

Results of audit: Internal control systems 2014–15

Report 1: 2015–16



Queensland Audit Office

Location Level 14, 53 Albert Street, Brisbane Qld 4000

PO Box 15396, City East Qld 4002

Telephone (07) 3149 6000

Email qao@qao.qld.gov.au

Online www.qao.qld.gov.au

© The State of Queensland. Queensland Audit Office (2015)

Copyright protects this publication except for purposes permitted by the *Copyright Act 1968*. Reproduction by whatever means is prohibited without the prior written permission of the Auditor-General of Queensland. Reference to this document is permitted only with appropriate acknowledgement.



Front cover image is an edited photograph of Queensland Parliament, taken by QAO.

ISSN 1834-1128

Your ref:
Our ref: 10675



July 2015

The Honourable P Wellington MP
Speaker of the Legislative Assembly
Parliament House
BRISBANE QLD 4000

Dear Mr Speaker

Report to Parliament

This report is prepared under Part 3 Division 3 of the *Auditor-General Act 2009*, and is titled
Results of audit: Internal control systems 2014-15.

In accordance with s.67 of the Act, would you please arrange for the report to be tabled in
the Legislative Assembly.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Andrew Greaves', is written over a light blue horizontal line.

Andrew Greaves
Auditor-General

Contents

Summary	1
Conclusions	1
Internal control	2
Queensland Shared Services	3
Internal financial management reporting	3
IT disaster recovery planning	4
Recommendations	4
Reference to comments	5
1. Context	7
Internal control framework	7
Management responsibilities	8
Audit objective, method and cost	9
Report structure	11
2. Financial controls	13
Background	14
Conclusions	14
Overall assessment	15
Control environment	17
Risk management	18
Control activities	19
Information and communication	20
Monitoring of controls	21
Outsourced service provision	21
3. Internal financial management reporting	23
Background	24
Audit objectives	25
Conclusions	26
Summary of findings	30
Opportunities for improvement	30
Right people	31
Right information	34
Right time	37
4. IT disaster recovery planning	41
Background	42
Audit scope	43
Conclusions	43
Summary of findings	44
Recommendations	45

Appendix A— Comments	49
Appendix B— Principles of an integrated system of financial control.....	59
Appendix C— Update on prior year control deficiencies	60
Appendix D— Better practice—Types of information in dashboard reporting.....	61
Appendix E— Assessing internal financial management reporting	64
Appendix F— Assessing disaster recovery planning.....	65
Appendix G— Department acronyms.....	66
Appendix H— Glossary	67

Summary

As the accountable officers, the Director-General of each department and the chief executives of Queensland government agencies are legally responsible for establishing and maintaining effective financial controls throughout the financial year.

This report summarises the results of our evaluations of the systems of financial control and our selective testing of the internal controls that operated within the 21 government departments during the 2014–15 financial year.

This year we scrutinised the effectiveness of internal financial management reporting in greater depth. Measurement and monitoring of financial performance is one of the most important management controls directed primarily towards ensuring each department is achieving its organisational objectives.

We also examined the disaster recovery planning used in four departments to recover their computer systems after a disruptive event, such as floods or power outages. A disaster recovery plan is a set of procedures to assist in the recovery of an agency's infrastructure and data in the event of a disaster or significant business disruption. This is a topical issue, given the weather events across Queensland in the recent past.

Conclusions

The internal financial controls in most departments continue to strengthen, as indicated by the reduction in the number of internal control issues we identified in the current year compared to the last two years. Most departments have actively reduced the risk of material misstatements occurring in their external financial reports, whether due to fraud or error, against prior years. We recognise the efforts of these departments to bring about improvement.

We found that in two departments the number of internal control issues increased. This indicates that their internal controls were less effective in reducing financial reporting risk than their peers and a focused effort by these departments is required to strengthen internal controls.

Internal financial management reporting is generally operating as an effective management control supporting strategic decision-making and internal financial control. The opportunity exists for departments to improve efficiency in collection, analysis and presentation of information through better use of technology and by adopting recognised better reporting practices.

After the 2010–11 Queensland floods and the 2014 world leaders' summit in Brisbane (G20), we expected to find departments improving or have a mature capability to prepare for or recover from disasters. Our review of four departments questions the validity of this premise. While two of the four departments we audited have approved and tested Information Technology (IT) disaster recovery plans in place, the remaining two departments cannot be confident that they will restore their critical functions within acceptable timeframes for government service delivery in the case of a disruptive event.

Internal control

We found 44 control deficiencies in our 2014–15 audits of departments representing three broad themes and opportunities for improvement.

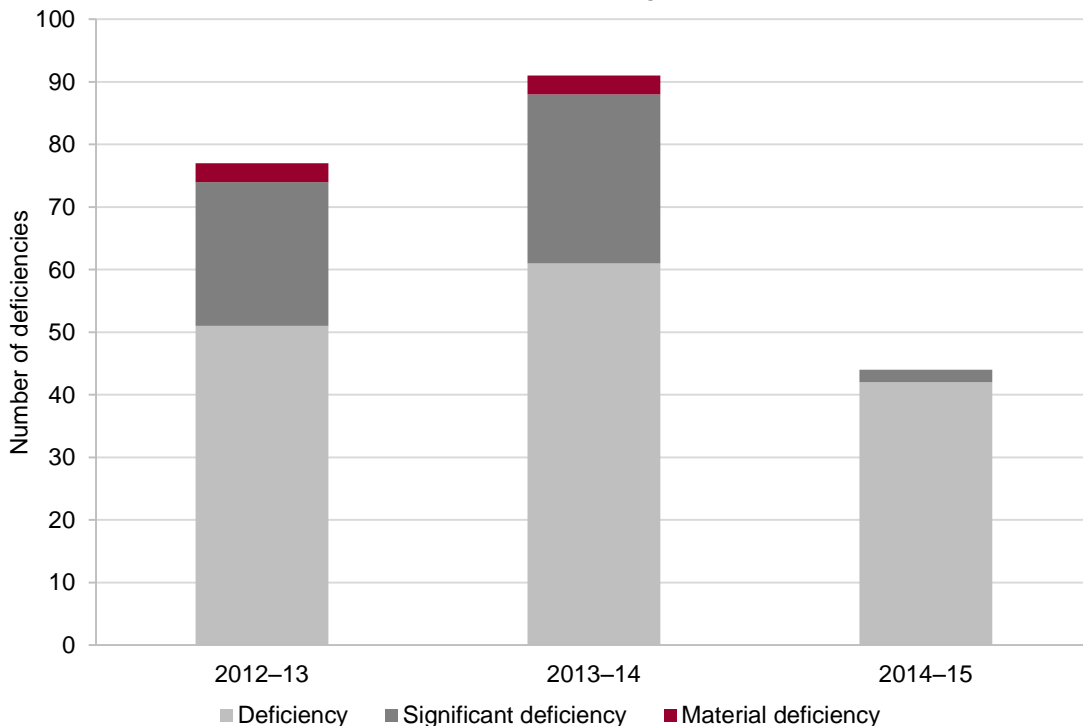
Figure A
Control deficiency themes in departments

Inconsistently applied controls	Information systems weaknesses	Monitoring of payroll
Controls not being applied consistently to all transactions which they are designed to cover—this reduces the effectiveness of the control in preventing or detecting misstatements.	Information system weaknesses relating to user access management—these weaknesses increase the risk of users having access to system functions beyond their work requirements, enabling the users to modify system data inappropriately and perpetrate fraud.	Inadequate monitoring and review of payroll information such as salaries, allowances, timesheets and overtime—this increases the risk of incorrect payments made to employees, inaccurate employee entitlement balances and fictitious employees.

Source: Queensland Audit Office

Figure B illustrates the change in the number of control deficiencies we identified across all departments for 2014–15 compared to the previous two financial years, excluding deficiencies found at Queensland Shared Services.

Figure B
Control deficiencies in departments



Source: Queensland Audit Office

We found an overall decrease in the number and severity of internal control issues in the current year compared to the previous two years and no serious control deficiencies that may lead to a material misstatement of financial reports.

In addition, 17 control deficiencies identified in the prior year have been re-raised, remain unresolved or management are still undertaking corrective action. Information security control weaknesses identified last year are still prevalent across multiple departments, in particular:

- poor management of user accounts with broad access to all system transactions
- users having inappropriate access to sensitive or restricted transactions
- inadequate monitoring and review of user activities.

Ninety-four per cent of financial delegation issues and 63 per cent of risk management matters identified in area of control focus reviews have been resolved. The only remaining significant deficiency relates to a lack of segregation of duties in one department's purchasing system due to self-approval privileges.

Matters outstanding for risk management relate to the integration of risk management with the department's strategic and operational planning. Since conducting our audits departments have improved their monitoring of risks and risk treatments. We will continue to follow up with departments on these matters.

Queensland Shared Services

Queensland Shared Services (QSS) facilitates a range of corporate services for 19 departments. These services include finance and payroll processing and the maintenance of related information technology systems. QSS has identified financial reporting risks and documented a total of 29 control objectives to address those risks. We assess the design and effectiveness of their related controls each year.

The overall QSS control environment is suitably designed within the constraints of the IT systems that it operates. Two of the (Lattice) payroll systems are well overdue for replacement and have inherent system limitations so that some key controls cannot be implemented.

This year we assessed the QSS control environment as being effective, with 28 of its 29 internal control objectives being met. The control objective relating to managing privileged access was not achieved. Management has agreed with our audit recommendations and has plans to remedy all issues within reasonable time frames.

An issue continues in relation to QSS processing transactions for 11 departments using outdated finance systems. These systems may not be able to cope if there is major change to business or legislation. QSS limits the number of system changes to reduce the likelihood of system failure. With the exception of this issue, all prior year issues identified at QSS in 2013–14 have been resolved.

Internal financial management reporting

Departments have established management reporting practices that ensure the right information is provided to the right people at the right time. This allows managers to track performance and make informed decisions to achieve the department's objectives.

While the internal financial management reporting frameworks are satisfactory, our audits identified a number of improvement opportunities in relation to report content, compilation, policies and processes.

Figure C
Improvement opportunities for management reporting

Continuous improvement	Better leverage technology solutions	Combine financial and non-financial information
<p>Embed a continuous review approach to reporting practices to ensure that they remain relevant, efficient and effective. An initial area of focus is the review and streamlining of month-end activities.</p>	<p>Investigate modern technology solutions to aggregate and integrate legacy system information. This will provide greater automation and accuracy of reporting.</p>	<p>Use dashboards to combine and visualise key financial and non-financial performance data. This will enable each agency to concisely and holistically track its performance in achieving service delivery objectives.</p>

Source: Queensland Audit Office

IT disaster recovery planning

We found notable gaps in the readiness of two of the four departments we reviewed to recover from a disaster based on their level of planning.

Two departments have IT disaster recovery plans that are based on a business impact analysis, defined roles and responsibilities, and are reviewed and tested annually. However, one of these departments does not have formal processes to ensure their third party infrastructure provider performs regular testing. Not all of the business units in the second department specified the maximum time to recover the IT systems.

The remaining two departments do not have complete, up-to-date, approved and tested disaster recovery plans. There is no assurance that these departments will be able to recover their information within acceptable time frames in the event of a disruption.

Recommendations

The control matters raised in this report have been represented separately to each department as required by auditing standards. We expect that each department will take remedial action where weaknesses and areas for improvement have been identified. Our recommendations on disaster recovery planning apply to all government departments, not just the four departments that were assessed in this report.

Where not already occurring, all departments should:

1. update and approve disaster recovery plans based on business impact, providing oversight and co-ordination for all business areas
2. define disaster recovery targets for all business units
3. increase the frequency of disaster recovery testing to twice yearly
4. obtain and monitor periodic reports on disaster recovery testing (including those from service providers where applicable)
5. use emerging technology to expand their options in providing cost-effective backup and disaster recovery testing
6. develop a plan to improve the maturity of the disaster recovery program, and manage to that plan.

Reference to comments

In accordance with s.64 of the *Auditor-General Act 2009*, a copy of this report was provided to all of the departments within the scope of this report with a request for comments.

Their views have been considered in reaching our audit conclusions and are represented to the extent relevant and warranted in preparing this report.

The comments received are included in Appendix A of this report.

1. Context

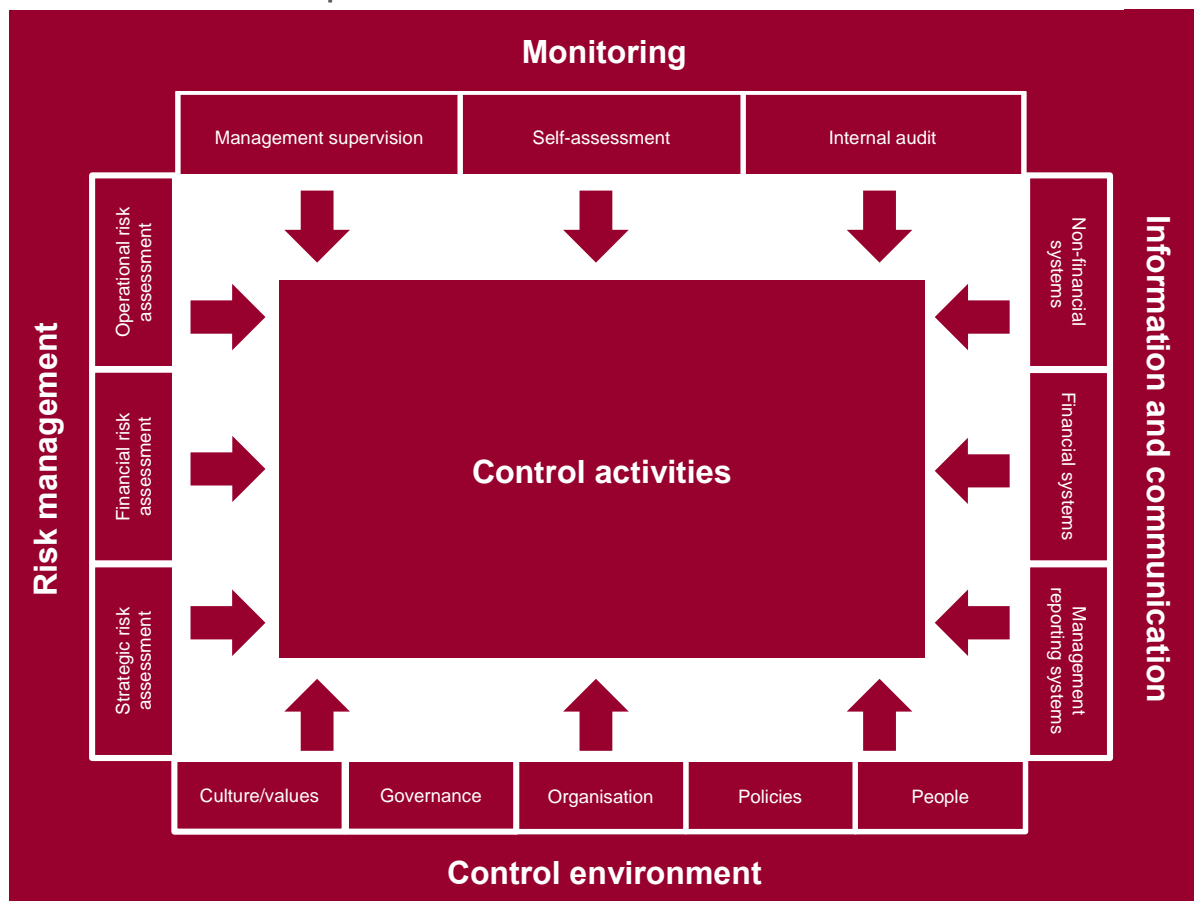
Internal control framework

Financial controls are processes (including policies, procedures and systems) that are established, operated and monitored by the management of a department to provide reasonable assurance on the achievement of its objectives in the following categories:

- the effectiveness and efficiency of their operations
- the reliability of their internal and external financial reports
- their compliance with applicable laws, regulations and policies
- the safeguarding of department assets.

We assess financial controls using the Committee of the Sponsoring Organisations of the Treadway Commission (COSO) internal controls framework, which is widely recognised as a benchmark for designing and evaluating internal controls. All of the components identified in Figure 1A need to be present and operating together effectively as an integrated system of financial controls. When this is the case, departments reduce the risk of not achieving their objectives.

Figure 1A
Components of an internal control framework



Source: Queensland Audit Office adapted from *Internal Control: Integrated Framework—Committee of Sponsoring Organizations of the Treadway Commission (COSO)*, American Institute of Certified Public Accountants, 2011

The five core elements of an integrated system of financial controls are:

- **Control environment**—management’s actions, attitudes and values that influence day-to-day operations. Control environment factors include management’s integrity and operating style, departmental culture and values, organisational structure, the assignment and delegation of authority, and processes for obtaining and developing qualified and skilled employees.
- **Risk management**—management’s processes for considering risks to achieving the department’s objectives and for forming a basis as to how the risks should be identified, assessed and managed.
- **Control activities**—the implemented policies and procedures that help ensure management directives are carried out and that necessary actions are taken to address identified risks. Control activities operate at all levels and in all functions. They include activities such as approvals, authorisations, verifications, reconciliations; reviews of operating performance; securing of assets; and segregation of incompatible duties and IT controls including establishment and testing of disaster recovery plans.
- **Information and communication**—those systems used to provide information in a form and time frame that allows employees to discharge their responsibilities and the ways that control responsibilities are communicated throughout the department. This aspect of internal control also considers how management generates financial reports and how they are communicated to internal and external parties to support the functioning of internal controls.
- **Monitoring of controls**—the methods management employs to oversee and assess whether internal controls are present and operating effectively. This may be achieved through ongoing supervision, periodic self-assessments and separate evaluations. They also concern the evaluation and communication of control deficiencies in a timely manner to effect corrective action.

The five core elements of the internal control framework can be further broken down into 17 key principles. These principles are listed in Appendix B.

Management responsibilities

Section 61 of the *Financial Accountability Act 2009* (FAA) states that accountable officers and statutory bodies are to:

- ensure the operations of the department or statutory body are carried out efficiently, effectively and economically
- establish and maintain appropriate systems of financial controls.

Section 8 of the *Financial and Performance Management Standard 2009* (FPMS) requires departments and statutory bodies to establish cost effective internal control structures.

An effective system of financial controls will help to ensure:

- financial records and related information are complete and accurate
- assets are safeguarded
- errors and other irregularities are prevented or detected and corrected.

The FAA and the FPMS also detail the obligations that each accountable officer and statutory body has in the preparation of the agency’s financial statements and presentation of those statements to the Auditor-General for audit.

The system of financial controls underpins the information presented in the annual financial statements and helps to ensure these statements give a true and fair view of the agency’s transactions and financial position for each financial year.

Audit objective, method and cost

Audit objective

The primary objective of our financial audits, as identified in the Auditor-General of Queensland Auditing Standards (incorporating the Australian Auditing Standards), is to provide independent assurance to parliament and the community that the information contained in each financial statement is, in all material respects:

- free of misstatement, whether due to fraud or error
- presented fairly in accordance with applicable accounting standards and legislative requirements.

The findings detailed in this report focus principally on selective financial controls testing and our evaluations of elements of the integrated financial control framework across the range of financial audits we perform for public sector entities.

Audit methodology

Internal financial controls operate to produce reliable financial information and ensure compliance with prescribed requirements. Consequently, we are required to consider their effectiveness as part of our annual audit of each department's financial statements.

This involves us considering the way management runs the department, the control environment, and the design and implementation of relevant controls.

Our assessment of each department's overall internal controls during our audit planning stage assists us in determining the nature, timing and extent of testing procedures to be performed at our interim and final audit stages.

The particular controls we test in each cycle depends on the risks pertaining to that cycle, the strength of the department's control environment and the strategy we adopt to achieve an efficient and effective audit. Cycle level controls are those controls which operate in specific transaction classes such as revenue, expenditure or payroll.

Sometimes, cycle level transactions are processed by an external service provider. Where applicable, the controls over the processing of those transactions need to be considered as part of our assessment of the department's internal controls.

If, in our professional judgement, we determine that the department or the service provider's controls are not well designed, that any of the controls did not operate as intended, or that controls should be in place but are missing, we are required by the auditing standards to communicate these deficiencies to management. We assign a risk category to the financial control deficiencies we raise so management can gauge relative importance and prioritise for remedial action.

Figure 1B
Risk categories for financial control deficiencies

Risk category	Client impact	Prioritisation of remedial action
Material deficiency	A significant deficiency that will lead to a material misstatement of the financial report and will result in a qualified audit opinion if not corrected	Requires immediate management action
Significant deficiency	A deficiency or combination of deficiencies that may lead to a material misstatement of the financial report	Requires prompt management action to resolve within two months
Deficiency	The control is not working or non-existent and, therefore, will not prevent, detect or correct misstatements in the financial report	Requires a management action plan in the same reporting period
Other matters, including improvement opportunities	Matters relevant to those charged with governance but not related to deficiencies in internal control	Implemented at management's discretion

Source: Queensland Audit Office

We have used the risk categories in Figure 1B from 1 July 2014. Prior year issues have been reclassified in accordance with this methodology for comparison.

Financial control deficiencies that we categorise as material or significant must be communicated in writing to those charged with the governance of the department due to the potential for material misstatement. Other financial control deficiencies and matters are generally communicated directly to line management and reported.

Section 60 of the *Auditor-General Act 2009* requires the Auditor-General to draw attention to any case in which the functions relating to the financial management of the public sector agency were not performed adequately and properly. By reporting on the significant control deficiencies we observed in departmental financial control systems, we have satisfied these requirements.

Audit cost

The cost of financial audits is billed directly to each relevant department. The cost of preparation of this report was \$155 000.

Report structure

The remainder of the report is structured as follows:

- Chapter 2—summarises the results of our initial control evaluations and of our selective testing of the financial reporting controls that existed within the 21 government departments that operated during the 2014–15 financial year. These departments represent the bulk of the general government sector revenues and expenses.
- Chapter 3—reports on internal financial management reporting, which is a critical component of a department's internal control framework. This chapter includes the results of our evaluations of whether the 21 departments have established effective financial reporting frameworks that are tailored to the varying needs of tiers of management.
- Chapter 4—examines four departments' information technology disaster recovery plans, processes and procedures to ascertain that they are in place, up to date and tested.
- Appendix A contains responses received to this report prior to publishing by impacted departments.
- Appendix B includes a description of the five components and 17 principles of an integrated system of financial controls.
- Appendix C provides an update on prior year control deficiencies.
- Appendix D provides better practice information used in departmental internal financial management dashboard reporting.
- Appendix E includes a checklist to help departments assess their own internal financial management reporting.
- Appendix F includes a checklist to help departments assess their own disaster recovery planning.
- Appendix G provides a list of the departments included within the scope of this report.
- Appendix H contains a glossary of terms used in this report.

2. Financial controls

In brief

Background

Financial controls are integral to reliable financial reporting. A sound control environment with processes that are established, operated and monitored by the management of a department provides reasonable assurance about:

- achievement of the department's financial objectives
- compliance with applicable legislation
- the accuracy and fair presentation of their financial reporting.

As part of our financial audit, we assess the design and operating effectiveness of selected key internal controls within the financial control framework. We raise any weaknesses which may require corrective action with the department's management.

Conclusions

The internal financial controls in most departments continue to strengthen, as indicated by the reduction in the number of internal control issues we raised in the last three years. Most departments have actively reduced the risk of material misstatements occurring in their external financial reports, whether due to fraud or error, against prior years. We recognise the efforts of most departments to bring about these improvements.

However, we found that in two departments the number of internal control issues increased. This indicates that their internal controls were less effective in reducing financial reporting risk than their peers and a focused effort is required in these departments to strengthen internal controls.

Findings

- Our 2014–15 audits identified 44 deficiencies, including two significant deficiencies. We found no material deficiencies this year. Thirteen agencies had a reduction in deficiencies identified compared to the prior year.
- Controls over departments' financial systems operated by Queensland Shared Services have significant weaknesses relating to the provision of privileged user access to appropriate persons and monitoring of such access. We also noted similar deficiencies in the departments which do not primarily rely on Queensland Shared Services for their financial systems.
- Eleven departments are still using outdated financial systems that no longer have vendor support.
- Departments have implemented improvements in financial delegations arising from last year's audit.
- A number of departments have not been timely in their resolution of risk management matters. The main area of unresolved matters is the integration of risk management into strategic and operational planning processes.
- Six departments are not effectively monitoring and reviewing payroll information and one department has multiple deficiencies affecting the accuracy and completeness of payroll data processing.

Background

For departments to achieve their service delivery objectives, management need to establish effective financial control processes including policies, procedures and systems.

The findings detailed in the following sections focus principally on selective financial controls testing and our evaluations of elements of the integrated financial control framework across the range of financial audits we perform for public sector entities.

Conclusions

The risk of undetected fraud or error within financial systems and departments' financial reporting decreased in 2014–15 based on improvements by departments to their financial internal control systems. We found strengthening of the overall control environment and fewer and less severe control deficiencies through our audits.

Common themes in those departments that do not have strong overall control environments and opportunities for further strengthening are:

- the impact of organisational change and restructuring on the control environment and control activities
- weaknesses in the information technology (IT) control environment
- delays in correcting control deficiencies identified in previous audits
- design weaknesses in controls associated with expenditure, payroll, fixed assets and IT.

Of the 44 control deficiencies we identified in 2014–15 audits, we found that generally departments have developed sound frameworks for the components that support an internal control system. There is an opportunity for departments to ensure that the control activities themselves are implemented and operating consistently and effectively across all transactions.

We found that deficiencies remain in information systems security across most departments, particularly in the management of user accounts that have broad access to sensitive system functions and transactions. The nature of these information system deficiencies makes error and fraud more difficult to prevent and detect.

In addition, 11 departments continue to use outdated finance systems which no longer have vendor support. This can have a material impact on the effectiveness and efficiency of operations—including compliance with regulations, and the reliability, accuracy and timeliness of financial reporting.

Some information system deficiencies have also been reported in prior years. While some issues are in the process of being resolved, it is of concern that similar issues continue to arise each year.

Our selective controls testing also found that:

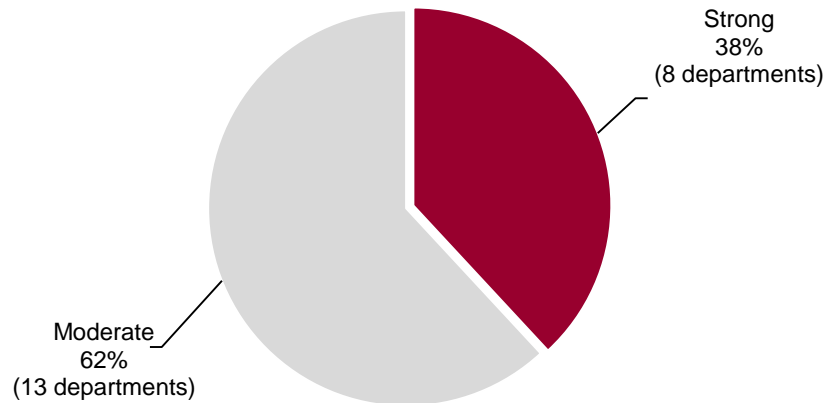
- two departments were not following up debts in a timely manner
- one department had not followed proper procurement practices and could not demonstrate probity and value for money for some of its purchases
- six departments were not effectively monitoring and reviewing payroll information
- one department had multiple deficiencies around the inconsistent application of payroll processing controls that ensure the accuracy and completeness of payroll data.

Departments have made satisfactory improvements to their systems of financial delegations as a result of our area of control focus audit last year. Some departments are still in the process of implementing risk management improvements, especially relating to integrating risk management with their strategic and operational planning.

Overall assessment

Based on our preliminary planning procedures, we assessed the 21 departments have moderate or strong overall internal controls. The results are summarised in Figure 2A. We found there has been an improvement from 2013–14 where 33 per cent of departments were assessed as strong.

Figure 2A
Overall control assessment of departments



Source: Queensland Audit Office

In departments with strong overall internal controls, we observed good governance practices, a high level of integrity and experience displayed by senior management, effective organisational structures and lines of authority, and a proactive approach to monitoring and improving internal controls.

In departments which were assessed as moderate, common issues and opportunities for improvement so they can move to a strong assessment include:

- Issue: a high level of organisational change and restructuring occurring in some departments with impacts on the control environment and control activities. Opportunity: consider the impact on governance arrangements, delegations of authority and policies when implementing organisational change and restructuring.
- Issue: weaknesses in the IT controls. Opportunities: consider the IT control deficiencies identified in this report; ensure that system administration functions and other user profiles are restricted to be commensurate with job responsibilities; and establish appropriate monitoring and review of administrator activities.
- Issue: delays in correcting control deficiencies identified in previous audits. Opportunity: audit committees should monitor the implementation of audit recommendations from both internal and external audit and hold management accountable for timely resolution.
- Issue: design weaknesses in cycle level controls associated with expenditure, payroll, fixed assets and IT. Opportunity: the FPMS requirements for the Chief Financial Officer (CFO) certification specifies that there should be a continuous assessment of financial reporting risks and those controls established to mitigate them throughout the whole financial year. Design weaknesses need to be identified early to ensure risk of misstatement of financial statements error is mitigated.

Findings from controls testing

As at 10 June 2015, we reported to management 44 new control deficiencies arising from our 2014–15 audits, including area of control focus reviews. This is a decrease from the same period in the prior two years both in the number and severity of deficiencies. We found no material deficiencies this year.

Figure 2B depicts the number and severity of deficiencies identified each year and the number of departments with deficiencies.

Figure 2B
Control deficiencies by risk rating

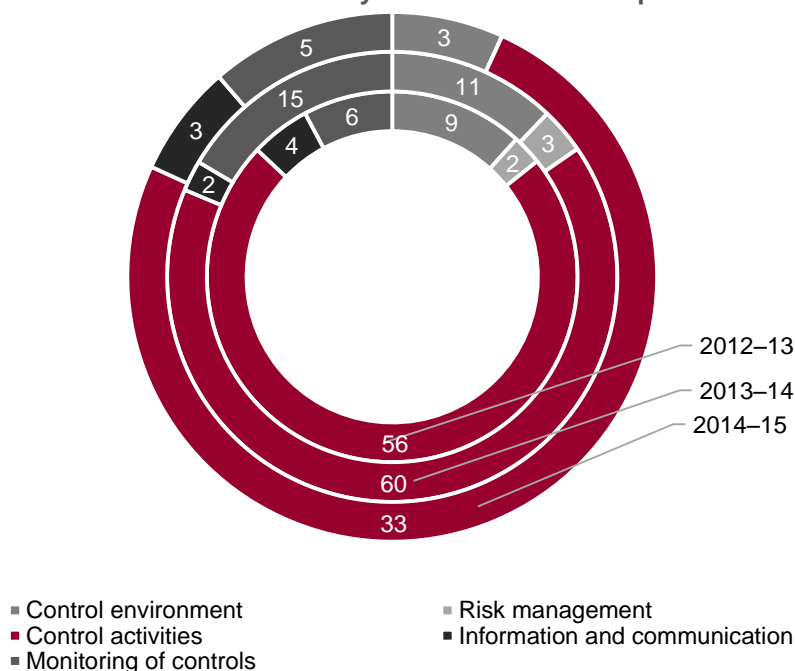
	2012–13 No. of departments	2012–13 No. of issues	2013–14 No. of departments	2013–14 No. of issues	2014–15 No. of departments	2014–15 No. of issues
Material deficiency	3	3	1	3	0	0
Significant deficiency	11	23	9	27	2	2
Deficiency	13	51	18	61	13	42
Total		77		91		44

Note: The control deficiencies reported do not include issues arising from our testing of controls at Queensland Shared Services (QSS).

Source: Queensland Audit Office

Figure 2C shows internal control deficiencies raised in 2014–15 compared with the previous two financial years, by COSO component. Deficiencies in control activities continue to form the majority of issues we raised this year. This suggests that departments have generally developed sound frameworks for all components that support an internal control system, but the controls themselves are not always implemented or operating consistently and effectively.

Figure 2C
Control deficiencies by internal control component



Source: Queensland Audit Office

Seventeen control deficiencies identified in the prior year have been re-raised, remain unresolved or management are still undertaking corrective action. Control activities deficiencies arising from information security control weaknesses are still prevalent across multiple departments.

Each year, when following up on prior year audit issues, we confirm whether departments are addressing control deficiencies identified by audit in a timely manner. The status of prior year audit issues is reported in Appendix C.

Control environment

The control environment components of an internal control framework are shown in Figure 2D.

Figure 2D
Control environment within an internal control framework

Control environment				
Culture/values	Governance	Organisation	Policies	People

Source: Queensland Audit Office (extract from Figure 1A)

The audits of the control environment in the current year identified three deficiencies and no significant deficiencies.

Financial delegations

In 2013–14 we performed an in-depth review of financial delegations. Controls in relation to financial delegation operates across all components of a system of internal control. Our review included the delegations framework (COSO principle 3), the actual operation (COSO principle 12) and monitoring of delegations (COSO principle 16).

We found that financial delegations across all departments were well aligned with their organisational structures and were articulated clearly. Overall, the use of financial delegations was effective and in accordance with policies and procedures.

We recommended improvements around monitoring of financial delegations for nine departments. One department is still in the process of implementing our recommendations. We also identified 13 instances of actual non-compliance with financial delegations across six departments in the prior year. The departments concerned have since taken action, including training of staff and updating of policies and procedures to reduce the risk of future breaches. We can confirm that departments' controls have improved, as we only found one new deficiency in one department relating to breach of financial delegations this year.

In 2013–14, we also highlighted a number of limitations with manual authorisation of expenditure, compared to automated approvals in the system. This year, we have confirmed that QSS has continued its efforts to implement eForms for processing direct invoices, which are now being used at 10 departments (COSO principle 12).

All significant deficiencies identified for financial delegations have been resolved, except for a lack of segregation of duties in one department's purchasing system due to self-approving privileges.

Risk management

The risk management components of an internal control framework are shown in Figure 2E.

Figure 2E
Risk management within an internal control framework



Source: Queensland Audit Office (extract from Figure 1A)

We found no new control deficiencies related to risk management in 2014–15.

Last year, we conducted a deeper review through an area of control focus audit on this component. We had found that all departments' risk management frameworks and processes for identifying and mitigating risks met the minimum requirements of the *Financial Accountability Act 2009*. However, a number of matters raised as a result of our review remain unresolved, including the ineffective integration of risk management with the department's planning processes (COSO principle 6) and deficiencies around risk register and the risk identification and response process (COSO principle 7).

We also identified risk monitoring processes (COSO principle 16) were not fully effective in 17 departments. Fourteen departments have improved their monitoring of risks during the current financial year by implementing measures such as:

- incorporating more discussions of risk management on agendas at senior management committee meetings
- assigning responsibility for ownership of risks and associated risk status updates
- having more regular reviews of risk registers by audit and risk committees, risk sub-committees and senior management.

Last year, we also found that seven departments had not effectively integrated risk management into their strategic and operational planning processes (COSO principle 6). Five of these departments are still working on our recommendations.

Figure 2F summarises the outstanding matters which audit is continuing to work with management to resolve.

Figure 2F
Outstanding prior year risk management matters



Source: Queensland Audit Office

Control activities

This year, we tested departments' control activities over the following areas:

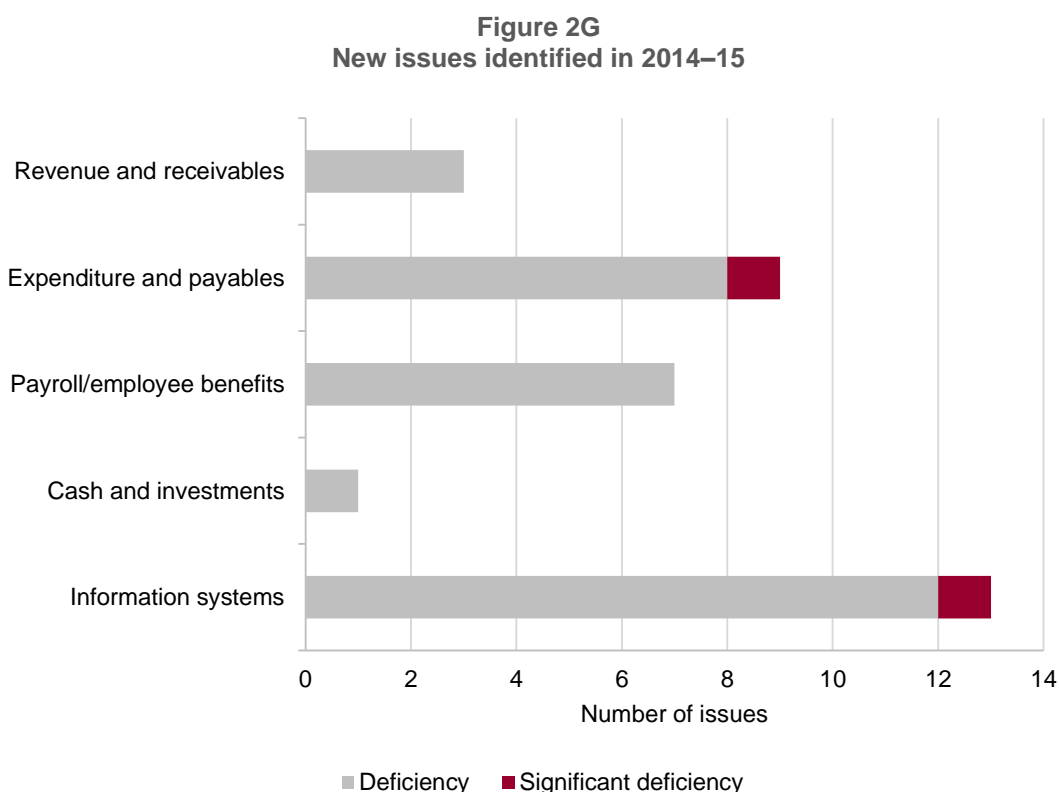
- revenue and receivables for six departments
- expenditure and payables for 20 departments
- payroll and employee benefits for 16 departments
- cash and financing for 14 departments
- fixed assets (property, plant and equipment) for five departments
- IT general controls for all 21 departments; this includes controls tested at Queensland Shared Services (QSS) on systems affecting multiple departments.

In summary, we noted multiple deficiencies in complying with all three COSO principles relating to the control activities component. These included the following:

- some departments do not have in place appropriate control activities to address risks of error or fraud (principle 10)
- some departments have weaknesses in their IT general controls (principle 11)
- some departments have designed appropriate control activities, but have not properly deployed them consistently and effectively in operation (principle 12).

We found deficiencies across eight departments relating to principle 12, where properly designed controls are not operating effectively in practice. It is the responsibility of management to ensure that the controls are defined in policies and procedures, and clearly communicated to staff so they are aware of their responsibilities. Monitoring activities are also important to allow management to review whether controls are functioning properly and to identify any deficiencies.

Figure 2G depicts the numbers and types of deficiencies in control activities identified this year across the 21 departments.



Source: Queensland Audit Office

Revenue and receivables

In revenue and receivables testing, we identified that two departments had failed to follow up debts in a timely manner. For one of the departments, the volume and amount of outstanding debts were significant. This deficiency increases the likelihood of financial losses should those debts become unrecoverable.

Expenditure and payables

We found a significant deficiency in one department where there were multiple departures from proper procurement practices. These departures included instances of insufficient quotes being obtained, lack of market research to identify suitable contractors, lack of documentation to support the decisions made when awarding contracts, and payments being made to contractors before the contracts were formally signed. As a result, the department was unable to demonstrate probity and value for money for some of its purchases.

Payroll and employee benefits

The common theme in payroll deficiencies relates to review of payroll information in four departments, such as fortnightly salary and allowance reports. One of these issues was a significant deficiency still unresolved from the prior year. One additional department had multiple instances where established payroll controls are not being performed consistently. The controls relate to processing of new starters, payroll master data, separations, rosters and ad hoc payroll payments. These deficiencies increase the risk of inaccurate and incomplete payroll records.

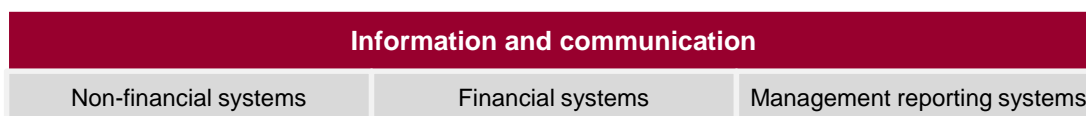
Information systems

The significant number of information systems issues highlighted weaknesses in the management and monitoring of privileged accounts (that is, accounts that give users broad access to system transactions), inappropriate system access assigned to users, and incomplete logging of transactions. Section on *Outsourced service provision* on page 21 details similar issues from our testing of systems operated by QSS. In addition, deficiencies were identified from a review of disaster recovery planning. This is discussed in detail in Chapter 4.

Information and communication

The information and communication components of an internal control framework are shown in Figure 2H.

Figure 2H
Information and communication within an internal control framework



Source: Queensland Audit Office (extract from Figure 1A)

Overall, departments have sound financial systems which provide timely and relevant information to support their operation of internal controls and preparation of financial reports. Minor deficiencies were identified however no common themes emerged.

Our area of control focus audit on internal financial monthly reporting also confirmed these findings. Refer to Chapter 3 for the key findings.

Monitoring of controls

The monitoring components of an internal control framework are shown in Figure 2I.

Figure 2I
Monitoring within an internal control framework

Monitoring		
Management supervision	Self-assessment	Internal audit

Source: Queensland Audit Office (extract from Figure 1A)

While the majority of departments have suitable monitoring activities, we noted deficiencies in two departments where there is insufficient monitoring of payroll controls around overtime, timesheets and fortnightly payments. One issue relates to a significant deficiency identified in the prior year which is still unresolved. Without effective monitoring of these controls, the risk of overpayments to employees is increased. Further, excessive overtime may result in staff fatigue and loss of productivity.

Outsourced service provision

QSS provides a range of services to 19 departments. These services include IT management, finance and payroll services. QSS does not provide these services to the Department of Health and the Department of Education and Training.

QSS provides assurance over its control environment to these departments and their auditors. This is through an audited controls report in line with the Australian Auditing Standard ASAE 3402 *Assurance Reports on Controls at a Service Organisation*. QAO is engaged each year by QSS to provide assurance over the design and operating effectiveness of control activities to achieve those control objectives for the period 1 July to 31 March.

In all material respects, QSS has designed its internal control activities to meet the required control objectives and has achieved 28 of its 29 control objectives.

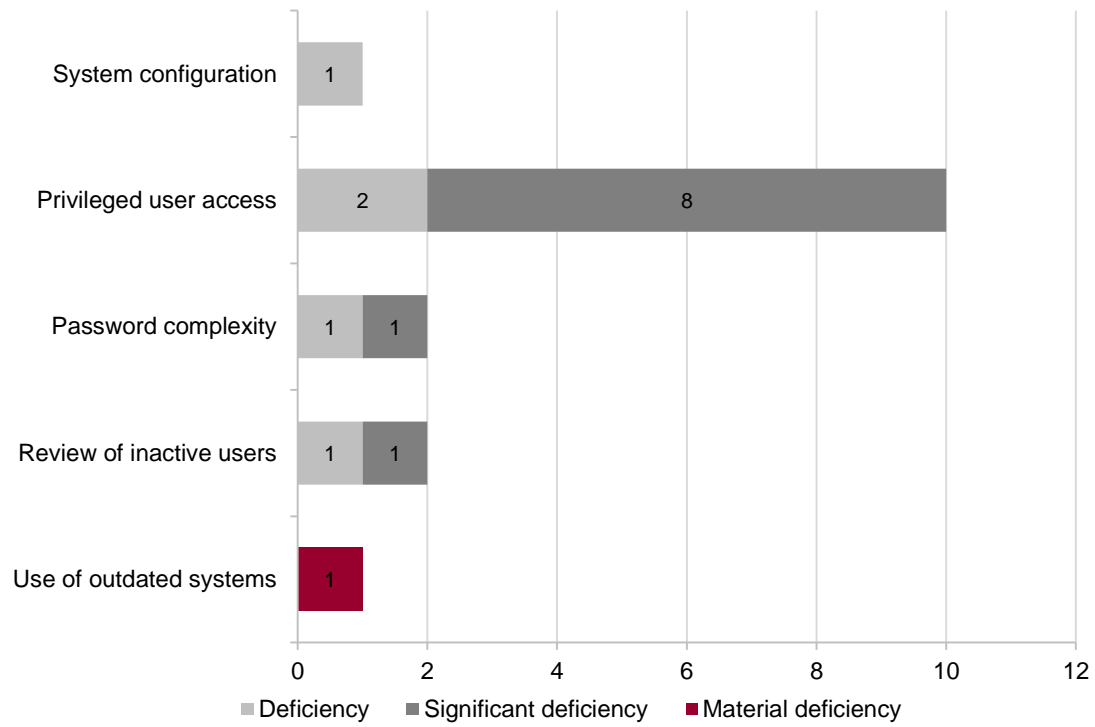
The IT control objective for managing privileged user access has not been achieved. Privileged user access allows wide-ranging functions within systems. These include the ability to change and delete system and financial data as well as audit trails. Activities of these privileged users are not monitored regularly. This makes it difficult to detect fraudulent activities and any transactions that these users may process in error.

In addition, 11 departments are using outdated finance systems. This risk was previously highlighted in *Information systems governance and security* (Report 4: 2011) and the *Queensland Government ICT Audit 2012*.

We consider this a material deficiency as it can have a material impact on the effectiveness and efficiency of operations, including compliance with regulations. It can also have a material effect on the reliability, accuracy and timeliness of financial reporting. It is important that the financial systems are migrated using a planned approach before significant change in business or legislation necessitates urgent replacement.

Figure 2J provides a summary of the number and severity of deficiencies identified during the audit. There are 16 deficiencies in total and they all relate to IT controls. This is a significant improvement from the prior year of 27 control deficiencies for the same control objective.

Figure 2J
QSS control deficiencies



Source: Queensland Audit Office

3. Internal financial management reporting

In brief

Background

Sound internal financial management reporting is essential for efficient and effective decision support. Internal financial management reports provide managers with regular information on how the department is performing.

Conclusions

Departments have internal financial reporting policies and processes in place that meet their day-to-day needs and are adequate for addressing changing user requirements.

Measured against a capability maturity model for internal management reporting, 76 per cent of departments had established reporting practices in place, achieving ratings of level 3 and above for all key elements of monthly financial reporting.

A large proportion of departments have indicated that they will be upgrading their accounting systems over the next two years to systems which will support increased functionality in the use of business intelligence tools for reporting purposes. The improvements in accounting systems will be a key opportunity for departments to develop more cost-efficient automated processes and integrated IT systems that deliver faster reporting of financial performance.

Findings

- Reporting is aligned with departmental structures and program structures and tailored for different levels of management.
- High level financial management responsibilities are documented and understood by users.
- Monthly report content includes both financial and non-financial information, and full accrual financial reports are prepared.
- Performance data, in terms of achievement of service delivery statement and strategic and operational plan measures, is not provided for context on at least a quarterly basis by five departments.
- Thirty-eight per cent of financial reports with commentary and analysis of the results are provided to those charged with governance in 10 days or less.
- Ten departments are using business intelligence tools for reporting.

Key opportunities for improvement

- Agencies' reporting frameworks should include a requirement for a continual review of reporting practices and associated systems to ensure that they remain relevant, efficient and effective.
- Holistic, succinct monthly reporting can be achieved using dashboards to combine both key financial and non-financial performance data. This will enable each agency to track its performance in achieving its objectives.
- Earlier reporting can be achieved by reviewing and streamlining month-end activities or by leveraging technology solutions to integrate financial and non-financial information and provide greater automation of reporting.

Background

Reporting is not an end in itself but a means to an end—to help users make informed decisions and assess whether performance is on track to achieve objectives. Sound internal financial reporting is essential to the efficient and effective management of a department. Internal financial management reports (IFMR) provide managers with reliable, regular information on how the department is performing which supports good decision-making.

Legislation and guidance

The Financial and Performance Management Standard 2009 requires information on an agency's performance against its objectives to be provided to the accountable officer at least once every three months. It contains minimum standards for performance information systems and requires accountable officers to comply with *A guide to the Queensland Government performance management framework* as prepared by the Department of the Premier and Cabinet.

Queensland Treasury's *Financial Accountability Handbook* suggests that management reports be prepared and actioned on a monthly basis, providing management with the information required for day-to-day activities, including:

- reports on key performance indicators
- capital project reports
- budget/forecast versus actual results (financial and non-financial performance).

Queensland Treasury has also provided guidance on monthly processes to assist with the earlier preparation of annual financial statements and early resolution of accounting issues. While not mandated, this guidance encourages departments to:

- perform variance analysis with meaningful explanations
- undertake reconciliations
- report on contingent assets and liabilities
- identify and outline strategies to address new and emerging financial risks on a monthly basis.

Year end alignment

The year end financial reporting process should be an extension of a department's continuous month-end reporting. Where month-end reporting—including journal processes, calculation and estimation of accruals and identification of commitments and contingencies—is prepared on a similar basis as year end financial reporting, financial statements will be completed in a more timely and efficient manner.

Principles

Good management reporting is about getting the **right information** to the **right people** at the **right time** to allow managers to effectively manage their business. Figure 3A summarises these three principles for good management reporting.

Figure 3A
Management reporting

Right people
All key stakeholders need financial information to support the decisions they need to make.

Those charged with governance

Executive management

Operational management

Right information
The quality of reporting information covers both what information is in reports as well as how the information is presented. Good management reports contain relevant and reliable information that is comparable and understandable.

What's presented
- relevant
- reliable

How it's presented
- comparable
- understandable

Right time
Good management reports need to be underpinned by streamlined and responsive reporting processes to make reports easily accessible and get information to decision makers as quickly and efficiently as possible.

Process

- accessible
- streamlined
- responsive

Source: Queensland Audit Office

Audit objectives

The audit objective was to assess the effectiveness of all departments' internal financial management reporting against the three principles for good management reporting.

We considered how these principles applied in practice, and looked at management reporting practices across three tiers of each department. The three tiers reflect that users at different levels have different information needs due to the different types of decisions they make and the responsibilities they are assigned.

We interviewed a sample of preparers and users of internal financial management reports from each department and examined internal financial management reports and associated policies and procedures.

We scored each department against nine elements of internal financial management reporting to arrive at an overall capability maturity assessment of between 1 and 5. The assessment scores are described in Figure 3B.

Figure 3B

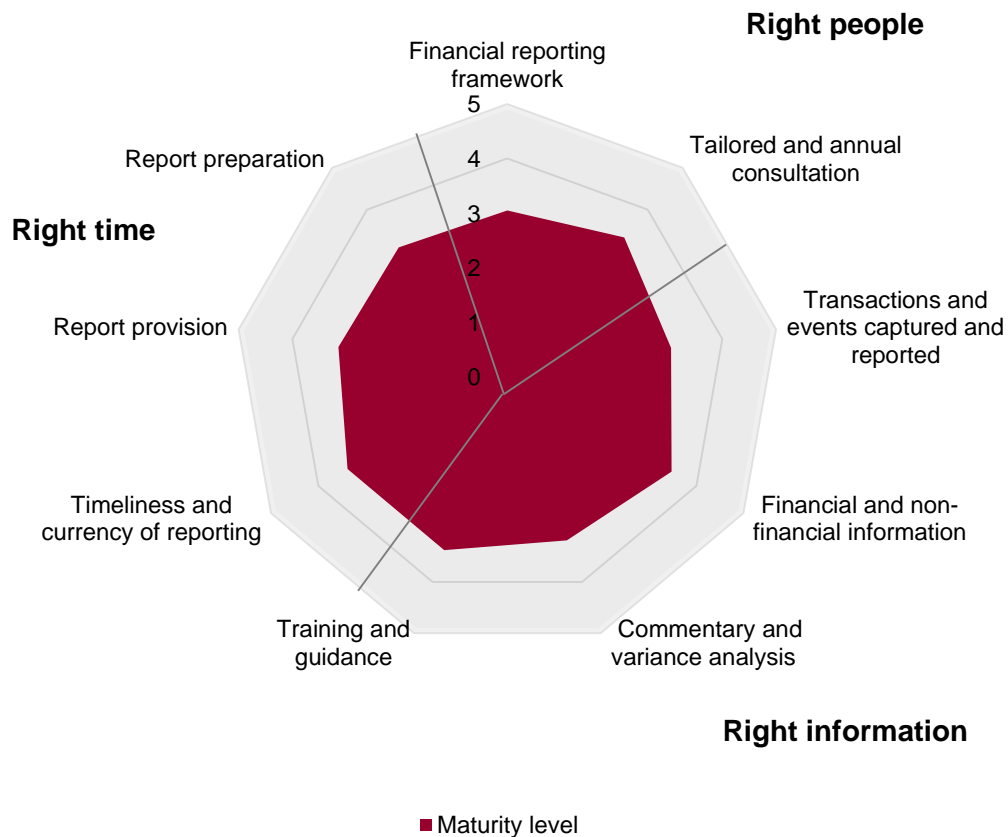
Capability maturity assessment score
5—Optimised
The department has in place internal financial reporting practices that are leading edge. These allow it to anticipate both changing user needs and key opportunities in order to optimise performance.
4—Integrated
The department has in place professional internal financial reporting practices which enable it to effectively respond to changing user needs and identify some opportunities to improve performance.
3—Established
The department has in place internal financial reporting practices that meet day-to-day requirements and enable it to respond adequately to changing user needs.
2—Developing
The department has in place internal financial reporting practices that are adequate to meet the day-to-day requirements of the business under stable circumstances and enable it to develop. They will not be sufficient in challenging times.
1—Basic
The department has in place internal financial reporting practices that are basic and allow it to function on a day-to-day basis. They do not support development.

Source: Queensland Audit Office, developed in reference to: 'Financial Management Maturity Model', National Audit Office, January 2010, United Kingdom and other better practice guides issued by audit offices in Australia.

Conclusions

Departments overall have in place sound internal financial management reporting practices that meet their day-to-day requirements and allow them to respond adequately to changes in user needs. Figure 3C shows how agencies have performed as a group against the elements required to deliver the right information to the right people at the right time.

Figure 3C
IFMR average maturity evaluations across departments



Source: Queensland Audit Office

Overall, 76 per cent of departments achieved ratings of level 3 and above for all elements. The even distribution of average scores against each of the elements shows that there are sound practices in place with no area limiting the ability of departments to achieve the principles of good reporting.

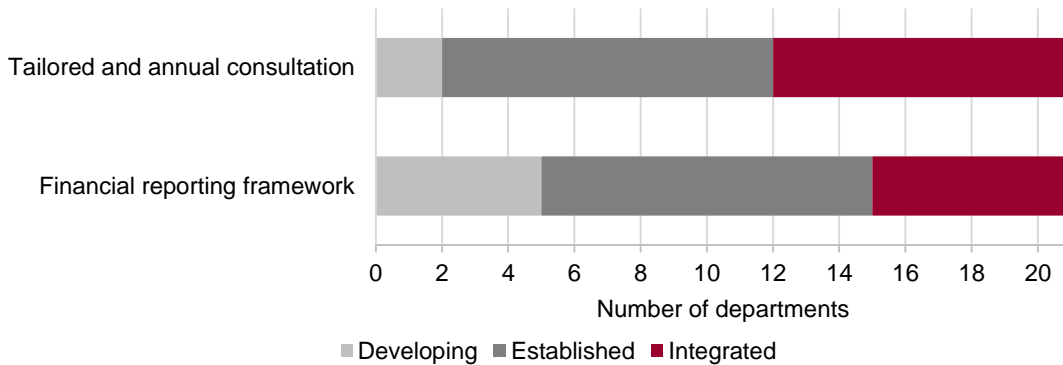
Opportunities still exist to make reporting more useful for strategic and operational decision-making and performance monitoring. This can be done through better use of technology and by adopting recognised better reporting practices.

A large proportion of departments have indicated that they will be upgrading their accounting systems over the next two years to systems which will support increased functionality in the use of business intelligence tools for reporting purposes. These improvements in accounting systems will be a key opportunity for departments to develop more cost-efficient automated processes and integrated IT systems that deliver faster reporting of financial and non-financial performance. Considering these improvements as a part of the project deliverables through a cost-benefit lens will ensure efficient and effective reporting.

The following sections assess individual departments' performance against the three principles of good reporting for identification of better practice and opportunities to develop capabilities further.

Right people

Figure 3D
IFMR maturity evaluations—Right people



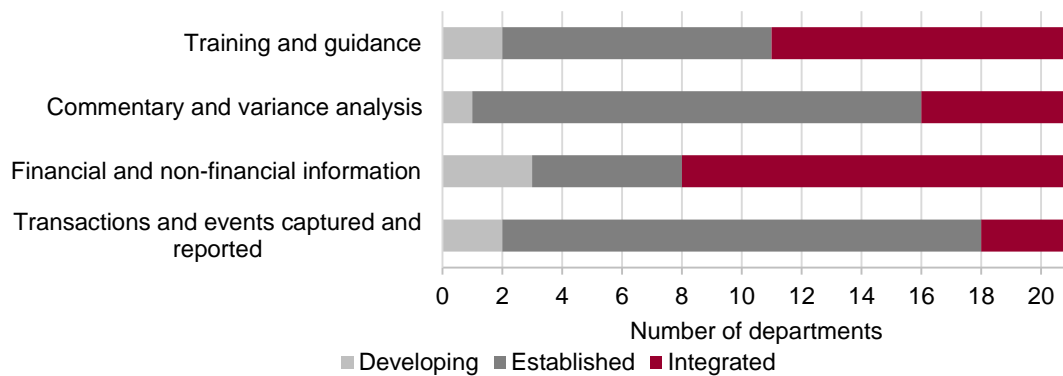
Source: Queensland Audit Office

Most departments have established financial reporting frameworks and consultation processes which enable them to support their report users at all levels of management. In these departments, reports are tailored to the needs of their users and regularly updated to reflect changes in the business environment.

Agencies that are developing (level 2) their people capabilities should focus on their ability to respond to machinery of government and organisational changes so that their reporting frameworks continue to reflect changing user and business needs. Embedding appropriate consultation approaches will assist.

Right information

Figure 3E
IFMR maturity evaluations—Right information

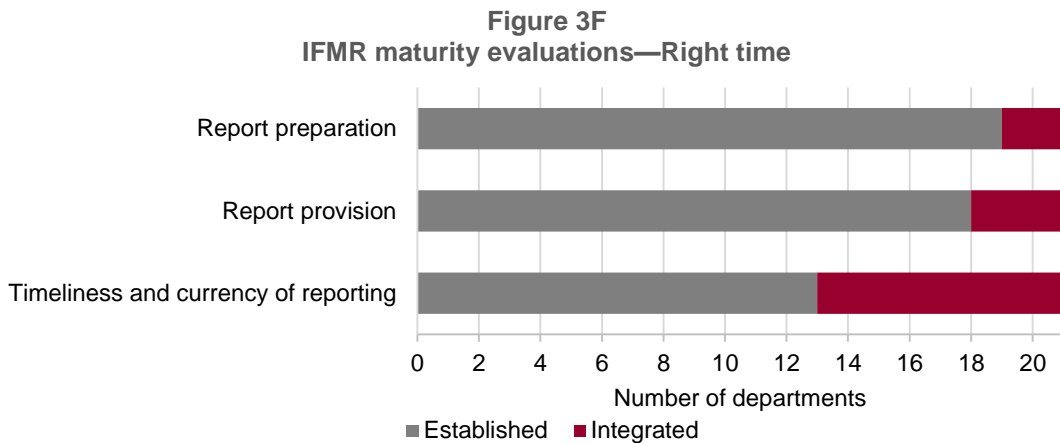


Source: Queensland Audit Office

The provision of accrual financial and non-financial information is a strength in the majority of departments. It enables those accountable to make quality decisions in relation to financial performance and resource allocation. It also provides management with insights to better identify opportunities for improvement.

Departmental officers have sufficient knowledge and understanding to interpret and analyse their financial information due to the provision of ad hoc and formal training on financial management.

Right time



Source: Queensland Audit Office

The timing and delivery of reporting throughout the departments is enabling the report users to access current information to make informed decisions.

Report preparation still involves manual intervention in all departments. Greater use and leveraging of integrated IT systems and business intelligence tools to automate the delivery and production of reports is the main area departments must address to reach optimal performance in terms of efficient and faster reporting.

Summary of findings

The diversity in the form and content of the reports produced by departments reflects that departments are tailoring internal financial reporting to address the needs of users. Overall findings are positive:

- departments have documented management's financial management responsibilities at a high level
- a range of procedural documents have been developed to provide guidance for preparers and users of monthly financial reports
- reports are prepared that meet the general needs of users and are provided to those charged with governance (TCWG), executive management and operational management
- formal and ad hoc feedback is sought from users of financial reports
- reports are prepared on a full accrual basis and contain key selected financial and non-financial data and an analysis of the operations to date
- income statements are provided at all departments and across all three tiers. Cash flow statements and statements of financial position are provided at least on a quarterly basis to TCWG in only three departments. However, a further 12 agencies provide information and analysis on selected numbers within financial statements, including cash
- non-financial performance information on the status of service delivery statement (SDS) measures and strategic and operational planning objectives is provided on a quarterly, six monthly or annual basis rather than monthly in some departments
- analysis and associated commentary is generally of a retrospective nature, but does include some information on action taken, as well as impacts on future forecasts. This is not consistently applied across all tier reports or for all variances identified
- internal benchmarking is well used by all agencies in monthly reporting; however, external benchmarking is not performed on a routine basis as it is considered less relevant by agencies. External benchmarking, where occurring, is considered as a separate exercise to internal financial management reporting (IFMR)
- reports with analysis and commentary for tier 1 and 2 are produced within five to 14 days of month-end
- accounting and other reporting systems can provide financial data for analysis in real time or within 24 hours, with some limited reporting available in both cases
- all departments use spreadsheets or business intelligence software to produce monthly financial reports. The business intelligence software is integrated to financial accounting systems in 10 out of 21 agencies. The preparation of reports still requires manual manipulation to include commentary and non-financial information and other selected analysis.

Opportunities for improvement

Each department received a report outlining the observations from the audit against each element of the three principles of good management reporting. A number of improvements were recommended to agencies to increase their level of capability maturity in internal financial reporting.

Common themes for departments across these reports are:

- enhance reporting procedural documentation to ensure that ownership and responsibilities for preparation and review of monthly financial reporting are assigned and managed through a documented division of roles and responsibilities across all tiers of management
- provide annual opportunities for formal feedback from report users. Given sufficient time, users can consider the content and presentation of their reports and the timing and method of communication. Formal feedback can be facilitated through a number of different avenues—annual surveys, workshops, and annual agenda items at key committee meetings
- provide more non-financial performance information on a monthly basis to enable those charged with governance to consider their financial results in the context of their achievement of the department's key strategic, operational and SDS objectives. A summary dashboard report may be suitable
- provide a quarterly operating statement, balance sheet and cash flow statement to those charged with governance to track performance and enable timely reporting at year end. Where financial reporting practices are similar in character to statutory financial statements, departments will experience less difficulties and delays in completing year end processes. In addition, this will ensure management has a good understanding of the financial performance and financial position as well as any associated financial accounting issues
- provide more consistent variance analysis that will enable the reader to understand the cause of the variance, the action required to remediate and the impact on future results
- assess users' and preparers' training needs and implement a formal training program to address them
- implement a process of continuous improvement of the financial reporting process that focuses on:
 - improvements to business processes and IT systems
 - streamline reporting to enable reports to be provided in 10 days or less by establishing standardised processes and timetables and performing some processes prior to month-end
 - integrate financial and non-financial data in a warehouse which enables further automation of reporting with analysis online and in real time.

As these are opportunities for improvement and not deficiencies, management need to consider the cost and benefit of implementation.

Right people

Clarity over financial management accountability—including the roles and responsibilities of users and preparers of reports—is essential in ensuring internal financial management reports meet the needs of those accountable. Reports should be aligned to the department's organisational structure and objectives. Figure 3G summarises the responsibilities and information needs for different levels of management in departments.

Figure 3G
Three tiers of users

Level	Responsible for	Information needs	Examples
Tier 1 Director-General, and the senior executive leadership team	Setting strategic direction, including program and service delivery Fiduciary accountability	Is the department doing the right things, doing them well and achieving its objectives?	<ul style="list-style-type: none"> ▪ Whole of department financial position and performance ▪ Performance by division/service ▪ SDS reporting and strategic plan key performance indicators (KPIs) ▪ Accrual based accounting
Tier 2 Executive managers	Delivering services and programs	Are services and functions being delivered efficiently, effectively and economically in accordance with the objectives of the department?	<ul style="list-style-type: none"> ▪ Performance by division/service ▪ Service summary information ▪ Breakdown by project/activity ▪ Operational plan KPIs ▪ Accrual based accounting
Tier 3 Operational managers	Implementing projects and activities	Are projects and activities meeting budgets and targets?	<ul style="list-style-type: none"> ▪ Budget to actual information for projects and activities ▪ Accrual based accounting

Source: Queensland Audit Office

Departments' internal financial reporting frameworks are generally outlined in their financial management practice manual (FMPM), corporate governance frameworks and in key committees' terms of reference. These documents set out financial management responsibilities. Our interviews with users, preparers and reviewers of internal financial management reporting identified that they have a clear understanding of their roles and responsibilities.

Agencies have generally developed a range of guidance material to assist officers in achieving their financial management responsibilities including:

- month-end reporting calendars and month-end email communications
- month-end close procedures
- budget preparation and reporting manuals
- monthly business unit financial reporting user guides
- desktop guidelines for the preparation and review of key monthly financial reports
- report process flow documentation
- month-end checklists and task lists
- variance analysis and commentary guidance.

Fit-for-purpose guidance is a key element in an efficient reporting process. The process needs to be well defined so that users and preparers have a clear picture of what the report is being used for, who is responsible for specific tasks (including review) and what deadlines apply to the process. Figure 3H shows a better practice reporting guideline from the Department of Education and Training (DET).

Figure 3H

Better practice—DET reporting user guide

This guide:

- provides a background—legislation and FMPM
- outlines key roles and responsibilities, for example, for a board of management member, a performance reporting team, financial support officers, or responsible cost centre managers
- outlines objectives and the importance of financial performance reporting and has links to the departmental governance framework—in particular DET's planning and reporting cycle
- outlines the key financial reports at each tier of management. A matrix lists the name of the report, a description of the report, key components in the report, the audience and the contributors
- contains a table that outlines the month-end process by day including high level soft close and hard close procedures
- outlines the key dimensions of the financial reporting framework and alignment to the organisational chart, activity structure and account structure
- defines characteristics of better practice reporting and references better practice guidelines
- identifies the key systems and tools used to perform monthly reporting, including systems and software, templates and guidance material
- provides procedural guidance on using report templates and general conventions
- provides procedural guidance on exception-based reporting and variance analysis. This includes thresholds for variance reporting, checklist for variance analysis, examples of supporting activities and practical examples of what good and poor variance analysis looks like. It requires variance analysis to consider the financial and non-financial impact
- provides procedural guidance on budget forecasting
- provides procedural guidance on emerging issues, including the requirement to quantify the financial and non-financial associated impacts (for example, the impact on service delivery)
- provides important information about using key workforce metrics
- outlines the consolidation process from a unit to a branch to a departmental level
- provides useful links—to the strategic plan, governance framework, FMPM and procedural guidance through the finance team site.

Source: DET Monthly Business unit financial reporting user guide

Five agencies with developing (level 2) capabilities do not have tailored documented frameworks across all tiers of management reporting. This is largely due to machinery of government changes, organisational change and business direction changes impacting on governance and associated reporting.

Interviews with department users identified that they are generally satisfied with the content and timing of the receipt of reports. Users of reports in 10 departments advised they are only consulted on an ad hoc basis regarding whether reporting is suitable for their needs. Better practice was identified in eight departments where formal consultation with tier 1 and 2 users on reporting is documented and actioned through committee minutes or annual reviews of committee activities.

Reviewing reporting processes on a regular basis reaffirms the efficiency of month-end tasks and the quality and timeliness of the reports. While we noted most FMPMs and terms of references for committees require regular reviews of the activities of key committees and policies, there is no documented requirement to review reporting practices and systems for efficiency and effectiveness.

To drive continuous improvement in financial reporting processes, reviews need to consider the efficiency and effectiveness of reports, reporting systems and alternative contemporary reporting practices.

Right information

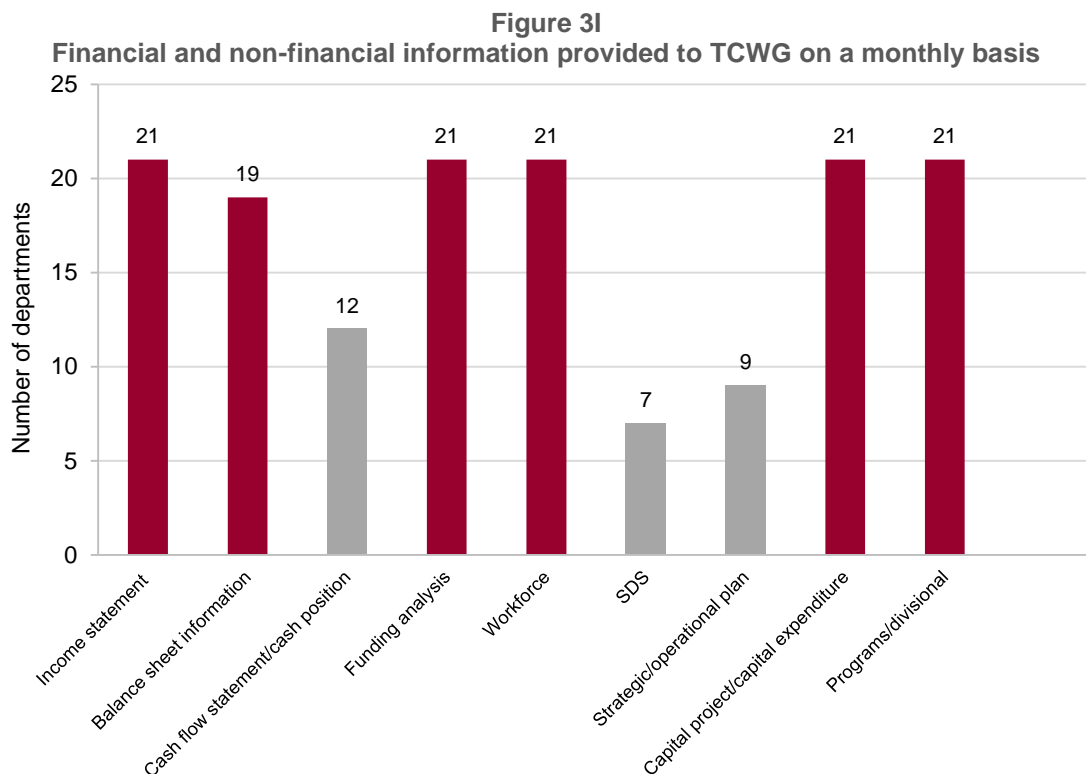
Decision makers need relevant and reliable information that is comparable and understandable in order to assess their progress in achieving service delivery objectives.

Management reports typically include financial information associated with revenue, expenditure, assets and liabilities against budgets, prior year financial information or other predetermined limits. Effective management reports contain non-financial information that supplements or elaborates on the financial information.

Regular monitoring against financial and non-financial performance measures and targets allows for early intervention where the department's objectives are at risk.

Relevant

Figure 3I benchmarks the level of key financial and non-financial information provided to management across departments and shows where there are opportunities for improvement in providing relevant information. Notably, reporting on non-financial information in relation to SDS and strategic and operation plan objectives is provided to TCWG on a quarterly, six monthly or annual basis in some departments.



Source: Queensland Audit Office

All department's financial reports are prepared on an accrual basis. Three of the 21 departments provide their senior executive leadership committee or audit committee with a departmental income statement, balance sheet and cash flow statement in a statutory format on a monthly to quarterly basis.

Another 19 departments report to TCWG with a departmental income statement and a balance sheet or analysis of selected financial position balances. While cash flow statements are not regularly provided, nine agencies report their monthly cash position or cash movements. Tier 1 and 2 reports in all departments include a variety of funding analysis for selected programs and services. The range of analysis includes deferrals and budget adjustment, grant funding, own-sourced revenue, and base and limited life appropriation funding against actual results and budget.

Cash management is largely performed at the operational level with agencies reporting at a departmental level on cash forecasts to the Queensland Treasury Corporation (QTC) on a daily basis. In addition, cash flow statements are produced and submitted to Queensland Treasury (QT) on a monthly basis. Discussions with officers from QTC and QT did not identify any significant issues with cash management by agencies.

In some agencies, there is limited monitoring of property, plant and equipment (PPE) balances by senior executive committees on a monthly basis. Reasons supplied by management include:

- the month to month PPE balance movement is largely depreciation, which is monitored through the operating statement
- maintenance expenditure is monitored through the operating statement
- capital acquisitions and associated projects are monitored monthly
- reviews of valuations of assets and estimated useful lives are reported through to TCWG or to the audit committee as an annual activity.

Reporting at the operational management level is predominantly in formal income statements or information on income and expenditure. Where departments have commercialised business units, they also prepare income statements, balance sheets and cash flow statements.

Reliable

Reliable information is accurate, complete and prepared consistently free from bias, errors or material misstatement.

An established quality assurance process will ensure that data and information is checked by both preparers and users to confirm accuracy. For completeness, financial reports should be prepared on an accrual basis with additional information provided on off balance sheet matters (such as contingencies and commitments).

All departmental monthly reports are prepared on an accrual basis consistent with year end reporting. Quality assurance practices have been built into reporting processes and include checks of data and commentary by business support officers in business units and divisions, central finance sections and users of the reports.

Comparable and understandable

Comparisons provide the context that helps decision makers understand results and decide whether action needs to be taken. Types of comparison used in departmental financial reports include:

- results compared to budgets and forecasts
- results compared to prior year
- movement and direction of results over specific time periods (months or years)
- benchmarking against other business units and divisions
- benchmarking against internal performance targets
- limited external benchmarks for workforce metrics against overall public service rates.

Good reports are both clear and concise and draw users' attention to the most important information on a highlight and exception basis. They explain what is important and why.

Highlight and exception based information and analysis should also provide retrospective, perspective and prospective views of the department's performance including:

- interpretation of why the variance occurred—changes in timing, quantity or price driven by internal or external factors that were controllable or uncontrollable (retrospective)
- impacts on financial and non-financial results or performance and proposed actions—reducing or increasing service delivery, renegotiating contracts or agreements, seeking additional funding, or accepting and monitoring (perspective)
- effect on end of year forecasts or service delivery (prospective)
- other risks, trends and contingencies that may impact favourably or unfavourably on future results (prospective).

Agencies vary in the quality and quantity of explanations provided. The analysis is primarily retrospective, with agencies inconsistently providing perspective and prospective commentary for each of the variances identified.

Figure 3J provides general examples of poor and better practice variance commentaries.

Figure 3J

Variance commentary examples	
Poor examples of variance commentary	Better practice variance commentary
<p>The variance of \$335 000 relates to an underspend of grants. (This information is inadequate because it does not explain the cause or corrective action or timing.)</p>	<p>The variance of \$335 000 relates to under payment of grants resulting from:</p> <ul style="list-style-type: none"> ▪ workload issues in relating to AA grant assessments which should be resolved by March ▪ delays in payments resulting from recipients not providing progress reports. Reports are expected to be received by the end of February. <p>Milestones, deliverables and payments will continue to be monitored.</p>
<p>The variance of \$200 000 is due to delays in engaging contractors for the financial reporting project. (This only partly addresses the cause, and there is no corrective action or timing.)</p>	<p>The variance of \$200 000 is due to reprioritisation and timing of key activities associated with the financial reporting project. Contractors have been engaged from November. Monthly estimates will be revised. There is no impact for total project costs as the project is still expected to be completed by 30 June.</p>

Source: Queensland Audit Office

The level of detailed analysis focuses on material variances, both positive and negative. Executive summaries of financial reports provide a collation of the variance analysis undertaken and commentary on any emerging financial risks identified.

Information displayed visually in appropriate charts, graphs and dashboards can be quicker and easier to understand than data in tables or lengthy explanations.

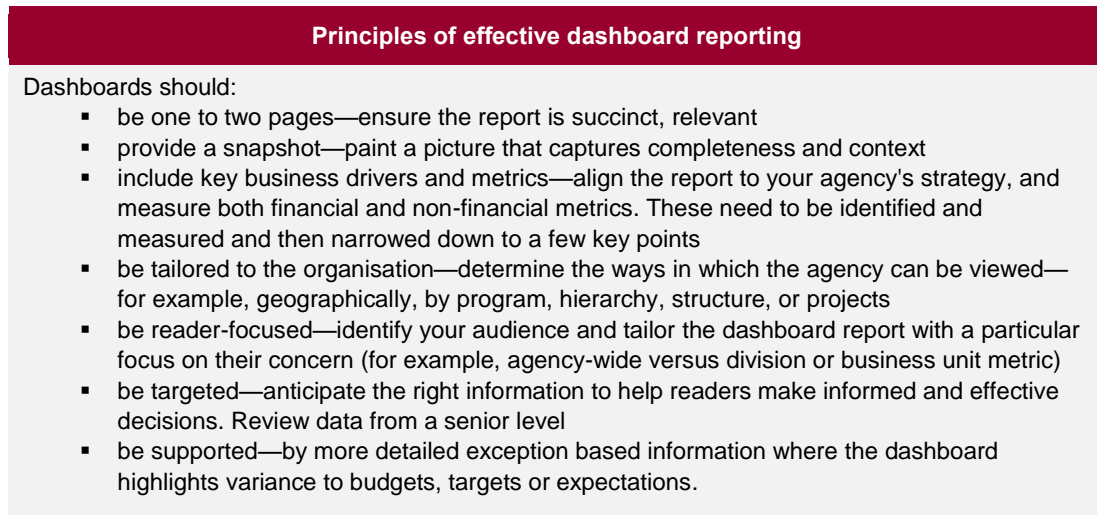
A summary page followed by more detailed supporting information provides users with an overall understanding while assisting them in navigating to the information which is most relevant to them. If the information is useful but not essential or critical, agencies should consider including it in an appendix. This keeps the user focussed on the critical data.

All agencies use charts, graphs and tables in their reporting. Nine out of 21 agencies provide dashboard reporting in addition to the monthly financial report. The dashboard reports provide either a mix of financial and non-financial information or only performance information, for example, a workforce performance dashboard.

Dashboards add value by helping management focus on the key financial and non-financial department matters and providing a succinct update on progress and success. Examples of better practice information included in department dashboard reporting is included at Appendix D.

Figure 3K summarises the principles of effective dashboard reporting.

Figure 3K



Source: Adapted from Business Guidance Note 15, the Institute of Chartered Accountants in Australia.

Communication and training

Effective communication and training helps officers understand their financial reports and financial management roles and responsibilities. Training in around half of departments is largely ad hoc and informal, or conducted by finance officers as needed.

Departments provide formal financial management training through online training or other formal programs including:

- budget development and management
- financial compliance and monitoring
- financial awareness
- induction—financial management responsibilities
- project management
- company secretaries training (provided to board and committee members).

All agencies provide their staff with financial, budget and other reporting system user training. Chief finance officers also regularly conduct one on one meetings with executive managers and other tier 1 users. They also brief finance and senior executive committees. Two agencies hold forums for preparers of financial reports to discuss issues and share ideas.

Right time

Effective management reports need to be underpinned by good reporting processes with a focus on getting the information to decision makers as quickly and efficiently as possible.

The challenge facing departments when seeking to optimise monthly financial reporting processes is around information technology systems—in particular integration between multiple and differing accounting systems and other relevant non-financial systems.

Accessible

We identified that primary access to reports at all tiers is through email, where officers or their executive assistants either print off the reports for their use or view them online.

Two agencies make their tier 1 monthly financial report available to staff via departmental intranets or SharePoint sites. One department does not provide the full report but provides the financial report data on a dashboard with drill down capability to all staff via the intranet.

Most agencies have data and or limited reporting available via their accounting system or other linked reporting systems available in real time or at the previous days close. However, reporting with analysis and commentary (including material accruals) is only performed and available at month-end.

Streamlined and responsive

Timing of month-end is reflective of a department's culture and trade-off between accuracy and timeliness. Greater accuracy requires more time to process transactions and a detailed assurance process. Faster reporting requires earlier processing of estimates and a higher level of review. The benefits of faster reporting are that users get prompt and reliable information for decision making and finance sections can allocate their resources to other activities.

We found that 13 agencies produce tier 1 reports between 10 and 14 days and eight agencies produce them in less than 10 days. Better practice suggests that agencies with faster year end external reporting processes are able to deliver because their monthly reporting processes replicate year end processes and become an integral part of the day-to-day finance operations.

All agencies import data from their accounting systems using spreadsheets or through automation to a data warehouse. With both of these processes, the rekeying of data is minimised. Two departments also incorporate some non-financial data into the data warehouses for reporting purposes.

The final report compilation process of all departments involves manual input of commentary and variance analysis, other non-financial information, and the pasting of tables and graphs into word processing programs from spreadsheets.

An optimised financial reporting process will focus on minimising any manual processes and enhancing system integration and automated processes. Agencies wishing to optimise their reporting processes without automation or further technology change should identify the activities that can be carried out prior to month-end.

Discussions with agency officers indicate that the major impediments to faster reporting are:

- reliance on service providers and other internal stakeholders for information. This particularly inhibits their ability to quickly combine financial and non-financial data
- machinery of government changes, which have resulted in some agencies having a number of disparate systems in place that require more effort to consolidate and automate through data warehouse software
- limits of current IT systems, with some agencies on older versions of accounting software which do not have advanced data warehouse capabilities
- costs of investigations and implementation for further automation and technology advances.

The case study below describes QT's strategies for shortening their reporting timelines without technology change.

Case study 1

Strategies to streamline month-end reporting without system change or further automation

Background

As a part of their drive for continuous improvement in their internal management reporting, Queensland Treasury (QT) reviewed their month-end close processes. This review included the month-end timetable and associated processes, including data integrity and month-end journal activity.

The aim of the review was to identify opportunities to eliminate or re-sequence processes and develop other appropriate strategies that would contribute to a reduction to the book close process and thus reduce reporting timeframes. QT had previously undertaken a review of their financial report content, compilation and presentation for reporting to the key executive and governance committees. The result was the identification of strategies for improvement in the processes.

Strategies for streamlining month-end reporting

- Consult with internal and external stakeholders to fully challenge and explore how best to manage year end dependencies and delivery of key financial information:
- consult with service providers and consider using functions in accounting systems whereby journals could be prepared by the service provider and reviewed by QT officers when journals are material
- agree on a revised timetable for delivery of key information earlier than working day (WD) 4
- consider a revised sign-off schedule with internal stakeholders to be provided prior to book close.
- Review the appropriateness of materiality thresholds across the business for journals by performing an analysis of month-end journal activity by user profile and processing date. Establish one level of materiality across the business and increase the materiality level from \$5 000 to \$10 000.
- Perform a comprehensive monthly review of reporting requirements and determine what general ledger-sourced information is important for decision making. Based on these discussions, management can decide which other journals and reconciliations could be excluded from the month-end process without impacting on end users or the material correctness of month-end reporting.
- Re-engineer the month-end timetable and where possible realign tasks and responsibilities from WD 6 and earlier. Implement procedures to make the following assessments and perform tasks prior to month-end:
 - tasks and journals not reliant on the month-end system close or those transactions that do not have significant movement in the days leading into month-end to be carried out before month-end (for example, negative WD 1 or WD 2)
 - journals for accruals, prepayments, asset depreciation and long service leave accruals could be prepared and posted prior to month-end.
- Redefine roles and where possible separate tasks so activities can be undertaken in parallel rather than sequentially.
- To mitigate reliance on key internal individuals, provide training to finance staff so that they are able to rotate roles and increase capability, and establish month-end email for triage of support requests with prioritisation. Develop a distribution list of support staff who are contactable for month-end support.

Source: Queensland Treasury

4. IT disaster recovery planning

In brief

Background

Departments must consider how to protect their critical business functions through disaster recovery plans for their computer systems. New technologies enable cost-effective recovery options and facilitate frequent testing and re-evaluation of disaster recovery plans.

We selected four departments to assess how mature their processes are in recovering their computer systems in the case of a disruptive event, such as floods or power outages. The four departments chosen have a high reliance on information and communication technology.

Conclusions

Two of the departments have IT disaster recovery plans that are based on a business impact analysis, define roles and responsibilities, and are reviewed and tested annually. The remaining two departments cannot provide sufficient assurance that they will recover their information in line with business needs as they have not adequately planned for disruptive events impacting the information technology environments. They do not have complete, up to date, approved and tested disaster recovery plans.

Findings

- Disaster recovery plans are tested infrequently given the high rate of change in business and technology.
- The Department of Transport and Main Roads (DTMR) has a disaster recovery plan, but not all business units have defined the maximum time to recover key systems.
- The Department of Natural Resources and Mines (DNRM) also has a disaster recovery plan, but does not have formal processes to ensure that its key service provider regularly tests the infrastructure.
- The Department of Science, Information Technology and Innovation (DSITI) does not have a central disaster recovery plan. The levels of maturity in planning varies across business units.
- The Department of Justice and Attorney-General (DJAG) does not have up to date and ready for use disaster recovery plans. In addition, it does not have a facility to test recovery plans for information systems.

Recommendations

Our recommendations from this assessment apply to all government departments, not just the four departments that were assessed.

Where the following are not already occurring, all departments should:

1. update and approve disaster recovery plans, providing oversight and co-ordination for all business areas
2. define disaster recovery targets for all business units
3. increase the frequency of disaster recovery testing to twice yearly
4. obtain and monitor periodic reports on disaster recovery testing (including those from service providers where applicable)
5. use emerging technology to expand their options in providing cost-effective backup and disaster recovery testing
6. develop a plan to improve the maturity of the disaster recovery program, and manage to that plan.

Background

A disaster recovery plan is a documented process, or set of procedures, to assist in the recovery of a department's information technology (IT) infrastructure and data in the event of a disaster or significant business disruption.

Departments use computers to deliver services, quickly and effectively process information and store large volumes of data. Much of the data is essential for continued operations and to meet each department's legislative obligations.

Employees constantly use emails, tablets, smart phones, business applications, laptops and wireless devices to create, process, and communicate information. They are very reliant on the technology.

Modern computer systems require hardware, software, power management, cooling, operations personnel and connectivity to function. Without one component, the systems may not run.

It is therefore important that departments make provision to recover all of the components of key computer systems, should they become unavailable due to a disruptive event, based on likely disaster scenarios, big or small. Having a well understood and tested disaster recovery plan in place for business critical systems helps to minimise the impact of a disruptive event on the business of the department.

Legislation and guidance

Pursuant to the Financial and Performance Management Standard 2009, all accountable officers and statutory bodies must safeguard their assets through the establishment of internal controls. The Information Standard 18: Information Security applies to all accountable officers and statutory bodies as defined in the *Financial Accountability Act 2009*.

Business continuity management and disaster recovery planning are covered in *Information Standard 18: Information Security*. Departments can obtain specific guidance on disaster recovery planning from 'Whole-of-government business continuity management and disaster recovery implementation guideline'.

Maturity model

We used a capability maturity model to assess how well the departments' disaster recovery planning would support critical business processes in terms of:

- analysing the impact of losing critical computer systems on business operations
- planning, monitoring, supervising and automating the disaster recovery activities
- testing and reviewing the plans
- considering continuous service when entering into agreements with vendors and major suppliers
- enhancing and aligning their IT disaster recovery plan with continuous service planning and business needs.

The maturity ratings assessed are described in Figure 4A.

Figure 4A
Maturity levels

Maturity matrix
5—Optimised
The department has in place a disaster recovery program that is leading edge. The program enables automation and continuous improvement. It enables the department to anticipate future disaster recovery risks, resources, demands and capabilities. There is a provisioned recovery site, with little exposure to common threats, which is tested regularly.
4—Integrated
The department has in place a disaster recovery plan which enables effective recovery of critical processes and systems. The planning process is in response to changing business needs and external factors. Recovery expectations and delivery are aligned with continuous service testing and updating of plan.
3—Established
The department has in place a disaster recovery plan that is adequate in meeting most of the needs of the critical processes. Business impact analysis is conducted for each key process. Roles and responsibilities are defined and plans are reviewed and tested annually.
2—Developing
The department has in place a disaster recovery plan that meets some of the needs of the critical processes. Some business impact analysis has been done. Management processes support event response and some of the planning has been reviewed. Limited testing is done.
1—Basic
The department has in place a basic disaster recovery plan that does not support critical processes.

Source: ANAO Better Practice Guide June 2009, Gartner (September 2010), Queensland Audit Office

Audit scope

The following departments are in the scope of this audit:

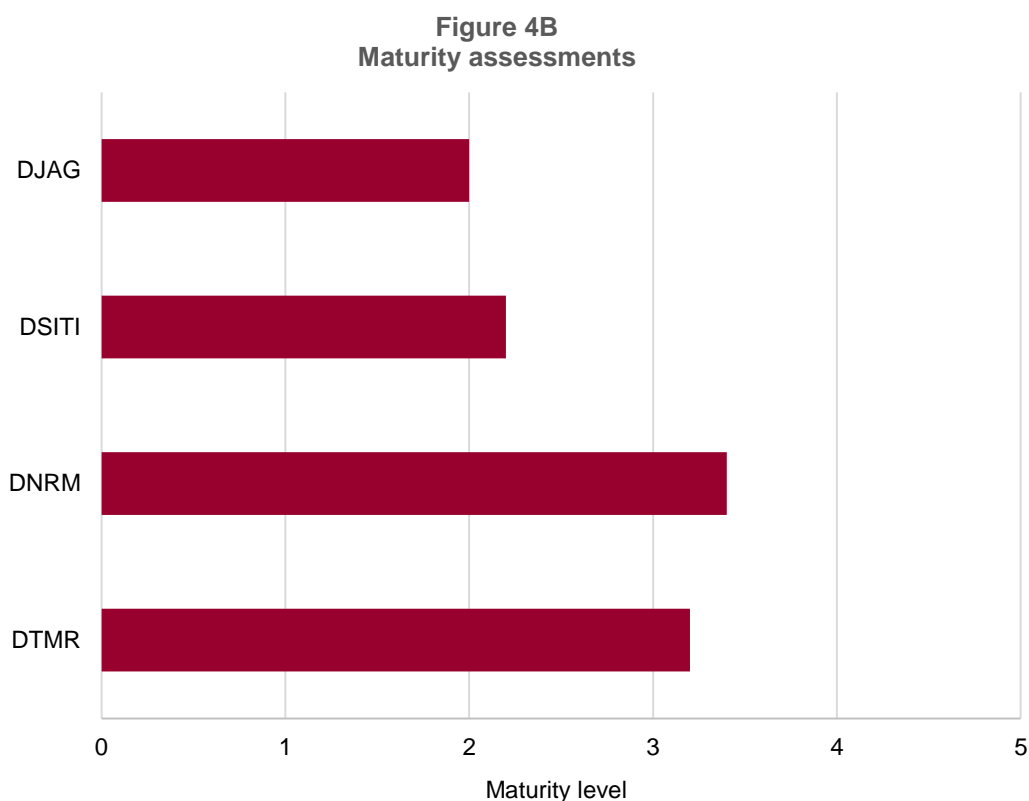
- Department of Transport and Main Roads (DTMR)
- Department of Natural Resources and Mines (DNRM)
- Department of Science, Information Technology and Innovation (DSITI)
- Department of Justice and Attorney-General (DJAG).

These departments operate a large number of computer systems that support business operations and also use information and communication technology services from external service providers.

Conclusions

The ability to recover from disruptive events cannot be assured in two departments. They infrequently update the plans to take into account business and technology changes. Only two out of the four departments we audited have approved and tested their current IT disaster recovery plans. The remaining two departments cannot be confident that they will be able to restore their critical functions within acceptable timeframes. This suggests that these departments are not prioritising activities relating to planning for disruptive events.

Figure 4B shows the maturity assessment of each of the departments we sampled.



Source: Queensland Audit Office

Summary of findings

The maturity of disaster recovery capability varies noticeably across the four departments. Two departments test their disaster recovery plans once a year and the remaining two have not tested theirs in the last year. The departments infrequently update the plans to take into account business and technology changes.

Two departments achieved an overall maturity level of Established (level 3). This means that the departments have a disaster recovery plan that is based on a business impact analysis, defined roles and responsibilities and is reviewed and tested annually.

The other two departments are assessed at the developing maturity level (level 2). This means that they do not have a complete, up-to-date, approved and tested disaster recovery plan.

The four departments are discussed in more detail below:

Department of Transport and Main Roads

DTMR has an up-to-date IT disaster recovery plan that includes maximum tolerable periods of disruption for systems in line with their assessed criticality. This is reviewed and tested each year. However, not all of the business units had confirmed the maximum time within which they need key systems to be recovered with those recorded in the IT disaster recovery plan. As a result, the IT recovery processes for those business units may not align with their needs.

Department of Natural Resources and Mines

DNRM has up-to-date disaster recovery plans for all its critical information systems. In addition, DNRM reviews and tests its disaster recovery plans once in a year.

However, it does not have formal processes to ensure that its key service provider (Information Technology Partners) also regularly tests the infrastructure components, such as data centres, servers and computer networks.

Department of Science, Information Technology and Innovation

DSITI does not have a central IT disaster recovery plan. While individual business areas maintain their own plans, there is no oversight of disaster recovery planning across all business areas of the department. As a result, there are different levels of maturity across business units.

Two out of seven business areas do not have an updated IT disaster recovery plan. Those business areas that have a plan have not tested it. Therefore, the department cannot be assured that its response to a disaster will be planned and co-ordinated.

DSITI has several agreements with IT service providers. Disaster recovery targets are not specified in these service agreements. Therefore, the department does not have assurance that those services will be restored within acceptable time frames.

Department of Justice and Attorney-General

DJAG does not have up to date and ready for use disaster recovery plans. In addition, it does not have a facility to test recovery plans for business information systems.

The department has an improvement initiative for disaster recovery planning and this activity has reached the final delivery phase.

Recommendations

Our recommendations from this assessment apply to all government departments, not just the four departments that were assessed.

Where the following are not already occurring, all departments should:

1. update and approve disaster recovery plans, providing oversight and co-ordination for all business areas
2. define disaster recovery targets for all business units
3. increase the frequency of disaster recovery testing to twice yearly
4. obtain and monitor periodic reports on disaster recovery testing (including those from service providers where applicable)
5. use emerging technology to expand their options in providing cost-effective backup and disaster recovery testing
6. develop a plan to improve the maturity of the disaster recovery program, and manage to that plan.

Areas to consider when assessing a department's disaster recovery plans are included in Appendix F.

Appendices

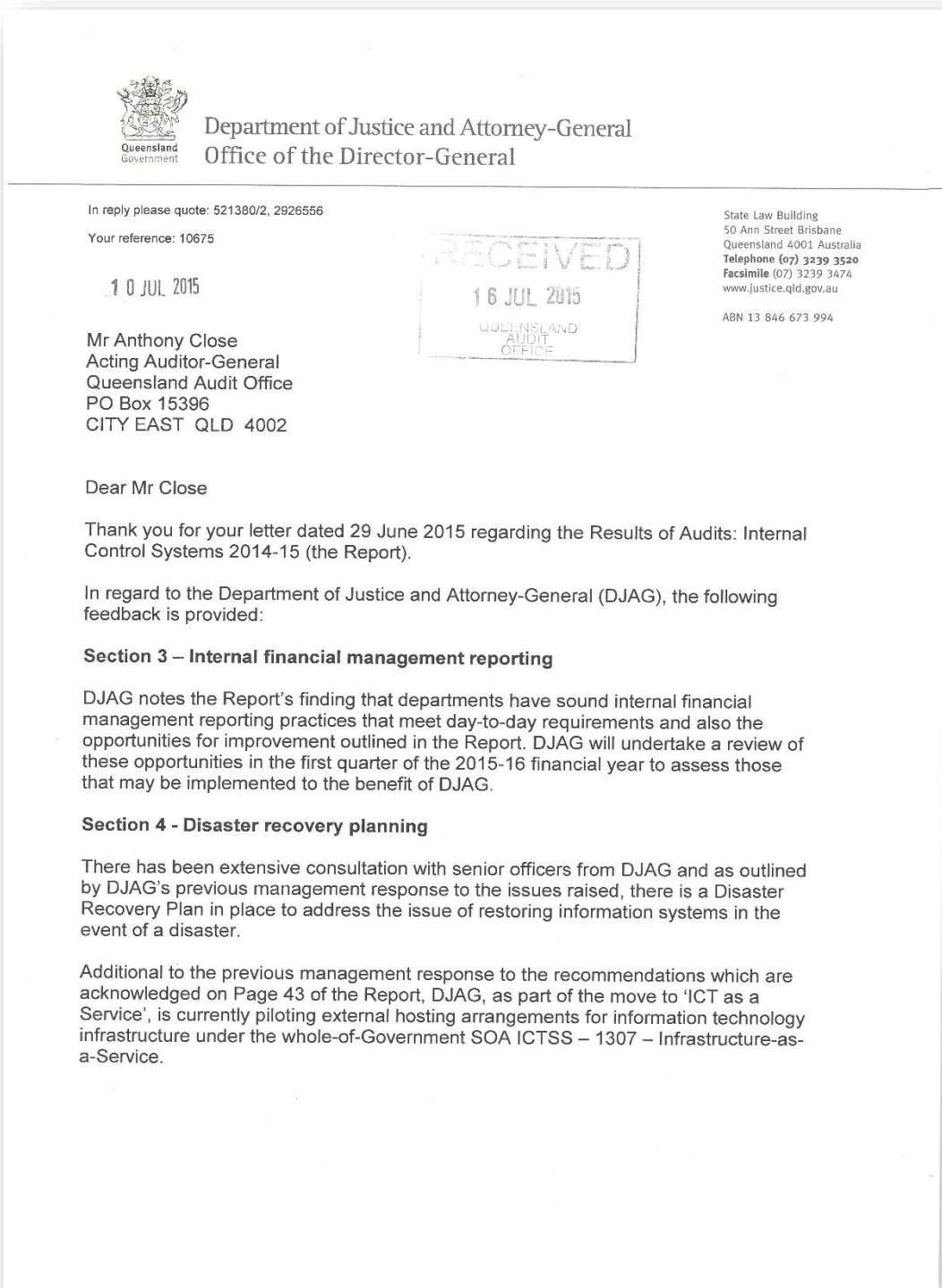
Appendix A— Comments	49
Comments received from Director-General, Department of Justice and Attorney-General.....	50
Comments received from Director-General, Department of Science, Information Technology and Innovation	52
Comments received from Director-General, Department of the Premier and Cabinet	54
Comments received from Director-General, Department of Communities, Child Safety and Disability Services	55
Comments received from Under Treasurer, Queensland Treasury.....	57
Comments received from Director-General, Department of Transport and Main Roads.....	58
Appendix B— Principles of an integrated system of financial control.....	59
Appendix C— Update on prior year control deficiencies	60
Appendix D— Better practice—Types of information in dashboard reporting.....	61
Appendix E— Assessing internal financial management reporting	64
Appendix F— Assessing disaster recovery planning.....	65
Appendix G— Department acronyms	66
Appendix H— Glossary	67

Appendix A—Comments

In accordance with s.64 of the *Auditor-General Act 2009*, a copy of this report was provided to all of the departments within the scope of this report with a request for comment.

Responsibility for the accuracy, fairness and balance of the comments rests with the heads of these departments.

Comments received from Director-General, Department of Justice and Attorney-General



Comments received from Director-General, Department of Justice and Attorney-General

(2)

The establishment of these arrangements, through these pilot exercises, allows for the department to access an expanded version of infrastructure services in the event of a disaster that physically effects the underlying ICT infrastructure that DJAG has both in-house and at CITEC.

Progression of the pilots will assist in developing ICT disaster recovery model options that will address the ongoing risk issues and address the overall recommendations outlined on Page 39 of the Report.

I trust this information is of assistance.

Yours sincerely



David Mackie
Director-General

Comments received from Director-General, Department of Science, Information Technology and Innovation



Department of
Science, Information
Technology and Innovation

Ref: 00961-2015
Your ref: 10675

Mr Anthony Close
Acting Auditor-General
Queensland Audit Office
PO Box 15396
CITY EAST QLD 4002

Dear Mr Close

Thank you for your letter of 29 June 2015 regarding your draft report to Parliament on internal control systems.

I have noted the findings and would like to provide you with an overview of the actions the department has undertaken since the audit was completed.

In relation to the findings on financial controls, the department took immediate action to address privileged user access in April 2015 and June 2015. The department has also initiated a Finance System Future project which will address the audit issues related to the outdated customer agencies' finance system supported and maintained by Queensland Shared Services.

In relation to the finding on disaster recovery planning, the department is actively enhancing its business continuity management and information and communication technology (ICT) disaster recovery capability. A department-wide exercise has been scheduled for July 2015 to test the business unit's continuity plans against a series of service disruption scenarios.

The department's Chief Information Office has established an ICT Disaster Recovery Working Party with representation from all business units to develop an overarching ICT disaster recovery strategy for the department, which will include disaster recovery testing, disaster recovery training plans and service level reviews with third party ICT service providers. The strategy will be presented to the department's Information Steering Committee in July 2015.

Level 7A, 80 George Street
Brisbane 4000

GPO Box 5078 Brisbane
Queensland 4001 Australia

Telephone +61 7 3215 3700
Website www.qld.gov.au

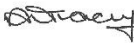
Comments received from Director-General, Department of Science, Information Technology and Innovation

- 2 -

The integration of risk management with the department's strategic and operational planning processes has been enhanced by revising the planning documentation and templates, ensuring alignment with the Department of the Premier and Cabinet's planning requirements. The enhancements have also been more widely consulted to foster a more integrated approach to planning and risk management.

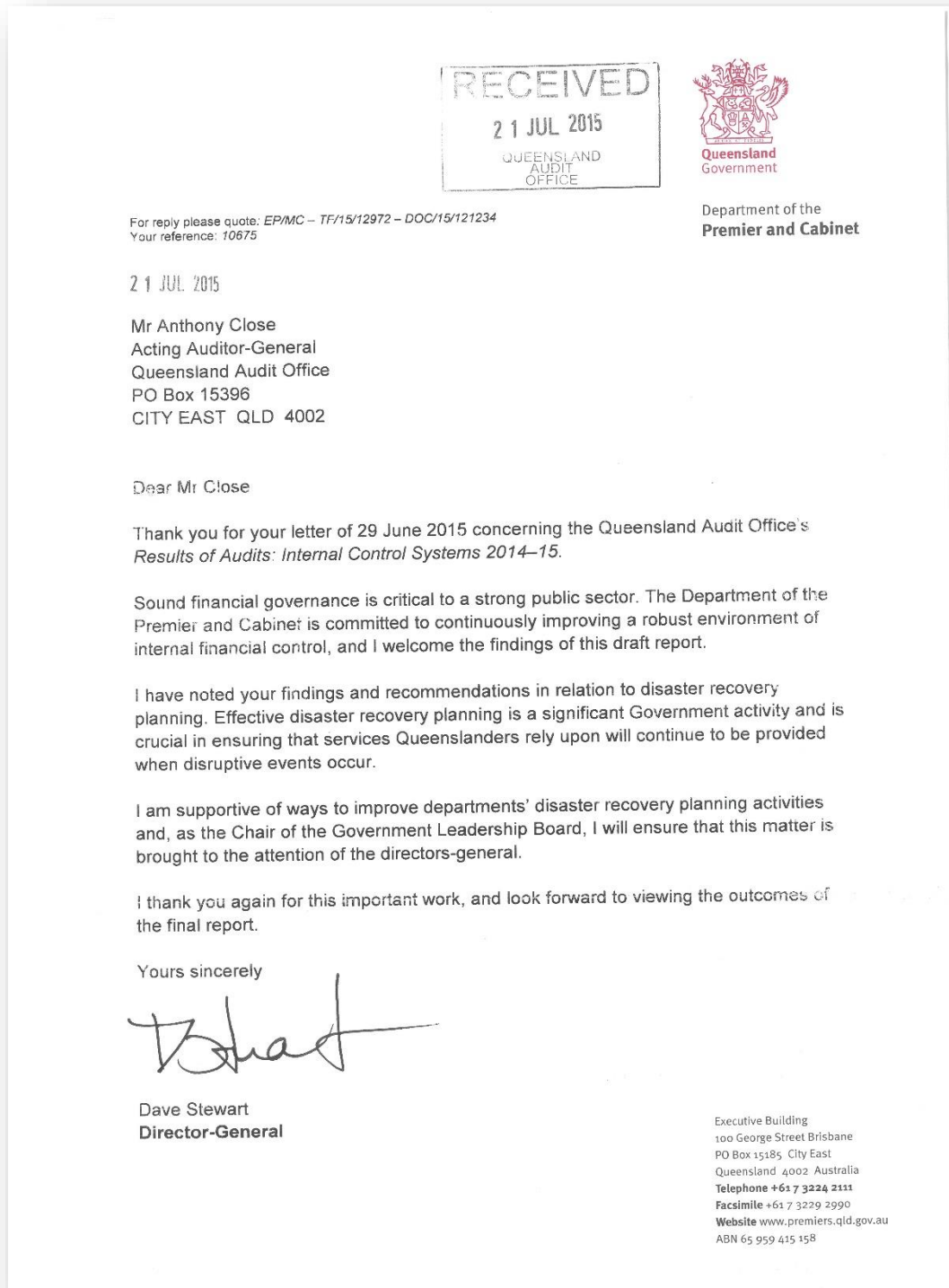
Should you require any further information, you may contact Mr Danny Short, Chief Finance Officer, Department of Science, Information Technology and Innovation by email at danny.short@dsiti.qld.gov.au or on telephone 07 3719 7725.

Yours sincerely

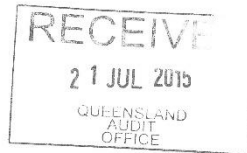

Sue Rickerby
Director-General
20/07/15

Department of Science, Information Technology and Innovation

Comments received from Director-General, Department of the Premier and Cabinet



Comments received from Director-General, Department of Communities, Child Safety and Disability Services



Your reference: 10675; P Brahman 3149 6020
Our reference: COM 04934-2015

Office of the
Director-General

Department of
Communities, Child Safety
and Disability Services

21 JUL 2015

Mr Anthony Close
Acting Auditor-General
Queensland Audit Office
PO Box 15396
CITY EAST QLD 4002

Dear Mr Close

Thank you for your letter concerning the draft report to Parliament on internal control systems and for providing the opportunity to comment on its contents.

I note that I am not required to provide a formal response; however, I welcome your invitation to provide comment on the report.

The department's 2014–15 internal control environment was modelled on the Committee of Sponsoring Organizations framework cited in the current and earlier reports. The integrated approach has proven invaluable when designing, implementing and evaluating control measures and through this our goal is to achieve a strong assessment in the current financial year.

The department is very committed to maintaining business continuity and has a disaster recovery plan dedicated to information technology and a further plan to address the recovery of all other facets of the department's activities. Each of these plans is tested biannually and the outcomes of these tests presented to the department's Executive Management Team and the Audit Committee. Your recommendations will be considered during the testing and review of these plans.

Further, the department has devoted specific attention to the information technology recommendations, which included recommendations surrounding information security that had remained outstanding across financial years and, in collaboration with your staff, has been able to resolve these.

With respect to the observations noted in the report around lack of vendor support for some agencies' financial systems, I wish to advise that the department has received confirmation from the Department of Science, Information Technology and Innovation (DSITI) that the department's SAP 4.6c instance and the general whole-of-government ECC5 environment is being fully supported by SAP, whilst agencies migrate to advanced versions of that system.

13th Floor 111 George Street
Brisbane Queensland 4000
GPO Box 806 Brisbane
Queensland 4001 Australia
General Enquiries
Telephone +61 7 3235 4312
Facsimile +61 7 3235 4327
Email dgoffice@communities.qld.gov.au
Website www.communities.qld.gov.au

Comments received from Director-General, Department of Communities, Child Safety and Disability Services

-2-


With respect to your review of this agency's internal financial management reporting capabilities, I welcome your assessment that the department's systems and processes are well regarded. This is a pleasing result and the recommendations for improvement opportunities are being pursued for this current financial year.

The department has integrated risk management into its planning and performance frameworks, and your recommendations provide the opportunity for the department to further strengthen development in this area.

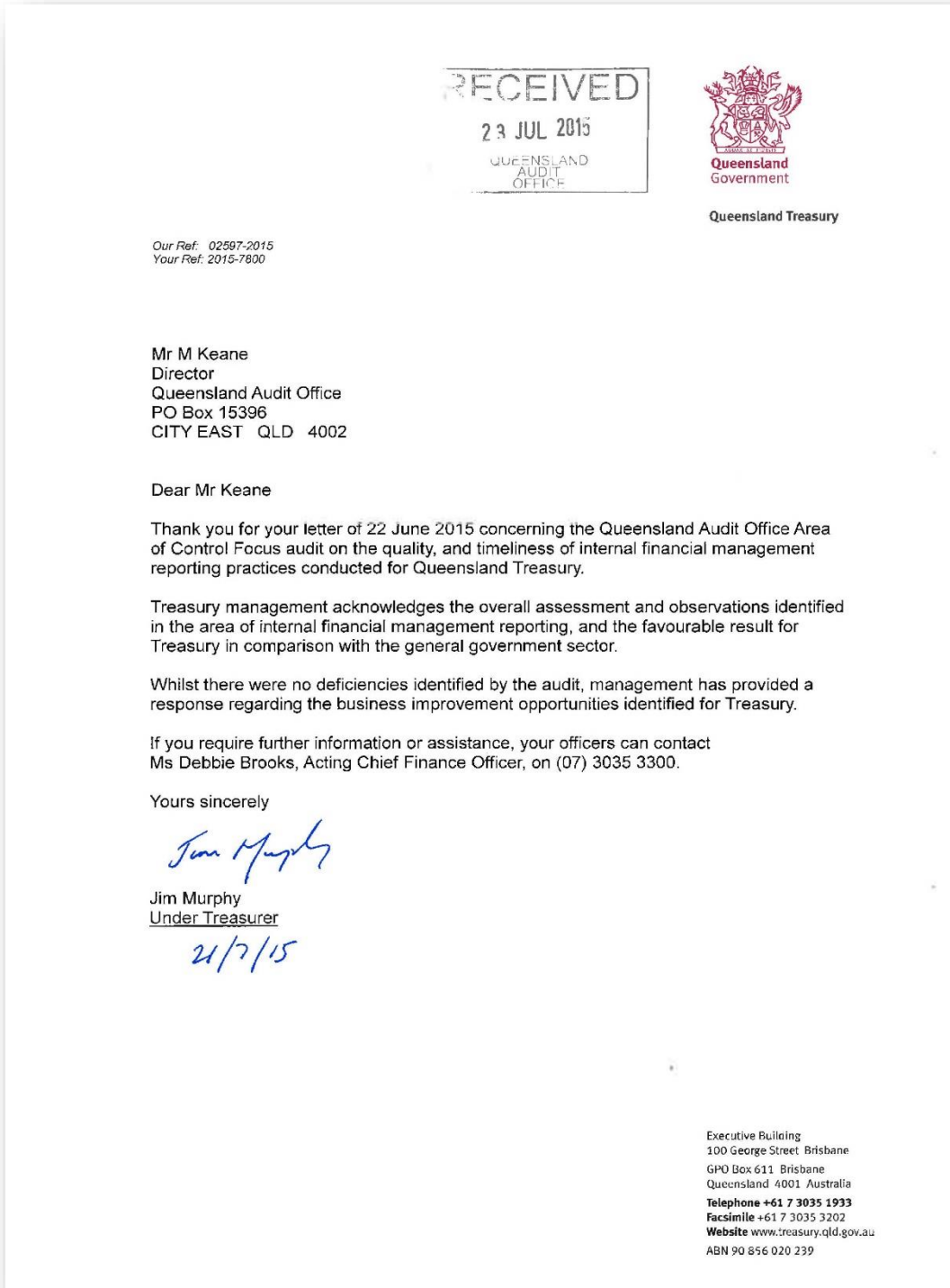
I wish to take this opportunity to thank your office for the collaborative approach in the conduct of audits and the guidance on best practice principles, and look forward to further working with you and your staff.

If you require any further information or assistance in relation to this matter, please do not hesitate to contact Mr Arthur O'Brien, Chief Finance Officer, Department of Communities, Child Safety and Disability Services on 3035 7208.

Yours sincerely


Michael Hogan
Director-General

Comments received from Under Treasurer, Queensland Treasury



Comments received from Director-General, Department of Transport and Main Roads

A fair summary of the response received on 17 July 2015:

...I accept it was the case at the time of audit that not all our business units had confirmed the maximum tolerable periods of disruption for their IT systems, with those shown in the IT disaster recovery plan. However, we did and continue to have in place a disaster recovery plan to enable effective recovery of critical processes and systems.

We have a zero level of tolerance for outage of our critical customer facing systems – prime examples include our registration and licensing system, TRAILS, supporting customer service centre systems; and the 131940 Traffic and Travel Information website/ phone service, which is critical for messaging road conditions, particularly during natural disasters. Successive Premiers and Ministers have promoted 131940 as the mechanism to determine the up to date position on road condition in the event of a tropical cyclone.

It is difficult to imagine two more critical systems than TRAILS and 131940, and while I accept that we have not confirmed the maximum tolerable outages for all business units' IT systems at the time of your audit, I can assure you our focus is on recovery of critical customer facing systems such as TRAILS and 131940.

We will continue to further integrate responses to changing business needs, including external factors, into our IT disaster recovery planning, move to continuous service testing and continued updating of the plan so it remains aligned to recovery expectations and delivery, leading to increased maturity of the programme. Your recommendations will assist in this...

Appendix B—Principles of an integrated system of financial control

The five components are: control environment, risk management, control activities, information and communication, and monitoring activities.

The 17 principles, each of which falls under a component, are as follows.

Control environment

- Principle 1: The organisation demonstrates a commitment to integrity and ethical values.
- Principle 2: The board of directors demonstrates independence from management and exercises oversight for the development and performance of internal control.
- Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- Principle 4: The organisation demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
- Principle 5: The organisation holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk management

- Principle 6: The organisation specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
- Principle 7: The organisation identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.
- Principle 8: The organisation considers the potential for fraud in assessing risks to the achievement of objectives.
- Principle 9: The organisation identifies and assesses changes that could significantly impact the system of internal control.

Control activities

- Principle 10: The organisation selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
- Principle 11: The organisation selects and develops general control activities over technology to support the achievement of objectives.
- Principle 12: The organisation deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Information and communication

- Principle 13: The organisation obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
- Principle 14: The organisation internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.
- Principle 15: The organisation communicates with external parties regarding matters affecting the functioning of other components of internal control.

Monitoring activities

- Principle 16: The organisation selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
- Principle 17: The organisation evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Appendix C— Update on prior year control deficiencies

The table below provides an update on the resolution of prior year control deficiencies.

Figure C1
Update on prior year issues

Control category	Common issues identified last year	Update as of May 2015
Control environment	Lack of service level agreements for shared service arrangements	Resolved in all but one affected department
	Absence of a reporting system to monitor compliance with legislation	Resolved in all affected departments
Control activities	Weak controls over the authorisation of changes to the vendor master files	Resolved in all affected departments
	Delays in clearing long-outstanding, unmatched items in the goods received/invoice received account	Resolved in all affected departments
	Lack of review of payroll reconciliation and verification reports	Remains unresolved in two departments
Information security	Inadequate review of user roles and activities	This issue is still prevalent across the majority of departments, particularly around privileged users. Refer to audit findings on pages 19 and 21
	Users having inappropriate access to sensitive or restricted transactions	This issue is still prevalent across the majority of departments. Refer to audit findings on pages 19 and 21
	Vulnerability to external attack from the internet	Resolved in all but two affected departments
	Poor management of user accounts with broad access to all system transactions, including not maintaining strict access to these accounts and not monitoring account activity	This issue is still prevalent across the majority of departments. Refer to audit findings on pages 19 and 21

Source: Queensland Audit Office

Appendix D—Better practice—Types of information in dashboard reporting

The table below provides examples of better practice information included in departmental dashboard reporting. Dashboard reports should include the key financial and non-financial metrics that will provide a snapshot of departmental performance. This enables users to track performance against departmental strategic and operational objectives.

This is not meant to be a complete list. There may be other key metrics/drivers of business performance that are specific to your agency that should also be considered.

Figure D1

Better practice—types of information included in dashboard reports	
Financial information	
Cash flow	<ul style="list-style-type: none"> ▪ monthly cash flow trend, actual, budget ▪ cash flow indicators—outflow and inflow variance commentary
Operating and financial position	<ul style="list-style-type: none"> ▪ total end of year (EOY) forecast status ▪ actual operating position per department against budget ▪ actual operating position per division against budget ▪ actual operating position trend by month, actual, budget, EOY forecast
Revenue	<ul style="list-style-type: none"> ▪ revenue by funding source, actual against budget ▪ sales revenue trend analysis, actual, budget, forecast ▪ sales revenue fuel gauge ▪ user charges, actual, budget, forecast
Payroll	<ul style="list-style-type: none"> ▪ active and paid full time equivalent (FTE) expenditure by division ▪ employee expenses, actual, budget, forecast, division- and department-wide ▪ employee expenses per month against budget ▪ average fortnightly salary for pay level by gender ▪ trend analysis of monthly salaries and leave expenditure ▪ salary overpayments year to date, number of overpayments outstanding
Expenditure	<ul style="list-style-type: none"> ▪ total expenditure, budget against actual ▪ expenditure by nature, budget versus actual and status of expenditure ▪ expenditure by nature, traffic lights reflecting significance of variances from budget to actual ▪ per cent of total operating expenses, actual, budget, forecast ▪ consultancies and contractors' expenses by division, actual and budget ▪ supplies and services by nature, actual and budget

Better practice—types of information included in dashboard reports

Assets

- cash balance, actual, budget, forecast
- surplus cash
- capital acquisitions—total, actual, budget, forecast
- capital expenditure by division, actual, per cent spent, budget
- capital expenditure by asset category, actual, budget
- debtor ageing, debtor ratio, debtors greater than \$10 000 and 60 days
- per cent of trade debtors greater than 90 days, actual, budget, EOY forecast
- net assets controlled and administered—this month, last month and EOY forecast

Liabilities

- total debt position, actual, prior year, budget
- aged vendors analysis
- per cent of aged vendors greater than 30 days, actual, budget
- borrowings—this month, last month and EOY forecast
- annual leave liability—actual, budget, EOY forecast
- excessive annual leave liability, actual, budget, EOY forecast
- usage of annual leave central scheme
- excessive leave, cost per month, per year, three years, excessive leave headcount

Budget/funding

- budget adjustments/deferrals for month
- external funds by program
- federal funds by program
- funding surplus/deficit

Non-financial information

Workforce

- active and paid FTE by number, actual, budget
- workplace health and safety statistics
- staff attendance/absenteeism rate against Queensland public sector benchmark attendance
- actual vacant positions by division
- sick leave by division, average sick days per FTE
- appointments and separations by division
- vacancy rate per month trend
- excessive leave rate trend per month
- staff engagement rate, actual prior year (based on *Working for Queensland* survey results)
- YTD number of WorkCover claims, YTD open WorkCover claims

Projects and programs

- achievements
- major projects, budget versus actual
- status—traffic light
- status—comments
- deliverables/business plan milestones for month
- major programs, budget versus actual
- consultancies in progress—YTD actual, YTD budget and commentary

Better practice—types of information included in dashboard reports

Risks and issues

- strategic risk status
- high level issue summary
- contingent assets and liabilities
- unacquitted corporate cards by number
- unbudgeted events
- value of payments greater than 30 days unpaid

Strategic plan and operational plan performance

- strategic plan performance targets—actual versus target
- operational plan performance measures, target in numbers or dollars, result to date numbers or dollars, reasons for variances
- service delivery improvements—initiative, progress, status, customer benefit
- achievements—activity, purpose, outcome

SDS measure performance, government commitments

- SDS performance summary by measure—actual versus target, trend by quarter
- SDS status of measures—traffic light
- SDS status of numbers of measures
- government commitments progress—numbers—delivered, on-track, superseded, minor issues
- six month action plan progress—numbers—delivered, on-track, superseded, minor issues

Internal audit recommendations

- open recommendation statistics
- new recommendation statistics
- closed recommendation statistics
- past due recommendation statistics

External audit recommendations

- open recommendation statistics
- new recommendation statistics
- closed recommendation statistics
- past due recommendation statistics

Source: Queensland Audit Office

Appendix E—Assessing internal financial management reporting

Those charged with running public sector agencies, executive managers and cost centre managers need relevant, reliable, timely and concise information to make decisions and track performance and generally manage their business to ensure it is achieving its objectives. The following questions need to be answered and addressed for all departments.

Reporting framework

- Are agency expectations for financial reporting and monitoring of reports known and documented?
- Has the agency established formal guidance and procedural documentation that clearly assigns ownership of:
 - reporting and the associated responsibilities for financial management?
 - the preparation and review of financial reports?
- Has the agency established a reporting framework that requires tailored reporting which aligns to the organisational and program structure? Does it work for all levels of management?
- Is management consulted regularly to ensure reporting is tailored to suit their needs?
- When was the last time the framework was reviewed?

Financial information

- Does reporting include information on all material revenue, expenditure, assets and liabilities? If not, how is performance being monitored?
- Are agency officers provided with relevant non-financial information that provides context for the financial data? Does this information include key workforce, project, service/program, strategic plan, operational plan and service delivery statement (SDS) metrics and data (outputs and outcomes)?
- Is comparable information provided—original budget, forecast, internal and external benchmarks, and key financial ratios?
- Does the provided commentary and material variance analysis enable an agency officer to identify the cause of variances, the action taken to fix them, and the impacts on future forecasts, emerging risks and opportunities?

Staff capabilities

- What financial management capabilities do agency officers have?
- Does the agency provide training in financial and budget management and associated system use?
- Does agency management require explanations from the Chief Financial Officer or business support staff to understand the reports provided?

System and process

- How does the agency know if the reported information is reliable and accurate?
- How does the agency know all the transactions and events are captured in reporting?
- How does the agency know that reporting systems and processes are efficient and effective and timely?
- When was the last time reporting systems and processes were reviewed?

Appendix F—Assessing disaster recovery planning

The information technology (IT) disaster recovery plan should outline the resources, actions, tasks, IT systems and data that are required to be recovered in the event of a disaster and or business interruption. Key aspects that need to be considered in developing or updating IT disaster recovery plans include business impact analysis, the plan aligning with business needs and a robust recovery process. The following questions need to be answered and addressed for all departments.

Business impact analysis

- Has a business impact analysis been documented and approved?
- Does the business impact analysis list each key business process, ranked in terms of priority?
- Does it include the allowable period for a disruption and expected recovery point?

IT disaster recovery plan

- Has the IT disaster recovery plan been documented?
- Is there a register of IT and information assets ranked by priority based on how critical they are to the business? Does the register include information on IT services that have been outsourced and the level of disaster recovery services associated with each service? Does the plan include:
 - The procedure for invoking the plan?
 - Priority for restoring business services?
 - Effective mitigation measures for all critical business process infrastructure components?
 - The estimated time required to restore each key business service?
 - Backup schedules and policies?
 - Communication protocols to be followed in the event of a disaster?
 - Recently updated contact details of suppliers, business stakeholders and staff?
 - Maximum outage time as defined by business?
 - Recovery time and point to recover to?
- Are staff trained in using the plan?
- Is the plan located off-site as well as on the premises?
- Is the plan updated in response to changes in business and emerging technologies?

Recovery

- Is the plan regularly reviewed?
- Is the plan tested at least twice a year?
- Is the plan updated based on any lessons learnt during testing?
- Have the recovery processes been communicated across the agency?
- Are any changes to the recovery process communicated with the business?
- Is backup and recovery equipment regularly tested?

Appendix G—Department acronyms

Government departments:

- Department of Aboriginal and Torres Strait Islander Partnerships (DATSIP)
- Department of Agriculture and Fisheries (DAF)
- Department of Communities, Child Safety and Disability Services (DCCSDS)
- Department of Education and Training (DET)
- Department of Energy and Water Supply (DEWS)
- Department of Environment and Heritage Protection (DEHP)
- Department of Health (DOH) (which does not include the Hospitals and Health Services)
- Department of Housing and Public Works (DHPW)
- Department of Infrastructure, Local Government and Planning (DILGP)
- Department of Justice and Attorney-General (DJAG)
- Department of National Parks, Sport and Racing (DNPSR)
- Department of Natural Resources and Mines (DNRM)
- Department of Science, Information Technology and Innovation (DSITI)
- Department of State Development (DSD)
- Department of the Premier and Cabinet (DPC)
- Department of Tourism, Major Events, Small Business and the Commonwealth Games (DTEsb)
- Department of Transport and Main Roads (DTMR)
- Public Safety Business Agency (PSBA)
- Queensland Fire and Emergency Services (QFES)
- Queensland Police Service (QPS)
- Queensland Treasury (QT).

Appendix H—Glossary

**Figure H1
Glossary**

Term	Definition
Accountability	Public sector entities have a responsibility to achieve their objectives in reliability of financial reporting, effectiveness and efficiency of operations, compliance with applicable laws and reporting to interested parties. This is accountability.
Accrual basis of accounting	The effects of transactions and other events are recognised when they occur (and not as cash or its equivalent is received or paid) and they are recorded in the accounting records and reported in the financial statements of the period to which they relate.
Comparative information	This refers to the amounts and disclosures included in the financial report in respect to prior periods (in accordance with the applicable accounting framework).
Internal benchmarking	This is the comparison of data against internal measures, for example, comparisons of actual results per area or division, comparison to internal budgets, prior year actuals, internal ratio or key performance indicators.
Financial position	This is the economic condition of an agency, having regard to its control over resources, financial structure, capacity for adaption and solvency.
Material information	This is information that if omitted, misstated or not disclosed, has the potential to affect the economic decisions of users of financial reports or the discharge of accountability by management or those charged with governance.
Misstatement	This refers to a difference between the amount, classification, presentation or disclosure of a reported financial report item and the amount, classification, presentation, or disclosure that is required for the item to be in accordance with the applicable financial reporting framework. Misstatements can arise from error or fraud.
Performance	This is the proficiency of an agency in acquiring resources economically and using those resources efficiently and effectively in achieving specified objectives.
Perspective financial information	Financial information that looks at the past and describes the impact on the next future period.
Prospective financial information	Financial information that is based on assumptions about events that may occur in the future and possible actions by the agency. It is highly subjective in nature and its preparation requires the exercise of considerable judgement. Prospective financial information can be in the form of a forecast, a projection or a combination of both, for example, a one year forecast plus a five year projection.
Retrospective financial information	Financial information that looks backwards and explains what has happened.
Risk appetite	The amount and type of risk that an agency is willing to take in order to meet their objectives.

Term	Definition
Statement of cash flows	These are reports on an agency's cash flow activities, particularly its operating, investing and financing activities.
Statement of financial position	These are reports on an agency's assets, liabilities, and equity at a given point in time.
Material variance	A variance is considered to be material if it exceeds a certain percentage or dollar amount or if its presence or absence would alter the decisions of a user of an agency's financial statements.

Source: Queensland Audit Office

Auditor-General Reports to Parliament

Reports tabled in 2015–16

Number	Title	Date tabled in Legislative Assembly
1.	Results of audit: Internal control systems 2014–15	July 2015

www.qao.qld.gov.au

Linked 

Queensland Audit Office

