

Report on Internal Controls & Governance 2017

20 DECEMBER 2017



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*.

Our major responsibility is to conduct financial or 'attest' audits of State public sector agencies' 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 agencies to ensure sound financial management.

Following a financial audit the Audit Office issues a variety of reports to agencies and reports periodically to parliament. In combination these reports give opinions on the truth and fairness of financial statements, and comment on agency 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 agency 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 agency's operations, or consider particular issues across a number of agencies.

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.

© 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.



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 52A of the *Public Finance and Audit Act 1983*, I present a report titled **Internal Controls and Governance 2017**.

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

Margaret Crawford
Auditor-General
20 December 2017

Contents

Internal controls and governance 2017

Executive summary	1
1. Overall trends	8
2. Information technology	18
3. Asset management	29
4. Governance	41
5. Ethics and conduct	49
6. Risk management	55
Appendix one – List of 2017 recommendations	65
Appendix two – Status of 2016 recommendations	67
Appendix three – Agencies selected for this volume	75



Executive summary

Effective internal controls and governance systems help agencies to operate efficiently and effectively and comply with relevant laws, standards and policies. We assessed how well agencies are implementing these systems, and highlighted opportunities for improvement.



1. Overall trends

New and repeat findings

The number of reported financial and IT control deficiencies has fallen, but many previously reported findings remain unresolved.

High risk findings

Poor systems implementations contributed to the seven high risk internal control deficiencies that could affect agencies.

Common findings

Poor IT controls are the most commonly reported deficiency across agencies, followed by governance issues relating to cyber security, capital projects, continuous disclosure, shared services, ethics and risk management maturity.



2. Information technology

IT security

Only two-thirds of agencies are complying with their own policies on IT security. Agencies need to tighten user access and password controls.

Cyber security

Agencies do not have a common view on what constitutes a cyber attack, which limits understanding the extent of the cyber security threat.

Other IT systems

Agencies can improve their disaster recovery plans and the change control processes they use when updating IT systems.



3. Asset management

Capital investment

Agencies report delays delivering against the significant increase in their budgets for capital projects.

Capital projects

Agencies are underspending their capital budgets and some can improve capital project governance.

Asset disposals

Eleven per cent of agencies were required to sell their real property through Property NSW but didn't. And eight per cent of agencies can improve their asset disposal processes.



4. Governance

Governance arrangements

Sixty-four per cent of agencies' disclosure policies support communication of key performance information and prompt public reporting of significant issues.

Shared services

Fifty-nine per cent of agencies use shared services, yet 14 per cent do not have service level agreements in place and 20 per cent can strengthen the performance standards they set.



5. Ethics and conduct

Ethical framework

Agencies can reinforce their ethical frameworks by updating code-of-conduct policies and publishing a Statement of Business Ethics.

Conflicts of interest

All agencies we reviewed have a code of conduct, but they can still improve the way they update and manage their codes to reduce the risk of fraud and unethical behaviour.



6. Risk management

Risk management maturity

All agencies have implemented risk management frameworks, but with varying levels of maturity.

Risk management elements

Many agencies can improve risk registers and strengthen their risk culture, particularly in the way that they report risks to their lead agency.

This report covers the findings and recommendations from our 2016–17 financial audits related to the internal controls and governance of the 39 largest agencies (refer to Appendix three) in the NSW public sector. These agencies represent about 95 per cent of total expenditure for all NSW agencies and were considered to be a large enough group to identify common issues and insights.

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 2017 cluster financial audit reports tabled in Parliament from October to December 2017.

This new report offers strategic insight on the public sector as a whole

In previous years, we have commented on internal control and governance issues in the volumes we published on each 'cluster' or agency sector, generally between October and December. To add further value, we then commented more broadly about the issues identified for the public sector as a whole at the start of the following year.

This year, we have created this report dedicated to internal controls and governance. This will help Parliament to understand broad issues affecting the public sector, and help agencies to compare their own performance against that of their peers.

Without strong control measures and governance systems, agencies face increased risks in their financial management and service delivery. If they do not, for example, properly authorise payments or manage conflicts of interest, they are at greater risk of fraud. If they do not have strong information technology (IT) systems, sensitive and trusted information may be at risk of unauthorised access and misuse.

These problems can in turn reduce the efficiency of agency operations, increase their costs and reduce the quality of the services they deliver.

Our audits do not review every control or governance measure every year. We select a range of measures, and report on those that present the most significant risks that agencies should mitigate. This report divides these into the following six areas:

1. Overall trends
2. Information technology
3. Asset management
4. Governance
5. Ethics and conduct
6. Risk management.



1. Overall trends

Our report begins by reviewing the overall trends in the number and nature of deficiencies we found in agency controls and governance systems.

The number of identified internal control deficiencies are falling, however one-quarter are repeat deficiencies

The number of reported financial and IT control deficiencies has reduced over the past three years. Repeat deficiencies still make up a sizeable proportion of all internal control deficiencies. We also found seven high risk internal control deficiencies at agencies, which expose them to increased risk of:

- fraud
- material misstatements in financial statements
- material loss of data
- significant increases in costs.

Recommendations

Agencies should focus on emerging IT risks, but also manage new IT risks, reduce existing IT control deficiencies, and address repeat internal control deficiencies on a more timely basis.

Agencies should rectify high risk internal control deficiencies as a priority.

Some deficiencies were common across agencies

The most common internal control deficiencies were poor or absent IT controls related to:

- user access management
- password management
- privileged access management
- user acceptance testing.

The most common governance deficiencies related to:

- management of cyber security risks
- capital project governance
- management of shared service arrangements
- conflicts-of-interest management
- gifts-and-benefits management
- risk management maturity
- ethical behaviour policies and statements.

Recommendation

Agencies should coordinate actions and resources to help rectify common IT control and governance deficiencies.



2. Information technology

Deficiencies in IT control processes are exposing agencies to security risks

While 95 per cent of agencies have policies about IT system user access, almost one-third had identified instances where they were not fully complying with these policies. Most agencies do not sufficiently monitor or restrict privileged access to their systems and some do not enforce password controls.

Recommendations

Agencies should strengthen user access administration to prevent inappropriate access to sensitive systems. Agencies should:

- establish and enforce clear policies and procedures
- review user access regularly
- remove user access for terminated staff promptly
- change user access for transferred staff promptly.

Agencies should tighten privileged user access to protect their information systems and reduce the risks of data misuse and fraud. Agencies should ensure they:

- only grant privileged access in line with the responsibilities of a position
- review the level of access regularly
- limit privileged access to necessary functions and data
- monitor privileged user account activity on a regular basis.

Agencies should review and enforce password controls to strengthen security over sensitive systems. As a minimum, password parameters should include:

- minimum password lengths and complexity requirements
- limits on the number of failed log-in attempts
- password history (such as the number of passwords remembered)
- maximum and minimum password ages.

Agencies need a clearer cyber security framework, improved processes and more expertise

The extent of the cyber security threat is unknown because agencies define a 'cyber attack' differently. And while most agencies have dedicated resources to address cyber security, they can strengthen their strategies, expertise and staff awareness. The Audit Office of NSW is currently undertaking a performance audit on cyber security. The report is planned to be released by the second quarter of 2018.

Recommendations

The Department of Finance, Services and Innovation should revisit its existing framework to develop a shared cyber security terminology and strengthen the current reporting requirements for cyber incidents.

The Department of Finance, Services and Innovation should:

- mandate minimum standards and require agencies to regularly assess and report on how well they mitigate cyber security risks against these standards
- develop a framework that provides for cyber security training.

Agencies should ensure they adequately resource staff dedicated to cyber security.

Agencies should ensure robust disaster recovery plans cover critical business systems

Agencies can do more to adequately assess critical business systems to enforce effective disaster recovery plans. This includes reviewing and testing their plans on a timely basis. A smaller percentage of agencies need to improve change control processes to avoid unauthorised or inaccurate system changes.

Recommendations

Agencies should complete business impact analyses to strengthen disaster recovery plans, then regularly test and update their plans.

Agencies should consistently perform user acceptance testing before system upgrades and changes. They should also properly approve and document changes to IT systems.



3. Asset management

Agencies are investing significantly in capital assets, but are underspending their budgets

The NSW Government has capital works commitments of \$80.1 billion over the next four years.

Sixty-four percent of agencies have capital investment ratios above 1.0, which means they are in a phase of high investment in new capital. But their underspends against capital budgets have increased over the last three years. The 39 agencies we reviewed had major capital projects that were underspent by 13 per cent (or \$540 million) against budget. The causes of agency budget underspends warrant investigation to ensure the NSW Government's infrastructure commitment is delivered on time.

Recommendation

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.

Agencies can improve their project governance on major capital projects

Agencies can improve the way they prepare business cases and use project steering committees (or equivalent) to oversee major capital projects. Agencies that have project management processes that include robust business cases and regular updates to their steering committees are better able to provide those projects with strategic direction and oversight.

Agencies have improved asset disposals but can strengthen some processes

Recommendations

Agencies should have formal processes for disposing of surplus properties.

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.



4. Governance

Governance refers to the frameworks, processes and behaviours that help an agency to operate effectively and comply with relevant laws and standards.

Agencies' continuous disclosure policies promote improved performance and public trust

Sixty-four per cent of agencies promote transparency and accountability by publishing on their websites a continuous disclosure policy that provides for, and encourages:

- regular public disclosure of key performance information
- disclosure of both positive and negative information
- prompt reporting of significant issues.

Agencies can better manage shared services to ensure quality and efficiency

Most agencies use shared service arrangements to centralise corporate services functions. While 86 per cent have service level agreements in place to manage these arrangements, many of these agreements can be improved by specifying controls, performance or reporting requirements.

Agencies are better able to manage the quality and timeliness of shared service arrangements where they have a service level agreement in place. Ideally, the terms of service should be agreed before services are transferred to the shared service provider and:

- specify the controls the provider must maintain
- specify key performance targets
- include penalties for non-compliance.

Agencies achieve better results managing shared service providers where they regularly monitor their performance using key measures for the benefits realised, costs saved and quality of services received.

Before agencies extend or renegotiate a contract with a service provider, they should comprehensively assess the services received and test the market to maximise value for money.



5. Ethics and conduct

Good governance is supported by high standards of ethical conduct by public sector employees.

Most agencies maintain an ethical framework, but can improve their processes

All agencies we reviewed have a code of conduct as part of their ethical framework. Improvement is possible by agencies strengthening processes for updating and managing their codes to reduce the risk of fraud and unethical behaviour. Similarly, related processes, such as dealing with external clients, customers, suppliers and contractors can be enhanced by publishing a Statement of Business Ethics, which communicates agency values and culture and what third parties can expect of agencies.

Recommendation

Agencies should regularly review their code-of-conduct policies and ensure they keep their codes of conduct up-to-date.

Most agencies have weaknesses in how they manage conflicts of interest

All agencies have a conflicts-of-interest policy, but most can strengthen the associated processes. Similarly, while agencies have formal gifts-and-benefits policies, we found gaps in how this is managed by some that can increase the risk of unethical conduct.

Recommendations

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.

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



6. Risk management

Our final chapter reviews how well agencies are developing systems to manage the risks they face. We started by looking at the maturity of their overall risk management. The Audit Office of NSW is currently undertaking a performance audit on risk management culture and capability. The report is planned to be released in the first quarter of 2018.

All agencies have risk management frameworks with varying levels of maturity

Agencies have introduced risk management frameworks and practices as required by the Treasury's:

- 'Risk Management Toolkit for the NSW Public Sector'
- 'Internal Audit and Risk Management Policy for the NSW Public Sector'.

However, more can be done to progress risk management maturity and embed risk management in agency culture. When reviewed against five critical assessment criteria, agencies fared best in strategy and governance, but most need to improve their risk culture, systems and intelligence.

Agencies can strengthen their risk culture and reporting within agencies and clusters

Most agencies have started to embed risk management into the culture of their organisations, and some have successfully done so. Some agencies do not report their significant risks to their lead agency, which increases the likelihood that significant risks are not being mitigated appropriately and consistently across the cluster.

Agencies can improve their risk culture by:

- setting an appropriate tone from the top
- training all staff in effective risk management
- ensuring desired risk behaviours and culture are supported, monitored, and reinforced through business plans, or the equivalent and employees' performance assessments.



1. Overall 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.

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 then illustrates this year's controls and governance findings in more detail.

Issues	Recommendations
1.1 New and repeat findings	
<p>The number of internal control deficiencies reduced over the past three years, but new higher-risk information technology (IT) control deficiencies were reported in 2016–17.</p> <p>Deficiencies repeated from previous years still make up a sizeable proportion of all internal control deficiencies.</p>	<p>Recommendation</p> <p>Agencies should focus on emerging IT risks, but also manage new IT risks, reduce existing IT control deficiencies, and address repeat internal control deficiencies on a more timely basis.</p>
1.2 High risk findings	
<p>We found seven high risk internal control deficiencies, which might significantly affect agencies.</p>	<p>Recommendation</p> <p>Agencies should rectify high risk internal control deficiencies as a priority.</p>
1.3 Common findings	
<p>The most common internal control deficiencies related to poor or absent IT controls.</p> <p>We found some common governance deficiencies across multiple agencies.</p>	<p>Recommendation</p> <p>Agencies should coordinate actions and resources to help rectify common IT control and governance deficiencies.</p>

1.1 New and repeat findings

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

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

Number of findings

Recommendation

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.

Our 2016–17 audits identified 219 internal control deficiencies, comprising:

- 124 financial control deficiencies
- 95 IT control deficiencies.

We reported these deficiencies to agency management and others 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.

Financial control deficiencies have decreased by a third in the last three years

The number of identified financial control deficiencies we found in agencies fell by 33 per cent over the last three years: from 185 in 2014–15 to 124 in 2016–17. The number of new financial control deficiencies also decreased, down by 43 per cent (147 to 84) over the same period.

However, we found that 60 per cent of reported financial control deficiencies were rated as moderate or high risk, up from 51 per cent in 2014–15.

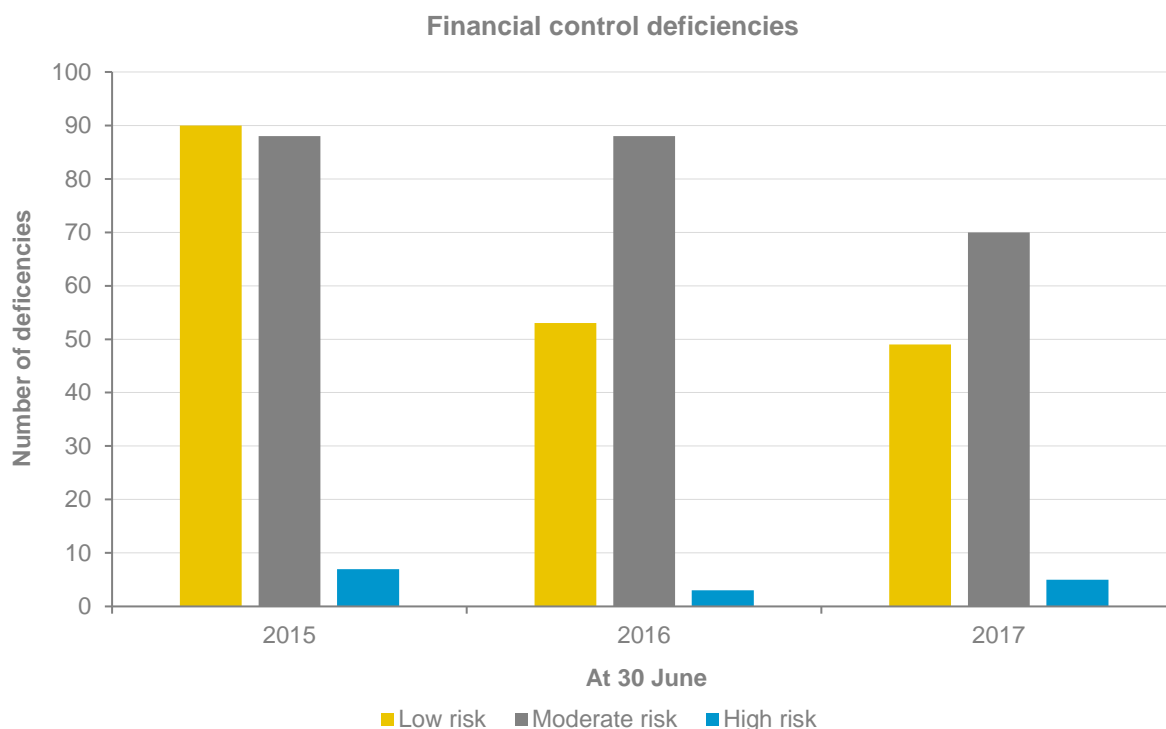
Deficiencies in internal controls increase the risk of intentional and accidental errors in processing information, producing management reports and generating financial statements. This can impair decision-making, affect service delivery and expose agencies to fraud, leading to financial loss and reputational damage.

Poor controls may also mean agency staff do not follow internal policies, inadvertently causing the agency not to comply with legislation, regulation and State policies.

This report provides examples of how weak controls affect agency performance, financial reporting, asset management, IT security and governance.

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 experience losses or suffer some impact on service delivery. Our risk assessment matrix aligns with the risk management framework in the Treasury's [Risk Management Toolkit for the NSW Public Sector](#).

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

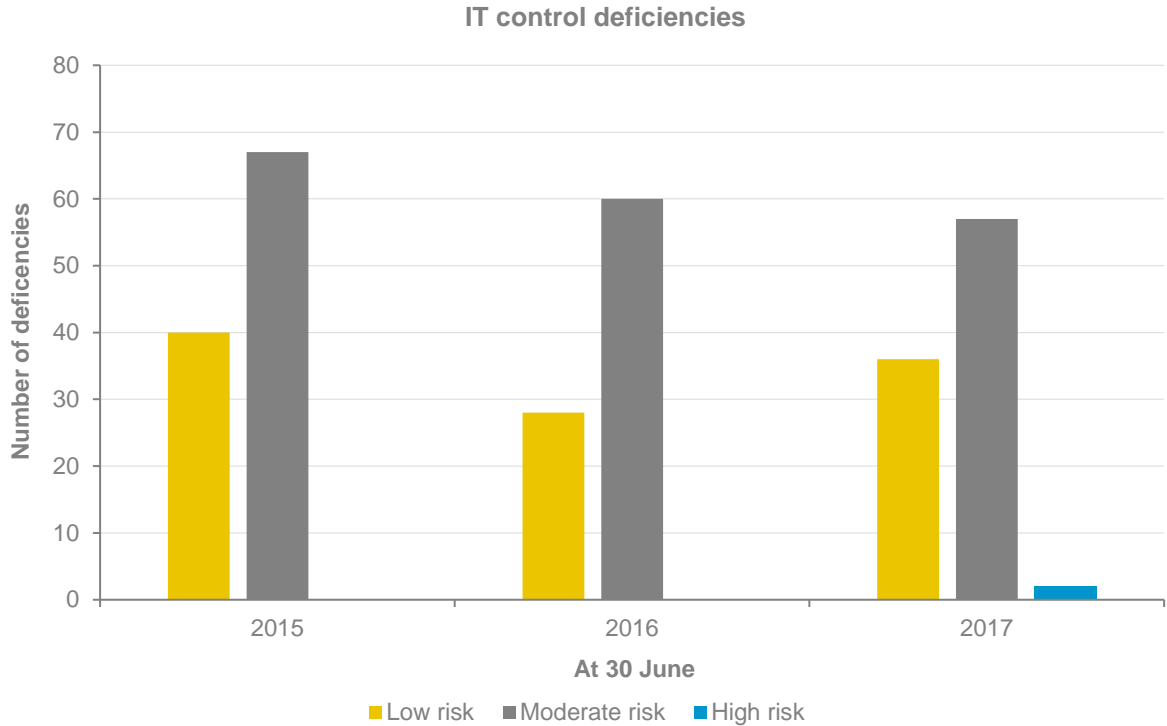


Source: Audit Office management letters.

IT control deficiencies have decreased, but new high risk deficiencies are emerging

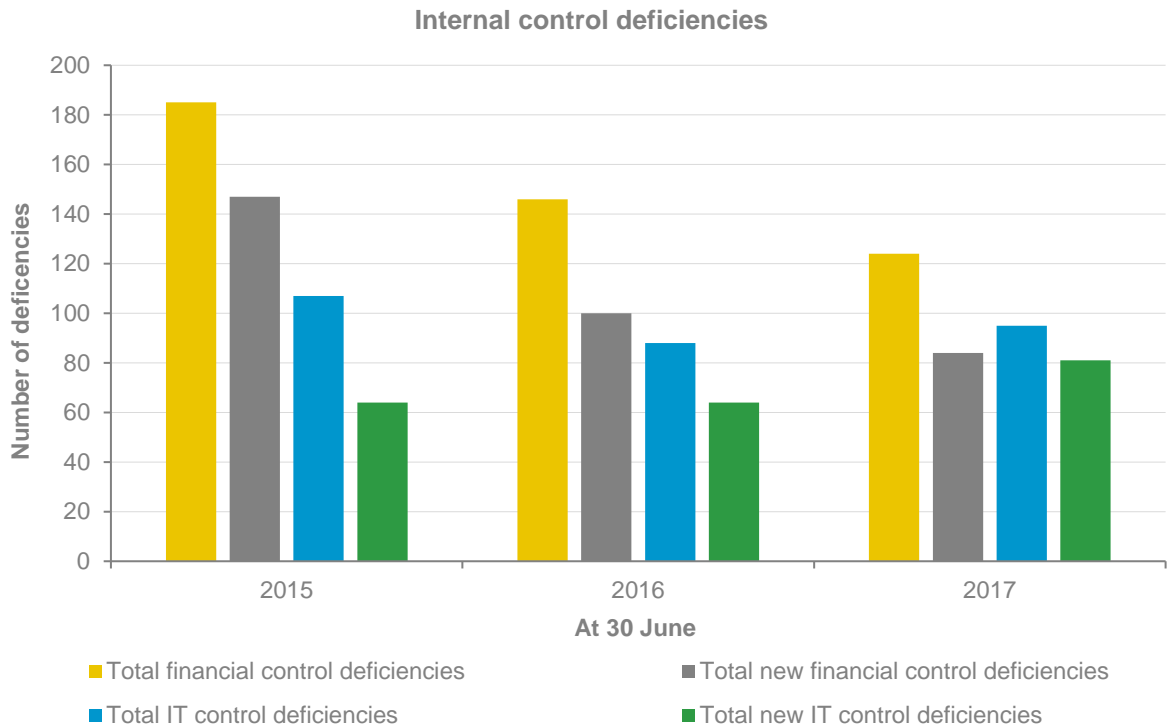
Good IT controls underpin the effectiveness of processes, policies and procedures for managing information systems, securing sensitive information and ensuring the integrity of agency data. Poor IT controls increase risks to agencies, including unauthorised access, cyber security attacks, data manipulation and information theft.

The number of reported IT control deficiencies fell by 11 per cent over the last three years, from 107 in 2014–15 to 95 in 2016–17. But we still found IT control deficiencies at 69 per cent of agencies (62 per cent in 2014–15 and 56 per cent in 2015–16). The number of new IT control deficiencies rose by 27 per cent in the same period (up from 64 to 81) including two new high risk deficiencies this year.



Source: Audit Office management letters.

Taken together, these results suggest that agencies have improved their internal controls, but they should prioritise emerging IT risks and control deficiencies in the year ahead.



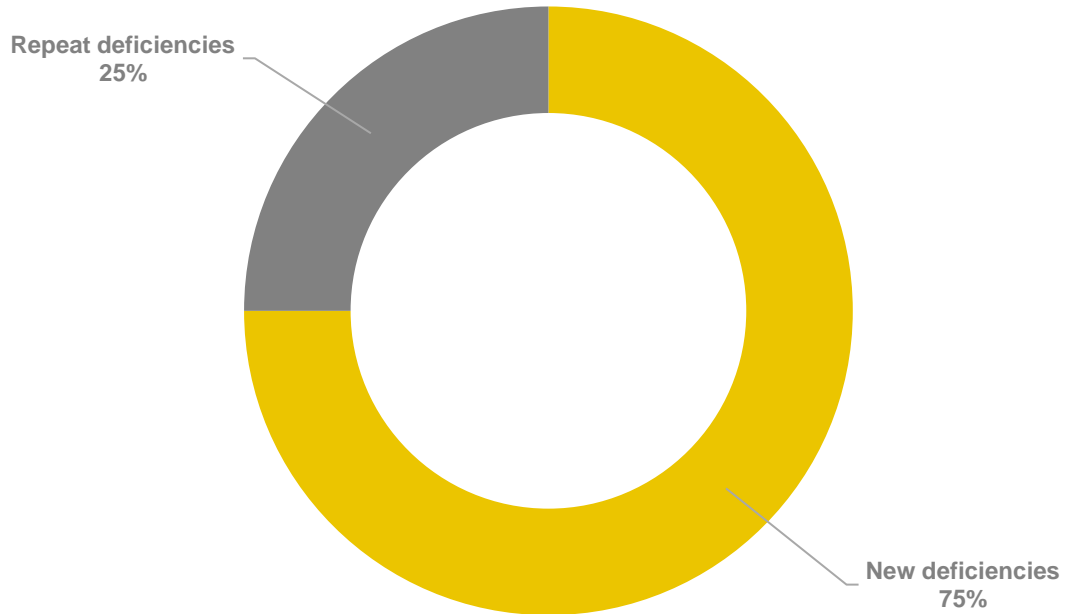
Source: Audit Office management letters.

Repeat deficiencies fell by 33 per cent, but still make up one-quarter of all deficiencies

The number of recurring control deficiencies fell as agencies responded to our audit findings. While some control deficiencies take longer to resolve than others, all agencies should address control deficiencies we bring to their attention as soon as possible.

The number of repeat internal control deficiencies we reported for the last three years fell by 33 per cent: from 81 in 2014–15 to 54 in 2016–17. Repeat deficiencies made up 25 per cent of total deficiencies in 2016–17.

New versus repeat internal control deficiencies



Source: Audit Office management letters.

We found one repeat high risk financial control deficiency in 2016–17, which is discussed in more detail in the next section of this report.

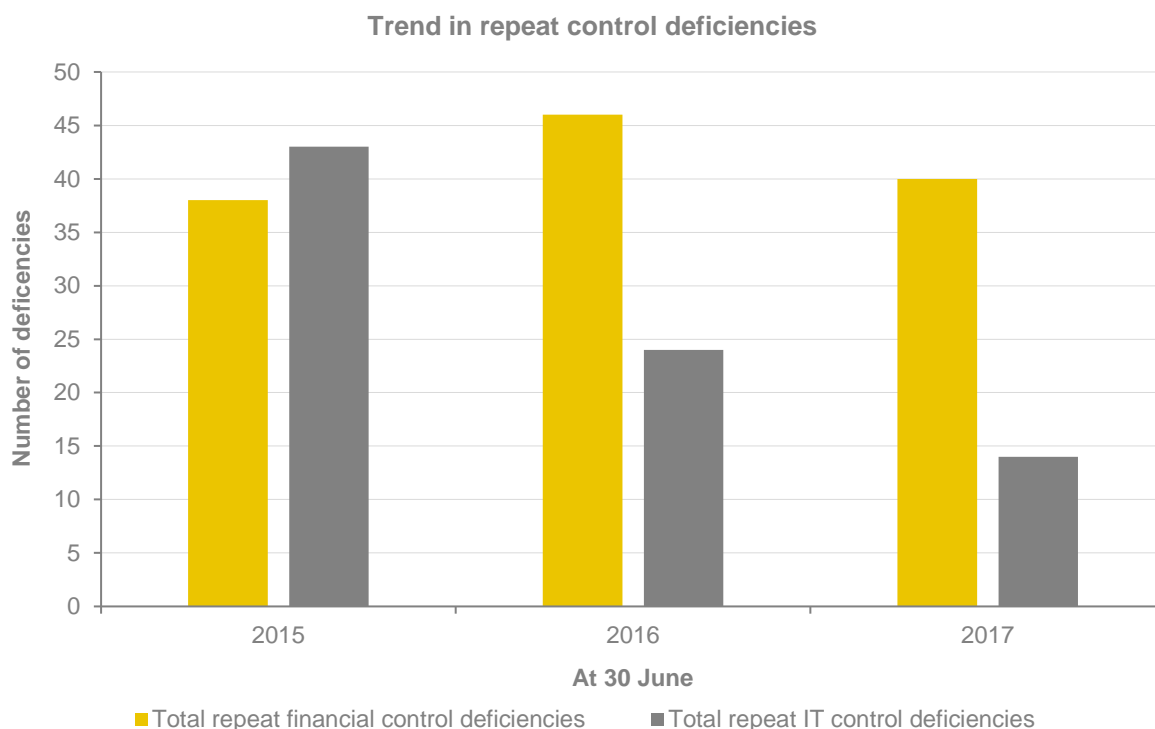
In the last three years, the number of repeat IT control deficiencies fell by 67 per cent, down from 43 deficiencies to 14. There are now 11 agencies (13 in 2014–15) with repeat IT control deficiencies.

However, we found that 71 per cent of repeat IT control deficiencies were rated as moderate risk (no high risk repeat IT control deficiencies were reported in 2016–17), up from 63 per cent in 2014–15.

The number of repeat financial control deficiencies remained steady over the last three years, averaging 41 each year. And almost half (46 per cent) of agencies had repeat deficiencies in 2016–17. While this was an improvement on the 51 per cent of agencies with repeat deficiencies in 2015–16, it was higher than the 33 per cent of agencies with repeat deficiencies in 2014–15.

We found that 63 per cent of repeat financial control deficiencies were rated as moderate or high risk, up from 53 per cent in 2014–15.

The graph below shows that, while agencies are facing more emerging IT control deficiencies, they are more proactive in resolving them than their existing financial control deficiencies.



Source: Audit Office management letters.

1.2 High risk findings

The next measure we use to assess internal controls is the number of high risk findings.

Recommendation

Agencies should rectify high risk internal control deficiencies as a priority.

We found seven high risk internal control deficiencies, with one repeat high risk deficiency

High risk internal control deficiencies can have significant impacts. For example, control deficiencies that arose as part of implementing a new financial reporting system in one agency led to:

- untimely and inaccurate payment of suppliers
- salaries being paid to terminated staff
- inaccurate legacy system data, which hampered reconciliations.

The number of high risk internal control deficiencies remains consistent: seven in 2014–15 and in 2016–17. Five of the seven high risk deficiencies related to financial controls and two to IT controls. These were:

- deficiencies migrating data when implementing a system, involving poor risk management, incomplete data testing, untimely approvals, and missing documentation
- several instances of agency staff not declaring their conflicts of interest as directors of private companies that dealt with the agency
- deficiencies implementing a new financial reporting system, including inadequate governance, lack of project staff with the required skills, and poor recording and treatment of risks in a register

- purchase orders created and approved only after purchasing the goods and services
- ineffective revenue quality reviews
- key personnel risk coupled with a lack of detailed operating procedures for revenue
- outdated legislative compliance registers.

The issue relating to purchase orders was the only high risk repeat deficiency. In 2014–15, five high risk control deficiencies were repeated from the previous year. However, we continue to detect moderate-risk deficiencies in both financial and IT controls in most agencies.

The table below shows the percentage of agencies with high, moderate and repeat deficiencies over the past three years. Moderate rated deficiencies are discussed in the next section on common findings.

Type of control deficiencies found	2014–15	2015–16	2016–17
	(%)	(%)	(%)
High risk financial	8	8	8
Moderate risk financial	79	59	67
Repeat high or moderate risk financial*	23	33	31
High risk IT	0	0	5
Moderate risk IT	56	41	56
Repeat high or moderate risk IT*	28	13	23

* Repeat findings are included in the numbers above.

The table above does not include low risk deficiencies.

Source: Audit Office management letters.

1.3 Common findings

While it is important to monitor the number and make-up of deficiencies across the sector, it is also useful to assess whether some deficiencies commonly occur across agencies. Where deficiencies relate to multiple agencies, the lead agency in the cluster can play a role in ensuring responses are consistent, timely, efficient and effective.

Recommendation

Agencies should coordinate actions and resources to help rectify common IT control and governance deficiencies.

Common internal control findings

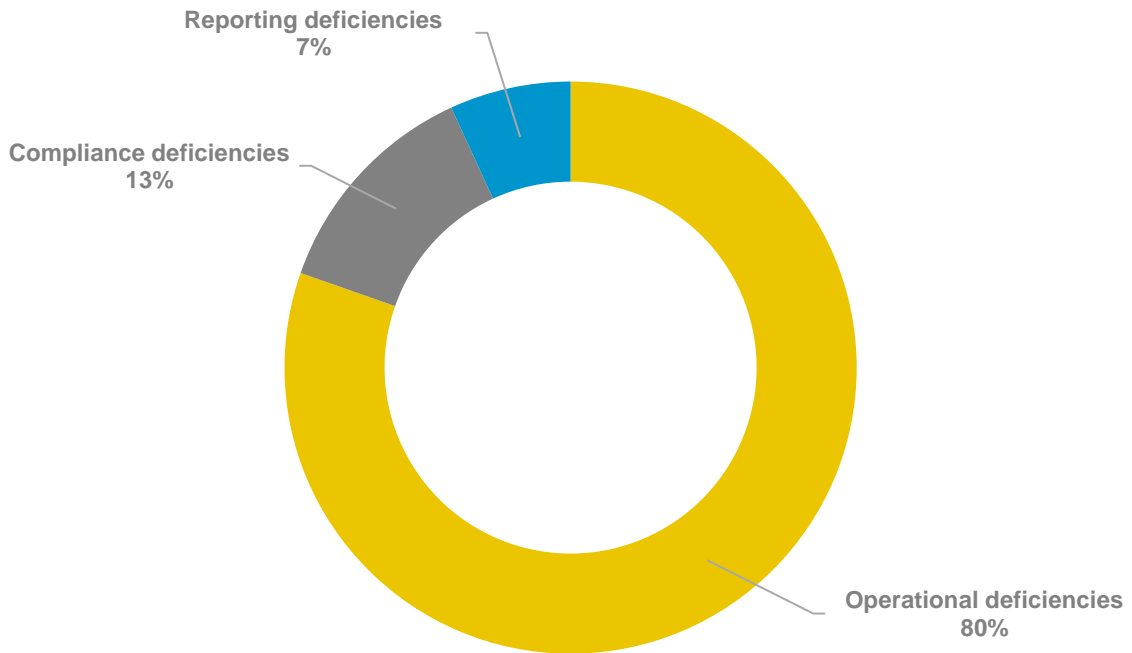
Operational internal controls continue to be a challenge, especially in IT

We classified the 219 internal control deficiencies we identified in 2016–17 into three groups:

- operational deficiencies
- compliance deficiencies
- reporting deficiencies.




The graph below shows that most deficiencies (80 per cent) were operational, with the rest split between compliance (13 per cent) and reporting (seven per cent) deficiencies.






Internal control deficiencies in 2016–17






Source: Audit Office management letters.

The table below describes the most common deficiencies across agencies, including their risk rating and the number of repeated deficiencies.

Risk rating and number of deficiencies	Deficiency summary
Operational	
<p> High: 4 new, 1 repeat</p> <p> Moderate: 76 new, 25 repeat</p> <p> Low: 54 new, 16 repeat</p>	<p>Operational deficiencies accounted for 80 per cent of all control deficiencies. Of these, IT controls deficiencies accounted for 53 per cent. IT control deficiencies included:</p> <ul style="list-style-type: none"> • weak or non-existent policies and processes for administering user access • failure to remove user access after terminating staff • lack of formal, periodic user-access reviews • password parameters not meeting agency policies and/or too simple • excessive levels of access to agency systems • inadequate monitoring of privileged access users' activities • poor or non-existent documentation of user acceptance testing. <p>Other common operational deficiencies included:</p> <ul style="list-style-type: none"> • expired or non-existent service level agreements • inadequate monitoring of capital works in progress, causing errors in the timing of asset capitalisation, incorrect categorisation of assets, and misstatement of depreciation and/or amortisation expenses.

Risk rating and number of deficiencies	Deficiency summary
Reporting	
 Moderate: 7 new, 3 repeat  Low: 3 new, 2 repeat	Common reporting deficiencies included: <ul style="list-style-type: none"> poor financial reconciliation processes inadequate segregation of duties for preparing and approving financial journals.
Compliance	
 High: 2 new  Moderate: 10 new, 6 repeat  Low: 9 new, 1 repeat	Common compliance deficiencies included: <ul style="list-style-type: none"> inadequately maintained contracts registers, with incomplete and/or not promptly updated information missing conflicts-of-interest declarations weak, non-existent or outdated policies and procedures.

These high , moderate  and low  risk icons indicate the level of risk based on the likelihood of the risk occurring and the consequences if it does.

IT control deficiencies made up 53 per cent of all operational deficiencies and 26 per cent of repeat internal control deficiencies across agencies. Repeat IT control deficiencies included:

- weak or absent policies and processes for administering user access
- failure to remove user access after terminating staff
- lack of formal, periodic user access reviews
- password parameters not meeting agency policies and/or too simple
- excessive levels of access to agency systems
- poor reconciliation processes.

IT control deficiencies can be costly to address and solutions can take a long time to fully implement. Our audits highlighted the need for agencies to prioritise improvements in their IT control systems and design proper controls when scoping new systems. We discuss this further in Chapter 2 of this report.

Common governance findings

Strong governance helps agencies to:

- meet stated objectives
- comply with legislative and other requirements
- protect their reputations.

Several governance-related deficiencies are common across agencies

Our 2016–17 financial audits identified several common governance deficiencies across agencies. In each case, there are already clear requirements and standards for agencies to follow, often within sector-wide policies published by lead cluster agencies and central agencies. We outline these in more detail in chapters 2 to 6 of this report.

Lead and central cluster agencies responsible for governance policy should consider how they can best reinforce the expected standards and help agencies to comply.

Common governance deficiencies included:

Area	Deficiencies
Information technology	<ul style="list-style-type: none"> • Poor management of cyber security, including deficiencies in IT controls to mitigate the risk of cyber attacks and a lack of cyber security awareness.
Asset management	<ul style="list-style-type: none"> • Lack of, and deficiencies in, agency business impact analyses and disaster recovery plans. • Lack of steering committees to provide strategic direction and oversight of major capital projects. • Deficiencies in information provided to steering committees of major capital projects. • Lack of, and deficiencies in, business cases to support major capital projects.
Governance	<ul style="list-style-type: none"> • Missing, ineffective, expired or unenforced service level agreements with shared service providers.
Ethics and conduct	<ul style="list-style-type: none"> • Outdated code-of-conduct policies that do not require staff training in the policy, and/or missing annual compliance declarations. • Weaknesses in conflicts-of-interest management, including no requirement for annual declarations. • Missing statements of business ethics. • Weaknesses in gifts-and-benefits management, including not updating registers promptly, and/or not reporting trends to their Executive.
Risk management	<ul style="list-style-type: none"> • Agencies assessed as being in the early stages of developing their risk management frameworks. • Lack of reporting of major risks at a cluster level.



2. Information technology

Information technology (IT) has become increasingly important for government agencies' financial reporting and to deliver their services efficiently and effectively. Our audits reviewed whether agencies have effective controls in place over their IT systems. We found that IT security remains the source of many control weakness in agencies.

Issues

Recommendations

2.1 IT security

User access administration

While 95 per cent of agencies have policies about user access, about two-thirds were compliant with these policies. Agencies can improve how they grant, change and end user access to their systems.

Recommendation

Agencies should strengthen user access administration to prevent inappropriate access to sensitive systems. Agencies should:

- establish and enforce clear policies and procedures
- review user access regularly
- remove user access for terminated staff promptly
- change user access for transferred staff promptly.

Privileged access

Sixty-eight per cent of agencies do not adequately manage who can access their information systems, and many do not sufficiently monitor or restrict privileged access.

Recommendation

Agencies should tighten privileged user access to protect their information systems and reduce the risks of data misuse and fraud. Agencies should ensure they:

- only grant privileged access in line with the responsibilities of a position
- review the level of access regularly
- limit privileged access to necessary functions and data
- monitor privileged user account activity on a regular basis.

Password controls

Forty-one per cent of agencies did not meet either their own standards or minimum standards for password controls.

Recommendation

Agencies should review and enforce password controls to strengthen security over sensitive systems. As a minimum, password parameters should include:

- minimum password lengths and complexity requirements
- limits on the number of failed log-in attempts
- password history (such as the number of passwords remembered)
- maximum and minimum password ages.

2.2 Cyber security

Cyber security framework

Agencies do not have a common view on what constitutes a cyber attack, which limits understanding the extent of the cyber security threat.

Recommendation

The Department of Finance, Services and Innovation should revisit its existing framework to develop a shared cyber security terminology and strengthen the current reporting requirements for cyber incidents.

Issues

Cyber security strategies

While 82 per cent of agencies have dedicated resources to address cyber security, they can strengthen their strategies, expertise and staff awareness.

Recommendations

Recommendations

The Department of Finance, Services and Innovation should:

- mandate minimum standards and require agencies to regularly assess and report on how well they mitigate cyber security risks against these standards
- develop a framework that provides for cyber security training.

Agencies should ensure they adequately resource staff dedicated to cyber security.

2.3 Other IT systems

Change control processes

Some agencies need to improve change control processes to avoid unauthorised or inaccurate system changes.

Recommendation

Agencies should consistently perform user acceptance testing before system upgrades and changes. They should also properly approve and document changes to IT systems.

Disaster recovery planning

Agencies can do more to adequately assess critical business systems to enforce effective disaster recovery plans. This includes reviewing and testing their plans on a timely basis.

Recommendation

Agencies should complete business impact analyses to strengthen disaster recovery plans, then regularly test and update their plans.

2.1 IT 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.

Our audits reviewed the key controls agencies should have in place to minimise these risks. We found agencies can improve how they administer access to their systems and manage passwords.

User access administration

Recommendation

Agencies should strengthen user access administration to prevent inappropriate access to sensitive systems. Agencies should:

- **establish and enforce clear policies and procedures**
- **review user access regularly**
- **remove user access for terminated staff promptly**
- **change user access for transferred staff promptly.**

Almost one-third of agencies breach their own security policies on user access

In 2016–17, our information systems audits identified 54 control deficiencies related to user access administration, with eight (15 per cent) being repeat deficiencies.

The deficiencies we found mainly relate to weak or missing controls in reviewing the access that staff have to their financial systems, and removing access once staff have left an organisation.

Ninety-five per cent of agencies have formal policies for administering user access. Eighty-two per cent of agencies comply with their policies when granting, changing or removing user access to their systems.



Poor management of user access:

- exposes agencies to the risk of fraud
- compromises data integrity and confidentiality
- increases the risk of unauthorised or invalid transactions
- increases the risk of those user profiles being used for cyber attacks.

Good control over user access should include:

- setting clear policies and procedures
- reviewing user access regularly
- removing user access for terminated staff promptly
- changing user access for transferred staff promptly.

If agencies do not implement these controls, they may also breach NSW laws and policies and the international standards that they reference. For example, section 11 of the *Public Finance and Audit Act 1983* requires agencies to have effective systems of internal control. The ['NSW Government Digital Information Security Policy'](#) mandates that agencies complete a self-attestation of compliance with the core requirements of the policy. This policy requires that agency information security management systems take account of the controls in ISO 27001 'Information technology - Security techniques - Information security management systems - Requirements'. This standard requires the regular review of users' access rights, and the removal or adjustment of access rights upon termination of employment or transferral.

Insufficient user access controls pose a greater risk to agencies where they relate to privileged access, which we discuss next.

Privileged access

Recommendation

Agencies should tighten privileged user access to protect their information systems and reduce the risks of data misuse and fraud. Agencies should ensure they:

- **only grant privileged access in line with the responsibilities of a position**
- **review the level of access regularly**
- **limit privileged access to necessary functions and data**
- **monitor privileged user account activity on a regular basis.**

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 with privileged user access who tend to be 'trusted insiders' such as employees, business partners, or third-party contractors. Privileged users access normally restricted systems and information. In some cases, privileged users can access critical agency operational systems.

Most agencies are not effectively managing privileged access

We found that 68 per cent of agencies do not adequately manage privileged access to their systems. This increases the risk that privileged accounts can be misused to:

- commit fraud
- access confidential information above what is needed for their role
- access files, install and run programs, and change configuration settings
- maliciously or accidentally delete or distribute information.

Personal information collected by public sector agencies about members of the public is of high value to cyber criminals, as it can be used to create false identities to commit other crimes. Despite these risks, we found that one agency had 37 privileged user accounts, including 33 that were dormant. The agency had no formal process to create, modify or deactivate privileged users.

We also found that 61 per cent of agencies do not regularly monitor the account activity of privileged users. This places those agencies at greater risk of not detecting compromised systems, data breaches and misuse. And 31 per cent of agencies do not limit or restrict privileged access to appropriate personnel. Of the 31 per cent, only one-third monitor the account activity of privileged users.

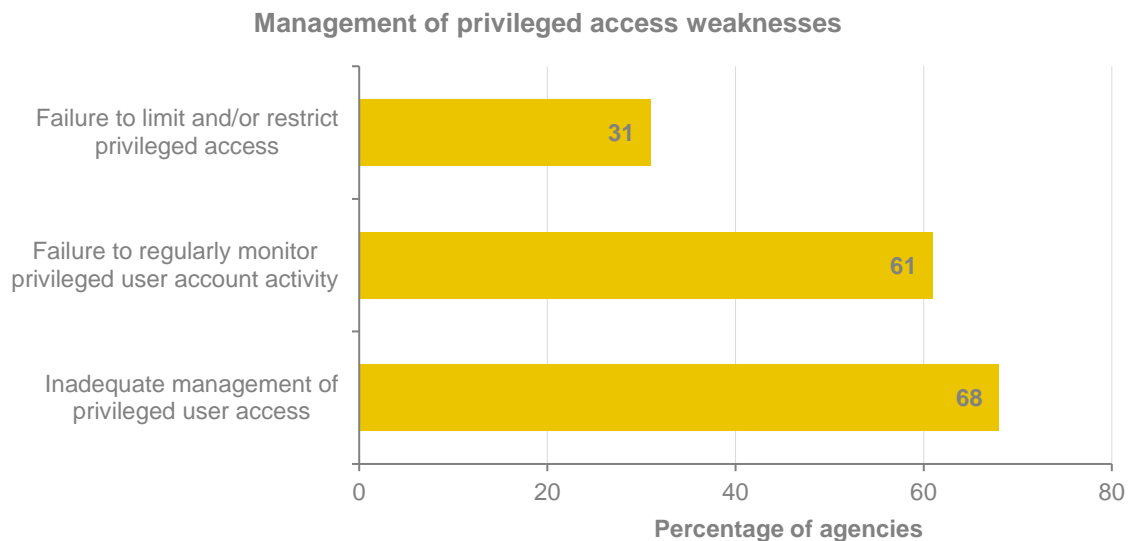
To address these findings, all agencies should ensure they:

- only grant privileged access in line with the responsibilities of a position
- regularly review the level of privileged access
- limit privileged access to necessary functions and data.

Agencies should also monitor their logs of privileged user account activity so they can promptly identify the types of activity associated with inappropriate use. Privileged user activities associated with inappropriate use should be reported to someone independent of the IT function.

As with user-access administration discussed above, poor management of privileged access may breach Section 11 of the *Public Finance and Audit Act 1983* and the 'NSW Government Digital Information Security Policy'. This policy requires that agency information security management systems take account of ISO 27001. This standard requires that privileged access rights are controlled and restricted.

The graph below highlights the significant percentage of agencies that are not adequately managing privileged access to their systems and data.



Source: Provided by agencies (audited).

Password controls

Recommendation

Agencies should review and enforce password controls to strengthen security over sensitive systems. As a minimum, password parameters should include:

- minimum password lengths and complexity requirements
- limits on the number of failed log-in attempts
- password history (such as the number of passwords remembered)
- maximum and minimum password ages.

Poor password controls put the security of agency systems at risk

Weak passwords increase the risk of unauthorised use of, and changes to, financial information. This compromises the confidentiality, integrity and availability of data. We found many password control deficiencies at agencies this year. Forty-one per cent of agencies either did not comply with their own policy on password parameters or did not enforce the minimum expected standard.

For example, some agencies' systems allow staff to use passwords that were not long enough, complex enough, or were recycled from those recently used. In other cases, they did not limit the number of failed attempts to log into a system, or did not force staff to change their password frequently enough.

Around 10 per cent of the management letters we sent to agencies for 2016–17 raised repeat issues in password controls. This means those agencies have failed to resolve password control issues that we raised in a previous audit.

The table below summarises the deficiencies we found in password controls.

Password parameter not enforced or that did not comply with agency policy	Percentage of agencies (%)
Minimum password length	8
Password complexity requirements	15
Limit on the number of failed login attempts	18
Password history (i.e. the number of passwords remembered)	8
Maximum password age	22
Minimum password age	34

2.2 Cyber security

Poor management of cyber security threats can expose agencies to a broad range of risks, including financial loss, reputational damage and data breaches. Losses can arise from:

- theft of corporate and financial information and intellectual property
- theft of money
- denial of service
- destruction of data
- costs of repairing affected systems, networks and devices
- legal fees and/or legal action from losses arising from denial-of-service attacks causing system downtime in critical systems
- third-party losses when personal information stored on government systems is used for criminal purposes.



We sought to assess the extent of the cyber security threat to the NSW public sector, and how ready agencies are to meet it.

Cyber security framework

Recommendation

The Department of Finance, Services and Innovation should revisit its existing framework to develop a shared cyber security terminology and strengthen the current reporting requirements for cyber incidents.

Effective management of cyber security starts by understanding the extent of the problem that agencies face. We collected data about which agencies experienced cyber attacks and how many attacks they recorded in the last year.

Without a clear and robust framework, the extent of cyber security attacks is unknown

Sixty-four per cent of agencies reported that they intercepted cyber attacks during 2016–17. These agencies reported 8,503 cyber attacks. This is an increase in intercepted cyber attacks with 1,558 attacks reported for 2015–16 and 603 attacks in 2014–15. As there are different approaches to what agencies record and report, and agencies apply different definitions for a 'cyber attack', the number and nature of cyber attacks is unknown.

Data reported by agencies showed that thirty-three per cent said they had no cyber attacks at all (21 per cent in 2015–16 and 38 per cent in 2014–15). On the other hand, two agencies reported 7,040 cyber attacks during 2016–17.

Three per cent of agencies were unable to quantify the number of cyber attacks that occurred during 2016–17 (28 per cent in 2015–16 and 26 per cent in 2014–15). Further, 85 per cent of agencies recognise the risk of cyber attacks as either 'High' or 'Medium', believing that this level of risk was 'inherent'. But five per cent of agencies do not consider that cyber attacks pose a risk at all.

An agreed definition of what a cyber attack is, would assist agencies and the Department of Finance, Services and Innovation to:

- determine the type of cyber security incident response capability required
- resource support functions
- better share experiences and learnings from other agencies.

More consistent and accurate recording and reporting of cyber attacks, would assist agencies and the Department of Finance, Services and Innovation to:

- accurately assess the risk they are exposed to
- understand the overall threat and develop appropriate mitigation strategies
- properly implement and resource risk mitigation.

The Australian Signals Directorate (ASD), a Commonwealth authority responsible for cyber and information security has developed the ['Australian Government Information Security Manual'](#), which provides guidance on cyber security and governance.

The Department of Finance, Services and Innovation advises work is currently underway to revise the 'NSW Government Digital Information Security Policy', including strengthening definitions and terminology, as well as reporting requirements for cyber incidents.

Cyber security strategies

Once agencies have established the extent of cyber security issues they face, they will be better placed to develop strategies and responses that will mitigate those risks.

While all agencies reported that they regularly review their IT risk registers, 18 per cent have not documented or assessed their strategies to mitigate cyber security risks. Most agencies who have done so used a range of external frameworks and standards.

Recommendations

The Department of Finance, Services and Innovation should:

- **mandate minimum standards and require agencies to regularly assess and report on how well they mitigate cyber security risks against these standards**
- **develop a framework that provides for cyber security training.**

Agencies should ensure they adequately resource staff dedicated to cyber security.

The ASD has developed a [prioritised list of mitigation strategies](#). It refers to this as the 'Essential Eight' measures that organisations should implement to protect their networks from security threats. Out of these eight, it prioritised the 'Top 4' as:

- application 'whitelisting', allowing only approved software applications to run on computers
- patching applications to fix security vulnerabilities in software applications
- patching operating systems to fix security vulnerabilities in operating systems
- restricting administrative privileges.

The Top 4 are mandatory for Australian Federal Government agencies, but not for NSW Government agencies. The ASD advises that implementing these four alone mitigates the threat posed by more than 85 per cent of targeted cyber attacks. We discussed above our findings on the administration of privileged access in NSW, and that 67 per cent of agencies do not adequately manage privileged access to their systems. Controlling privileged access is one of the 'Top 4' that the ASD recommends helping reduce cyber vulnerability.

The National Institute of Standards and Technology has also developed the 'Cybersecurity Framework', which is a set of optional standards, best practices and recommendations for improving cyber security at an organisational level.

Agencies can strengthen their cyber security controls

We found every agency has installed anti-virus software on all computers and performs regular virus scans. Only one agency did not regularly update its anti-virus signatures.

We found that while all agencies have a patching process, five per cent did not have up-to-date security patches applied to desktop computers. Patching helps reduce vulnerability to cyber attack.

Agencies need to improve cyber security expertise and staff awareness

We also looked at whether agencies have enough expertise to meet cyber security threats, and how aware staff are of the role they need to play.

Eighty-two per cent of agencies reported they already employ dedicated staff and/or contractors to control cyber security threats and attacks, at a cost of around \$25.4 million in 2016–17. Yet the remaining 18 per cent had no cyber security resources, even though 86 per cent of them had rated the risk of a cyber attack as high.

Cyber security requires all staff to be aware of the threats that their agency faces and how they can protect it from attack. Security breaches often occur due to simple mistakes and a lack of awareness, or well-meaning people trying to be helpful.

One of the key reasons organisations are vulnerable to 'phishing' and 'spear-phishing' attacks is that they do not train employees on their role in maintaining system security. We found 23 per cent of agencies provide no training in cyber security awareness. Of those who do:

- some provide training only to specific staff, such as senior management and IT staff
- seven per cent of agencies do not regularly train staff, and some have not provided training for more than five years.

We also found 77 per cent of agencies identify the staff most at risk of a damaging cyber attack. The remaining 23 per cent do not, and as a result do not provide role-specific cyber security awareness and training. Staff most at risk of cyber attack are likely to be targeted by social attacks, mainly through phishing emails. And public sector organisations are amongst the sectors most targeted.

2.3 Other IT systems

We also looked at other key controls that protect IT systems and service delivery. We highlighted two areas that agencies should address.

Change control processes

Recommendation

Agencies should consistently perform user acceptance testing before system upgrades and changes. They should also properly approve and document changes to IT systems.

Agency change control processes have improved, but some overlook key steps

Quality change control processes mean having a group of subject matter experts test how software will function using real-life scenarios before they deploy it. We found that between six and 12 per cent of agencies were not using an effective change control process. For example, six per cent of agencies did not carry out user acceptance testing before changing programs. And double that number either did not approve those changes, or did so after they had implemented the change.

User acceptance testing lets users themselves provide feedback on the systems they will be expected to use. We reported in 2014 how change controls for the [Learning Management and Business Reform Program](#) roll out failed because too few users were trained in the proper use of the system, and when they left no-one knew how to use it.

In 2016–17, we found a lack of user acceptance testing in one agency contributed to issues it experienced when migrating its IT system to an external service provider. This may also have affected the way the system functioned and the reliability of its data.

In another case, an agency expects to spend over \$1.8 million to address issues related to a new financial system for a cluster.

We noted change control problems such as:

- inadequate understanding of business issues
- lack of skill assessment for project staff
- no project risk register
- a lack of management understanding of the actual business readiness
- inadequate stakeholder and change management.

We also found that 13 per cent of agencies had not maintained adequate documentation to support their user acceptance testing.

These examples show that, while the percentage of agencies that are not implementing effective change control is relatively low, the impact can be significant. Weak 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.

Disaster recovery planning

Recommendation

Agencies should complete business impact analyses to strengthen disaster recovery plans, then regularly test and update their plans.

Disaster recovery planning helps an agency to predict how its IT may be affected by a disaster, and put systems in place to minimise disruption to its services. This starts with a sound business impact analysis of agency IT systems.

Some agencies have not adequately assessed business impact

We found that some agencies have not analysed their critical business systems sufficiently, and as a result many had deficiencies in their recovery plans as well.

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.

We found that 11 per cent of agencies did not adequately identify their critical systems and business functions, and three agencies were still identifying what their critical systems are. Thirteen per cent do not maintain a complete inventory of IT systems, software and hardware.

We found that 38 per cent of agencies had not completed a business impact analysis for their most critical business function and system, and most of these (57 per cent) had not identified how critical their systems and business requirements are.

Where agencies did complete a business impact analysis, 46 per cent had deficiencies such as not:

- detailing recovery timeframes or priorities
- coordinating effectively between IT and business staff.

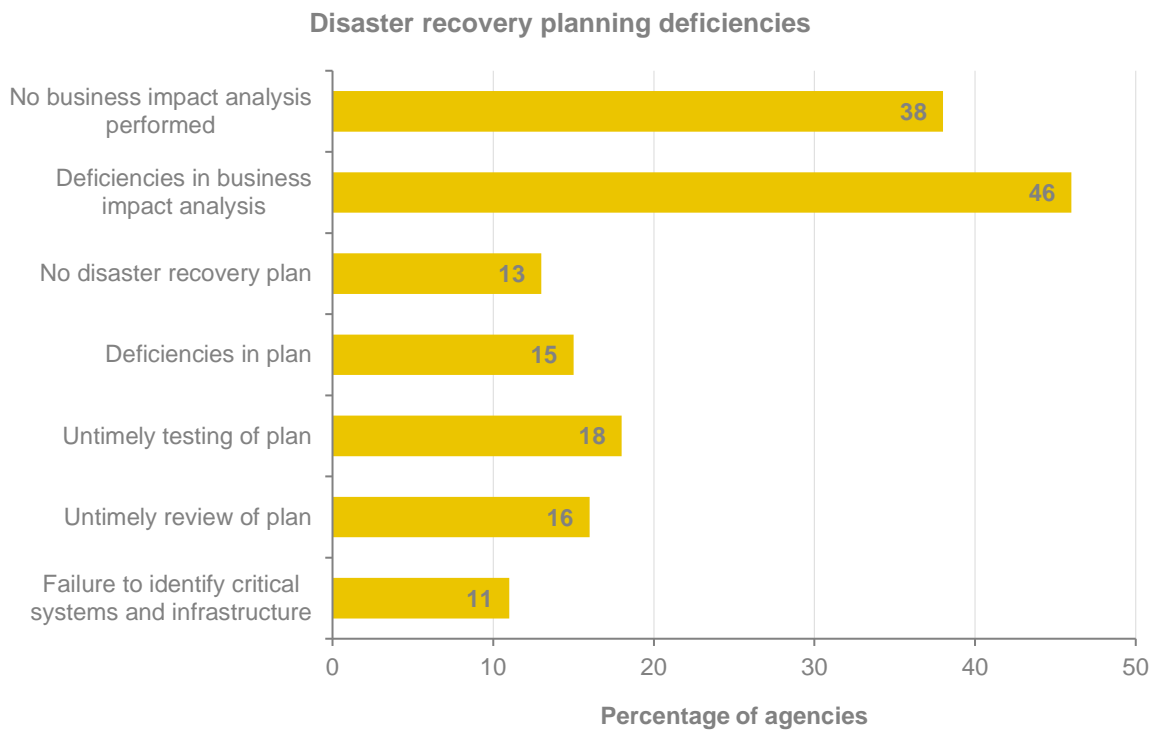
Once an impact analysis is done, it is important that agencies translate the results into effective recovery plans. The Department of Finance, Services and Innovation's ['NSW Government Digital Information Security Policy'](#) (DISP) requires agencies to develop, review and test their disaster recovery plans. This department also publishes [guidelines](#) to help agencies meet these requirements. DISP is not mandatory for State owned corporations, however it is recommended for adoption.

Thirteen per cent of agencies do not have a plan in place for all critical systems. Fifteen per cent of agency plans had deficiencies, such as not recording:

- the critical system owner
- all the IT software and hardware needed to restore the system
- how to restore the system
- lessons learned in tests.

In previous reports to Parliament, we recommended that agencies test and review their disaster recovery plans at least every 12 months. This year, we found 82 per cent of agencies regularly test their plans, and 84 per cent had reviewed their plans in the last 12 months. However, one agency last reviewed its plan four years ago.

The graph below summarises the disaster recovery planning deficiencies we found.



Source: Provided by agencies (audited).



3. Asset management

Agency service delivery relies on developing and renewing infrastructure assets such as schools, hospitals, roads, or public housing. Agencies are currently investing significantly in new assets. Agencies need to manage the scale and volume of current capital projects in order to deliver new infrastructure on time, on budget and realise the intended benefits. We found agencies can improve how they:

- manage their major capital projects
- dispose of existing assets.

Issues	Recommendations or conclusions
3.1 Capital investment	
<p>Capital asset investment ratios</p> <p>Most agencies report high capital investment ratios, but one-third of agencies' capital investment ratios are less than one.</p> <p>Volume of capital spending</p> <p>Most agencies have significant forward spending commitments for capital projects. However, agencies' actual capital expenditure has been below budget for the last three years.</p>	<p>Recommendation</p> <p>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.</p> <p>Conclusion</p> <p>The significant increase in capital budget underspends warrant investigation, particularly where this has resulted from slower than expected delivery of projects from previous years.</p>
3.2 Capital projects	
<p>Major capital projects</p> <p>Agencies' major capital projects were underspent by 13 percent against their budgets.</p> <p>Capital project governance</p> <p>Agencies do not consistently prepare business cases or use project steering committees to oversee major capital projects.</p>	<p>Conclusion</p> <p>The causes of agency budget underspends warrant investigation to ensure the NSW Government's infrastructure commitment is delivered on time.</p> <p>Conclusion</p> <p>Agencies that have project management processes that include robust business cases and regular updates to their steering committees (or equivalent) are better able to provide those projects with strategic direction and oversight.</p>
3.3 Asset disposals	
<p>Asset disposal procedures</p> <p>Agencies need to strengthen their asset disposal procedures.</p>	<p>Recommendations</p> <p>Agencies should have formal processes for disposing of surplus properties.</p> <p>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.</p>

3.1 Capital investment

All agencies need physical assets to deliver their services, ranging from infrastructure, buildings and vehicles to machinery or information technology.

We sought to gauge how well agencies are investing in new assets to ensure they meet future service delivery challenges. We looked at two aspects:

- capital investment ratios
- volume of capital spending.

Capital asset investment ratios

Capital asset investment ratios measure the extent that an organisation renews or grows (or depletes) its capital assets. These ratios are particularly useful for agencies that rely on capital facilities, such as the infrastructure-dependent transport, education, justice and health cluster agencies.

Two ratios help us assess renewal of assets through agency investment

- The **capital asset investment ratio**, which is calculated by dividing capital spending (excluding non-depreciable assets such as land) by depreciation expenses.
- The **average capital asset investment ratio**, which averages the capital asset investment ratio for the last three years.

When these ratios are higher than 1.0 for an extended time, this suggests an agency is investing heavily in creating and renewing capital assets, which in turn may provide more or better services to the public. But if the ratios are below 1.0 for an extended time, this indicates an agency may not be sufficiently maintaining, replacing or renewing its existing capital assets, which might then impair its service delivery.

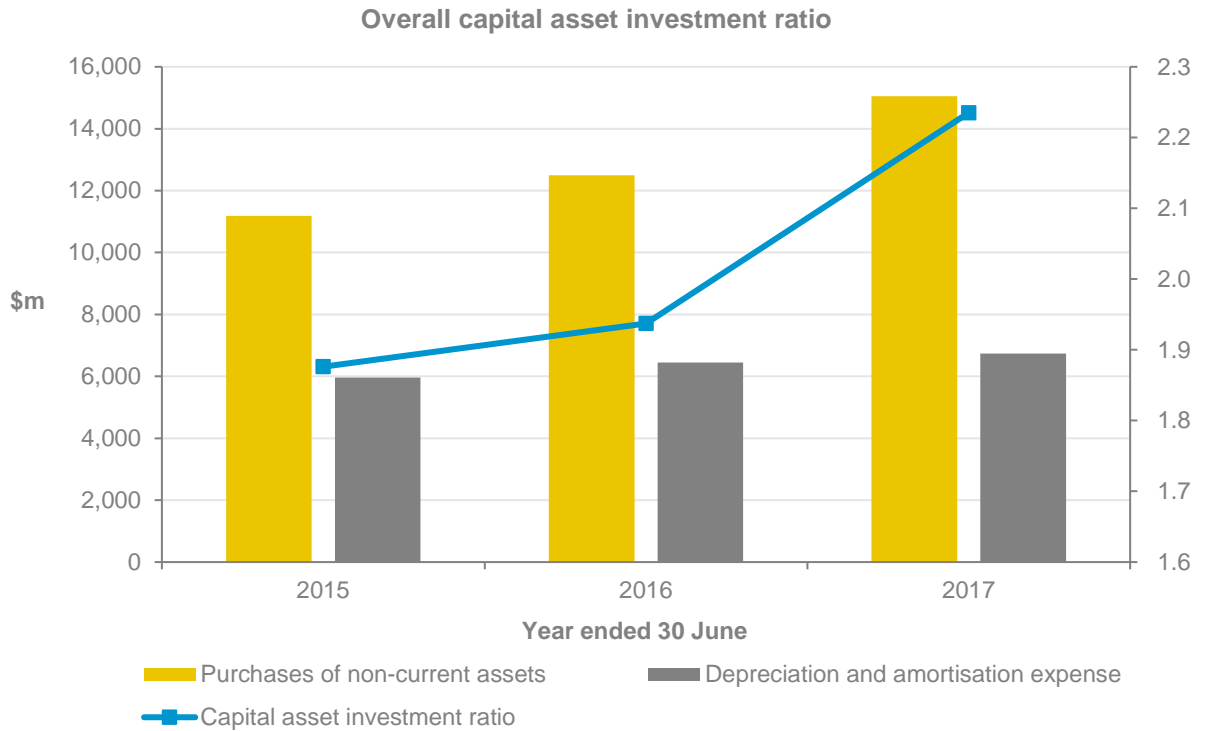
Recommendation

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.

Most agencies are investing heavily in capital assets

The NSW Government has committed to \$80.1 billion in capital spending over the next four years (to 2021). Sixty-four per cent of agencies had an average capital asset investment ratio above 1.0 for the last three years, with the overall average capital asset investment ratio at 2.6. High volumes of capital spending can present challenges for agencies to deliver projects on time, to budget, at sufficient quality and manage project risks. Investment includes the purchases and construction of non-current assets such as infrastructure, plant and equipment, buildings and intangibles such as software.

The graph below shows the trend for the capital asset investment ratio as a whole over the last three years.



Source: Provided by agencies (unaudited).

The graph shows:

- the overall capital asset investment ratio is steadily rising
- depreciation and amortisation, which only start when construction is complete and the asset is ready for use, are growing at a slower rate.

This pattern is typical when a capital investment ratio exceeds 1.0.

There are challenges with maintaining a capital asset investment ratio above 1.0 over the longer term. While renewing or acquiring assets to deliver services can be positive, it can also strain an agency's resources and compromise its ability to deliver projects on time, on budget, at sufficient quality, and with good risk management.

At the same time, a capital asset investment ratio below 1.0 poses operational risks if an agency does not sufficiently invest in its physical assets, such as buildings or equipment, to maintain its service levels. This may also lead to higher maintenance spending in the future and increased operational risks.

For the last three years, one-third of agencies had average capital asset investment ratios below 1.0. These agencies should review whether their capital investment rates are sufficient to deliver services and satisfy their operational needs.

Volume of capital spending

Given that most agencies currently have a high capital investment ratio, we sought to map the volume of capital spending and determine the risks it poses.

Conclusion

The significant increase in capital budget underspends warrant investigation, particularly where this has resulted from slower than expected delivery of projects from previous years.

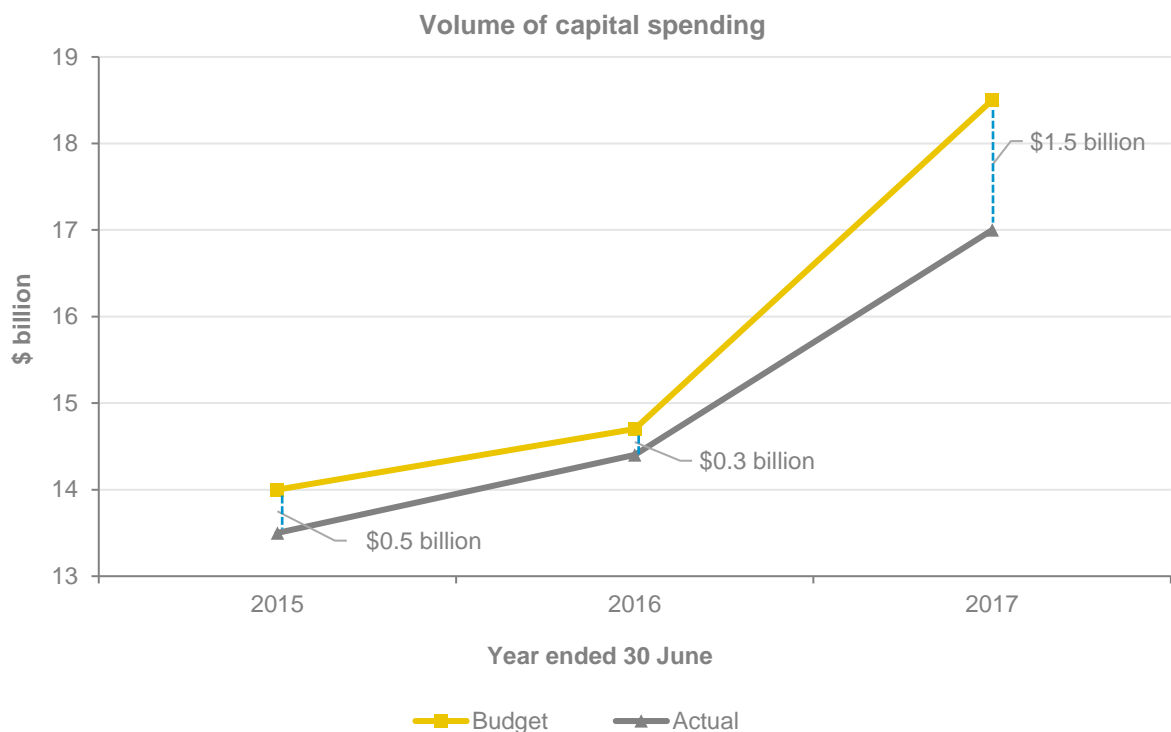
Agencies have underspent their capital expenditure budgets for the last three years

The graph below confirms that agencies continue to invest significantly in capital, spending \$17.0 billion in 2016–17. This has increased from \$14.4 billion in 2015–16 and \$13.5 billion in 2014–15.

The capital budgets cover a wide range of projects, ranging from the Lismore Hospital Redevelopment to the Sydney Light Rail and WestConnex projects.

However, agencies' actual capital expenditure has been below budget for the last three years. The reasons for budget underspends could be:

- imprecise assumptions underpinning budget projections
- unexpected savings
- delayed delivery.



Source: Provided by agencies (unaudited).

The capital expenditure budget increased from \$14.0 billion in 2014–15 to \$18.5 billion in 2016–17. Agencies have recorded budget underspends of:

- \$1.5 billion in 2016–17
- \$0.3 billion in 2015–16
- \$0.5 billion in 2014–15.

Some agencies reported delays in commencing and delivering projects because of reasons outside their control, such as extended community consultation periods. These had resulted in approvals of revised budgets.

The table below shows agency performance against budget over the last three years, divided between physical and IT assets.

	Actual	Budget	Overspend/ (underspend)	Overspend/ (underspend)
	(\$b)	(\$b)	(\$b)	(%)
Physical assets				
2016–17	14.0	15.4	(1.4)	(9)
2015–16	11.9	12.2	(0.3)	(2)
2014–15	12.4	13.1	(0.7)	(5)
IT assets				
2016–17	3.0	3.1	(0.1)	(3)
2015–16	2.5	2.5	(0.0)	(0)
2014–15	1.1	0.9	0.2	22

Source: Provided by agencies (unaudited).

3.2 Capital projects

Given the increases in capital spending, we also looked at the way agencies are managing individual capital projects. The volume of projects managed by the 39 agencies in this report meant we could not review all projects they are currently delivering. We selected a total of 97 projects that were at least 50 per cent complete.

Major capital projects

Conclusion

The causes of agency budget underspends warrant investigation to ensure the NSW Government's infrastructure commitment is delivered on time.

The current level of major capital spending is significant

The NSW Government has budgeted that the 39 agencies in this report will spend \$20.5 billion on the 97 major capital projects we reviewed over the next four years to 2021. They have already spent \$11.5 billion on these projects as at 30 June 2017.

The table below summarises the 2016–17 budgeted versus actual capital expenditure for the major capital projects we sampled that are being delivered by the agencies included in this report. Since the revised and original project budgets are substantially the same, it does not appear underspending is the result of cost savings. The revised budgets suggest the original budgets were not inaccurate in significant respects.

Cluster	Forecast completion year	Original project budget	Revised project budget at 30 June 2017	Total project spend to 30 June 2017
		(\$m)	(\$m)	(\$m)
Education	2018–20	207	247	17
Family and Community Services	2017–18	625	626	556
Finance, Services and Innovation	2017–20	285	316	172
Health	2017–20	1,478	1,417	988
Industry	2016–20	213	218	79
Justice	2017–19	832	873	491
Planning and Environment	2016–21	923	925	663
Premier and Cabinet	2016–17	4	4	4
Transport	2016–20	15,930	15,873	8,477
Treasury	2017–18	9	13	9
Totals		20,506	20,512	11,456

Source: Provided by agencies (unaudited).

The table below summarises the 2016–17 budgeted versus actual capital expenditure for major projects for those agencies included in this report. This shows that they underspent by some \$540 million during the year against their planned budgets.

Clusters	2016–17		
	Original budgeted capital expenditure	Actual capital expenditure	Overspend/ (underspend)
	(\$m)	(\$m)	(\$m)
Education	32	12	(20)
Family and Community Services	105	111	6
Finance, Services and Innovation	84	85	1
Health	318	320	2
Industry	58	51	(7)
Justice	393	351	(42)
Planning and Environment	239	78	(161)
Premier and Cabinet	4	4	0
Transport	2,763	2,446	(317)
Treasury	11	9	(2)
Totals	4,007	3,467	(540)

Source: Provided by agencies (unaudited).

Some agencies advise they obtained approval from the Treasury to roll forward a portion of their 2016–17 capital expenditure budget on projects where they were experiencing significant delays outside of their control.

Capital project governance

As well as the risks posed by the sheer volume of capital investment, we looked at the processes agencies use to manage major capital projects.

Conclusion

Agencies that have project management processes that include robust business cases and regular updates to their steering committees (or equivalent) are better able to provide those projects with strategic direction and oversight.

Appropriate governance is critical to delivering major capital projects effectively. This includes:

- developing robust business cases to support the proposal
- appointing a capital project steering committee to oversee the project
- providing the steering committee with regular reports and status updates.

Up to one-third of business cases had some deficiencies

As a first step, all capital projects should emerge from a strong business case that determines their priority and informs decision-making. Treasury Policy Paper TPP 08-05 'Guidelines for Capital Business Cases' requires that all agencies prepare business cases for capital proposals. This states that an effective business case should:

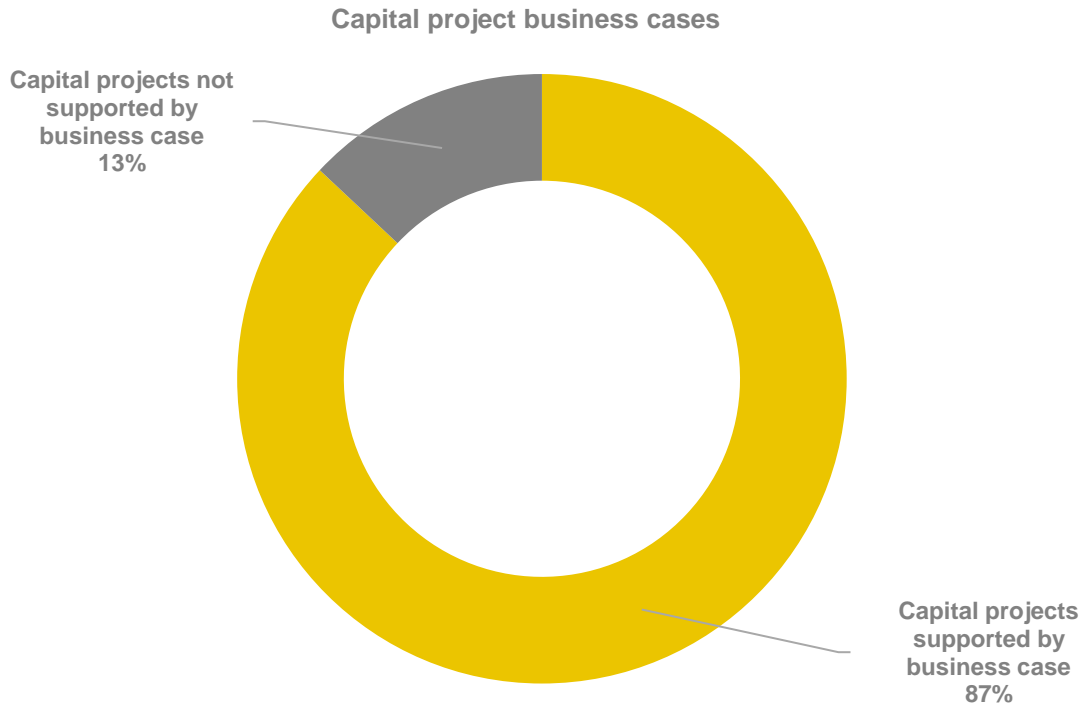
- demonstrate, justify and prioritise the service need
- evaluate the costs, benefits, risks, technical standards and legislative requirements
- document the project plan, governance arrangements, procurement, change management, benefits realisation, and stakeholder consultation strategies and resourcing requirements.

Without this, major capital projects might:

- be inconsistent with government priorities
- waste resources or not offer value for money
- be inadequately resourced
- not deliver the anticipated benefits.

While 87 percent of major capital projects were supported by business cases, we found several deficiencies in those business cases:

- 32 per cent of business cases had not been updated with significant changes to costs, timelines, scoping and workarounds
- 22 per cent of business cases had not considered lessons learnt from similar projects (although this wasn't possible for some new or unique projects).



Source: Provided by agencies (audited).

These findings also mean some agencies may not comply with Treasury Circular TC 12-19 'Submission of Business Cases', which mandates that they provide Treasury with business cases based on the size and risk profile of the project.

Steering committees are not all operating as effectively as they should be

As well as business cases, capital projects need a steering committee to provide strategic direction, oversight and accountability. The steering committee must ensure that:

- the project delivers agreed business outcomes and expected benefits
- the project is on time and in line with the agreed scope and schedules
- project performance is regularly monitored
- an appropriate risk management plan is in place and in use
- risks are addressed appropriately and promptly.

Further, the steering committee should receive regular project reports and status updates. Without these, it cannot effectively monitor progress and address budget variances, delays and scope changes.

We found that 82 per cent of capital projects are governed by a steering committee, but eight per cent of these steering committees had not received a project report in the last three months.

We also found deficiencies in the information provided to these steering committees:

- 20 per cent of status updates did not include sufficient details, such as the current status of the project, what will happen in the next three months and the escalation of risks
- three per cent of project reports did not explain major variances in time, costs, contingency funds, scope and approved budgets
- one per cent of project reports did not measure the extent of unmitigated risks, time and cost overruns, use of contingency funds, scope changes and overall status of the project.

The traffic light approach for managing project risk is embedded in the Infrastructure Investor Assurance Framework developed by Infrastructure NSW. The objective is to ensure the Government's key infrastructure projects are delivered on time and on budget through a risk-based, external assurance framework.

By and large, agencies reported and managed project risks in accordance with the Framework. We found that:

- 88 per cent of agencies used a traffic light approach
- six per cent of agencies used another framework.

However, six per cent of agencies did not include any reporting on project risks.

Agencies overspent \$250 million on consultants and contractors

When project governance is lacking, there is a major risk of incurring additional unbudgeted costs. For example, we found that agencies engaged consultants and/or contractors on 82 per cent of major capital projects. Of these agencies, 28 per cent exceeded their original budget for these external costs and used the project contingency funds to absorb the increase. To date, these agencies have exceeded their original budgets for consultants and/or contractors by \$250 million.

Of the agencies that deliver significant capital projects, 72 per cent use other appropriate project governance processes, such as:

- using probity auditors to oversee tendering processes
- doing independent assurance reviews
- using external entities to oversee the entire project and report to the Audit and Risk Committee and/or Secretary.

The table below summarises the main deficiencies we found in project governance.

Capital project governance deficiencies	Percentage (%)
Capital projects not supported by a business case	13
Business case not updated for significant changes	32
Business case has not considered lessons learnt	22
Capital projects exceeded original budget for consultants/contractors	28
No capital project steering committee	18
Project risks are not reported	6
Project status update deficiencies	20

Source: Provided by agencies (audited).

3.3 Asset disposals

As well as new capital investment, we reviewed how well agencies are managing their disposal of assets.

Asset disposal procedures

Agencies dispose of assets when those assets:

- have come to the end of their useful lives
- must be disposed under a policy, such as if they no longer comply with workplace health and safety standards
- will no longer be needed due to changed procedures, functions or use
- reach their optimum selling time
- contain hazardous materials or are beyond repair.

Disposal commonly involves selling assets such as land, buildings or machinery. It can also involve trade-in for replacement assets or the destruction of assets that have no residual value.

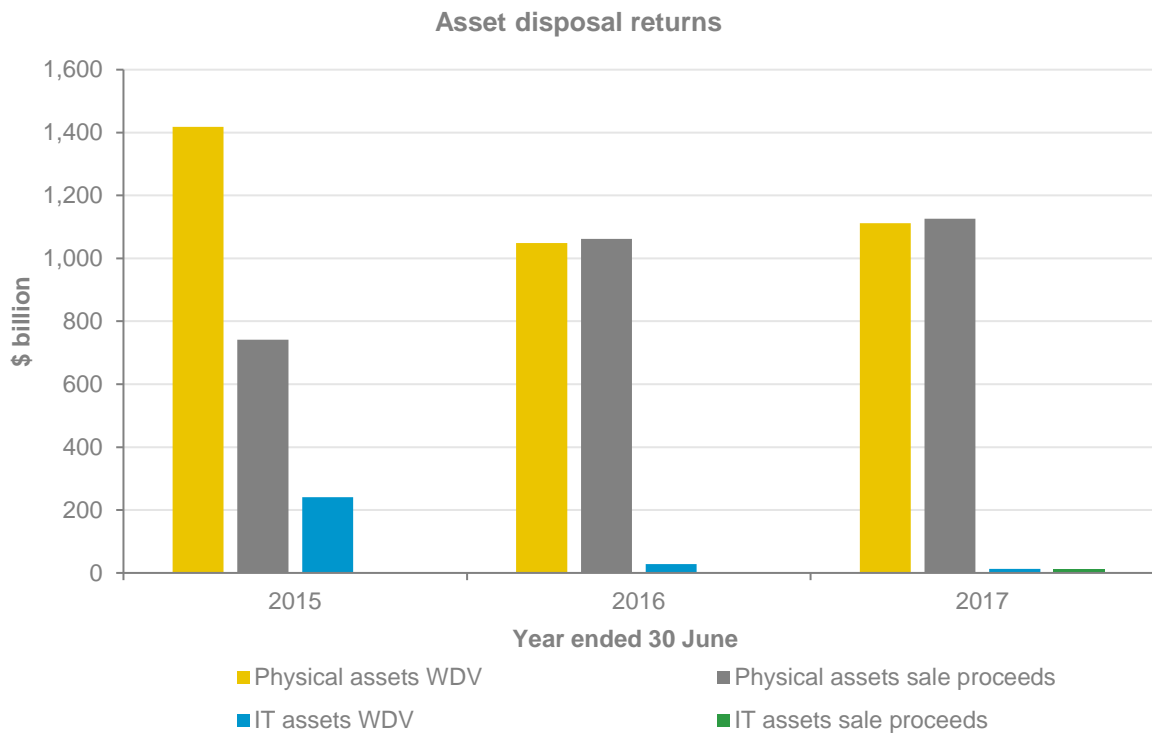
Recommendations

Agencies should have formal processes for disposing of surplus properties.

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.

Agencies made a return of \$14 million from the disposal of assets in 2016–17

The graph below shows that agencies were selling assets below their written-down values (WDVs) in 2014–15. This was either because assets were sold for less than they were worth, or they were being carried at a price above their 'fair value'. The Treasury mandates fair value as the accounting policy for all NSW agencies. More agencies are now recovering the WDV of their assets or selling them marginally above this value.



Source: Provided by agencies (audited).

The following table details the net gain or loss from asset disposals over the last three years. The results are reported in aggregate.

	2014–15 (\$m)	2015–16 (\$m)	2016–17 (\$m)
Sale proceeds	741	1,062	1,138
WDV value of disposed assets	1,659	1,077	1,124
Net gain/(loss)	(918)	(15)	14

Source: Agency financial statements (audited)

Agencies need to strengthen asset disposal procedures

Although agencies as a whole improved the return they realised on asset sales, we found that some did not follow established policies when doing so. For example, 11 per cent of the agencies that must sell their real property through Property NSW did not do so, and did not get approval for this. And eight per cent of agencies do not have an established disposal process.

The Department of Premier and Cabinet's Premier's Memorandum M2012-20 'Government Property NSW and Government Property Principles' requires that Property NSW manage and approve all disposals of real property unless it approves another agency doing so. State owned corporations are exempt from this memorandum, however they are encouraged to use the services of Property NSW where their organisations do not have the necessary in-house expertise.



4. Governance

Governance refers to the high-level frameworks, processes and behaviours that help an organisation to achieve its objectives, comply with legal and other requirements, and meet a high standard of probity, accountability and transparency.

This chapter sets out the governance lighthouse model the Audit Office developed to help agencies reach best practice. It then focuses on two key areas: continuous disclosure and shared services arrangements. The following two chapters look at findings related to ethics and risk management.

Issues	Recommendations and conclusions
4.1 Governance arrangements	
<p>Continuous disclosure</p> <p>Continuous disclosure promotes improved performance and public trust and aides better decision-making. Continuous disclosure is only mandatory for NSW Government Businesses such as State owned corporations.</p>	<p>Conclusion</p> <p>Some agencies promote transparency and accountability by publishing on their websites a continuous disclosure policy that provides for, and encourages:</p> <ul style="list-style-type: none"> regular public disclosure of key performance information disclosure of both positive and negative information prompt reporting of significant issues.
4.2 Shared services	
<p>Service level agreements</p> <p>Some agencies do not have service level agreements for their shared service arrangements.</p> <p>Many of the agreements that do exist do not adequately specify controls, performance or reporting requirements. This reduces the effectiveness of shared services arrangements.</p>	<p>Conclusion</p> <p>Agencies are better able to manage the quality and timeliness of shared service arrangements where they have a service level agreement in place. Ideally, the terms of service should be agreed before services are transferred to the service provider and:</p> <ul style="list-style-type: none"> specify the controls a provider must maintain specify key performance targets include penalties for non-compliance.
<p>Shared service performance</p> <p>Some agencies do not set performance standards for their shared service providers or regularly review performance results.</p>	<p>Conclusion</p> <p>Agencies can achieve better results from shared service arrangements when they regularly monitor the performance of shared service providers using key measures for the benefits realised, costs saved and quality of services received.</p> <p>Before agencies extend or renegotiate a contract, they should comprehensively assess the services received and test the market to maximise value for money.</p>

4.1 Governance arrangements

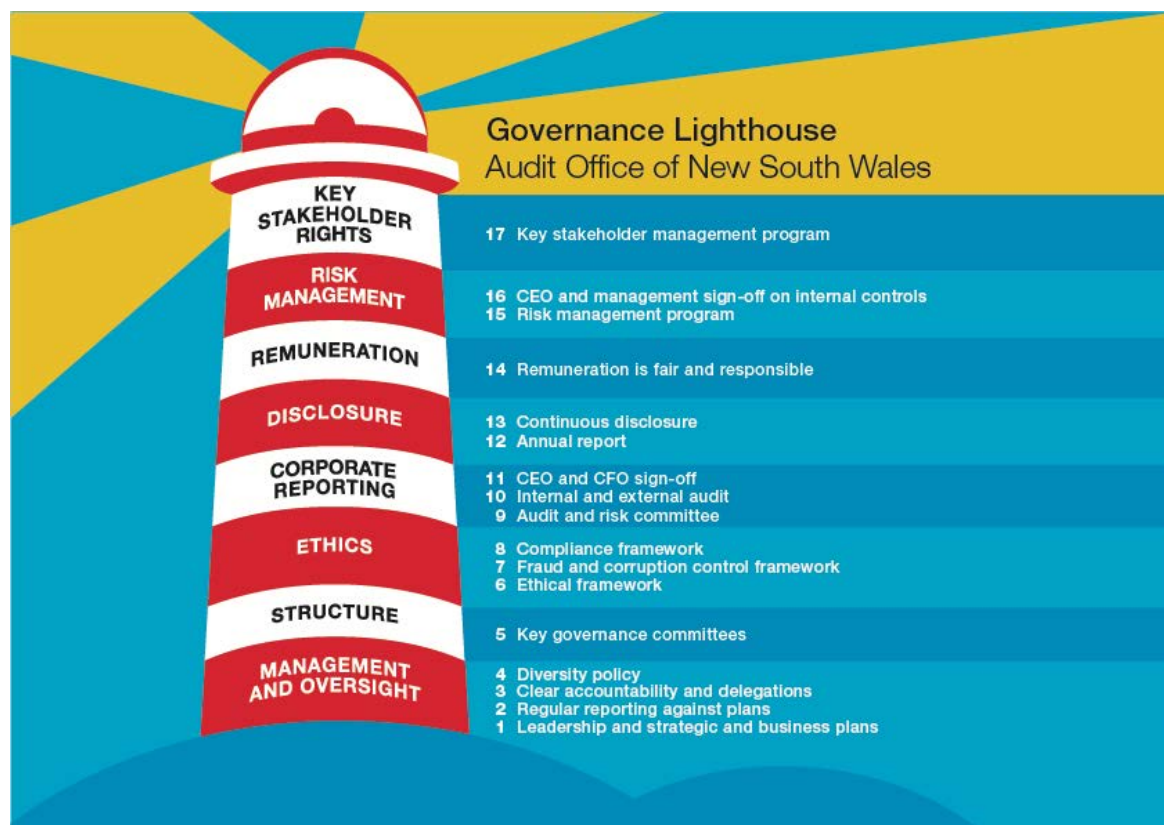
The NSW public sector is divided into ten 'clusters' (groups of agencies), each overseen by a Secretary. Appendix three outlines the agencies included in this report by cluster. The Department of Premier and Cabinet publishes a [Governance Chart](#) of the NSW cluster arrangements, which outlines the agencies within each cluster.

Governance lighthouse

In 2015, the NSW Audit Office released our [Governance Lighthouse](#) to provide a best practice model of public sector governance for agencies to follow. It covers eight principles and 17 key elements of good governance.

Each year, we select different elements of this model and review how well agencies are meeting best practice standards. This year, we are reporting on the following areas:

- Disclosure – Continuous disclosure (Chapter 4)
- Management and Corporate Reporting – Shared services arrangements (Chapter 4)
- Ethics – Ethical framework (Chapter 5)
- Risk Management – Risk management program (Chapter 6).



Continuous disclosure

Continuous disclosure is one of the cornerstones of good corporate governance. In the private sector, this promotes fair and efficient markets and ensures investors are confident and informed. In the public sector, continuous disclosure makes agency operations more transparent and makes them more accountable for the way they use public resources.

While many agencies voluntarily adopt continuous disclosure as better practice, more can be done by other agencies to regularly disclose clear information about their performance.

Conclusion

Some agencies promote transparency and accountability by publishing on their websites a continuous disclosure policy that provides for, and encourages:

- **regular public disclosure of key performance information**
- **disclosure of both positive and negative information**
- **prompt reporting of significant issues.**

Some agencies disclosure processes promote improved performance and public trust

Treasury Policy Paper TPP 05-02 'Reporting and Monitoring Policy for Government Businesses' mandates continuous disclosure by all NSW government businesses (such as State owned corporations), but there is no legislative requirement for general government agencies to do so.

The main way agencies report on their performance is through their annual report. This has legal requirements for disclosing an agency's annual financial statements and reporting on its achievements and challenges in the previous year. Annual reports are published several months after the end of each financial year.

Some agencies adopt better practice by disclosing information continuously. Sixty-four per cent of agencies have a documented continuous disclosure policy endorsed by the agency head and/or its board.

The *Government Information Public Access Act 2009*, requires agencies to proactively release government information to the public to improve the transparency and integrity of the NSW public sector.

4.2 Shared services

Shared service arrangements can centralise corporate services functions such as human resources, financial accounting and information technology. This means that agencies share back office support resources rather than maintaining their own.

Service level agreements

Effective service level agreements (SLAs) are often an important factor for successful shared service arrangements, as they set clear expectations and performance standards.

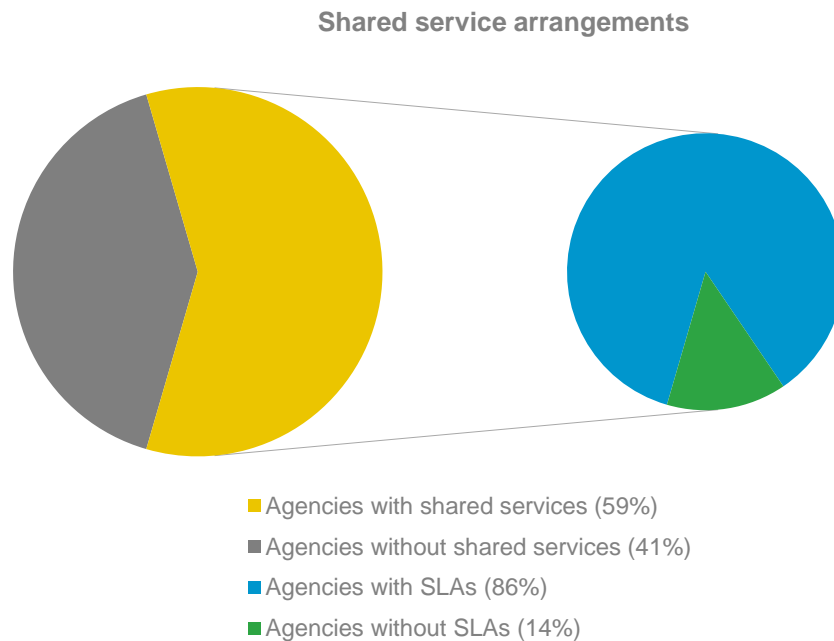


Conclusion

Agencies are better able to manage the quality and timeliness of shared service arrangements where they have an SLA in place. Ideally, the terms of service should be agreed before services are transferred to the provider and:

- **specify the controls the provider must maintain**
- **specify key performance targets**
- **include penalties for non-compliance.**

The graph below shows that 59 per cent of agencies use a shared services provider, and 86 per cent of these agencies have an SLA in place.



Source: Provided by agencies (audited).

Some agencies do not have service level agreements in place

In previous reports to Parliament, we recommended agencies establish clear SLAs before providing or receiving a shared service. These should detail the services and the roles, rights and responsibilities of all parties.

Eighty-six per cent of agencies using shared services do have SLAs in place.

An effective SLA can minimise the risk of:

- gaps in service delivery
- a lack of accountability for service failures, especially if the agreement has no penalty clause
- disputes over the service scope, cost, quality and timeliness
- a lack of ownership for solving problems
- poorly integrated systems that require manual workarounds that increase the risk of fraud and error.

Many service level agreements do not specify controls or penalise underperformance

We also reviewed the quality of SLAs where agencies do have them in place. We found that:

- 60 per cent did not specify what controls the service provider must maintain
- 84 per cent did not prescribe penalties for underperformance
- 20 per cent did not specify key performance targets for reporting.

If agreements do not specify the controls that a service provider must maintain, information may be inaccurate, incomplete, untimely or not properly secured or protected. This can lead to:

- inaccurate financial reporting
- breaches of confidentiality
- failure in the services provided to the public
- failure to respond to reasonable requests promptly.

Weak controls and delays in responding to requests for information can also affect an agency's financial audit. This can in turn substantially:

- limit the scope of the audit
- affect the auditor's opinion on all agencies using that shared service
- increase audit fees.

There is also a risk that agencies will not comply with Treasury Policy Paper [TPP 17-06 'Certifying the Effectiveness of Internal Controls Over Financial Information'](#). This requires that chief financial officers (CFOs) certify the effectiveness of internal controls over financial information.

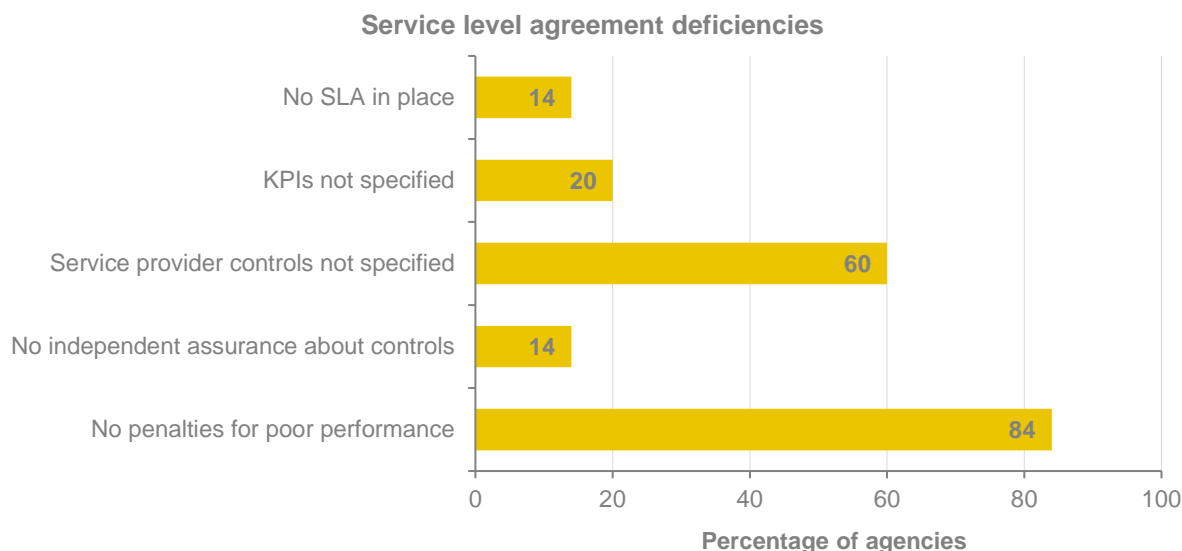
CFOs must do this by verifying certifications not just from agency management, but from service providers that record, process and report financial data. Yet we found that:

- 14 per cent did not get and/or provide certifications about the effectiveness of the service provider's controls
- 43 per cent of CFO certifications on the effectiveness of agency controls did not reference the control failures in the service provider's Independent Assurance Practitioner report.

When using SLAs, agencies should:

- consider including a performance component in the fee to encourage quality service
- properly integrate the provider and user systems
- regularly monitor service performance through key performance measures
- renegotiate when services change, or periodically after a performance review
- detail what controls a service provider must maintain
- ensure the user of the services has complementary controls
- specify what reports and assurances the service provider must give the user about the design, implementation and operation of these controls.

The graph below shows the deficiencies we found in SLAs.



Source: Provided by agencies (audited).

Shared service performance

Shared service arrangements are popular because they can reduce the back-office costs of agencies. Yet this may not translate into value for money if the service delivered is not at the same (or better) level of service.

For agencies to achieve value for money from shared services arrangements, clear performance standards should be set and monitored with service providers held accountable for poor results.

Clear performance standards and penalties for failure help agencies manage service providers and improve their value for money.

Conclusion

Agencies can achieve better results from shared service arrangements when they regularly monitor the performance of shared service providers using key measures for the benefits realised, costs saved and quality of services received.

Before agencies extend or renegotiate a contract, they should comprehensively assess the services received and test the market to maximise value for money.

Poor shared service performance could significantly affect user agencies, through:

- inaccurate, incomplete and untimely data processing
- control failures over the accuracy, completeness and confidentiality of information
- inaccurate financial and management reporting
- manual workarounds by the user agency
- increased costs.

Agencies can set clearer performance standards and monitor them more effectively

Twenty per cent of agency SLAs did not set minimum standards of acceptable performance. And 34 per cent of agencies do not require service providers to report on service performance, do not monitor performance, or do not report findings to an appropriate level of management. This can affect how those agencies are able to objectively and consistently measure the cost, quality and timeliness of the service provider's performance. They will also find it harder to hold the service provider accountable for service failures.

The performance measures that agencies can use include the:

- timeliness and accuracy of data processing and reconciliations
- timeliness of reports and requests for information
- availability of the system and server
- response and resolution time to issues or incidents
- recruitment time and quality of contractors.

Fifty per cent of agencies formally assess the benefits they are realising from their shared service arrangements. Of these, only 64 per cent sought feedback from end users in making their assessment. This can limit agencies determining whether they achieved the efficiencies they expected and whether they should continue, renegotiate, or re-tender the shared service arrangement when it expires.

In making these decisions, agencies would also benefit from benchmarking their results with other government organisations. Yet only 18 per cent of agencies benchmarked the service they received against providers inside and outside government. And only 55 per cent shared key performance results across the sector.

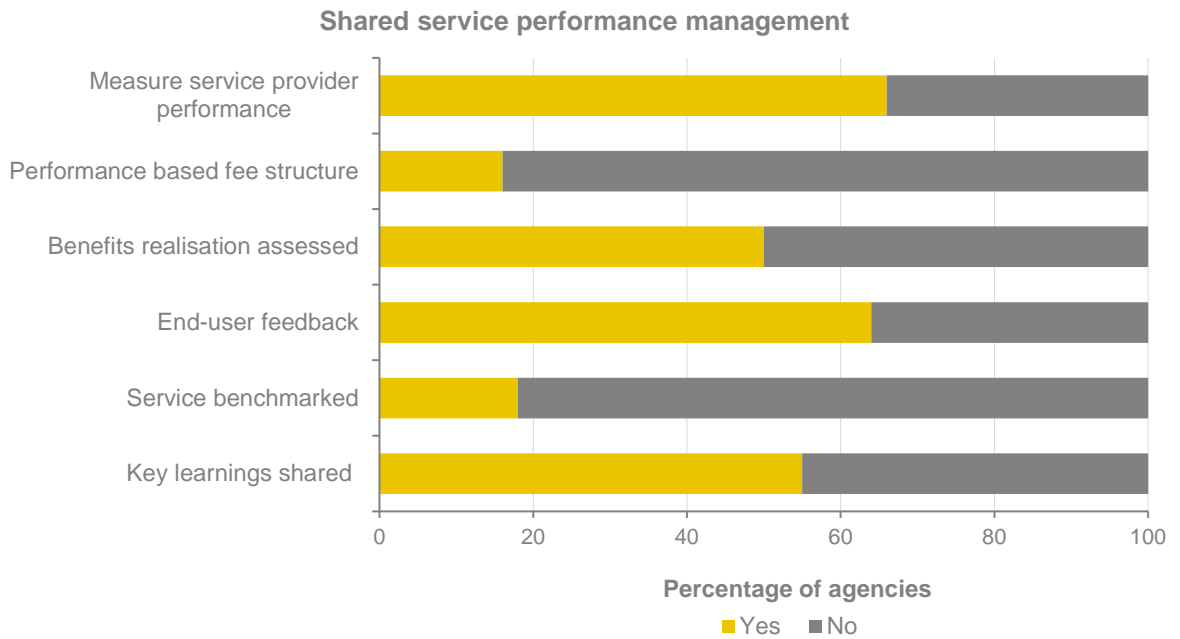
Penalty clauses would help hold shared service providers to account

Penalty clauses in SLAs with external service providers reinforce their obligation to meet minimum standards and address any gaps. Penalties can include service credits or withholding payments for service failure. Without penalty clauses, user agencies find it more difficult to hold a service provider accountable for poor service delivery or force them to remedy it.

We found that 84 per cent of agencies do not include a penalty clause in their SLAs. Some agencies who have had unsatisfactory experiences advise they intend to include a penalty clause in any new or renegotiated SLA. Others reported that they currently rely on the lead agency in their cluster to resolve service performance disputes.

It is common for an agency within the same cluster to provide a shared service. In many respects, these can be the most difficult agreements to manage. Service quality can remain unaddressed for extended periods because of the existing relationships. These relationships make it even more important for user agencies to set and monitor performance standards consistently, and escalate issues as they arise.

The graph below shows the performance management of shared service arrangements across agencies. The left hand portion shows the percentage of agencies implementing each performance management measure while the right hand portion shows the gap that agencies need to address.



Source: Provided by agencies (audited).



5. Ethics and conduct

All government sector employees must demonstrate the highest levels of ethical conduct, in line with standards set by [The Code of Ethics and Conduct for NSW government sector employees](#).

This chapter looks at how well agencies are managing these requirements, and where they can improve their policies and processes.

We found that agencies mostly have the appropriate codes, frameworks and policies in place. But we have highlighted opportunities to improve the way they manage those systems to reduce the risks of unethical conduct.

Issues

Recommendations and conclusions

5.1 Ethical framework

Code of conduct

All agencies we reviewed have a code of conduct, but they can still improve the way they update and manage their codes to reduce the risk of fraud and unethical behaviour.

Recommendation

Agencies should regularly review their code-of-conduct policies and ensure they keep their codes of conduct up-to-date.

Statement of business ethics

Most agencies maintain an ethical framework, but some can enhance their related processes, particularly when dealing with external clients, customers, suppliers and contractors.

Conclusion

Agencies can enhance their ethical frameworks by publishing a Statement of Business Ethics, which communicates their values and culture.

5.2 Potential conflicts of interest

Conflicts of interest

All agencies have a conflicts-of-interest policy, but most can improve how they identify, manage and avoid conflicts of interest.

Recommendation

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.

Gifts and benefits

While all agencies already have a formal gifts-and-benefits policy, we found gaps in the management of gifts and benefits by some that increase the risk of unethical conduct.

Recommendation

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

5.1 Ethical framework

Code of conduct

Recommendation

Agencies should regularly review their code-of-conduct policies and ensure they keep their codes of conduct up-to-date.

Agencies can improve the way they manage their codes of conduct

We found that all agencies have a formal code-of-conduct policy and include it in their staff inductions. However, agencies need to review their related processes to make sure they:

- review and update their code of conduct regularly
- support the code with training for all staff
- cover secondary employment
- record and address any code-of-conduct breaches.

We found that 67 per cent of agencies do not regularly review their code of conduct for relevance, and three last reviewed their code more than five years ago. Without regular review, agency codes may not reflect significant changes to government policy, legislation or business practice.

Agencies can enhance their code-of-conduct policy by requiring all staff to make an annual code-of-conduct declaration. We found 82 per cent of agencies do not require staff to complete an annual declaration, and 13 per cent do not have a process to follow-up missing declarations. One agency reported that 78 per cent of its staff had not signed their annual declaration by 30 June 2017.

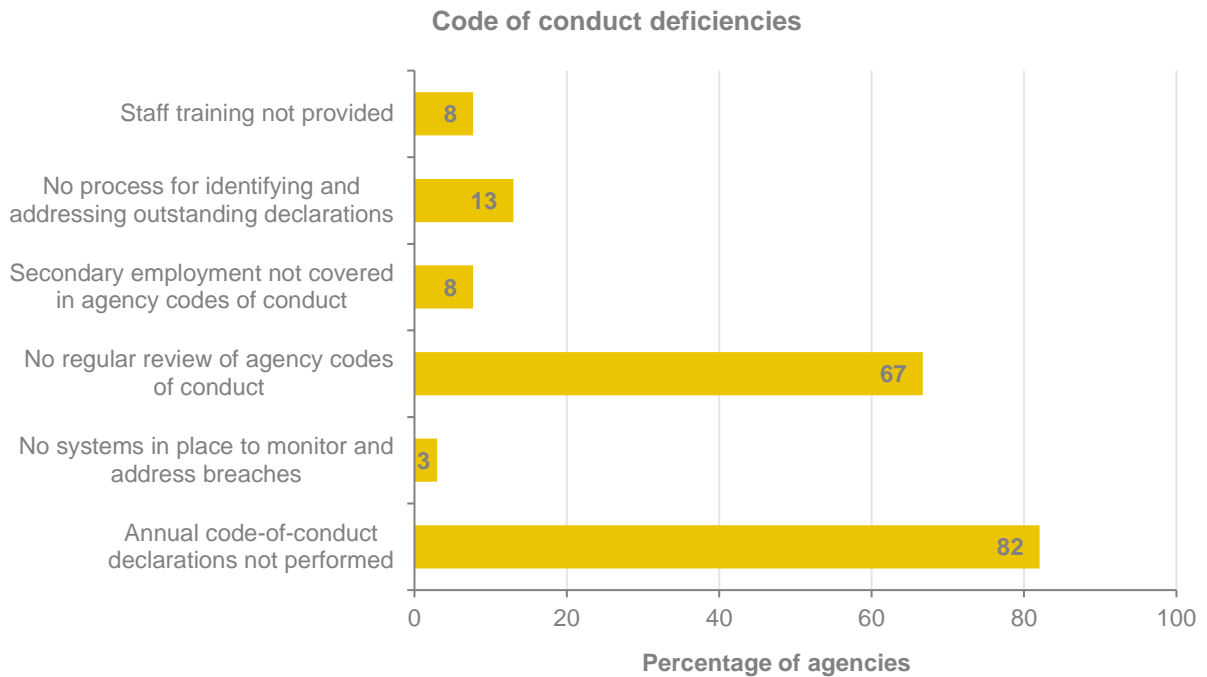
While all agencies include the code-of-conduct policy in their staff inductions, eight per cent did not provide training in the policy after induction. Without annual declarations supported by regular training, staff may not fully understand and comply with their agency's code.

It is important that agencies cover secondary employment in their codes of conduct, or other related policy. Not doing so may lead to conflicts of interest between official and private business interests. We found that eight per cent of agency codes do not currently cover secondary employment.

Most agencies had systems in place to monitor and address code-of-conduct breaches. However, we found one agency that did not do so.

These weaknesses may also lead to breaches of the *Government Sector Employment Act 2013*, which requires that agencies comply with directions made by the Public Service Commissioner. This includes a direction for agencies to implement the [Commission's code of ethics and conduct](#).

The graph below captures the issues we found:



Source: Provided by agencies (audited).

Statement of business ethics

Conclusion

Agencies can enhance their ethical frameworks by publishing a Statement of Business Ethics, which communicates their values and culture.

Most agencies maintain an ethical framework, but some can improve their related processes

We found that most agencies maintain an ethical framework, but 13 per cent have not developed and published a Statement of Business Ethics. This would clarify the standards of behaviour they expect from the companies and individuals with whom they do business.

Without a Statement of Business Ethics, clients, customers, suppliers and contractors may not be aware of an agency's values and culture, and the standard of behaviour expected of them when dealing with the agency and its employees. This also makes it harder for agencies to call them to account for any conduct that breaches the ethical standards of the NSW public sector.

Most agencies publish a Statement of Business Ethics, only 44 per cent of those that do so regularly review it, and some 26 per cent last reviewed it more than two years ago. We also found that 21 per cent of agencies had not trained staff in what their Statement of Business Ethics requires of them.

Publishing and managing a Statement of Business Ethics should become an integral part of the ethical framework that agencies operate under.

The *Government Sector Employment Act 2013* requires all staff in the government sector to act ethically and in the public interest. The Public Service Commission has produced a [guide on ethical behaviour](#) to help employees understand their obligations.

5.2 Conflicts of interest

The public expects that government agencies meet high standards of integrity. This includes the way agencies manage real or perceived conflicts of interest.

Conflicts of interest

Recommendation

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.

Most agencies can improve how they identify, manage and avoid conflicts of interest

While all agencies have a conflicts-of-interest policy, we found several issues in the way they manage conflicts of interest. Unless these are addressed, they could:

- undermine confidence in the NSW public sector
- damage the reputations of agencies and individuals
- increase the risk of financial loss.

Agencies should manage conflicts of interest by:

- removing employees from decision making where a conflict exists
- maintaining current registers of conflicts of interest
- providing annual training on conflicts of interest
- making annual declarations of conflicts of interest
- flagging conflict-of-interest declarations in the agendas of decision meetings.

The [Code of Ethics and Conduct](#) requires agency senior executives to make a conflicts-of-interest declaration at least annually. Agencies can enhance their conflicts-of-interest policy by requiring an annual declaration from all staff.

We found that 62 per cent of agencies do not require all staff to declare conflicts of interest annually. Of those that do, 35 per cent do not identify and follow up on outstanding declarations. And 10 per cent do not require the immediate update of their conflicts-of-interest register when a declaration is made.

Further, some 15 per cent of agencies do not train staff in their conflicts-of-interest policy, and eight per cent do not train new staff during induction. This increases the risk their staff may not be aware of their obligations to manage conflicts of interest.

These weaknesses may also lead to breaches of the *Government Sector Employment Act 2013*, which requires that most agencies comply with directions made by the Public Service Commissioner. This includes a direction under the [Code of Ethics and Conduct](#) to avoid and effectively manage any real or perceived conflicts of interest.

The table below summarises the issues we found.

Deficiencies in managing conflicts of interest	Percentage of agencies (%)
No annual conflict-of-interest declaration required by all staff	62
No process for following up outstanding declarations	35
No staff training in the policy	15
Policy not covered during induction of new staff	8
No requirement to immediately update the conflict register when a conflict emerges	10

Source: Provided by agencies (audited).

Agencies and staff can assess their current practice against a conflict-of-interest guide published by the [Independent Commission Against Corruption \(ICAC\)](#).

Gifts and benefits

Recommendation

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

Some agencies can strengthen the way they manage gifts and benefits

Ineffective management of gifts and benefits can have serious consequences for an agency and its staff. These include intangible impacts such as the loss of public trust, as well as direct financial losses and exposure to legal action.

While all agencies already have a formal gifts-and-benefits policy, we found that some can improve the way they manage gifts and benefits in practice.

Effective management for this control starts by making staff aware of the agency's policy. Yet 10 per cent of agencies do not train new staff in the requirements of their gifts-and-benefits policy, whether as part of their induction or after.

Without these controls, staff may unwittingly accept gifts that influence, or are perceived to have influenced, their decisions.

Agencies should also manage the risks of gifts and benefits by keeping an up-to-date gifts and benefits register and reporting to its Executive on current trends. We found that 15 per cent of agencies do not require staff to update their register directly after the offer or receipt of a gift or benefit. And 33 per cent of agencies do not discuss trends at Executive level.

Addressing these gaps in the management of gifts and benefits can minimise the risk of unethical conduct that misuses public resources.

Poor management of gifts and benefits can result in breaches of the *Government Sector Employment Act 2013* and the [Public Service Commission's direction](#) to implement minimum standards to manage gifts and benefits.



The table below summarises the issues we found.

Deficiencies in managing gifts and benefits	Percentage of agencies (%)
Trends not shared with the Executive	33
No requirement to immediately update the register when an event occurs	15
No staff training in the policy	10
Policy not covered during induction of new staff	8

Source: Provided by agencies (audited).



6. Risk management

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

This year we looked at the overall maturity of the risk management frameworks that agencies use, along with two important risk management elements: risk culture and risk registers.

Issues

Recommendations

6.1 Risk management maturity

All agencies have implemented risk management frameworks, but with varying levels of maturity in their application.

Agencies' averaged a score of 3.1 out of five across five critical assessment criteria for risk management. While strategy and governance fared best, the areas that most need to improve are risk culture, and systems and intelligence.

Conclusion

Agencies have introduced risk management frameworks and practices as required by the Treasury's:

- 'Risk Management Toolkit for the NSW Public Sector'
- 'Internal Audit and Risk Management Policy for the NSW Public Sector'.

However, more can be done to progress risk management maturity and embed risk management in agency culture.

6.2 Risk management elements

Risk culture

Most agencies have started to embed risk management into the culture of their organisation. But only some have successfully done so, and most agencies can improve their risk culture.

Conclusion

Agencies can improve their risk culture by:

- setting an appropriate tone from the top
- training all staff in effective risk management
- ensuring desired risk behaviours and culture are supported, monitored, and reinforced through business plans, or the equivalent and employees' performance assessments.

Risk registers and reporting

Some agencies do not report their significant risks to their lead agency, which may impair the way resources are allocated in their cluster. Some agencies do not integrate risk registers at a divisional and whole-of-enterprise level.

Conclusion

Agencies not reporting significant risks at the cluster level increases the likelihood that significant risks are not being mitigated appropriately.

Effective risk management can improve agency decision-making, protect reputations and lead to significant efficiencies and cost savings. By embedding risk management directly into their operations, agencies can also derive extra value for their activities and services.

6.1 Risk management maturity

The more mature an agency's risk management, the better it will balance the tension that can exist between protecting its operations and embracing opportunities. A mature risk management process should:

- embed a risk-aware culture
- align strategic and business decision-making with risk management
- improve resilience in dealing with adversity
- increase agility in pursuing opportunities.

This year we assessed the risk management maturity level of agencies using the Audit Office's ['Risk Management Maturity Assessment Tool'](#).

This section discusses our findings about risk management maturity, first by reporting on the overall stage that agencies have reached, and then by detailing how they fared against each of the five critical assessment criteria we used.

Conclusion

Agencies have introduced risk management frameworks and practices as required by the Treasury's:

- **'Risk Management Toolkit for the NSW Public Sector'**
- **'Internal Audit and Risk Management Policy for the NSW Public Sector'**.

However, more can be done to progress risk management maturity and embed risk management in agency culture.

Risk management framework

Each agency in NSW is responsible for its own risk management, and must tailor its risk management approaches, tools and techniques in a fit-for-purpose risk framework. This means that some agencies will need more sophisticated risk management processes to suit the size and complexity of their activities.

We looked at the maturity levels of agency risk frameworks and classified agencies at one of five stages:

7. Initial
8. Inconsistent
9. Consistent – designed
10. Consistent – implemented
11. Optimised.



Most agencies have reached the middle stage for risk management maturity

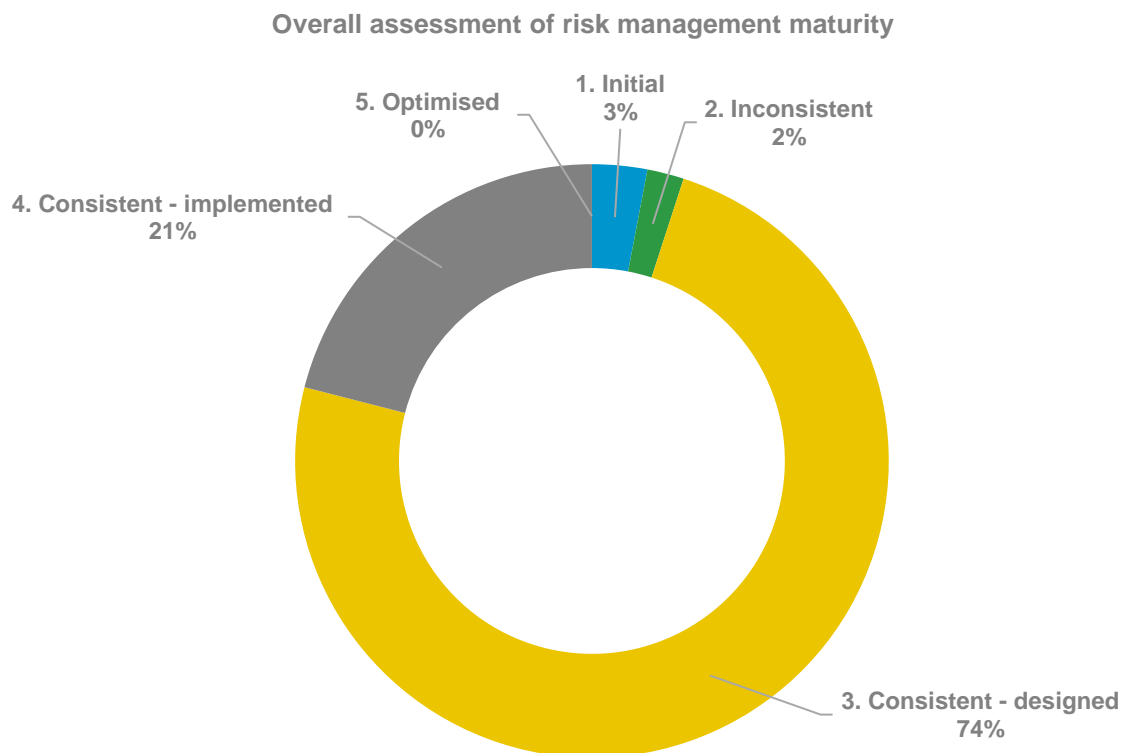
We found that most agencies (74 per cent) are in the designed stage of applying a risk management framework, with the overall maturity assessment across agencies averaging 3.1 out of five. This means that more work is needed to embed enterprise-wide risk management.

More importantly, we found that only 21 per cent of agencies had fully implemented an enterprise risk management framework. The five per cent of agencies in the initial or inconsistent stages should accelerate their risk management processes as a high priority.

Without a robust risk management framework, including a risk appetite statement and strategic risk registers, agencies might not:

- recognise and mitigate risks
- manage risks in a systematic and structured way, or resource this task appropriately
- have appropriate strategies in place to mitigate risks and maximise opportunities
- embed a risk-aware culture in their organisations.

The graph below shows our overall assessment of the maturity of agencies' risk management.



Source: Provided by agencies (unaudited).

The next section details the way we evaluated risk management maturity to arrive at these results.

Risk management criteria

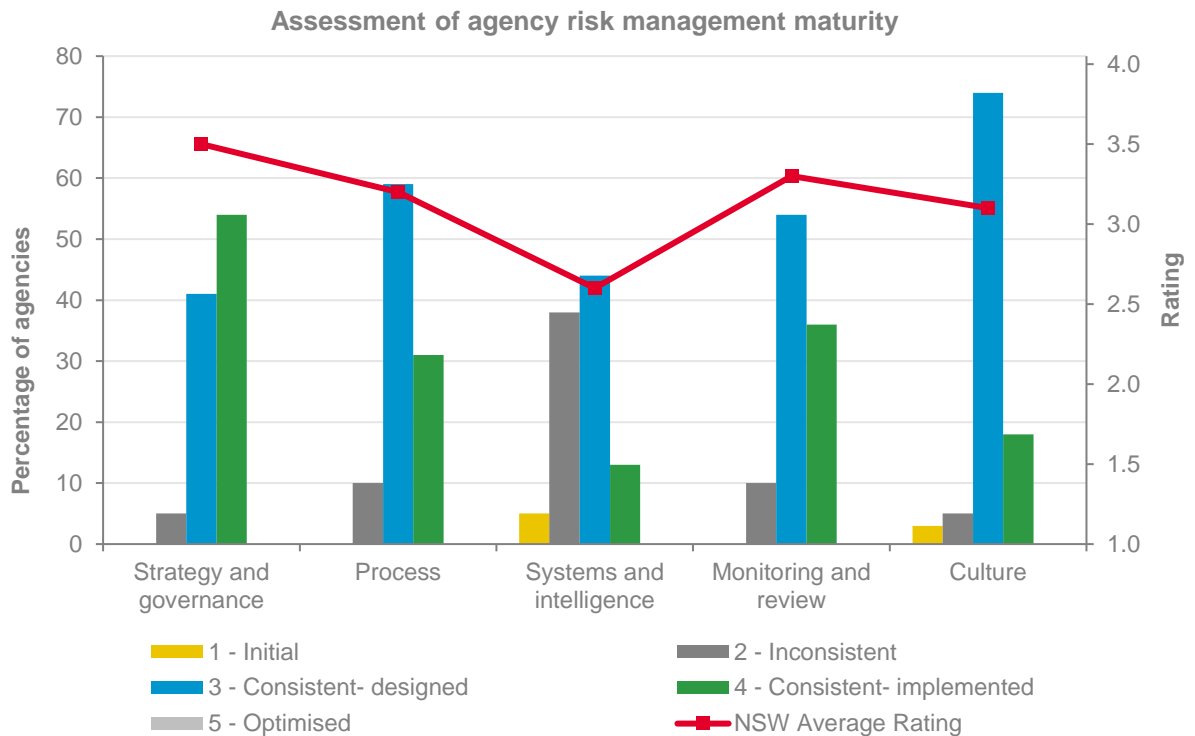
To assess agencies' risk management maturity, we applied five critical assessment criteria:

1. Strategy and governance
2. Process
3. Systems and intelligence
4. Monitoring and review
5. Culture.

A successful risk management framework will closely integrate all five of these areas.

All areas of risk management need to improve, but some areas are weaker than others

We found that agencies generally can improve in all five areas.



Source: Provided by agencies (unaudited).

The two areas that most need to improve relate to systems and intelligence and to risk culture, which achieved maturity ratings of 2.6 and 3.1 out of five respectively. This means agencies are not fully integrating the analysis and reporting of risks or embedding it in staff management, communication and training. Just 13 per cent of agencies have implemented systems and intelligence measures and 18 per cent had implemented a risk management culture.

Strategy and governance systems performed the best, with 54 per cent of agencies having appropriate systems, such as a risk management framework, integrating risk management in planning and reporting and defining risk management responsibilities. But 54 per cent falls well short when considering the public sector as a whole. And unless identified risks are linked to internal audit plans, agencies cannot be certain they are implementing appropriate controls.

The results for risk management processes and for the monitoring and review of risks show only 31 per cent and 36 per cent of agencies respectively had fully implemented these systems. Unless risk management is embedded in day-to-day operations, agencies may not report and address incidents.

The following table details the key weaknesses we identified across the five critical criteria. This maps the ways that agencies can improve their risk management practices.

Agency ratings	Summary of key weaknesses
Strategy and governance	
1. Initial (0%)	• Draft, expired or no risk management frameworks in place.
2. Inconsistent (5%)	• Draft risk registers in use and/or not endorsed.
3. Consistent - designed (41%)	• Risk not a standing agenda item at executive meetings.
4. Consistent - implemented (54%)	• Roles and responsibilities for risk management not clearly defined.
5. Optimised (0%)	• Risk not incorporated into strategic planning.
	• Risk appetite and tolerance levels not developed or yet to be placed into operation.
Process	
1. Initial (0%)	• Risk management not fully integrated into day-to-day operations on all levels or not applied consistently across agency.
2. Inconsistent (10%)	
3. Consistent - designed (59%)	• Internal audit plans endorsed before risk management frameworks refresh.
4. Consistent - implemented (31%)	• Unfinalised divisional risk registers.
5. Optimised (0%)	• Risk management not included in project management plans.
	• Draft risk incident reporting processes in place.
	• No alignment of internal audit plans and agency risk registers.
	• Key risk indicators not used or reported on.
Systems and intelligence	
1. Initial (5%)	• No integrated risk management systems in place for capturing and reporting risks.
2. Inconsistent (38%)	
3. Consistent - designed (44%)	• Risks captured manually using spreadsheets.
4. Consistent - implemented (13%)	• Manual reporting with limited data integrity.
5. Optimised (0%)	• No ability to perform data analytics.
	• Limited capacity to track risk management and exposure through risk incidents and events.
Monitoring and review	
1. Initial (0%)	• No formal risk acceptance policies.
2. Inconsistent (10%)	• Formal risk escalation processes not fully operational.
3. Consistent - designed (54%)	• Review of risk management frameworks only performed by external parties.
4. Consistent - implemented (36%)	
5. Optimised (0%)	• Insufficient governance oversight and monitoring.
Culture	
1. Initial (3%)	• Formal training on risk management not provided to all staff.
2. Inconsistent (5%)	• No agency-wide communication on risk management.
3. Consistent - designed (74%)	• Risk KPIs not included in staff performance appraisals.
4. Consistent - implemented (18%)	• Tone set by management strong but inconsistent at lower levels.
5. Optimised (0%)	• No budgets for risk management processes.

6.2 Risk management elements

As well as reviewing the overall risk management maturity, each year we assess specific areas of risk management to explore how well agencies are performing. This year, we looked at two elements:

- risk culture
- risk registers and reporting.

Risk culture

As we discussed above, culture is one of the five critical assessment criteria in our '[Risk Management Maturity Assessment Tool](#)'.

An agency's risk culture is made up of the ethics, values, behaviours and actions of staff that affect decision-making and business outcomes. A strong culture helps to embed successful risk management in an organisation by:

- encouraging open and upward communication
- sharing knowledge and best practices
- continuously improving processes
- reinforcing the commitment to ethical and responsible business behaviour.

Conclusion

Agencies can improve their risk culture by:

- **setting an appropriate tone from the top**
- **training all staff in effective risk management**
- **ensuring desired risk behaviours and culture are supported, monitored, and reinforced through business plans, or the equivalent and employees' performance assessments.**

Most agencies have started to embed a risk-aware culture but can do more

We found that most agencies (74 per cent) had started to embed a risk-aware culture. However, they have not fully implemented all processes across their operations; around three per cent were only at the initial stages and need to do more work in this area.

Without an effective risk culture, agencies may not be identifying, assessing, communicating and managing risks across all levels of the agency. This can lead to damaged reputations and financial cost.

We identified several practical steps that agencies can take to strengthen their risk culture. The first involves the 'tone' set by the executive and management team. A positive tone means that an agency has open communication about the risks it faces and how to respond to them. This in turn makes it more likely that staff will manage them effectively.

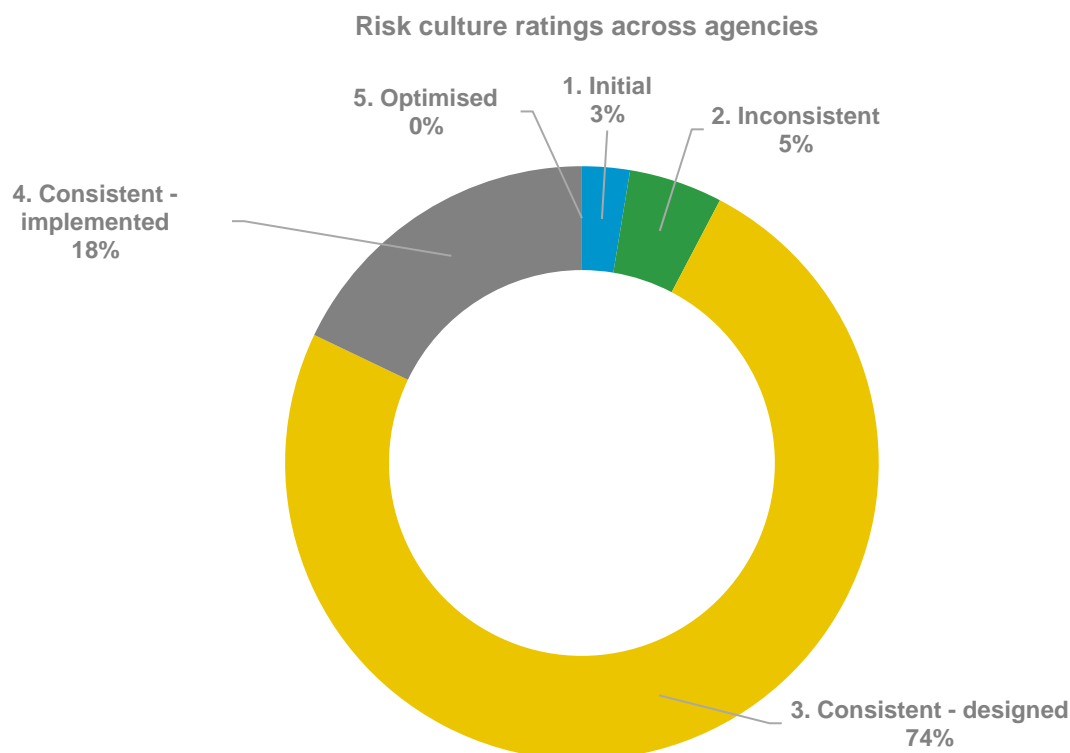
In fact, staff awareness and understanding of risks is crucial to risk management. Yet some agencies only train selected levels of staff in risk management, and in some cases do not provide training on risks at all. This makes it less likely that staff will effectively capture or mitigate risks.

Another vital way to reinforce this awareness is to ensure desired risk behaviours and culture are supported, monitored and reinforced through employees' performance assessments. Without this, staff may not feel accountable for mitigating organisational risks, as they do not see it as their individual responsibility.

The agencies we surveyed that demonstrated a more mature risk culture used some or all of the following measures:

- a clear and consistent tone from the top on taking and avoiding risk
- transparent and timely flow of risk information within the agency
- acceptance across the agency of the importance of risk management
- clear accountability for, and ownership of, specific risks and risk areas
- risk management behaviour as a metric in staff performance evaluations
- encouragement of risk reporting and whistleblowing.

The graph below shows agencies' risk culture ratings against the Office's risk maturity scale.



Source: Provided by agencies (unaudited).

Risk registers and reporting

Agencies in the NSW public sector are grouped into 10 'clusters' under the state's [governance framework](#). This brings together complementary agencies to better coordinate services within the same broad policy area of a particular cluster. The Secretary of a lead agency oversees each cluster.

We reviewed how well risk management was being reported at a cluster level as well as within individual agencies.

Conclusion

Agencies not reporting significant risks at the cluster level increases the likelihood that significant risks are not being mitigated appropriately.

Some agencies do not report major risks at the cluster level

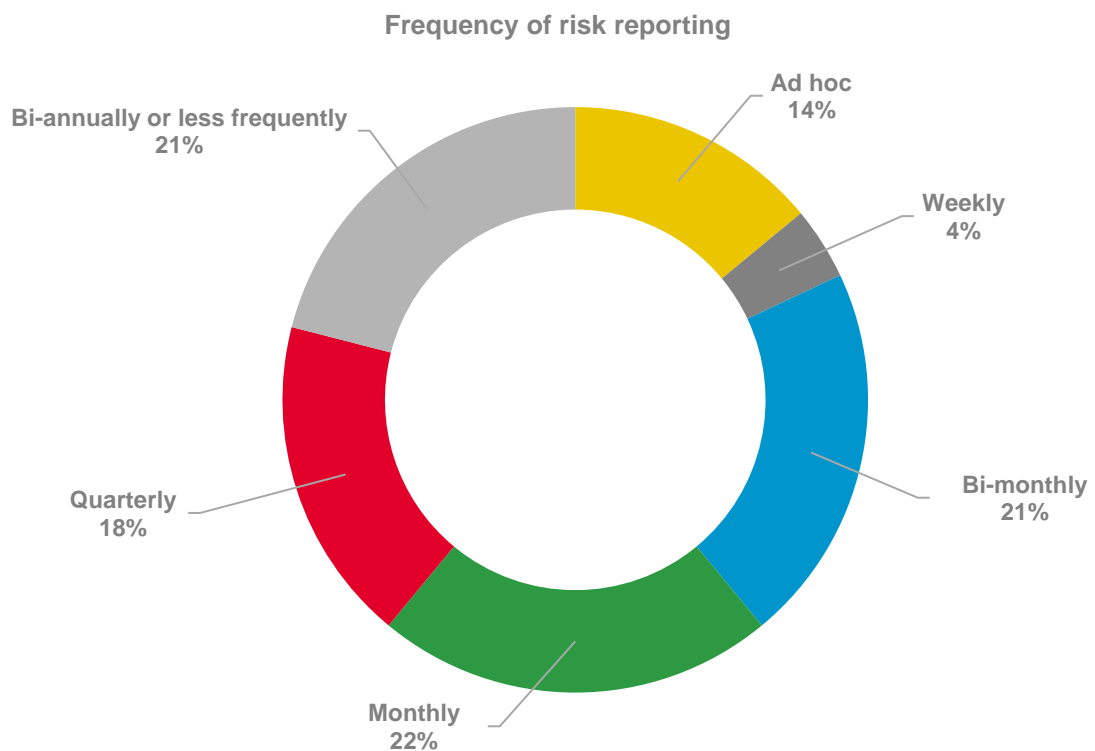
Risk management in NSW is largely driven agency by agency. Each entity within a cluster has its own risk profiles and risk management frameworks. As a result, we found varying approaches and levels of maturity in the way that agencies capture, escalate and report risks to the lead agency in their cluster.

Nineteen per cent of agencies do not report top-level risks to the Secretary and Executive of the lead cluster agency at all. Lack of cluster reporting also means that a common risk may not be understood and mitigated in the same way by agencies across the cluster. This is particularly relevant where similar services are delivered by different agencies in different regions.

Clause 1.2.8 of Treasury Policy Paper TPP 15-03 'Internal Audit and Risk Management Policy for the NSW Public Sector', requires agencies to implement processes to ensure that significant risks likely to affect other agencies are formally communicated to those agencies.

As the following chart shows, the 81 per cent of agencies that do report top-level risks to the cluster do so with varying frequency. Only 47 per cent of agencies report at least monthly and 39 per cent report quarterly, bi-annually or even less frequently.

Cluster lead agencies should review whether the current timing of risk reporting is sufficient and effective for their risk management of the cluster as a whole.



Source: Provided by agencies (unaudited).

Risk reporting can also improve within agencies

Agencies should document their risk assessments in 'risk registers' that list all of the risks an agency has identified. Ideally, this should work at two levels: enterprise-wide and divisionally. This strengthens risk management by combining a top-down and bottom-up approach.

This year we reviewed how well agencies were managing their risk registers so that key stakeholders can make informed decisions about risk management.

We found that, while all agencies maintain enterprise-wide risk registers, 21 per cent do not underpin it with divisional risk registers. Of those agencies with divisional risk registers:

- 10 per cent of divisional risk registers do not inform enterprise-wide risk registers
- 10 per cent of enterprise-wide risk registers do not inform divisional risk registers.

We also found that:















- three per cent of agencies have not established risk reporting structures that clearly communicate, escalate and monitor risk (internally and externally)
- three per cent of agencies do not involve those charged with governance and key management personnel in developing their enterprise-wide risk registers
- five per cent of agencies do not regularly review their enterprise-wide risk registers
- 24 per cent of enterprise-wide risk registers do not inform corporate planning or divisional planning.

The Treasury has developed a '[Risk Management Toolkit for the NSW Public Sector](#)' that can help agencies develop and implement their risk management processes. It also provides [templates for effective risk registers](#).

The following table summarises our findings on risk registers.

Risk register statistics	Percentage of agencies (%)
Enterprise-wide risk register implemented	100
Regular review of enterprise-wide risk register	95
Reporting of risks at a cluster level	81
Regular reporting of risks at a cluster level	47
An established risk reporting structure	97
Those charged with governance and key management involved in register development	97
Divisional risk registers implemented	79
Divisional risk registers inform enterprise-wide risk registers (bottom up)	90
Enterprise-wide risk registers inform divisional risk registers (top down)	90
Enterprise-wide risk registers inform corporate planning or divisional planning	76

Source: Provided by agencies (unaudited).

		The Department of Finance, Services and Innovation should:				
		<ul style="list-style-type: none"> mandate minimum standards and require agencies to regularly assess and report on how well they mitigate cyber security risks against these standards develop a framework that provides for cyber security training. 				
		Agencies should ensure they adequately resource staff dedicated to cyber security.				
	2.4 Other IT systems	Agencies should consistently perform user acceptance testing before system upgrades and changes. They should also properly approve and document changes to IT systems.				
		Agencies should complete business impact analyses to strengthen disaster recovery plans, then regularly test and update their plans.				
	3. Asset management					
	3.1 Capital investment	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.				
	3.3 Asset disposals	Agencies should have formal processes for disposing of surplus properties.				
		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.				
	5. Ethics and conduct					
	5.1 Ethical framework	Agencies should regularly review their code-of-conduct policies and ensure they keep their codes of conduct up-to-date.				
	5.2 Potential conflicts of interest	Agencies should improve the way they manage conflicts of interest, particularly by: <ul style="list-style-type: none"> 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. 				
		Agencies should improve the way they manage gifts and benefits by promptly updating registers and providing annual training to staff.				
Key		Low risk		Moderate risk		High risk



Appendix two – Status of 2016 recommendations




For a number of years, the Auditor-General has reported on financial control and governance issues as part of our annual reports to Parliament on each sector or cluster. This year, we have brought together our financial controls and governance audit findings into a single volume. This will help Parliament to better understand the finance and governance issues facing the NSW public sector as a whole.








While taking this strategic approach, the Audit Office continues to monitor how well agencies have implemented the recommendations we made in previous years.










This appendix lists the recommendations we made in our 2015–16 volumes for the 39 agencies covered in this report. Of those 53 recommendations, it was pleasing to see that only three have not been addressed at all. The three agencies involved should do so as a high priority.




At the same time, agencies have only fully addressed 32 per cent (17) of last year’s recommendations. This means that most recommendations (33 or 62 per cent) remain partially addressed.









While agencies should carefully review the findings and recommendations of this year’s financial controls and governance report, they should also continue to address the recommendations listed in this appendix.









Recommendation	Current status
Education	
The Department of Education should:	
<ul style="list-style-type: none"> continue efforts to reduce employees’ excess annual leave balances to meet whole-of-government targets 	The number of staff with excess annual leave balances reduced in 2016–17. Each month the Department analyses leave data and excess leave management reporting. It also asks staff to submit leave plans. 
<ul style="list-style-type: none"> consider the effectiveness of workplace health and safety strategies for addressing the rise in psychological injuries. 	Under its Corporate Safety Strategy, the Department continues to implement initiatives and programs to improve health and safety. These programs encompass injury prevention, support and rehabilitation for injured staff. 
Family and Community Services	
The Department of Family and Community Services should:	
<ul style="list-style-type: none"> self-assess its contract management framework against the Audit Office’s ‘Better Practice Contract Management Framework’ have a central contracts register and regularly update it centrally monitor and report on contract compliance. 	The Department has:  <ul style="list-style-type: none"> used the Framework to review and update its procurement management plans developed a central contract register started central monitoring of contract compliance.

Recommendation	Current status
Finance, Services and Innovation	
Agencies should:	
<ul style="list-style-type: none"> strengthen user access to critical financial systems. 	<p>Agencies have addressed some user access issues identified in prior years. But they still need to improve, as we found further access issues during the 2016–17 audits.</p> <p style="text-align: right;"></p>
The Department of Finance, Services and Innovation should:	
<ul style="list-style-type: none"> re-examine the significant transition breakdowns and apply learnings to projects currently being transitioned to the private sector 	<p>The Department has assessed key learnings and started the GovConnect Restart program to enhance the relationship with GovConnect and improve its performance.</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> resolve any transition issues that remain between ServiceFirst and GovConnect immediately 	<p>The Department worked with GovConnect to improve its internal control environment. This avoided repeating the adverse opinion issued the previous year over the payroll process, and led to unqualified opinions for several business processes in 2016–17.</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> develop key performance indicators to measure and assess its risk culture 	<p>In this audit, the service auditor issued qualified opinions on:</p> <ul style="list-style-type: none"> information technology services provided by Infosys the department's SAP system general ledger, payroll and accounts payable business process activities. <p>The Department addressed these issues by 30 April 2017.</p> <p>The Department has developed a benchmarking program to measure and assess its risk culture.</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> review how risk management at an agency level is reported and monitored at the cluster level and introduce a more robust system to collate, manage, identify and escalate risk. 	<p>The Department reports on and monitors risk through the Quarterly Performance Review process, where each agency reports on its risk. The quarterly performance risk report allows each agency to highlight key risks and escalate risks or associated issues to the Secretary.</p> <p style="text-align: right;"></p>
Health	
The NSW Ministry of Health should:	
<p>issue guidance as soon as possible and work with each health entity to determine what should be done with dormant Restricted Financial Assets or funds whose purpose is unclear.</p>	<p>The Ministry issued guidance in October 2017 to help determine what should be done with:</p> <ul style="list-style-type: none"> dormant Restricted Financial Assets funds whose purpose is unclear. <p>The Ministry has asked health entities to report quarterly on the status of applications it has made to use dormant Restricted Financial Assets for other purposes.</p> <p style="text-align: right;"></p>
Industry	
Agencies should:	
<ul style="list-style-type: none"> improve the model for managing conflicts of interest using guidance from ICAC 	<p>Most agencies have addressed this recommendation, including updating their policies and procedures in line with the Public Service Commission's 'Behaving Ethically: a guide for NSW government sector employees' and the guidance from ICAC.</p> <p>Some agencies still need to improve, with one not regularly maintaining its conflicts-of-interest register.</p> <p style="text-align: right;"></p>

Recommendation	Current status	
<ul style="list-style-type: none"> ensure they have an appropriately designed government contracts register that complies with Part 3 Division 5 of the <i>Government Information (Public Access) Act 2009</i> 	Agencies continue to address this recommendation by: <ul style="list-style-type: none"> implementing new procedures to cross-reference contracts with the published GIPA response on e-Tender reconciling registers and finance information monthly implementing a centralised contracts register. 	
<ul style="list-style-type: none"> continue efforts to reduce employee annual leave balances to meet whole-of-government targets. 	Agencies continue to address this recommendation by: <ul style="list-style-type: none"> monthly monitoring and reporting of excessive leave requiring staff with excess leave to submit plans for taking leave. 	
The Department of Industry should:		
<ul style="list-style-type: none"> action internal control issues promptly 	The Department is addressing this recommendation, but some internal control issues remain unresolved.	
<ul style="list-style-type: none"> implement risk management across the cluster 	The Department implemented a revised risk framework as part of its approach to continually improve its risk maturity. Improvements include increasing the links between the cluster's strategic planning and risk frameworks.	
<ul style="list-style-type: none"> sign service agreements with all serviced divisions and agencies. 	The Department has signed agreements with the entities it provides significant services to. These agreements include an annual review process. The Department has completed some simplified agreements for user entities it provides fewer services to. But it is still finalising others.	
The Office of Sport should:		
<ul style="list-style-type: none"> in its capacity as a shared service provider, provide agencies with independent assurance over the operating effectiveness of its controls 	The Office did not give any independent assurance in 2016–17. The Office does not consider itself to be a formal shared service provider as it only provides shared services to agencies within the sport portfolio. And employees of these agencies are employed by the Office.	
<ul style="list-style-type: none"> collect information on purchase orders raised after invoice date and set targets to improve performance 	The Office monitors and follows-up instances where purchase orders are raised after invoice date. However, it does not set targets to improve performance. The Office advised as part of the update of its KPIs, a target will be included and reported against from 2017–18 onwards.	
<ul style="list-style-type: none"> strengthen its asset management by developing: <ul style="list-style-type: none"> both financial and non-financial key performance indicators systems for collecting and monitoring asset management data. 	The Office has partly addressed this recommendation and is implementing key performance indicators.	
The TAFE Commission should:		
<ul style="list-style-type: none"> update, finalise and sign the service level agreement with its shared service provider. 	The Commission changed service providers in 2017 and has a signed service level agreement with the new provider.	

Recommendation	Current status
Justice	
Agencies should:	
<ul style="list-style-type: none"> action management letter recommendations promptly and avoid repeat recommendations 	Agencies continue to address this recommendation, and the number of repeat issues is falling. However, they still need to improve as several issues remain unresolved. 
The Department of Justice should:	
<ul style="list-style-type: none"> establish and finalise service level agreements where it performs finance functions on behalf of independently governed agencies 	The Department has started developing a single, integrated approach to establish service level agreements, covering departmental divisions and relevant external agencies. 
<ul style="list-style-type: none"> implement an overarching risk assessment and treatment plan 	The Department continues to work with cluster agencies, including sharing its enterprise risk management framework and policy and guideline documents. The Department also provides risk forums, oversight and leadership within the cluster. 
<ul style="list-style-type: none"> record, monitor and manage backlog maintenance by individual property 	The Department expects to complete a condition assessment program across most sites, compiled into a management system, by December 2017. 
<ul style="list-style-type: none"> continue to implement risk management across the department 	The Department has progressed this recommendation by:  <ul style="list-style-type: none"> approving and issuing its risk management policy, framework and guidelines developing an online learning module drafting a risk appetite statement, which will be circulated more broadly for comment the Audit and Risk Unit (ARU) supporting divisions in developing their risk registers, and facilitating risk identification and analysis workshops outlining risk reporting and escalation processes in the draft ERM Manual. This includes oversight by management and the ARU, with the Audit and Risk Committee providing an independent assessment.
<ul style="list-style-type: none"> ensure it has systems and controls to effectively maintain, manage and oversight its significant increase in capital projects 	The Department is progressing the implementation of an Enterprise Asset Management System. The Department advises that in 2017–18 it will seek to identify a funding source for full project implementation. 
<ul style="list-style-type: none"> provide annual written certifications to each entity it performs finance functions for 	The Department gave annual certifications to each entity it performed finance functions for. 
<ul style="list-style-type: none"> continue to develop and finalise department and cluster level governance arrangements as a matter of urgency. 	The Department has reviewed its corporate governance arrangements and published new arrangements in the Corporate Governance Framework that is available to all staff. Cluster agencies are encouraged to adopt the principles developed.  The Department is changing its approach to dealing with risk, issues and divisional performance. The Department will create a 'Justice Performance and Assurance' group with a view to increase the level of focus and maturity around enterprise governance.

Recommendation	Current status
Planning and Environment	
Agencies should:	
<ul style="list-style-type: none"> self-assess their contract management processes against the Audit Office's 'Better Practice Contract Management Framework' and address any identified gaps in their frameworks promptly 	<p>Some agencies have not assessed their contract management processes. We recommend our 'Better Practice Contract Management Framework' as a useful self-assessment tool.</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> develop a risk appetite statement to ensure risk tolerance levels are consistently designed and managed and develop key risk indicators to drive risk monitoring and enable prompt escalation, action, reporting and feedback 	<p>Agencies continue to address this recommendation. Some agencies have developed, or are developing, risk appetite statements to underpin enterprise risk management. Where there is no risk appetite statement, agencies are developing risk tolerance levels.</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> ensure contractors declare conflicts of interest on initial engagement document safeguards to manage the conflict and have this approved require staff to disclose secondary employment arrangements, assess the impact on their primary employment and have the arrangement approved ensure a process is in place to update the declarations annually 	<p>Agencies continue to address this recommendation. Some agencies have developed, are developing, or are refreshing policies and procedures.</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> self-assess their fraud control framework against the Audit Office's 'Fraud Control Improvement Tool Kit' and regularly update their fraud policies and procedures 	<p>Agencies continue to address this recommendation, with some agencies still to self-assess their control framework against the tool kit.</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> require contractors to report gifts and benefits offered or received, document this in the gifts and benefits register and assess whether appropriate action has been taken in accordance with the agencies' gifts-and-benefits policy incorporate regular reporting of breaches or potential breaches identified to their executive 	<p>Most agencies have fully addressed this recommendation by enhancing relevant policies and procedures for managing gifts and benefits. One agency still needs to improve its management of gifts and benefits as reporting of breaches is irregular.</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> strengthen management of user access over financial systems. 	<p>Some agencies have addressed user access issues identified in prior years. But some still need to improve, with user access issues remaining unresolved and further issues identified in 2016–17.</p> <p style="text-align: right;"></p>
The Department of Planning and Environment should:	
<ul style="list-style-type: none"> review compliance with the <i>Government Information (Public Access) Act 2009</i> and report the results to its Audit and Risk Committee. 	<p>The Department's Audit and Risk Committee is given regular updates on any non-compliance.</p> <p style="text-align: right;"></p>
Essential Energy should:	
<ul style="list-style-type: none"> identify where instances of alleged fraud and corruption resulted from weaknesses in internal controls, and address the weaknesses. 	<p>Essential Energy engaged an accounting firm to conduct a fraud investigation and as a result, implemented more internal controls to address the identified weaknesses. The progress and implementation status were reported to the Audit and Risk Committee.</p> <p style="text-align: right;"></p>





Recommendation	Current status
The Office of Local Government should:	
<ul style="list-style-type: none"> action management letter recommendations relating to internal control weaknesses promptly, with a focus on addressing repeat issues 	<p>The Office has addressed all management letter recommendations apart the recommendation relating to excessive annual leave. The Office has implemented an active program to reduce excessive annual leave. In 2016–17 excessive leave has reduced but remains an issue.</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> ensure the chief financial officer (CFO) certifies the effectiveness of internal controls before the agency head signs the financial statements. 	<p>The Office has addressed this recommendation.</p> <p style="text-align: right;"></p>
Premier and Cabinet	
The Department of Premier and Cabinet should:	
<ul style="list-style-type: none"> address the issues preventing invoices from being paid on time 	<p>The Department is working with the shared service provider to resolve this issue. The Department has improved in this area by strengthening its processes to allow better management of the flow of invoices to the shared service provider</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> release a revised NSW Public Sector Governance Framework. This should incorporate legislative and policy changes since February 2013 and define roles and responsibilities within the cluster 	<p>The Department has revised the Framework. The draft was presented to Cabinet for approval in October 2017.</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> strengthen procurement processes to ensure purchase orders are approved before goods and services are ordered 	<p>The Department is investigating users who are not complying with policy. It will send identified users a communication outlining what changes they must make to their processes.</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> collect information on purchase orders raised after invoice date and set targets to improve performance 	
<ul style="list-style-type: none"> as an agency using a shared service provider, ensure key performance targets and measures are monitored and reported on 	<p>The monitoring and reporting of key performance targets and measures is now addressed in the Service Performance meeting held with the shared service provider.</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> determine how risk management at an agency level is reported and monitored at the Premier and Cabinet cluster level 	<p>The Department advised it does not have a role in determining how risk management at the agency level is reported and monitored at the cluster level. The Department has no statutory jurisdiction over its cluster agencies. Cluster agencies' risk management frameworks are separate, with their own accountabilities.</p> <p style="text-align: right;"></p>
<ul style="list-style-type: none"> have a compliance management framework, monitor compliance and report breaches to the Audit and Risk Committee. 	<p>The Department has addressed this recommendation, with compliance managed through:</p> <ul style="list-style-type: none"> annual legislative compliance checks financial certification from senior management and the CFO a Governance Lighthouse compliance check risk management internal audit monitoring of recommendations oversight and reporting on delegations. <p style="text-align: right;"></p>

Recommendation

Current status

Transport



Agencies should:

- | | | |
|---|---|---|
| <ul style="list-style-type: none"> continue reviewing the effectiveness of approaches to managing excess annual leave in 2016–17 | <p>Staff continue to have excessive annual leave balances. Agencies advise they have policies to manage this leave, including encouraging managers to discuss this issue with staff and develop leave plans for those with excessive leave.</p> |  |
| <ul style="list-style-type: none"> terminate user access promptly and complete all user reviews so access rights are appropriate | <p>Transport for NSW advised a user access review has been done for every release of the Enterprise Resource Planning (ERP) program into transport agencies. As at 30 June 2017, the ERP program had not been delivered to all transport agencies. The ERP was fully delivered on 1 July 2017.</p> <p>In addition, user access in the Transport Equip (SAP) system is assigned to the position, not the person. So if a user is terminated, the access profile is automatically removed. Segregation of duty checks are also performed each time a new person is assigned to a position with user access.</p> |  |
| <ul style="list-style-type: none"> ensure transparency in the operation of signalling priorities with operators, through the creation of the Transport Asset Holding Entity (TAHE) and the operation of the new Rail Operations Centre in 2018 | <p>Sydney Trains advised that sufficient internal controls and protocols are in place to manage potential conflicts of interest. The creation of the TAHE and the Rail Operations Centre should enhance the transparency of this process.</p> |  |
| <ul style="list-style-type: none"> review project budgets and delivery schedules to address any impact of deferred implementation. | <p>Transport for NSW advised the ERP Program has remained within the allocated budget of \$196.3 million.</p> <p>Transport for NSW closely reviewed the Sydney Trains implementation and found it was within the allocated funding, even with the implementation deferred from January to July 2017.</p> <p>The ERP program was successfully delivered, within budget, to Roads and Maritime Services in July 2016 and NSW Trains in January 2017.</p> |  |

Treasury

These recommendations were made to agencies of the former Finance, Services and Innovation cluster that are now in the Treasury cluster. No recommendations were made to any agency of what was then the Treasury cluster.

Agencies should:

- | | | |
|---|--|---|
| <ul style="list-style-type: none"> develop key performance indicators to measure and assess their risk culture | <p>Agencies continue to work on this recommendation and are developing key performance indicators.</p> |  |
| <ul style="list-style-type: none"> strengthen user access to critical financial systems. | <p>Agencies continue to work on this recommendation. Super user monitoring needs to be strengthened to detect any unauthorised activities. Agencies will review super user activity regularly.</p> |  |

Recommendation**Current status**

Insurance and Care NSW should:

- review the outsourcing risks of the current transformation program to set up a strong risk governance framework and address key outsourcing risks early in the program
- develop a business continuity management policy that is consistent with the group's risk management strategy and framework.

Insurance and Care NSW reviewed its risk management framework and concluded they complied materially with APRA standards.



Insurance and Care NSW has implemented a business continuity management policy.

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



Appendix three – Agencies selected for this volume

NSW agencies by cluster selected for this volume include:

Agency

Education

[Department of Education](#)

Family and Community Services

[Department of Family and Community Services](#)

[New South Wales Land and Housing Corporation](#)

Finance, Services and Innovation

[Department of Finance, Services and Innovation](#)

[Place Management NSW](#)

[Property NSW](#)

[Service NSW](#)

Health

[NSW Health](#)

Industry

[Department of Industry](#)

[Destination NSW](#)

[Forestry Corporation of New South Wales](#)

[Office of Sport](#)

[TAFE Commission](#)

[Water NSW](#)

Justice

[Department of Justice](#)

[Fire and Rescue NSW](#)

[Legal Aid Commission of New South Wales](#)

[NSW Police Force](#)

[Office of the NSW Rural Fire Service](#)

Planning and Environment

[Department of Planning and Environment](#)

[Essential Energy](#)

[Hunter Water Corporation](#)

[Landcom](#)

[Office of Environment and Heritage](#)

[Office of Local Government](#)

[Sydney Water Corporation](#)

Agency

Premier and Cabinet

[Department of Premier and Cabinet](#)

Transport

[NSW Trains](#)

[Rail Corporation New South Wales](#)

[Roads and Maritime Services](#)

[Sydney Trains](#)

[Transport for NSW](#)

[WCX M4 PTY Limited](#)

[WCX M5 PTY Limited](#)

Treasury

[Crown Finance Entity](#)

[Insurance and Care NSW](#)

[Lifetime Care and Support Authority](#)

[NSW Treasury Corporation](#)

[NSW Self Insurance Corporation](#)

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

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