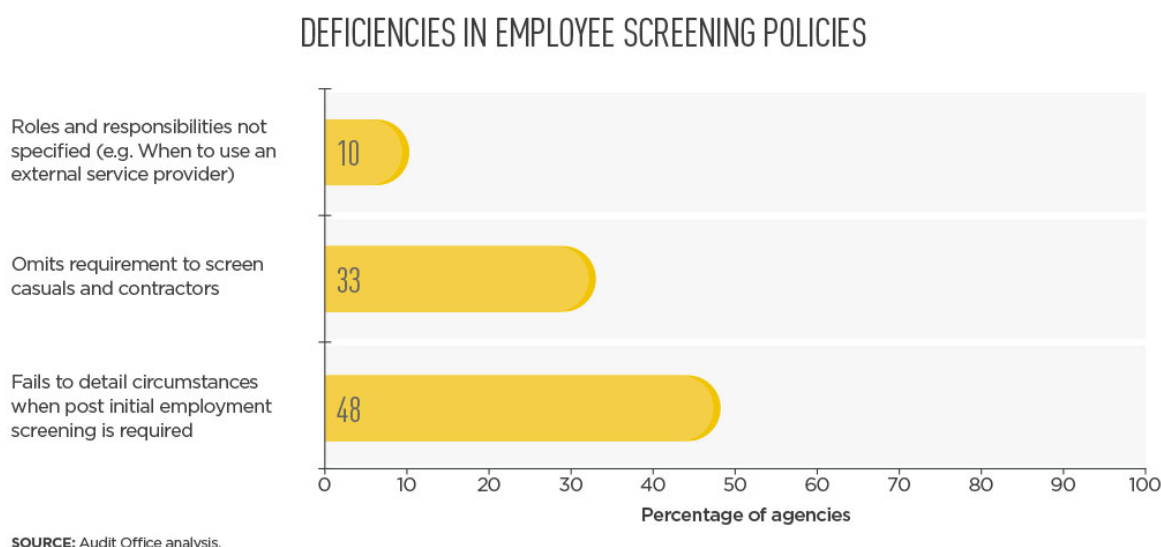
### Some agencies do not have employment screening policies, or have gaps in their policies

We found that 46 per cent of agencies did not have policies for employment screening either in a dedicated, or a broader hiring policy. Of the agencies that do have employment screening policies, opportunities exist to make their policies more comprehensive.

Employment application fraud is an indicator of future corrupt conduct and other acts of dishonesty, as highlighted in Exhibit 3 below. Without policies and procedures for employment screening, there is an increased risk that:

- inconsistent practices and/or gaps in practices will not be addressed
- the extent of employment screening will not proportionately address the role position, leading to either under or over screening potential employees
- an existing employee or contractor with a history of corrupt or criminal conduct being transitioned into a permanent role or higher risk role, without identification or safeguards being put in place.

The graph below shows some deficiencies we noted across the 54 per cent of agencies that had employment screening policies.



We did not look at all aspects of employment screening, instead focussing on the policies agencies have implemented to reduce the risk of employment application fraud. The Independent Commission Against Corruption (ICAC) published a report in February 2018 on [Strengthening Employment Screening Practices in the NSW Public Sector](#). Agencies can improve their processes by benchmarking to this report.

#### Exhibit 3 - Risk of employee application fraud

ICAC's report refers to several studies that indicate between 20 to 30 per cent of employee applications contain verifiably false information. The report also points to a number of case studies where fraudulent and corrupt conduct might have been prevented had the organisation implemented appropriate employee screening practices.

Despite this, only ten per cent of agencies identify employee application fraud as a risk that should be managed in their risk register.

### **Agencies have IT security policies, but gaps in IT security controls undermine their policies**

A key element of a prevention system is a specific IT security strategy aligned with the organisation's business strategy. This reflects the significant reliance on technology and the potentially serious consequences of a breach of IT security.

Poor IT security along with other gaps in agency prevention systems, such as employment screening practices heightens the risk of fraud and inappropriate use of data. Our audits continue to identify concerns over IT security controls. Section 3.2 of this report details our findings in greater detail.

## **6.2 Detection systems**

It is important for an agency to implement effective detection systems to mitigate fraud risks. Early detection limits the quantum of frauds by reducing the time the vulnerability can be exploited.

### **Agencies have internal controls to help prevent and detect fraud**

Internal controls are an effective way to detect fraud. Agencies need to maintain adequate internal controls, particularly during periods of change.

We found that agencies' systems of internal control are designed to allow it to prevent and detect fraud and error that could materially impact the financial statements. Section 2 of this report details our findings in greater detail.

### **The use of data monitoring programs is limited across most agencies**

A program of detective controls such as data monitoring and review supplements preventive internal controls, such as segregation of duties and line management reviews. Detective controls help agencies identify patterns, irregularities, anomalies and trends in large data sets. While several agencies reported they were developing a data monitoring program, only 38 per cent of agencies had actually implemented such a program. Some agencies have also used internal audit or other consultants to perform one-off or ad-hoc data analytics, but do not have a continuous data monitoring program in place.

A continuous data monitoring program can:

- detect fraud more quickly
- identify potential control gaps where the agency may be more susceptible to fraud or error
- provide other insights into the business that can help an agency save costs, improve processes, or realise other benefits.

The benefits are also highlighted in the [Association of Certified Fraud Examiners 2018 Global Fraud Study](#), which showed that:

- the use of proactive data monitoring and analysis and surprise audits was associated with a more than 50 per cent reduction in fraud losses
- data monitoring and analysis and surprise audits were correlated with the most significant reductions in fraud duration.

Ideally, agencies should link their data monitoring program to their fraud risk assessment to ensure they are targeting the right fraud risks.

## Exhibit 4 - Example of a data monitoring program for fraud detection

### Sydney Water Corporation's data analytics program for fraud and error detection

In response to ICAC's recommendations arising from Operation Siren, Sydney Water Corporation (SWC) established a data analytics program that is embedded into its controls monitoring, fraud detection, investigation activity and internal audits.

SWC have the ability perform over 150 data analytics tests across multiple data sets, captured in a data warehouse. This includes both internal and external data sets, including data from the financial management, payroll, developer works systems and the Australian Business Register.

The data analytics program sets out the objective of each test, the risk category, and details the nature of the test being performed. Tests are run daily, weekly or quarterly based on a risk profile. Reports are provided to relevant business units for follow up and action. Possible fraud and corruption matters are reported to the Investigations Specialist in Internal Audit for investigation.

Upon introduction of the data analytics program SWC reports that:

- the program has been successful in identifying errors in data processing or management oversight, including errors in payroll and cross-system errors
- they believe the program has acted as an overall deterrent against fraud
- the continued yearly cost of the program is now minimal and the program helps SWC develop potential internal audit topics and possible 'hot spots' for review.

### Most agencies' internal audit programs target fraud risks

Internal audits are also an important part of the fraud control environment. Seventy-two per cent of agencies have a targeted review of fraud controls on their three year internal audit plan.

## 6.3 Notification systems

Employees and external parties should be encouraged to report unethical behaviour, including fraud. It is important for employees to be able to make such reports without fear of reprisal and with confidence the report will be taken seriously and acted upon. The culture in an organisation is its greatest protection against fraud. Anonymous notifications of actual and suspected fraudulent activity figure prominently in every survey of how organisations in both the private and public sector detect fraud.

### Agencies have fraud and corruption notification policies in place, but some are past their review date

All agencies have policies associated with reporting actual or suspected fraud and corruption. However, 13 per cent of agencies had policies that are past their scheduled review date and many can improve their policies by:

- establishing clearer reporting lines
- allowing anonymous reporting
- clearly setting out the individual's and the agency's reporting obligations to ICAC, NSW Police and other oversight bodies.

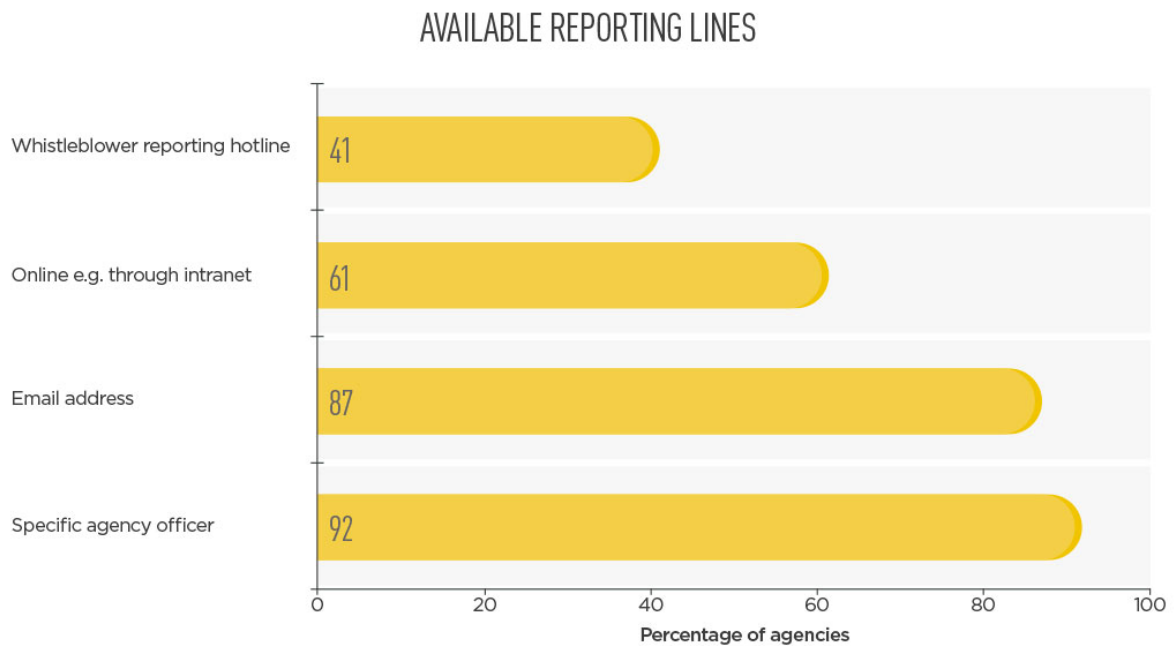
Up to date policies, clear reporting channels and well-publicised options for reporting fraud are all factors in making staff feel comfortable about reporting unethical behaviour.

The [Association of Certified Fraud Examiners 2018 Global Fraud Study](#) showed that 40 per cent of corruption cases were detected by tip-offs. This was 12 percentage points higher than other common methods (i.e. internal audit and management review) combined.

### Most agencies offer multiple ways for staff to report actual or suspected fraud and corruption

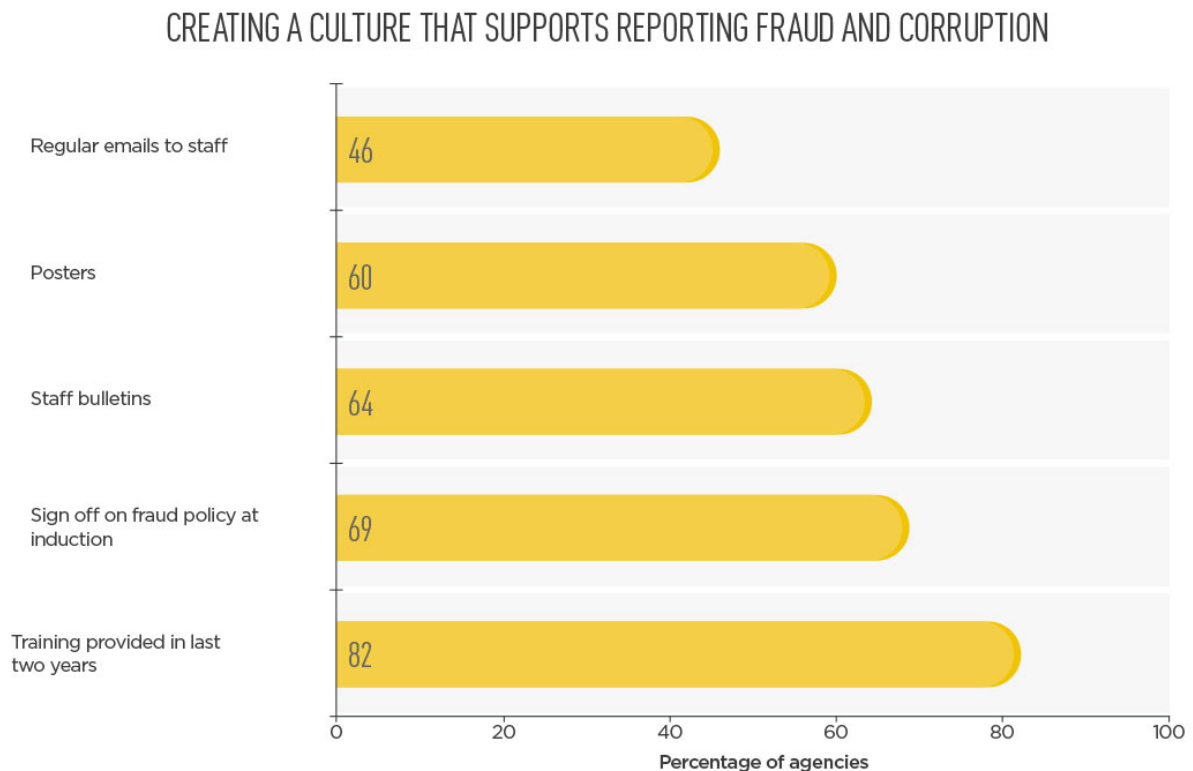
Eighty-five per cent of agencies provide more than one option for staff to report actual or suspected fraud and corruption. Multiple reporting lines accommodate the circumstances of the reporter and nature of the complaint.

The graph below shows the different reporting lines that agencies make available to staff.



SOURCE: Audit Office analysis.

The graph below details the different ways agencies publicise options for reporting fraud.



SOURCE: Audit Office analysis.

There are opportunities for some agencies to improve the culture that supports staff reporting actual or suspected fraud and corruption by increasing the number of reporting lines that are available to staff, and publicising these options more widely.

### **Agencies should report fraud and corruption matters to their audit and risk committees**

We found that 21 per cent of agencies' audit and risk committees did not have a standing item on the agenda for reporting of actual or suspected frauds.

Oversight by an audit and risk committee provides assurance that:

- fraud and corruption matters are being dealt with appropriately in line with agency policies and relevant legislation
- systemic issues are being identified and preventative and/or detective controls implemented to address the issue
- appropriate gravity is given to criminal behaviour, particularly if it is perpetrated by senior management.

Audit and risk committees play an important role in ensuring:

- fraud and corruption risks are being assessed and managed within agency enterprise risk frameworks
- appropriate systems and processes are in place to capture and effectively investigate fraud
- management act on staff reports of actual or suspected fraud.

## **Section two**

### Appendices



# Appendix one – List of 2018 recommendations

The table below lists the recommendations made in this report.



## 1. Internal control trends

### 1.1 High risk findings

Agencies should reduce risk by addressing high risk internal control deficiencies as a priority.



### 1.2 New and repeat findings

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.



## 2. Information technology

### 2.1 Management of IT vendors

Agencies should ensure their contract registers are complete and accurate so they can more effectively govern contracts and manage compliance obligations.



### 2.2 IT general controls

Agencies should strengthen the administration of user access to prevent inappropriate access to key systems.



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.

Agencies should ensure IT password settings comply with their password policies.



Agencies should maintain appropriate segregation of duties in their IT functions and test system changes before they are deployed.



## 3. Transparency and performance reporting

### 3.1 Reporting on projects

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.



## 4. Management of purchasing cards and taxis

### 4.1 Management of purchasing cards

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'.



Key



Low risk



Medium risks



High risks



## Appendix two – Status of 2017 recommendations

Recommendation	Current status	
<b>Overall trends</b>		
Agencies should focus on emerging information technology (IT) risks, but also manage new IT risks, reduce existing IT control deficiencies, and address repeat internal control deficiencies on a more timely basis.	The number of new and repeat IT control deficiencies increased this year. Refer to section 2.3 for further details.	!
Agencies should rectify high risk internal control deficiencies as a priority.	All but one of the high risk internal control deficiencies identified last year have been rectified.	–
Agencies should coordinate actions and resources to help rectify common IT control and governance deficiencies.	There has been a small reduction in the proportion of repeat internal control deficiencies. Refer to section 2.3 for further details.	–
<b>Information technology</b>		
Agencies should tighten privileged user access to protect their information systems and reduce the risks of data misuse and fraud. Agencies should ensure they: <ul style="list-style-type: none"> <li>only grant privileged access in line with the responsibilities of a position</li> <li>review the level of access regularly</li> <li>limit privileged user access to necessary functions and data</li> <li>monitor privileged user account activity on a regular basis.</li> </ul>	The use and monitoring of privileged users remains an issue at agencies. Refer to section 3.2 for further details.	!
Agencies should strengthen user access administration to prevent inappropriate access to sensitive systems. Agencies should: <ul style="list-style-type: none"> <li>establish and enforce clear policies and procedures</li> <li>review user access regularly</li> <li>remove user access for terminated staff promptly</li> <li>change user access for transferred staff promptly.</li> </ul>	User access administration remains an issue at agencies. Refer to section 3.2 for further details.	!
Agencies should review and enforce password controls to strengthen security over sensitive systems. As a minimum, password parameters should include: <ul style="list-style-type: none"> <li>minimum password lengths and complexity requirements</li> <li>limits on the number of failed log-in attempts</li> <li>password history (such as the number of password remembered)</li> <li>maximum and minimum password ages.</li> </ul>	Password controls remains an issue at agencies. Refer to section 3.2 for further details.	!

Recommendation	Current status	
The Department of Finance, Services and Innovation (DFSI) should revisit its existing framework to develop shared cyber security terminology and strengthen the current reporting requirements for cyber incidents.	Cyber security terminology is in the process of being developed with input from other jurisdictions and key stakeholders.  The current incident reporting process is not mandatory. DFSI is investigating options to make this reporting mandatory to overcome the current intermittent nature of reporting from agencies.	—
The Department of Finance, Services and Innovation should: <ul style="list-style-type: none"> <li>mandate minimum standards and require agencies to regularly assess and report on how well they mitigate cyber security risks against these standards</li> <li>develop a framework that provides for cyber security training.</li> </ul>	A draft version of minimum standards is being developed.  DFSI is working with clusters to understand current training already in place and leverage this information to develop training.	—
Agencies should consistently perform user acceptance testing before system upgrades and changes. They should also properly approve and document changes to IT systems.	Program change controls remains an issue at agencies. Refer to section 3.2 for further details.	—
Agencies should complete business impact analyses to strengthen disaster recovery plans, then regularly test and update their plans.	Absence of a disaster recovery or business continuity plan and/or testing during the year was identified at four agencies.	—
<b>Asset management</b>		
Agencies with high capital asset investment ratios should ensure their project management and delivery functions have the capacity to deliver their current and forward work programs.	Relevant agencies continue to monitor this recommendation. Agencies reported: <ul style="list-style-type: none"> <li>a reduction in their capital program, which reduces the risk of insufficient capacity to deliver the program</li> <li>that project risk management and delivery controls are in place to address this risk.</li> </ul>	—
Agencies should have formal processes for disposing of surplus properties.	Relevant agencies have developed a policy for disposal of surplus property or assessed that a policy is not required, as surplus property is rarely held.	✓
Agencies should use Property NSW to manage real property sales unless, as in the case for State owned corporations, they have been granted an exemption.	This exception did not arise during the audits of agencies. The relevant agencies have addressed this recommendation.	✓
<b>Ethics and conduct</b>		
Agencies should regularly review their code-of-conduct policies and ensure they keep their codes of conduct up-to-date.	Agencies have updated their code of conduct or advised that the code of conduct will be updated in 2018–19.	—

**Recommendation****Current status**

Agencies should improve the way they manage conflicts of interest, particularly by:

- requiring senior executives to make a conflict-of-interest declaration at least annually
- implementing processes to identify and address outstanding declarations
- providing annual training to staff
- maintaining current registers of conflicts of interest.

All agencies have a process that requires senior executives to make a conflict of interest declaration annually and update the conflict of interest register.

Some agencies are still implementing processes to identify and address outstanding declarations and provide training to staff.



Agencies should improve the way they manage gifts and benefits by promptly updating registers and providing annual training to staff.

Some agencies have not updated their policies to require immediate updating of the gifts and benefits register or provide annual training to staff.

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



## Appendix three – Cluster agencies

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

### Education

Agency	Website
Department of Education	<a href="http://www.dec.nsw.gov.au">www.dec.nsw.gov.au</a>

### Family and Community Services

Agency	Website
Department of Family and Community Services	<a href="http://www.facs.nsw.gov.au">www.facs.nsw.gov.au</a>
New South Wales Land and Housing Corporation	<a href="http://www.facs.nsw.gov.au">www.facs.nsw.gov.au</a>

### Finance, Services and Innovation

Agency	Website
Department of Finance, Services and Innovation	<a href="http://www.finance.nsw.gov.au">www.finance.nsw.gov.au</a>
Place Management NSW	<a href="http://www.property.nsw.gov.au">www.property.nsw.gov.au</a>
Property NSW	<a href="http://www.property.nsw.gov.au">www.property.nsw.gov.au</a>
Service NSW	<a href="http://www.service.nsw.gov.au">www.service.nsw.gov.au</a>
State Insurance Regulatory Authority	<a href="https://www.sira.nsw.gov.au/">https://www.sira.nsw.gov.au/</a>

### Health

Agency	Website
Ministry of Health	<a href="http://www.health.nsw.gov.au">www.health.nsw.gov.au</a>

### Industry

Agency	Website
Department of Industry	<a href="http://www.industry.nsw.gov.au">www.industry.nsw.gov.au</a>
Destination NSW	<a href="http://www.destinationnsw.com.au">www.destinationnsw.com.au</a>
Forestry Corporation of New South Wales	<a href="http://www.forestrycorporation.com.au">www.forestrycorporation.com.au</a>
TAFE Commission	<a href="http://www.tafensw.edu.au">www.tafensw.edu.au</a>
Water NSW	<a href="http://www.waternsw.com.au">www.waternsw.com.au</a>

### Justice

Entity	Website
Department of Justice	<a href="http://www.justice.nsw.gov.au">www.justice.nsw.gov.au</a>
Fire and Rescue NSW	<a href="http://www.fire.nsw.gov.au">www.fire.nsw.gov.au</a>
Legal Aid Commission of New South Wales	<a href="http://www.legalaid.nsw.gov.au">www.legalaid.nsw.gov.au</a>
NSW Police Force	<a href="http://www.police.nsw.gov.au">www.police.nsw.gov.au</a>
Office of the NSW Rural Fire Service	<a href="http://www.rfs.nsw.gov.au">www.rfs.nsw.gov.au</a>

## Planning and Environment

Agency	Website
Department of Planning and Environment	<a href="http://www.planning.nsw.gov.au">www.planning.nsw.gov.au</a>
Essential Energy	<a href="http://www.essentialenergy.com.au">www.essentialenergy.com.au</a>
Hunter Water Corporation	<a href="http://www.hunterwater.com.au">www.hunterwater.com.au</a>
Landcom	<a href="http://www.landcom.com.au">www.landcom.com.au</a>
Office of Environment and Heritage	<a href="http://www.environment.nsw.gov.au">www.environment.nsw.gov.au</a>
Office of Local Government	<a href="http://www.olg.nsw.gov.au">www.olg.nsw.gov.au</a>
Sydney Water Corporation	<a href="http://www.sydneywater.com.au">www.sydneywater.com.au</a>

## Premier and Cabinet

Agency	Website
Department of Premier and Cabinet	<a href="http://www.dpc.nsw.gov.au">www.dpc.nsw.gov.au</a>
Infrastructure NSW	<a href="http://www.infrastructure.nsw.gov.au/">http://www.infrastructure.nsw.gov.au/</a>

## Transport

Agency	Website
NSW Trains	<a href="http://www.nswtrainlink.info">www.nswtrainlink.info</a>
Rail Corporation New South Wales	<a href="http://www.transport.nsw.gov.au/railcorp">www.transport.nsw.gov.au/railcorp</a>
Roads and Maritime Services	<a href="http://www.rms.nsw.gov.au">www.rms.nsw.gov.au</a>
Sydney Trains	<a href="http://www.transport.nsw.gov.au/sydneytrains">www.transport.nsw.gov.au/sydneytrains</a>
Transport for NSW	<a href="http://www.transport.nsw.gov.au">www.transport.nsw.gov.au</a>
WCX M4 PTY Limited	<a href="http://www.westconnex.com.au">www.westconnex.com.au</a>
WCX M5 PTY Limited	<a href="http://www.westconnex.com.au">www.westconnex.com.au</a>

## Treasury

Agency	Website
Crown Finance Entity	<a href="http://www.treasury.nsw.gov.au">www.treasury.nsw.gov.au</a>
Insurance and Care NSW	<a href="http://www.icare.nsw.gov.au">www.icare.nsw.gov.au</a>
Lifetime Care and Support Authority	<a href="http://www.icare.nsw.gov.au">www.icare.nsw.gov.au</a>
NSW Treasury Corporation	<a href="http://www.tcorp.nsw.gov.au">www.tcorp.nsw.gov.au</a>
NSW Self Insurance Corporation	<a href="http://www.icare.nsw.gov.au">www.icare.nsw.gov.au</a>

## 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

**Purpose** – we have an impact, are accountable, and work as a team.

**People** – we trust and respect others and have a balanced approach to work.

**Professionalism** – we are recognised for our independence and integrity and the value we deliver.

Level 15, 1 Margaret Street  
Sydney NSW 2000 Australia

**PHONE** +61 2 9275 7100

**FAX** +61 2 9275 7200

[mail@audit.nsw.gov.au](mailto:mail@audit.nsw.gov.au)

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