

# Results of audits: Internal control systems 2013-14

Report 1 : 2014–15



---

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](mailto:qao@qao.qld.gov.au)

Online [www.qao.qld.gov.au](http://www.qao.qld.gov.au)

---

© The State of Queensland. Queensland Audit Office (2014)

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: 10668



July 2014

The Honourable F Simpson MP  
Speaker of the Legislative Assembly  
Parliament House  
BRISBANE QLD 4000

Dear Madam 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 2013–14 (Report 1 : 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', with a stylized flourish at the end.

Andrew Greaves  
Auditor-General



# Contents

<b>Summary .....</b>	<b>1</b>
Conclusions .....	1
Recommendations .....	4
Reference to comments .....	4
<b>1     Context.....</b>	<b>5</b>
1.1    Management responsibility .....	6
1.2    Audit responsibility .....	6
1.3    Structure and cost of the report.....	8
<b>2     Financial controls.....</b>	<b>9</b>
2.1    Background.....	10
2.2    Conclusions .....	10
2.3    Findings from our selective control testing .....	10
2.4    Shared services .....	12
2.5    Prior year audit issues—monitoring controls.....	13
<b>3     Risk management.....</b>	<b>15</b>
3.1    Background.....	16
3.2    Audit objectives .....	16
3.3    Conclusions .....	17
3.4    Summary of findings .....	17
3.5    Risk management frameworks.....	18
3.6    Risk management processes.....	22
3.7    Optimising risk management.....	26
<b>4     Financial delegations .....</b>	<b>27</b>
4.1    Background.....	28
4.2    Audit objectives .....	28
4.3    Conclusions .....	28
4.4    Summary of findings .....	28
4.5    Delegation framework .....	29
4.6    Delegations in operation .....	31
<b>Appendix A— Comments.....</b>	<b>39</b>
<b>Appendix B— 2007 recommendations .....</b>	<b>46</b>
<b>Appendix C— Entity acronyms .....</b>	<b>49</b>



## Summary

---

Financial controls are the structures, organisational capabilities, systems, processes, procedures and activities within entities that operate together to reduce the risk of fraud and error in financial reports. Controls do not and cannot eliminate these risks altogether—the cost of attempting to do so could outweigh benefits such as further improving the precision of amounts in the annual financial statements.

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

The Queensland Audit Office, as the external auditor, needs to consider the financial controls capability of each entity when planning our financial audits. We do this by first evaluating the design of financial controls. If they appear to be designed and implemented well and we consider it is efficient for us to rely on those controls, we may then test all or some controls in operation. If there are control deficiencies, we will rely on more substantive procedures to test management assertions.

This report summarises the results of our evaluations of the systems of financial controls and of our selective testing of controls that operated within the 21 government departments during the 2013–14 financial year. These departments account for most of the revenues and expenses of the General Government Sector.

The controls we choose to rely upon and to test differ between organisations and vary over time. This year we scrutinised the effectiveness of delegation of financial responsibility in all 21 departments and compared this to five other public sector agencies. We also examined the risk assessment processes used by accountable officers to manage their entities financial risks.

## Conclusions

The significant decline in the number of control weaknesses we identified this year points toward greater maturity and strengthening of systems of financial controls. This is a positive result that lowers the risk of fraud and error occurring or remaining undetected.

Building on this strong foundation, departments can now turn their focus to the efficiency of their systems of controls. In this respect, more sophisticated risk management processes will balance risk and controls better; strengthening controls that are important and reducing or eliminating unnecessary controls.

There is significant scope also to better harness the functionality afforded by IT systems to streamline expenditure processing without weakening control. Post-processing compliance checking can complement this approach to maintain controls effectiveness.

## Summary of results of our selective control testing

Figure A illustrates the change in the number of significant control weaknesses we identified across all departments for 2013–14 compared to the previous financial year.

**Figure A**  
**High or moderate risk control weaknesses in departments**

Controls element	2012–13		2013–14	
	Departments number	Issues number	Departments number	Issues number
Control environment	8	15	6	9
Control activities	15	66	6	26
Information systems	7	22	7	25
<b>Total</b>		<b>103</b>		<b>60</b>

Source: Queensland Audit Office

### Control environment—the foundation for effective controls

The control environment in departments has improved, and most prior year issues have been addressed. Opportunities remain to further strengthen aspects of the control environment:

- shared service arrangements—documenting service level agreements that clarify respective roles, responsibilities and performance expectations
- legislative compliance—implementing monitoring and reporting tools to better manage compliance with statutory obligations.

### Control activities—checks performed over transactions and balances

Both the number of departments with weaknesses in their control activities, and the number of issues identified, fell by 60 per cent. This demonstrates that internal control systems have matured following the machinery of government changes in 2012.

We were concerned last year by the lack of segregation of incompatible duties across expenditure, payroll and revenue. This year, we identified only one issue relating to the lack of segregation of duties.

### Information systems—controls over reliability, availability and security of financial data

Information security remains the primary area of audit concern, making up 84 per cent of information systems issues identified, compared to 64 per cent in 2012–13 and 83 per cent in 2011–12. The main security weaknesses identified were:

- inadequate review of system user roles and their activities
- users having inappropriate access to sensitive or restricted transactions
- vulnerability to external attack from the internet
- management of 'privileged' accounts, including restricting access to these accounts and monitoring of account activity.

## Summary of results of our sector-wide controls testing

In addition to our selective controls testing, this year we also focussed the effectiveness of the delegation of financial responsibility as well as risk management.

### Risk management

Approaches to managing risks are basic, focusing on 'de-risking' and providing comfort that risks are managed to remain at or below established risk tolerances. Much can still be done to make this a more sophisticated exercise that embraces risk management as part of an innovation agenda.

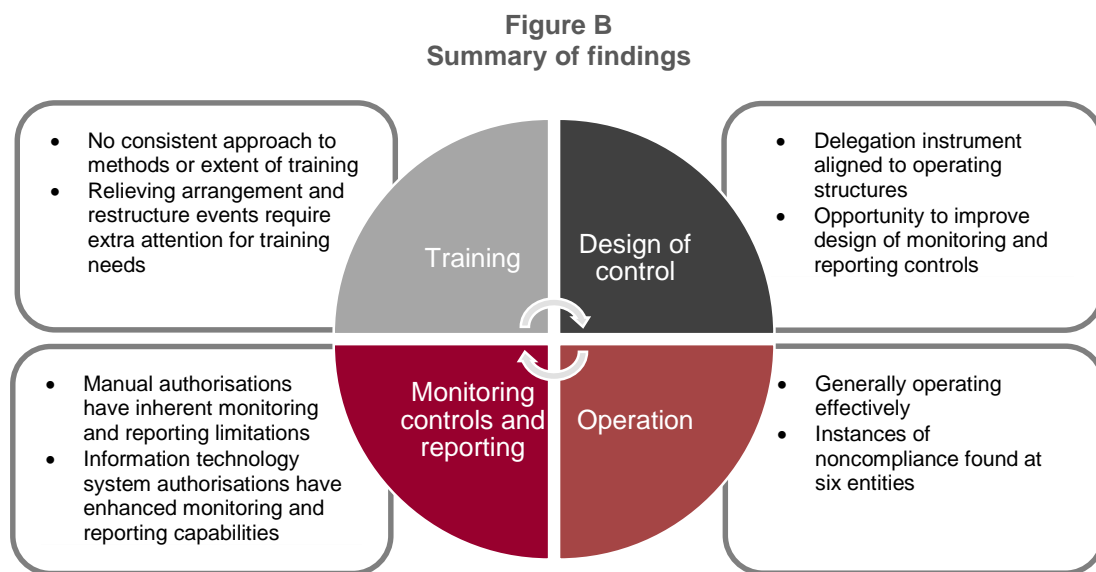


Two areas for improvement are the better integration of risk management and organisational planning; and better monitoring of risks and risk treatments.

- Only ten of the 24 entities we examined (42 per cent) integrate their risk management process well with their strategic and operational planning processes.
- In 17 entities (71 per cent) monitoring of risks and risk processes is not fully effective. In these entities, it was evident that risks had not been reviewed regularly; and governance committees were receiving limited information about the progress and effectiveness of new treatments to mitigate identified risks.

## Financial delegations

Figure B summarises our findings in scrutinising financial delegations.



Source: Queensland Audit Office

Financial delegation policies and instruments of delegation are well designed and align with each entity's operations and organisational structures.

All entities use some form of manual authorisation for their financial delegations and can leverage their information technology better so approval processes are made more efficient.

We found no evidence of systemic misuse of delegated authority. We detected instances of noncompliance at six entities where officers breached their financial delegation limit, and one case where authorisation inappropriately came from an individual at the entity's shared services provider.

Monitoring of delegated authority focuses on material purchases and payments. This is likely to be less effective at detecting low-value breaches of delegation limits, leaving entities exposed to misuse of these financial delegations. This risk can be mitigated by better use of forensic data analytics.

## Results of controls testing of shared services arrangements

The Queensland Shared Services control environment is effective: we assessed 46 of its 49 internal control objectives as having been achieved. We identified 14 moderate and two high risk control issues during the audit and made recommendations for corrective action.

Management has responded positively to our audit recommendations: many recommendations were resolved during the audit and management plans to remedy the remaining issues within reasonable time frames.

## Prior year audit issues: monitoring of controls

Our report to Parliament *Results of audit: Internal control systems* (Report 6: 2013–14) focused on monitoring controls within departments, including the chief financial officer (CFO) certifications, internal audit functions and audit committees. We also reported on controls over corporate cards.

### CFO Certifications

Most departments have improved processes and assurance programs to support the CFO certificate, which assures the Director-General about the adequacy of the risk management systems and financial internal controls.

### Internal audit

The number of long-outstanding, high-risk issues raised by internal auditors has decreased since last year. Some entities are strengthening the internal audit function with an internal or external peer review. One entity does not align itself with a better practice recommendation for its internal audit function to operate independently from management but is taking steps to reduce the risk from this arrangement.

### Audit committees

Audit committees should operate independent of management to assist the Directors-General to discharge their responsibilities. Two entities have maintained the Director-General as the head of the audit committee for 2013–14. One department still has more members on the audit committee than the numbers recommended in Queensland Treasury and Trade guidelines.

### Corporate cards

Monitoring of corporate card expenditure patterns, defining benchmarks and developing usage targets could provide significant administration benefits. Progress has been limited on this front.

## Recommendations

The control matters raised in this report have been represented separately to each department as required by auditing standards, with the intent that where weaknesses and areas for improvement have been identified, each department takes its own remedial action.

## Reference to comments

In accordance with section 64 of the *Auditor-General Act 2009*, a copy of this report was provided to all of the entities 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

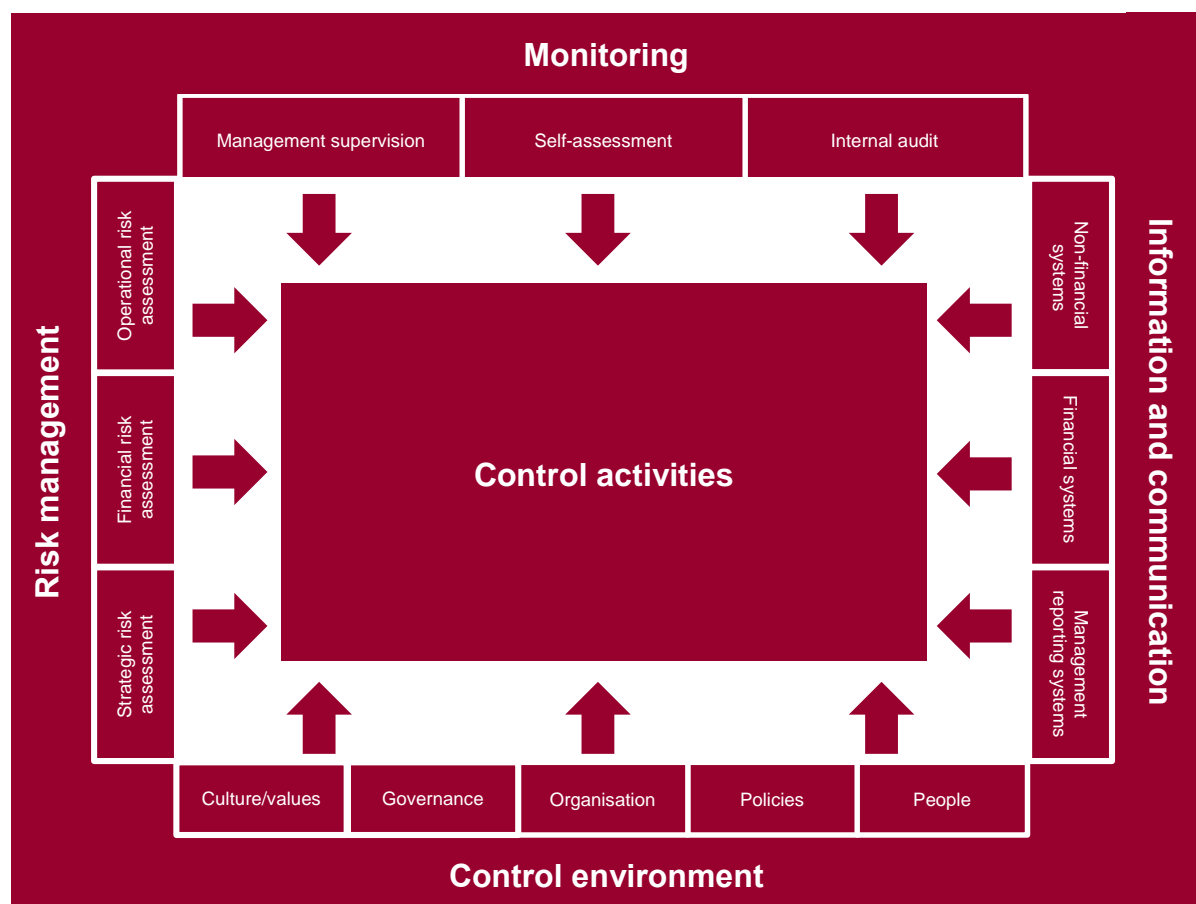
Financial controls are processes (including policies, procedures and systems) that are established, operated and monitored by the management of an entity to provide reasonable assurance to management and to its governing body about the achievement of its objectives.

When all of the components identified in Figure 1A are present in an integrated system of financial controls and they operate together effectively, it reduces risks to achieving objectives to levels acceptable to management.

Financial controls cannot eliminate risk. They operate to assure the governing body and management about:

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

**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, 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, policies and values that influence day to day operations. Control environment factors include management's integrity and operating style; organisational culture and values, organisation structure and the assignment and delegation of authority; and processes for obtaining and developing qualified and skilled employees.
- **Risk management**—management's processes to consider risks to achieving the organisation's objectives, forming a basis for how the risks should be managed.
- **Control activities**—the policies and procedures implemented 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 assets and segregation of incompatible duties.
- **Information and communication**—the systems used to provide information in a form and time frame that allows employees to discharge their responsibilities; and the way that controls responsibilities are communicated throughout the entity.
- **Monitoring of controls**—the methods management employs to oversee and assess the operating effectiveness of control activities in practice. This may be achieved through ongoing supervision, periodic self-assessments and separate evaluations.

## 1.1 Management responsibility

---

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; and are to 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 adequate system of financial controls will help to ensure financial records and related information are complete and accurate; assets are safeguarded; and errors and other irregularities are prevented or detected and corrected. As the system of financial controls underpins the information presented in the annual financial statements, it helps these statements give a true and fair view of the entity's transactions and financial position for each financial year.

## 1.2 Audit responsibility

---

The FAA and the FPMS 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 primary objective of our financial audits, as identified in the Auditor-General of Queensland Auditing Standards which incorporate the Australian Auditing Standards, is to provide independent assurance to Parliament and the community that the information contained in the financial statements 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.

Because internal financial controls operate to produce reliable financial information and to comply with prescribed requirements, we are required to consider their effectiveness as part of our annual audit of each entity's financial statements.

This involves considering the design of relevant controls under each of the five core elements of the integrated control structure. At this stage of the audit, we review and evaluate each department's key internal controls to assess its capacity to prevent and detect errors that may result in a material misstatement of the financial statements.

Our assessment of the effectiveness of the agencies' internal controls influences the timing and extent of our audit procedures. If we consider the controls to be well designed and implemented, we may choose to rely on the operation of selected controls. If we plan to rely on controls, we are required by the auditing standards to confirm that they operated in practice as intended.

If, in our professional judgement, we determine that controls are not well designed; that any of the controls that we tested did not operate as intended; or that controls should be in place but are missing, we are required by the auditing standards to communicate such controls deficiencies to management. We assign a risk rating to any financial controls deficiencies we raise so management can gauge their relative importance.

Significant controls deficiencies must be communicated in writing to those charged with the governance of the entity and we assign these either a high or moderate risk rating:

- A **high** risk rating is applied where we have identified a serious control weakness or breakdown in the operation of a key control or combination of key controls, indicating the risk of material error or fraud in the financial statements is unacceptably high. These require prompt management action with a detailed action plan implemented quickly, generally within three months.
- A **moderate** risk rating is applied where we have identified a significant control weakness or breakdown in the operation of a control that it is not likely to prevent or detect the errors for which it was designed. These require management action with a detailed plan to be implemented within six months.

We assign a low risk rating to any other controls deficiencies we identify and these are more likely to be communicated directly to line management:

- A **low** risk rating is applied where we have identified weaknesses or breakdowns of a procedural or housekeeping nature and where the controls in question either relate to immaterial areas or if they are compensating, rather than key, controls. These require management action with a detailed plan to be implemented within twelve months.

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 entity were not performed adequately and properly, if the Auditor-General considers the matter to be significant enough to require inclusion in the report. By reporting on the significant control deficiencies we observed in departmental financial control systems, this report satisfies these requirements.

## 1.3 Structure and cost of the report

---

The findings detailed in this report focus principally on selective financial controls testing and risk assessments performed by management, one of the five elements of an integrated financial controls framework.

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 2013–14 financial year. These departments represent the bulk of the General Government Sector revenues and expenses.

Central to effective risk assessments is the establishment of a robust risk management approach that identifies, analyses, assesses, treats and monitors risks so that they are managed to a level which is acceptable to the accountable officer, statutory body or governing board in the achievement of the entities' goals (Chapter 3).

The accountable officer or governing body is also responsible for the efficient, effective and economical operation of the entity. To achieve this practically, the accountable officer or governing body may need to delegate certain functions or responsibilities to other staff. This year, we assessed the relevance and appropriateness of delegated financial authorities including the assignment, acquittal and management of delegated financial authorities (Chapter 4).

The Public Safety Business Agency and Queensland Fire and Emergency Services were created in November 2013 following a machinery of government change resulting from the September 2013 Keely review of emergency services. These agencies are establishing governance structures and developing a risk management framework and associated risk management practices. They have not been considered further in this report; however, recommendations for their risk management framework and practices and financial delegations have been provided to management where applicable.

Appendix A provides the comments and responses to recommendations, or a fair summary of these, by entities.

Appendix B details the recommendations from report to Parliament *Beyond Agency Risk* (Report 6 : 2007).

Appendix C provides a list of the entities included within the scope of this report.

The cost of the audit was \$290 000.

## 2 Financial controls

---

### In brief

#### Background

Financial controls are processes that are established, operated and monitored by the management of the entity to provide reasonable assurance about the achievement of the entity's financial objectives.

As part of our financial audit, we test the operating effectiveness of the integrated components within the financial controls framework.

#### Conclusions

Financial controls have improved this year, as departmental control environments have strengthened. This has a positive effect as it reduces the risk of fraud and error occurring or remaining undetected.

Information systems security remains the area of most audit concern and it requires much greater management attention and focus. The nature of information systems means errors and fraud are intrinsically harder to prevent and to detect.

#### Key findings

- The number of controls issues raised by audit has decreased significantly from 2012–13.
- Information systems security and related weaknesses remains the area of greatest exposure:
  - weak controls over changes to the vendor master file
  - delays in resolving long outstanding purchase order transactions
  - absence of reviews for payroll reconciliation and verification reports
  - inadequate review of user roles and system access.
- Shared service arrangements are not documented to clarify respective responsibilities and performance expectations.
- Some entities are not monitoring their legal compliance obligations.

## 2.1 Background

For entities to achieve their objectives, management needs to establish effective financial control processes including policies, procedures and systems. As part of our financial audit, we selectively test the operating effectiveness of the integrated control components within each department's financial control framework.

## 2.2 Conclusions

Financial controls have improved this year, as departmental control environments have strengthened. This has a positive effect as it reduces the risk of fraud and error occurring or remaining undetected.

Information systems security remains the area of most concern and requires much greater management attention and focus. The nature of information systems means errors and fraud are intrinsically harder to prevent and to detect.

## 2.3 Findings from our selective control testing

Across all departments, we reported 60 control weaknesses to management during 2013-14 relating to their control environments, control activities and information systems.

**Figure 2A**  
Number of control weaknesses reported to management

Control element	2012–13		2013–14	
	Departments	Issues	Departments	Issues
Control environment	8	15	6	9
Control activities	15	66	6	26
Information systems	7	22	7	25
<b>Total</b>		<b>103</b>		<b>60</b>

Source: Queensland Audit Office

### Control environment

The control environment sets the context within which control activities are undertaken. It establishes the control culture and includes matters such as the assignment of authority; the capacity and capability of staff; and the scope and currency of the strategies, plans, policies and procedures that guide operations.

Overall, we identified fewer issues. Seven departments where we identified issues last year have resolved those issues. We found new issues in four departments in 2013–14.

While aspects of the control environment in most departments (15 out of 21) were sound, we observed opportunities to improve selected policies and frameworks in six departments. The nine issues identified in these departments related primarily to

- lack of service level agreements for shared service arrangements
- absence of a reporting system to monitor compliance with legislation.

The roles, responsibilities and performance expectations are more likely to be misunderstood where financial services are performed by a shared service provider and a signed service level agreement is not in place.

Without an appropriate policy and framework to manage, monitor and report on legal compliance, departments are less likely to satisfy their legal obligations.



## Control activities

Control activities are the specific procedures established to protect assets; ensure reliable accounting records; promote efficiency; and encourage adherence to the organisation's policies. Effective controls provide early warning of weaknesses or susceptibility to error, support for timely reporting and early identification of irregularities. They include controls such as separating duties that are in potential conflict—like issuing invoices, recording and banking receipts and providing for doubtful debts. They also include reconciling general ledger accounts to bank statements and having purchasing officers verify and certify that the goods and services they ordered have been received before another independent officer approves and pays the supplier.

Compared to last year, we noted a significant decrease in the number of departments with control activity weaknesses (decrease of 60 per cent) and in the total number of issues identified (decrease also of 60 per cent). This improvement can be attributed to the maturing of financial control systems in place at departments since the machinery of government changes in 2012.

The major controls issues we identified were:

- weak controls over the authorisation of changes to the vendor master files—this increases the risk of unauthorised changes to vendor details such as bank account numbers, resulting in fraudulent payments made to incorrect bank accounts
- delays in clearing long-outstanding, unmatched items in the goods received/invoice received (GR/IR) account—this increases the risk of non-payment or failure to make timely payment of invoices and failure to detect fraudulent payments
- lack of review of payroll reconciliation and verification reports—this increases the risk of fictitious employees created in the system, employees paid incorrect amounts and employees' entitlement balances being incorrect.

A major controls deficiency found across the departments in the prior year was inadequate segregation of duties across expenditure, payroll and revenue. This increased the risk of errors or fraud being undetected as a single person may be able to process a transaction completely without any other independent check to verify its validity or accuracy. An officer with the ability to create new vendors in the system, raise an invoice from that vendor and make the payment of that invoice can potentially make fraudulent payments to his or her own bank account. We identified only one segregation of duties issue this year, indicating improvement in this area.

## Information systems

Information systems initiate, record, process and report transactions, including the related business processes relevant to financial reporting.

Information system controls operate at two levels:

- general controls that relate to the entire information system, such as logical security controls and controls over software development
- application-specific controls over data validation, authorisation, monitoring and reporting, such as inbuilt edit checks and the automated restriction of access to certain functions only to authorised delegates.

Together, these controls operate to restrict access to systems, data and programs to authorised users and to align their access rights properly with their authority and responsibility. Without adequate controls, it is difficult to safeguard information against unauthorised use, disclosure or modification, damage or loss and the integrity of the data cannot be guaranteed.

Information security control weaknesses remains the primary area of concern for departments, representing 84 per cent of information system issues identified, compared to 64 per cent in 2012–13. The main types of security weaknesses identified were:

- inadequate review of user roles and activities—this may result in staff members who have inappropriate system access not being detected on a timely basis
- users having inappropriate access to sensitive or restricted transactions—inappropriate access may give these users the ability to perpetrate fraud or result in the leak of sensitive information
- vulnerability to external attack from the internet—security breaches could compromise the department's systems, operations and confidential information
- 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 increases the risk of these users having inappropriate access and performing unauthorised and potentially fraudulent transactions.

## 2.4 Shared services

---

Queensland Shared Services (QSS) facilitates a range of corporate services to 19 of the 21 departments, excluding the Department of Health and the Department of Education, Training and Employment. These services include finance, procurement, human resource management, facilities management and mail support services.

These 19 departments need to take appropriate measures to gain assurance of the completeness and accuracy of financial transactions and that there are no material weaknesses in the end to end processing. External audit plays a role in this assurance process pursuant to the Australian Auditing Standard ASAE 3402 *Assurance Reports on Controls at a Service Organisation*. This standard requires the auditor to report on the systems' descriptions and the design and operating effectiveness of the controls at the service organisation.

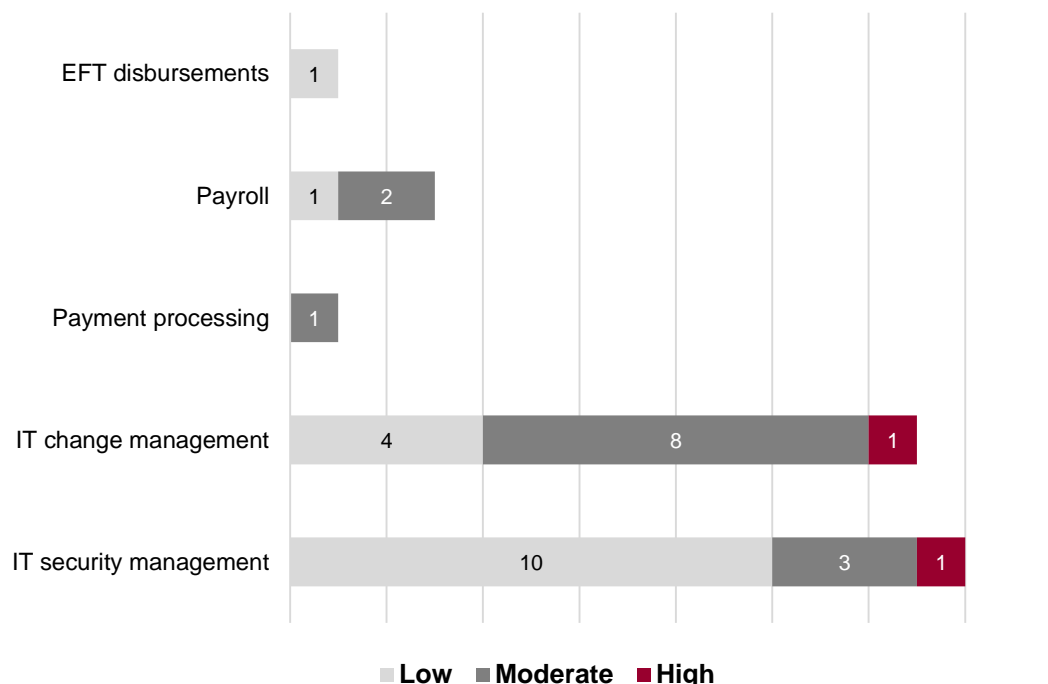
QSS engaged us to provide an assurance report on the descriptions of controls and whether the controls operated effectively throughout the period 1 July 2013 to 31 March 2014. The areas within the scope of the assurance report relate to payment processing, payroll, electronic funds transfer disbursements and general information technology controls.

We undertook a comprehensive review of the control environment to focus on those key processing controls with the potential to affect departmental financial statements. QSS identified financial reporting risks and documented 49 control objectives to address those risks.

The overall QSS control environment is suitably designed and the results of our audit show that 46 out of the 49 control objectives were achieved. Management has undertaken or planned corrective actions to address the control weaknesses.

We raised a total of 32 issues which comprised of 16 low, 14 moderate and two high risk issues. This is a slight decrease from the 34 issues raised in total for the 2012–13 financial year. Figure 2B provides a summary of the number and risk rating of issues raised for each control area.

**Figure 2B**  
**Number of issues and risk rating by control area**



Source: Queensland Audit Office—Queensland Shared Services ASAE 3402 Assurance Report

Additional audit testing did not identify any unauthorised transactions that would result in a material misstatement of financial statements for the client agencies.

## 2.5 Prior year audit issues—monitoring controls

Our report to Parliament *Results of audit: Internal control systems* (Report 6 : 2013–14) was tabled in Parliament in November 2013 and included a focus on monitoring controls within the main departments, including the chief financial officer (CFO) certifications, internal audit functions and audit committees. We also reported on the controls over corporate cards.

### 2.5.1 CFO Certifications

The *Financial Accountability Act 2009* requires each of the departmental CFOs to give a certificate each year to his or her Director-General, including a statement about whether the department's financial controls are operating efficiently, effectively and economically. The Financial and Performance Management Standard 2009 sets out the form of this certificate.

The purpose of the CFO certification is to provide confidence to the Director-General that the risk management systems and financial controls put in place by the CFO are operating and the likelihood of a material misstatement in the financial statements is low.

We found most departments have improved the design of the processes by better documenting how the process will work, consulting earlier with the Director-General and audit committees, and clearly aligning and describing the significant financial reporting risks with relevant account balances and with the key internal controls being assessed.

## 2.5.2 Internal audit

Last year, we found there were departments with high numbers of long-outstanding, high-risk audit issues. Departments have been proactive in reviewing their respective outstanding internal audit issues and have taken action to develop appropriate responses. The number of outstanding matters has significantly decreased. Some departments have instituted or are initiating internal or external peer review of their internal audit function as part of continuous improvement. Departments have evaluated and, where necessary, addressed the risk of potential under-resourcing of their internal audit functions.

Queensland Treasury and Trade (QTT) currently does not align itself with one accepted better practice, as the role of its head of internal audit (HIA) has been allocated to its CFO. These roles are inherently in conflict and this creates risk for the Under Treasurer and for the QTT audit committee in the ability of the HIA to maintain an independent outlook and achieve an appropriate balance in its internal audit program.

During 2013–14, QTT has modified the reporting protocol for the internal audit service provider to enable direct reporting to the Under Treasurer which mitigates the risk of the shared role to some degree. Further changes to this arrangement may occur as the result of proposed changes to the legislative requirements.

## 2.5.3 Audit committees

The QTT guidelines suggest that the maximum number of members for an audit committee should not exceed six. The guidelines also recommend that the Director-General should not undertake the role of chair of the audit committee.

Last year, we found two departments had audit committee memberships larger than the recommended number and three departments had the Director-General as the chair.

While one department has resolved to appoint a new member as the chair, two departments currently retain the Director-General as the head of the audit committee for 2013–14.

Whilst this decision is at the discretion of the Director-General, the independence of the audit committee from management is restricted in these circumstances and could potentially limit the ability of the committee to objectively probe the departmental approach to risk management, financial controls, legislative requirements and governance framework.

There is also one department with more than six members on the audit committee which reflects the needs of the Director-General at that department.

It is important that the composition of the audit committees is reviewed regularly. The level of independence and expertise required to diligently address the needs of the departments may vary as changes to operations and risks evolve over time.

## 2.5.4 Corporate card controls

Last year, we reported that all departments could benefit from monitoring of overall corporate card expenditure patterns and from defining benchmarks and targets to maximise the benefits of corporate card use.

The response by departments to this finding has been limited in the short time frame since we tabled our previous report to Parliament *Results of audit: Internal control systems* (Report 6 : 2013–14). We will continue to follow the progress of the departments in this area and provide updates in future reports to Parliament.

## 3 Risk management

---

### In brief

#### Background

The *Financial and Accountability Act 2009* and the Queensland Treasury and Trade *Corporate governance guidelines for government owned corporations* require accountable officers, statutory bodies and boards to establish and maintain appropriate systems for risk management.

#### Conclusions

- The risk management frameworks of the 24 entities examined satisfy the minimum requirements, as do their processes for identifying and assessing risks. However, generally, risks and the treatments put in place to mitigate risks are not being reported on or actively monitored, reviewed and updated.
- Based on the mixture of risk appetites and tolerances, entities typically set and accept 'moderate' levels for their risks. This 'de-risking' approach does not necessarily fit well where entities are seeking to innovate, and may not achieve cost efficiencies if risks are being overly controlled.

#### Key findings

- 71 per cent of entities reviewed have prepared strategic and operational plans and have updated operational registers and strategic risk registers for 2013–14.
- In 17 of the 24 entities, there was no evidence that risks had been reviewed regularly.
- Most entities do not categorise cross-entity and whole-of-government risks in their risk registers or identify their role as contributor or lead in risk treatment.
- While there have been improvements since our survey in 2007, we identified 97 deficiencies across all elements of risk management control.

## 3.1 Background

---

Every public sector entity manages and deals with risk as a part of the delivery and improvement of public services.

The use of a disciplined risk management framework strengthens an entity's ability to deal proactively with uncertainty. Used effectively to create a risk management culture, a risk management framework can maximise value for money in service delivery by avoiding or limiting effects on service objectives and by fostering innovation.

### 3.1.1 Legislation and guidance

The *Financial and Accountability Act 2009* requires all accountable officers to establish and maintain appropriate systems of risk management.

The Financial and Performance Management Standard 2009 prescribes that the agency's risk management system must provide for:

- mitigating the risk to the department or statutory body and the state from unacceptable costs or losses associated with the operations of the department or statutory body
- managing the risks that may affect the ability of the department or statutory body to continue to provide government services.

Subsequent to changes to financial management legislation in Queensland in 2009 and the release of a new Australia/New Zealand risk management standard, AS/NZS 31000:2009 *Risk management - principles and guidelines*, Queensland Treasury and Trade and the Department of the Premier and Cabinet collaborated to develop and issue *A Guide to Risk Management* (the Guide). The Guide is not mandatory.

The purpose of the Guide is to provide an overview of the key concepts of risk management, and how the risk management process can be applied practically by any Queensland public sector agency.

### 3.1.2 Our previous findings on risk management

In 2007, we conducted a performance audit and reported on its findings in our report to Parliament *Beyond Agency Risk* (Report 6: 2007). Overall, we assessed agencies as having adequate systems in place to manage risk at the operational and project level, although at varying levels of maturity.

We found there were no established processes to identify and collate information on risks which may have a broader effect for government. We found risk management practices to be more inward focused, rather than looking at how risks identified in the agency may have wider implications for other entities and government as a whole.

Appendix B to this report includes a table of recommendations from *Beyond Agency Risk* and their current status.

## 3.2 Audit objectives

---

As part of our annual planning for each financial audit, we are required by the auditing standards to:

- assess the effectiveness of each entity's risk assessment processes
- examine each entity's risk registers to determine whether and how any risks identified could affect the risk of fraud or error in the financial statements.

Effective risk assessment requires a robust, entity-level risk management framework that identifies, analyses, assesses, treats and monitors each type of risk. This needs to be done within a strategic context that ensures the number and types of risks facing an entity—both individually and as a whole—are managed to a level acceptable to the accountable officer.

To form a positive conclusion, we expect that:

- for risk frameworks:
  - the risk management governance arrangements, policies and procedures are appropriate for the size of the entity and provide clear and comprehensive information and instructions to staff members to manage risk in their day to day activities, in a consistent manner, across all business areas in the entity
  - risk management is integrated with strategic and operational planning and is monitored through appropriate governance structures
  - risk appetite is established and clearly articulates risks acceptable to the entity
  - the risk management system is reviewed regularly so it remains appropriate and effective; and monitoring controls are established so management is informed about an entity's risk exposures and the effectiveness of its risk mitigation strategies to achieve its desired outcomes
  - risk management practices promote awareness and training in staff responsibilities to identify, report and manage risks and opportunities proactively, including contributing to the identification and management of whole-of-government risks
- for risk processes:
  - risks are identified, assessed and evaluated
  - treatment strategies are developed to mitigate risks
  - risks and risk treatments are monitored, and regularly reviewed and updated.

### 3.3 Conclusions

---

The risk management frameworks of the 24 entities examined satisfy minimum requirements, as do their processes for identifying and assessing risks. However, risks and the treatments put in place to mitigate risks are not being reported nor actively monitored, reviewed and updated.

This means risk registers become exercises in form, not substance. This problem is compounded in entities where risk management has not been well integrated into their planning. Much more is required so that risk assessments feed into planning, rather than the other way around. Risk management is a dynamic process.

Queensland's change agenda has been clearly expressed; however, there is no whole-of-government risk appetite statement communicated by central agencies to departments and statutory bodies. Based on the amalgam of entities' risk appetites and tolerances, entities are accepting risks to a 'moderate' level. This level of risk may not be appropriate in an innovation context, and may not achieve cost efficiencies if risks are being overly controlled.

### 3.4 Summary of findings

---

Risk governance and accountabilities for risk management have been established by most entities and documented within their risk management policies. However seven out of 24 entities (29 per cent) do not integrate risk management well with their strategic and operational planning processes.

Monitoring of risks was not fully effective in 17 of the 24 entities. In these entities, there was no evidence that risks had been reviewed regularly; and governance committees receive only limited information about the progress and effectiveness of new treatments to mitigate risks.

Entities predominantly do not separately categorise cross-entity or whole-of-government risks in their registers to enable a consistent and comprehensive assessment of strategic and operational risks across the public sector.



## 3.5 Risk management frameworks

---

A risk management framework uses policies, processes, strategies, systems and plans to identify, assess and control strategic, business change and operational risks. It describes the reporting required for governance bodies that lead and support an entity's risk management.

We assessed whether:

- risk governance and accountabilities are appropriate for the size of the entity and provide clear and comprehensive information and instructions to staff members to manage risk in their day to day activities in a consistent manner across all areas
- risk assessment is effectively integrated with strategic and operational planning
- the risk appetite has been established to articulate clearly the levels of risk acceptable to the entity
- communication about risk and training in risk is effective
- the risk framework is reviewed regularly to identify areas for improvement.

### 3.5.1 Risk governance and accountability

Governance arrangements should clearly define the accountabilities for strategic and operational risk management. This requires clear leadership at the top to set the strategic context and monitor the overall risk management approach, supported by relevant reporting.

All staff members should clearly understand their roles in identifying, assessing, treating, monitoring and reviewing risks. Ideally, a centralised risk management function provides adequate resources to implement, maintain and continuously improve the risk management framework on behalf of the entity.

The entities examined have:

- developed appropriate governance structures, consisting of boards of management or boards and audit and risk committees and other sub committees to oversee, monitor and review risk management activities and the risk management framework
- clearly outlined in their risk management policies and guidelines, the responsibilities of officers, staff and governance committees
- established a 'champion' for risk management.

We identified a number of issues with risk policies:

- Two entities did not have tailored risk management policies approved and in place at the time of the audit.
- Six entities did not have a risk escalation process set out in their risk management policies which requires that new or changed risks are escalated within an agency or to their Minister, depending on the assessed risk level.
- Six entities had not finalised or updated their risk registers.
- Two entities had not consistently identified risk owners for risks in their risk registers.

### 3.5.2 Integration into planning processes

Strategic and operational planning are integral components of the Queensland Government's performance management framework.

Division 2 of the Financial and Performance Management Standard 2009 relates to planning processes. This standard recommends that departmental strategic and operational plans identify and analyse the potential effects of key risks and/or critical issues to achieving each entity's vision and purpose.

To be integrated effectively, the risk analysis should be used as a planning input to help management determine the need for new strategies, initiatives or actions to achieve organisational objectives.



Seven of the 24 entities we examined (29 per cent) had not integrated risk management effectively into their planning processes for 2013–14. They had not coordinated their efforts and it is evident that they treat the update and review of their risk assessments either as exercises separate from their planning processes, or an 'after the event' process.

Typically, their risk assessments are being performed or updated after their plans are developed, rather than contributing to these plans:

- operational plans for 2013–14 at six of the seven entities were still under development or had not been started
- in all seven entities, strategic and operational risk registers were under development or had not been reviewed and updated.

The key reasons given by officers of these entities for delays in completion of plans and the development of risk registers were:

- machinery of government changes
- internal restructures and reviews
- changes of strategic focus.
- changes in risk management focus.

In entities with strategic and operational plans in place, the linkages between risks identified in risk registers and the objectives and strategies in their plans were not always made explicit and so were unclear:

- three entities do not include their key strategic risks or challenges in the strategic plans
- six entities do not include operational risk and challenges in the operational plans.

### 3.5.3 Risk appetite and risk tolerances

Good risk management involves establishing the entity's risk appetite, as part of setting the organisational context within which risks are managed. Typically, this includes setting risk tolerance levels that, when exceeded, require escalation to pre-determined higher levels of management.

Risk appetite is the amount of risk that the agency is prepared to accept at any point in time. Risk tolerance is the variation from the pre-determined risk appetite an agency is prepared to accept.

Their use makes explicit each entity's unique attitude to risk, and their absence can lead to confusion over the levels of acceptable risk and to shortcomings in the response to risk.

In practice, an entity's risk appetite and tolerances are expressed in its risk management policy or through a specific risk appetite statement (RAS). A RAS should be dynamic, acknowledging the changing internal and external environment and should be reviewed annually and reassessed after significant events.

Figure 3A outlines the key attributes of an effective risk appetite statement.

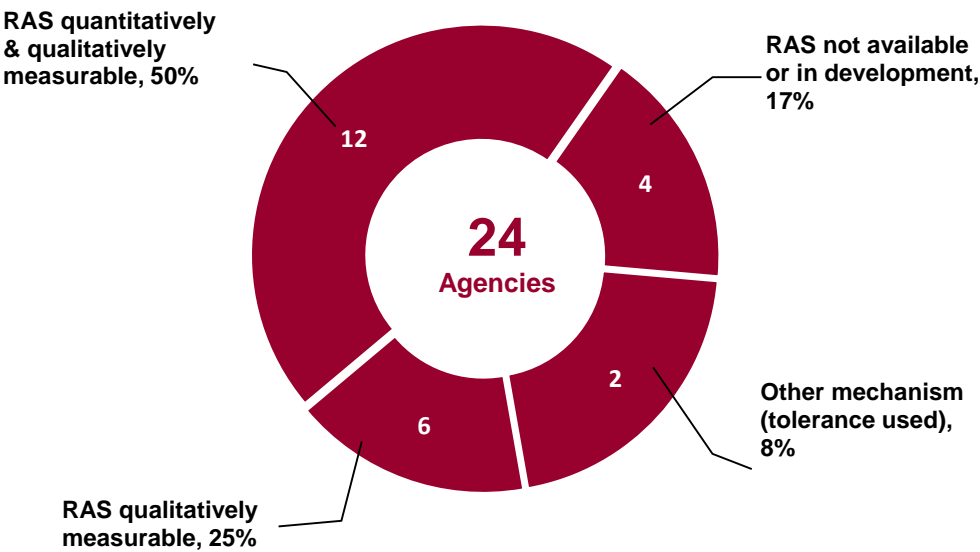
**Figure 3A**  
**Risk appetite**

Key attributes for an effective risk appetite statement	
<ul style="list-style-type: none"><li>• Aligned—is linked to the entity's mid and long term strategies.</li><li>• Complete—covers all fundamental risks in the agency risk profile.</li><li>• Measurable—contains a small number of succinct quantitative and qualitative statements used to define the risk that will or will not be assumed.</li><li>• Realistic—establishes a sufficient buffer between risk appetite and the entity's capacity to absorb risks/shocks and sets real boundaries that account for severe stress.</li></ul>	

Source: Adapted from 'Enabling more effective risk appetite frameworks', *Bank Governance Leadership Network, ViewPoints*, 26 September, 2013.

Figure 3B summarises the use of RAS and tolerance levels. It shows 18 of the 24 entities examined (75 per cent) use a RAS; two (eight per cent) express risk tolerance levels but without an overarching RAS; and the remaining four did not use either.

**Figure 3B**  
**Use risk appetite statements and tolerances**



Source: Queensland Audit Office

Of the 18 entities that use a RAS:

- four set different risk appetite levels by category of risk
- 10 use a common risk appetite level for all categories of risk or adopt a hybrid with different risk appetites for certain categories of risk and common or variable appetite for the remainder
- four vary their risk appetite for each individual risk, for which approval is escalated to higher management commensurate with the risk appetite applied—the greater the appetite sought, the higher the approval required.

Where used, risk appetites were assessed at either 'moderate' or 'low' risk levels. This meant 'moderate', 'high' and 'extreme' risks were considered for remedial treatment. The exception to this was Queensland Police Service where a high risk appetite has been set for three categories of risks; in isolated cases, a high risk appetite was set for individual risks by entities that varied risk appetite on an individual risk basis.

### 3.5.4 Communication and staff training

Effective communication and training helps staff understand and embrace the corporate commitment to risk management.

Staff awareness of risk management can be improved in 17 of the 24 entities examined. All entities relied on staff reading risk management policies and associated guidelines on the intranet. At 13 entities, discussions at team meetings, specific forums led by the risk coordinator, staff seminars, newsletters and staff bulletins enhanced risk awareness.

Training in risk in one-third of entities was ad hoc and informal, or conducted by departmental officers as needed.

Larger departments, statutory bodies and government owned corporations had communication and training strategies that were more formally developed. Some examples of better practice identified include:

- a high level overview of risk management is provided as part of induction training
- risk training needs analysis is completed after conducting an internal review of divisional risk management practices
- risk is a standing agenda item for discussion at staff seminars
- risk management newsletters, a risk awareness and cultural program and risk training is recorded and monitored
- an online risk management training module is being developed.

### 3.5.5 Continuous improvement

Periodic review of the risk management framework keeps it relevant to the changing needs of an entity.

Audit and risk committees in all entities were responsible for this review. All entities had processes in place so that their risk policies and associated guidelines were reviewed and updated at least every two years.

Half of the entities had independent reviews performed either by their internal audit function or an external consultant that covered:

- risk maturity
- risk culture
- risk registers
- governance arrangements including risk management.

Reviews that are performed by independent experts may provide greater assurance that risk management activities represent best practice and are effective and efficient.

A number of entities had planned to conduct independent reviews in 2013–14 and postponed these reviews due to our review. Six entities, established in 2012 following machinery of government changes, have indicated they will commence independent reviews once their risk management processes have been embedded.

## 3.6 Risk management processes

---

The Guide and standards define a logical risk management process:

- Risk identification—this process produces a list of risks and opportunities organised by risk category for all areas of an agency's business. The focus for risk identification is to gain an understanding from the universe of potential events that make up the agency's risk profile. The list requires prioritisation to focus senior management attention on key risks. Risk assessment accomplishes this prioritisation.
- Risk analysis and evaluation—without a standard process for comparison, it is not possible to compare and aggregate risks across an agency. Risk evaluation assesses the size of the risks, both individually and collectively, to focus attention on the most important threats and opportunities and to lay the groundwork for risk response.
- Risk treatments—the results of the risk evaluation process are used to determine a risk response to accept, reduce, share, or avoid the risk. Cost-benefit analyses are performed, a response strategy is formulated and a risk treatment plan is developed
- Monitoring risks—the monitoring process uses risk information gathered to make decisions about the effectiveness of risk responses and control activities in mitigating risk and feeds this information back into the strategic planning process.

### 3.6.1 Risk identification

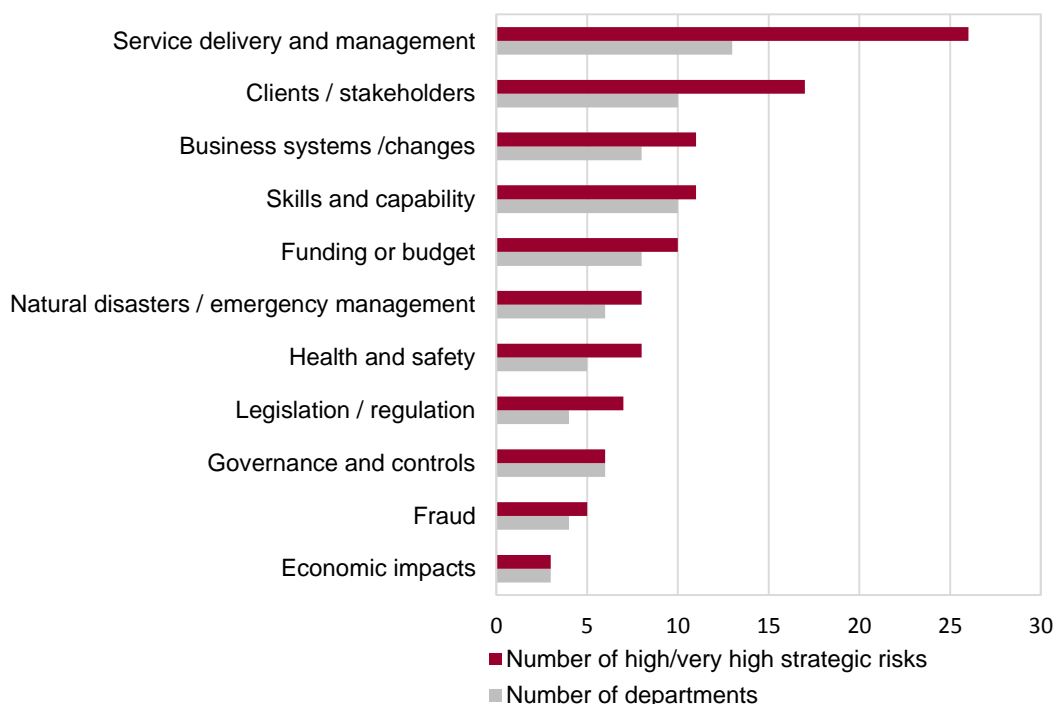
The risk identification process considers sources of risks, their causes and their potential consequences. It should be done systematically: both 'top down'—starting with threats to the achievement of strategic and operation objectives—and 'bottom up'—by considering risks associated with the nature of services delivered and the resources used in their delivery.

We found generally that risk identification processes are not documented, with the creation or update of a risk register being the only defined output once the process is complete. This lack of documentation makes it difficult to demonstrate that a systematic approach has been adopted and that all likely risks have been identified.

Numerous methods were employed to identify risks; including workshops, SWOT analysis, environmental scanning and discussions with key stakeholders. Entities recognised risks from all areas in the business, both internal and external.

The scale and criteria used in the risk assessment matrices of the entities is individually determined. Figure 3E provides a consolidated view of the risk registers of the entities we examined, showing the categories and numbers of strategic risks they assessed as being 'very high' or 'high'.

**Figure 3C**  
**Consolidated view of very high and high strategic risks**



Source: Queensland Audit Office

These risk assessments by entities, if comparable, indicate that most entities regard the area of frontline service delivery as their highest risk before treatment. Specific risks identified include:

- delivering on government commitments and managing multiple reform initiatives
- delivering on value for money outcomes
- having capacity and infrastructure to meet demand.

The identification of new and emerging risks was largely tied to risk register reviews and monthly management committee meetings and to reports provided to those meetings by risk owners.

QIC maintains breach and incident reporting registers to record potential risks and document its escalation processes. Officers in this agency are required to report all incidents and breaches within 24 hours of identification. Having a process that allows for the collation and reporting of significant and emerging risks in a timely way increases the effectiveness that this agency has in dealing with unexpected events.

### 3.6.2 Risk analysis and evaluation

There are four key principles for assessing risk:

- ensuring that there is a clearly structured process in which likelihood, effect and proximity are considered for each risk
- ensuring that the effect criteria includes qualitative and quantitative measures that can be understood by staff and are easily measurable
- recording the assessment of risk to monitor and identify risk priorities
- being clear about the difference between inherent and residual risk and recording two separate assessments.

Inherent risk relates to the exposure arising from a specific risk before any activity has been taken to control it. Residual risk relates to the risk exposure remaining after the risk control has been applied.

Entities are using a variety of 'exposure' and 'likelihood' matrices to assess their risk levels. There were 17 entities (71 per cent) that used a "5x5" matrix, with exposure assessed using a scale from insignificant, minor, moderate, major, to severe, and likelihood assessed on a scale from rare, unlikely, possible, likely, to almost certain. The remainder of the entities used a matrix approach but with fewer categories.

All entities use detailed criteria to assess possible risk consequences and record these assessments:

- all use qualitative criteria for individual risk categories
- 15 entities (62 per cent) also use quantitative criteria that was measurable, such as per cent of budget expenditure, dollar loss or variation from approved budgets at each level of the agency
- all but one entity assess and record the residual risk levels after controls.

Best practice was identified in the risk assessment criteria of the Department of Education, Training and Employment (DETE). In this department risk assessment criteria are described both qualitatively and quantitatively. DETE also breaks down risk assessment criteria into areas—operations, programs and projects. QIC and the Public Trustee of Queensland consider, assess and document the speed at which a risk may arise, useful for developing risk response plans.

By contrast, we identified conceptual flaws in risk assessments in two entities, casting doubt on their efficacy and reliability:

- One entity identified risk treatments/controls against 11 financial risks, but these had no apparent effect on the residual risk rating. It would be expected that, after treatment, the residual risk would be lower than the untreated inherent risk.
- We identified 34 instances in another entity's risk register where the residual risk was the same as the untreated risk. In each case, a number of treatments had been identified and assessed as strong. Twelve risks had a residual and goal risk rating of low, but future treatments were identified as still being required.

### 3.6.3 Risk treatments

A risk treatment plan is required when the level of inherent risk is unacceptable and risk treatment is deemed necessary. The risk treatment can include establishing ongoing controls or specific corrective treatments.

Actions within a risk treatment plan should ensure the residual risk is within the stated risk appetite of the entity. The Guide recommends risk treatment plans identify responsible owners, treatment actions and time frames, physical resources required and a cost-benefit analysis of the alternate treatments. Regular reporting and monitoring of the status of approved treatments should be performed.

Our review of risk registers, risk treatment plans (RTP), and risk reporting to the audit and risk committee identified the following deficiencies:

- at three entities—lack of summary detail of RTP, or not consistently provided
- at nine entities—no implementation dates for RTP, or not consistently provided
- at six entities—risk status was not provided, or not consistently provided
- at one entity—risk reports separately identified control activities from risk treatments; however, in a number of instances, these activities were not classified appropriately, making it difficult to identify the risk treatments to be tracked and the control activities to be monitored for effectiveness.

The Guide encourages entities to use risk indicators where possible and to develop performance targets for these indicators. Such performance indicators may align with those already developed for strategic and operational planning. Example of risk indicators have been included in Figure 3D.

**Figure 3D**  
**Examples of risk indicators**

Risk	Risk key performance indicator
Budget—cost efficiencies not achieved	Cost to income ratio
Legal and regulatory risk	Number of regulatory compliance breaches
Investment risk	Investment performance compared to benchmark
Workplace, health and safety (WH&S) risks	Number of WH&S incidents compared to industry benchmark or prior year

Source: Queensland Audit Office

Risk indicators which provide a measure of the effectiveness of risk treatment plans and control activities are not widely used. QIC and the Queensland Treasury Corporation used risk metrics to assess effectiveness.

### 3.6.4 Monitoring risks and risk treatments

Systematic risk management reporting that periodically measures progress against, and deviation from, the risk management plan is a key governance process.

Responsibility for monitoring of risks varied widely from entity to entity and was undertaken by risk owners, audit and risk committee and executive-level committees and management committees.

The frequency of monitoring of 'extreme' and 'high' risks varied widely, from monthly to annually. Risk policies in 21 of the 24 entities required monthly or quarterly reviews of extreme and high risks to be undertaken.

We identified significant deficiencies with monitoring agency risks and risk treatment plans by audit and risk committees or executive committees:

- three entities—no evidence of monitoring of risks by audit and risk committees or executive committee
- one entity—lack of consistent review of risks by governance committees
- one entity—significant regional office risks not centrally monitored
- seven entities—ineffective monitoring due to strategic or operational risk registers being incomplete or in draft, or delayed
- twelve entities—information reported did not include a summary of risk treatments or their status or likely implementation date.

These results indicate significant systemic weaknesses in the quality of monitoring risks undertaken by entities governance committees.

## Case study 1

### Better practice—QIC risk management monitoring and reporting

A key risk register, detailing all strategic risks and key operational risks across the entity, is provided to the audit and risk committee at least quarterly. The key risk register is updated by the organisational risk legal and tax team, through consultation with business areas.

Two accompanying reports are provided to the audit and risk committee. The first identifies new risks added to the registers and movement of previous risks reported, using a heat map which accompanies the key risk register. The second report is an update report from the chief risk officer, outlining new and emerging risks for the industry and their effects on QIC, changes to policies and procedures recommended and effects of new or changed legislation.

The key risk register provides summary details of risks, the risk owner, assessments of inherent and residual risk, relevant control activities, risks within appetite being monitored and risks above appetite being treated. Risk treatment plan summaries include status, details about the plan, expected completion date and risk metrics. Predictive or lag indicators were developed to measure risk treatment plan effectiveness.

Business unit risk registers are required to be reviewed quarterly or on identification of a new risk by business units. These registers are presented annually to the risk and compliance sub-committee on a rotational basis. Minutes noting the review of these registers are provided to the audit and risk committee. The chief risk officer chairs the risk and compliance sub-committee.

A separate breaches and incidents policy sets out the requirements for the escalation and reporting of incidents, events and breaches, including the reporting of an awareness of risk that could, if left untreated, become a breach. Breaches and incidents must be reported within 24 hours of an incident or compliance issue occurring. This information is recorded in an online register in SharePoint. Workflow ensures the risk is flowed or escalated to the appropriate officer or board for action. Reports on themes and significant breaches and incidents are reported to the risk and compliance sub-committee, the audit and risk committee and to the board. New issues are added to risk registers as appropriate.

The QIC chief risk officer and chief executive officer provide a monthly and yearly attestation to the Board on risk identification and management

Source: Queensland Audit Office

## 3.7 Optimising risk management

The Guide does not contain guidance on the State's risk appetite, tolerance and capacity for risk. It recommends entities set their own risk appetites after conversations with their stakeholders and Minister and consider commitments expressed by Parliament or Cabinet.

Most agency risk registers do not classify the risks they identify as cross-sector or whole-of-government; or identify if the agency is the lead or a contributor to cross-sector or whole-of-government risks. The Department of Aboriginal and Torres Strait Islander and Multicultural Affairs was the one entity that included this additional information in its strategic risk register.

Cross-sector risks are being identified only through informal networks between staff in other entities, or through attendance at cross sector committees or meetings.

By contrast the *Western Australian government risk management guide* requires entities to assess how wide the consequences of a risk could reach. The impact range descriptors used include:

- state-wide
- metro-wide
- directorate-wide
- division-wide.

This approach would allow easier identification and treatment of the common causes of cross-sector and whole-of-government risks.



## 4 Financial delegations

---

### In brief

#### Background

The accountable officer of a department, statutory body or government owned corporation's board is responsible for the efficient, effective and economical operation of his or her entity. To achieve this practically, accountable officers may need to delegate certain functions or responsibilities to other entities or the entity's staff.

#### Conclusions

- Financial delegations across the entities audited are well aligned with their organisational structures and the lines of authority to spend money were articulated clearly.
- Financial delegations are operating effectively.
- The strength of controls and information about exercise of delegation varied.

#### Key findings

- Instances of noncompliance with financial delegation policies were low.
- Monitoring controls used by most entities will only detect material errors in the use of financial delegations.
- Opportunities exist to improve the monitoring and review of financial delegations.

## 4.1 Background

---

The accountable officer of a public sector entity is responsible for the efficient, effective and economical operation of their entity. To achieve this practically, these officers need to delegate certain functions or responsibilities to the entity's staff or staff in other entities.

The power to delegate is contained in enabling legislation for statutory bodies, the *Government Owned Corporations Act 1993* for public sector companies and the *Financial Accountability Act 2009* for departments. An accountable officer, statutory body or board cannot delegate functions or responsibilities unless specifically allowed under legislation.

The challenge for the accountable officer is to optimise financial delegations in a way that contributes to the entity's objectives, complies with legislative requirements and produces value for money.

## 4.2 Audit objectives

---

As part of our annual financial audit, we routinely examine whether delegates have complied with their delegated authority. This year, we examined in greater depth:

- the frameworks used to establish delegated authority over financial transactions
- how well delegated authority operated over the period
- the forms of monitoring and content of reviews over the exercise of authority.

To form a positive conclusion, we expect that:

- there is strong alignment between the financial delegations hierarchy and the organisational hierarchy of the entity
- financial delegates understand the limits of their authority related to their area of operation and the extent of freedom of action available to them
- officers exercise their delegated authority in accordance with their entity's policies and procedures
- there is a continuous flow of information between the delegator and financial delegates about the efficient and effective exercise of authority
- management reporting and monitoring controls are in place so delegations are used appropriately and in compliance with documented policies and procedures.

## 4.3 Conclusions

---

Financial delegations across the entities audited are well aligned with their organisational structures and the lines of authority to approve expenditure are articulated clearly.

The use of financial delegations were effective, in accordance with policies and procedures. Most delegates demonstrated an understanding of their limits of authority.

Manual processing for expenditure vouchers remains the weakest type of authorisation and does not allow for the continuous flow of information about the exercise of authority.

## 4.4 Summary of findings

---

The design and implementation of financial policies and instruments at most entities was assessed as satisfactory. Financial delegations were aligned with organisational structures and have been appropriately reviewed.

Our sample testing of transactions across 26 entities detected 13 instances across six entities where financial delegations were exceeded. The reasons for this noncompliance included a lack of understanding of responsibilities, confusion over relieving arrangements or restructuring events. One of those instances related to expenditure being approved by an individual at the entity's shared services provider.

Entities mainly focus on monitoring controls which detect material errors in the use of financial delegations. As entities further adopt IS systems for expenditure authorisations, there are significant opportunities to improve the monitoring and review of financial delegations.

## 4.5 Delegation framework

---

### 4.5.1 Policies and procedures

Any framework for financial delegations will be covered by a policy and will have an associated instrument of delegation. These should be appropriately reviewed and approved. The policy should provide readers with a clear understanding as to the delegate's responsibilities and level of financial delegation authority.

Remediation or disciplinary action for noncompliance are covered through an entity's financial delegations policies and codes of conduct. Any areas of noncompliance should be recorded and promptly addressed by management. The evidence obtained from the monitoring controls allows an entity to determine the appropriate mitigation strategies.

### 4.5.2 Organisation structure alignment

A mature financial delegations framework will be closely aligned to the entity's lines of managerial authority—whether the organisation structure is aligned to key outputs, is hierarchical or flat in nature, or is centralised or decentralised.

We found all entities had clear and direct lines of delegated financial authority that were consistent with their organisation structures. Due to their large size and diverse regions of operations through Queensland, 14 of the entities we reviewed operate a decentralised organisational structure which aligns with their business activities.

All entities predominately had a hierarchical organisational structure. However the alignment of the delegation instruments varied with different types of delegations set by entities based on the nature, class and risk of the transaction. Transactions of higher risk, such as sponsorships and grant funding, followed a hierarchical structure where higher levels of delegated officers retained control over the authorisation. In contrast to lower risk recurrent transactions like rent and utility expenditure, the assignment of authority was much flatter where the lower level delegated officers could authorise the expenditure.

The results of the Queensland Commission of Audit's review on mobility and flexibility of the public sector suggested that entities are top heavy and congested with layers of management. The report's recommendations were for flatter organisational structures to enable a more responsive and streamlined decision making processes and to reduce administrative delays for business.

A restructure of the layers of management will require a review of operational and financial workflows. This will affect the allocation of financial delegations and responsibilities. The potential redesign of roles, consistent with the recommendations, may result in a smaller number of officers having a greater responsibility and elevated delegations for lower level officers. The key challenge for entities in transition is to delegate only to the extent required to achieve objectives whilst remaining within an entity's risk appetite ranges.

### 4.5.3 Communication and training

Ongoing staff training in the use of delegated authority increases each officer's understanding of his or her responsibilities. Formal training should be provided on commencement of a delegated position—whether permanent or temporary—and be reinforced by regular training updates. A more mature system would also regularly survey financial delegates so they understand their position requirements.

We found 16 entities have processes and procedures in place for delegates and other officers undertake formal training.

There was no consistent approach to the method and extent of training across the entities and, in some cases, within the various business units. Examples of training included:

- formal and informal one-on-one and group training
- induction, code of conduct, financial management and fraud training
- internal controls training and presentations
- webinars, online training courses and resources
- financial delegation competency assessment testing.

#### 4.5.4 Monitoring the delegation framework

The review of financial delegations is an opportunity for entities to reassess risk, operational changes and the findings from any monitoring controls to fine-tune the delegation limits and ensure the allocation is efficient and will deliver the entity's operational and financial objectives.

To remain current, the assignment of financial delegations should be reviewed at least annually and updated more regularly as positions and the organisation structure changes.

Although the review period was not always clear within some entities' policies, all entities have undertaken a review of financial delegations within the past 12 months.

## Case study 2

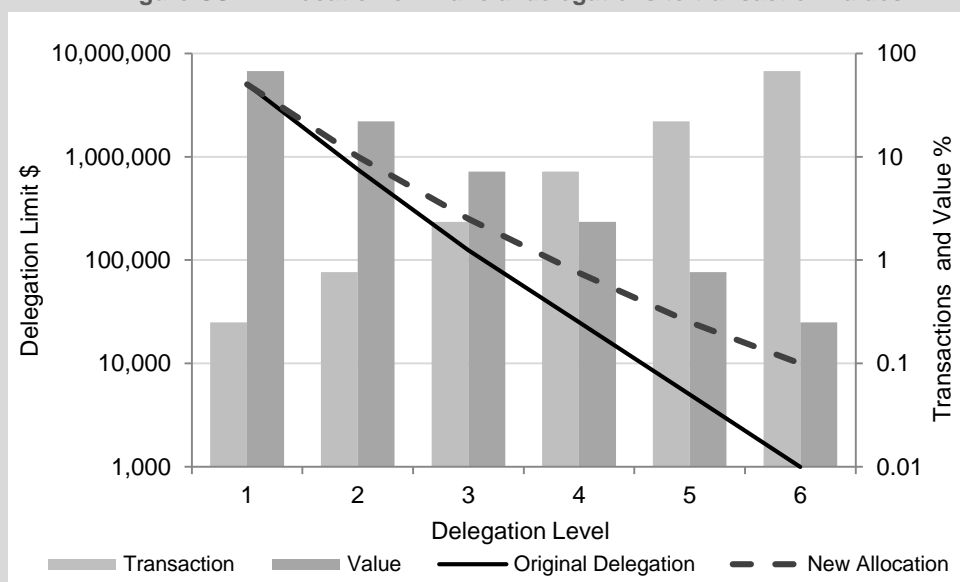
### Review of financial delegations

In reassessing the risks faced by a particular department, improvements in the financial transaction environment were:

- recent machinery of government changes have now settled and the new systems and processes have matured significantly since the merger of departments
- financial delegation training is being delivered on an annual basis so officers have a better understanding of their responsibilities
- an analysis of the expenditure transactions processed at the agency identified the majority of low value transactions under \$3 000 are now paid using corporate cards as we recommended in our report to Parliament *Results of audit: Internal control systems* (Report 6 : 2013–14).

As a result of these improvements, the agency has identified the opportunity for greater processing efficiency by increasing the lower level delegation limits. In this case, level 6 delegates can now authorise expenditure up to \$10 000 (original delegation \$1 000). The new allocation of financial delegations also reflects the changed risk profile of the department.

Figure CS2A Allocation of financial delegations to transaction values



Source: Queensland Audit Office

## 4.6 Delegations in operation

### 4.6.1 Financial delegation limits

The instrument of delegation for each entity should include the following:

- the delegation type
- list of positions holding each delegation type
- dollar or other thresholds for each delegation type
- any restrictions/limits (if applicable) placed on individual delegates.

The number of delegated levels, delegated officers and the limit assigned to each position varied for each department. We observed examples of delegations' limits allocated as a single set amount per position for specific individuals and other financial delegations within the same entity broken down into multiple types and limits levels.

Those entities that varied financial delegation of authority based on the category of expenditure discriminated between areas such as:

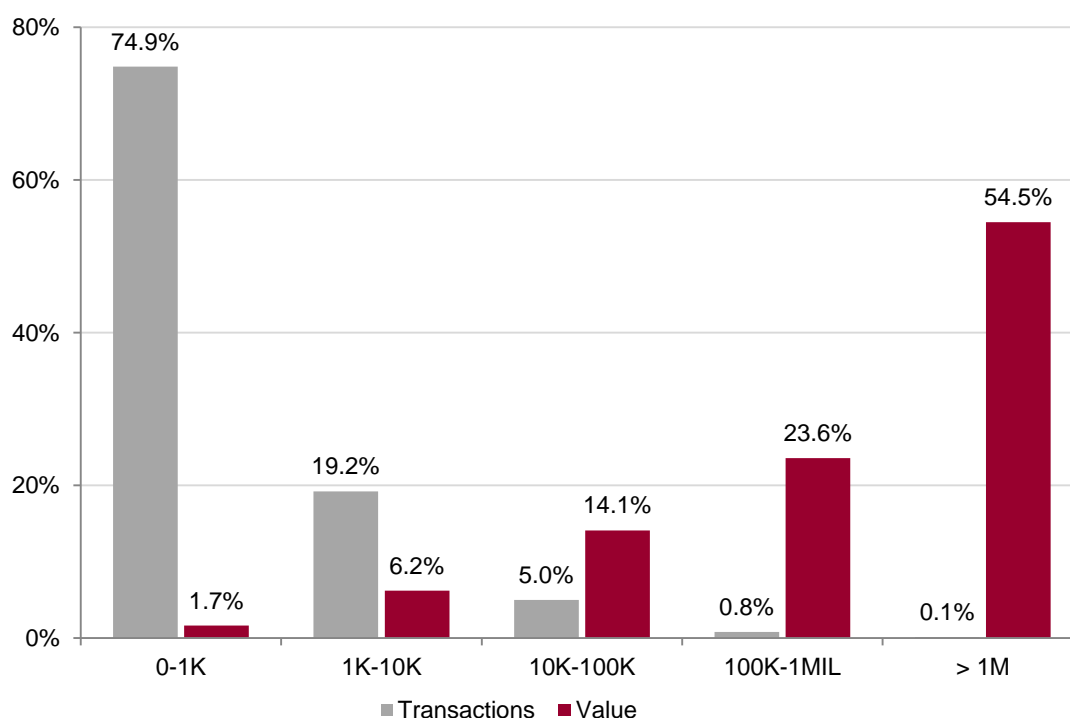
- procurement or direct invoice payment
- general expenditure, overhead, periodic and recurrent payments
- authorisation to enter into a contract and agreement
- grants and subsidies
- corporate card expenditure
- debt write offs, losses, asset disposals and special payments
- gifts, donations, entertainment and hospitality
- emergent works and disaster response.

For general expenditure, financial delegation limits are higher than the other categories of expenditure to allow for much larger transactions to be approved and are capped only by the budgets assigned to the various cost centres. This reflects the lower risk associated with these types of transactions. Some examples of recurrent expenditure include insurance, rent, electricity, rates, telecommunication, information technology maintenance, salaries and wages and shared service providers' costs.

At the highest level of delegation, the limit of financial delegations of authority by Directors-General is set at \$5 million. The respective Ministers of each budget department may approve the commencement of a project between \$5 million and \$10 million with Governor-in-Council approval required for all amounts greater than \$10 million. The lowest delegation limit most commonly observed was between \$1 000 and \$5 000.

Figure 4A analyses the combined number of transactions processed by all of the entities for the period 1 July 2013 to 31 January 2014, compared with the stratified dollar value of those transactions. This analysis indicates that 75 per cent of the transactions processed in that period, by number, represent less than two per cent of the dollar value.

**Figure 4A**  
**Stratification of number of invoices and total value**



Source: Queensland Audit Office

This distribution of transactions and value is consistent with the practice observed for setting financial delegation levels across all entities where the high value and low volume transactions are assigned to more senior staff levels.

## 4.6.2 Exercise of delegated authority

We tested a random sample of expenditure vouchers at each of the entities to assess the operation of the financial delegations. Our samples for 20 entities indicated full compliance with their respective financial delegation policy and delegation instruments.

For six entities, 13 instances of noncompliance with financial delegations were detected:

- one instance where the approving officer was from a business corporate partnership, not from the department
- 12 instances where delegation limits were breached, three of these during relieving arrangements and one during an organisational restructure.

We investigated all breaches of financial delegation limits and the underlying transactions were cleared of potential misuse of funds or fraud. The key causes of noncompliance were a lack of understanding by staff of the entity's delegation policy and changes to personnel roles and responsibilities due to relieving arrangements and restructuring.

## 4.6.3 Automating delegated approval and authorisation

A manual authorisation consists of a paper-based expenditure voucher which requires the delegate's signature, supported by the name and position title of the signing officer. The expenditure voucher usually requires a second signature from a recommending officer, which adds an extra layer of protection. Expenditure vouchers are then processed, based on these elements being present on the documentation.

A limitation of manual authorisation is the reliance on the user's knowledge of the correct and appropriate use of financial delegations. Signatures can also be forged so fraudulent transactions can be processed. 'One for one' checks of signature specimens are generally not conducted to confirm the identification of the authorising officer.

With a manual system of financial delegations, entities cannot analyse the approval of transactions easily. This can affect management's ability to review whether financial delegations are being used efficiently and effectively within the organisation.

The analysis of authorisations through information technology systems is not constrained by the inherent limitations of a manual paper based voucher system. Under an information technology system, access to approve expenditure transactions can be restricted to appropriate individual financial delegates. This can limit the amount of financial delegation errors and opportunities for fraud.

Other potential benefits of information technology systems over manual authorisation include:

- system segregation of duties for recommending and approving transactions
- automated, system-controlled approval workflows for financial transactions
- a complete electronic audit trail from purchase to pay
- the ability to analyse and report the efficiency and effectiveness of the use of financial delegations within the entity.

Information technology systems for financial delegations are used in 18 entities and these systems are at varying levels of maturity. All 26 entities still use a manual system for at least some portion of the expenditure transactions processed.

In November 2013, Queensland Shared Services started to implement the eForms system for departments, using SAP ECC5. eForms is a system for processing direct invoices and was initially established at the Department of Justice and Attorney-General. It has since been implemented at:

- Department of State Development, Infrastructure and Planning
- Department of Local Government, Community Recovery and Resilience
- Department of Premier and Cabinet
- Department of Science, Information Technology, Innovation and the Arts
- Queensland Police Service
- Department of Community Safety
- Department of Housing and Public Works.

eForms has a limited automated system workflow for the financial transactions processed. Where an information technology system does not have a fully automated workflow that enforces delegation limits, monitoring and exception reporting from those systems becomes more important.

This is a positive move away from the manual financial delegation systems. Entities using corporate cards for low value transactions will also benefit from the greater transparency that this electronic payment method provides.

#### 4.6.4 Monitoring the use of delegated authority

In a mature system of financial delegations, there is a continuous flow of information between the delegator and delegates about the exercise of authority. Management reporting and other monitoring controls ensure delegations are used appropriately and comply with documented policies and procedures.

All entities reviewed rely on a variety of high level mechanisms to monitor the use of financial delegations, including budget to actual reviews, internal audit and external audit work. The budget departments also use the process undertaken as part of the chief financial officer assurance statement to monitor compliance with financial delegations by staff members.

Of the 12 entities with centralised structures, two smaller entities perform a central review of all expenditure vouchers before they are processed, which incorporates checking for appropriate use of delegated authority. This preventative control requires additional resources and may not be appropriate for all entities.

All other entities rely on the individual delegated officers and monitoring controls designed to detect the instances of material misuse of financial delegations to ensure that the appropriate use of financial delegations occurs.

While this is the most efficient approach for maximum coverage over manual expenditure authorisations, the effectiveness of detecting the misuse of a financial delegation at values of less than \$1,000, which make up 75 per cent of all transactions, is significantly diminished unless lower levels of expenditure are specifically targeted.

Although 18 entities had information technology systems available for authorisation, none of the entities we reviewed solely relies on information technology systems and no entity had a fully automated workflow. Information technology systems also provide the opportunity to utilise forensic data analytic capabilities. These can be as simple as detecting noncompliance at all transaction levels. These capabilities may also extend to using the data to determine whether the current delegation design is being used efficiently or is causing bottlenecks at certain levels, negatively affecting the authorisation of expenditure.

For those departments who currently use eForms, self-service reporting is available, including a report on financial delegated approvers. As a direct monitoring control, this data could be analysed on a regular basis to enhance the department's monitoring and reporting capabilities.



The increased use of corporate cards for low value transactions would also allow for better monitoring control, due to the ability to analyse expenditure data and report the results to those charged with governance.

#### 4.6.5 Reporting

Robust exception reporting allows those charged with governance to determine the required responses to instances of noncompliance, including adjustments to the design of delegations or additional training.

Only one entity had a register to record delegation breaches and these are reported to the board. This process is used to prevent instances of noncompliance from occurring in the future. The process and procedures are covered by a documented policy.

None of the other entities we reviewed kept specific registers of delegation noncompliance, other than findings from internal or external audit reviews. When other instances of noncompliance with financial delegations are noted within these entities, they are corrected with minimal reporting of the noncompliance.



# Appendices

<b>Appendix A— Comments .....</b>	<b>39</b>
<b>Appendix B— 2007 recommendations .....</b>	<b>46</b>
<b>Appendix C— Entity acronyms .....</b>	<b>49</b>



## Appendix A—Comments

---

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

Responsibility for the accuracy, fairness and balance of the comments rests with the head of these entities.

## Comments received from Minister for Environment and Heritage Protection



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



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

-2-

Your whole-of-sector report does, however, indicate opportunities for strengthening delegation controls through the effective deployment of financial systems that allow for work-flowed approval of documents, as well as the deployment of 'smart e-forms'. This department utilises an old version of SAP which cannot support e-forms; however, is of the understanding that its SAP platform may be upgraded via the Department of Science, Information Technology, Innovation and the Arts led whole-of-sector projects within three financial years. The department will assess workflow approval/delegation opportunities as those system options crystalise.

One of the primary areas of audit concern raised in your draft report was information security. The department is attending to the matters raised in your 2013-2014 Interim Management Report issued 16 May 2014 and the implementation of those recommendations will help to address the information security concerns.

I wish to thank your team for their spirit of collaboration during this engagement, and look forward to working further with you during the conclusion of the audit process.

If you require any further information or assistance in relation to the responses provided in the draft report, please contact Ms Larissa Denysiv, Acting Director, Internal Audit and Compliances Services, Department of Communities, Child Safety and Disability Services on 3239 3382.

Yours sincerely



Michael Hogan  
**Director-General**



## Comments received from Director-General, Department of National Parks, Recreation, Sport and Racing



Our Ref: CTS 15027/14  
Your Ref: 10668



Office of the  
Director-General

Department of  
National Parks, Recreation,  
Sport and Racing

Mr Andrew Greaves  
Auditor-General  
Queensland Audit Office  
PO Box 15396  
CITY EAST QLD 4002

Dear Mr Greaves

Thank you for your letter of 17 June 2014 concerning the Queensland Audit Office report to Parliament, *Results of audits 2013-14: Internal control systems* (the Report).

While I acknowledge that the Department of National Parks, Recreation, Sport and Racing (NPRSR) has not been directly referred to in the Report, I appreciate the opportunity to respond to the areas of the report that are relevant to NPRSR.

#### Chapter 2 – Audit Committees

I advise that NPRSR now has an independent Audit and Risk Committee Chair.

#### Chapter 3 – Risk Management

I confirm that NPRSR recognises the strong alignment between operational planning and risk management, having made a commitment to finalise new operational risk registers that support service area operational plans by August 2014. Having strategic, operational and project risk management processes that use a consistent methodology in place allows NPRSR to seamlessly escalate new and emerging risks, when required, and de-escalate risks that have been successfully managed at the strategic and operational levels. I can also advise that NPRSR's Executive Management Team and the Audit and Risk Committee have been provided with quarterly risk management updates since late 2012.


In relation to risk appetite, I advise that NPRSR's risk management policy and procedure do make reference to risk appetite and tolerance. However, these references can be strengthened when the policy is to be reviewed (by the end of 2014).

#### Chapter 4 – Financial Delegations

I advise that action has been taken to address delegations management with NPRSR. I would also like to make you aware that during 2013-2014, two major reviews of NPRSR's delegations structure occurred. As a result, I am now confident that the delegations are fit-for-purpose and ensure the most efficient and effective approval of expenditure based on risk, nature of expenditure and geographical location of management.

Should your officers have any further enquiries, please have them contact Mr Richard Heinritz, Head of Internal Audit in my office on telephone (07) 3338 9332 or via email [richard.heinritz@nprsr.qld.gov.au](mailto:richard.heinritz@nprsr.qld.gov.au).

Yours sincerely

  
John Glaister  
Director-General

Level 7  
111 George Street Brisbane  
PO Box 15187 City East  
Queensland 4002 Australia  
Telephone + 61 7 3338 9301  
Facsimile + 61 7 3338 9335  
Website [www.nprsr.qld.gov.au](http://www.nprsr.qld.gov.au)  
ABN 11 322 391 452

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



Ref: AF/2014/1527  
Your ref: 10668

Department of  
**Science, Information  
Technology, Innovation  
and the Arts**

Mr Andrew Greaves  
Auditor-General  
Queensland Audit Office  
PO Box 15396  
CITY EAST QLD 4002

Dear Mr Greaves

Thank you for your letter of 17 June 2014 regarding your draft report to Parliament on internal control systems.

I have noted the findings, specifically your acknowledgement that the Queensland Shared Services control environment is effective with management responding positively to the implementation of your audit recommendations. Furthermore, I am also pleased to see internal control weaknesses fell by 60 per cent across all departments and agree with you that this reflects internal control system maturity since machinery-of-government changes in 2012.

At this time my department has no further comment in relation to the draft report other than to confirm our commitment to ongoing assessment and improvement to our systems of financial control. The improvement opportunities detailed within your draft report will be used by my department to focus our reform program in relation to internal control systems and their application to our business objectives.

Should your officers require any further information, they may contact Mr Danny Short, Chief Finance Officer, Department of Science, Information Technology, Innovation and the Arts by email at [danny.short@dsitia.qld.gov.au](mailto:danny.short@dsitia.qld.gov.au) or on telephone 07 3719 7725.

Yours sincerely



Sue Rickerby  
Director-General  
117114

Level 5 Executive Building  
100 George Street Brisbane  
GPO Box 5078 Brisbane  
Queensland 4001 Australia

Telephone +617 3224 8303  
Website [www.qld.gov.au](http://www.qld.gov.au)

## Comments received from Acting Public Trustee, The Public Trustee



## Appendix B—2007 recommendations

Figure B1  
2007 recommendations

Finding	Status
<p><b>Whole-of-government framework</b></p> <p>It is recommended that the Department of the Premier and Cabinet and the Treasury Department:</p> <ul style="list-style-type: none"> <li>develop, in consultation with key stakeholders, a robust and comprehensive whole-of-government risk management framework that will outline requirements and provide clear guidelines to agencies</li> <li>develop clear and practical guidelines that will assist agencies in: <ul style="list-style-type: none"> <li>integrating risk management into organisational practices and reporting functions</li> <li>identifying and escalating significant risks beyond the individual agency</li> <li>take a lead role in the coordination, monitoring and reporting of government risks</li> <li>encourage and support the development of public sector risk management skills and competencies.</li> </ul> </li> </ul>	<p><b>COMPLETED</b></p> <p>A guide to risk management was formally developed by the Department of the Premier and Cabinet and Queensland Treasury and Trade.</p> <p>The guide is intended as an information reference to help agencies adopt a consistent approach to risk management.</p> <p>It is not mandatory and does not provide any formal practical processes for the coordination, monitoring and reporting of government risks or for identifying and escalating significant risks beyond the individual agency.</p> <p>The guide encourages communication and training on risk. Central agencies do not have a role in providing or developing training.</p>
<p><b>Culture</b></p> <p>It is recommended that senior management at all agencies:</p> <ul style="list-style-type: none"> <li>develop and foster a corporate culture committed and responsive to risk management</li> <li>provide appropriate resources and training to support effective risk management</li> <li>appoint a 'Risk Management Champion' to actively drive risk management awareness, integration, policies and strategies across the organisation.</li> </ul>	<p><b>PARTLY COMPLETED</b></p> <p>The provision of risk management training is predominantly on-the-job training. Larger agencies have developed formal training programs or engaged outside expertise to deliver training. There are still some agencies providing very little formal training.</p> <p>All agencies have established a risk management champion or group for driving risk management awareness across the agency</p>

Finding	Status
<p><b>Context</b></p> <ul style="list-style-type: none"> <li>Clearly define the context in which they operate.</li> <li>Set a context broad enough to ensure it includes a wide range of influences, trends and time horizons to enable the timely identification of emerging risks both at the agency and beyond the agency levels.</li> <li>Conduct a systematic and regular examination of the context in which they operate using various strategic methods and techniques.</li> <li>Determine their risk profile (appetite and tolerance) through robust examination of the context in which they operate.</li> <li>Apply the established context to the entire risk management process, including defining the parameters and criteria.</li> </ul>	<p><b>PARTLY COMPLETED</b></p> <p>There is evidence that agencies are considering their internal and external contexts and shareholders in identifying risks. Most agencies have identified strategic and operational risks from their business areas.</p> <p>Identifying emerging and new risks is informal, although 18 agencies have formal processes in place to escalate and report risks once identified.</p> <p>Four agencies are yet to establish their risk appetite or tolerances.</p> <p>All agencies have established risk assessment tools which define the parameters and criteria to make risk assessments. Nine agencies have not established quantitative criteria which are measurable.</p>
<p><b>Integrated framework</b></p> <p>It is recommended that agencies:</p> <ul style="list-style-type: none"> <li>adopt and implement an integrated risk management framework</li> <li>ensure they are implementing all elements of the chosen risk management framework effectively and consistently throughout all organisational levels and functions</li> <li>align risk management with their corporate objectives and government priorities.</li> </ul>	<p><b>PARTLY COMPLETED</b></p> <p>Agencies have developed integrated risk management frameworks. Agencies are at varying levels of maturity. Progress towards an effective risk management framework, which is consistently applied and aligned to their objectives, has not yet been achieved for all agencies.</p>
<p><b>System implementation</b></p> <p>It is recommended that:</p> <ul style="list-style-type: none"> <li>senior management promotes and champions the importance and benefits of all elements of the risk management framework and its integration with existing business processes</li> <li>agencies implement robust controls to ensure all elements of the risk management framework are being implemented effectively</li> <li>the context agencies use to identify risks is consistent with the context established to determine the organisation's risk profile</li> <li>agencies regularly review the performance of adopted risk treatment strategies against set criteria to measure and report their effectiveness and determine future risk treatment needs</li> <li>the risk management framework is periodically reviewed to ensure relevance and continued effectiveness in its application.</li> </ul>	<p><b>PARTLY COMPLETED</b></p> <p>Communication and training covers roles and responsibilities and objectives of risk management.</p> <p>Whilst agencies have implemented controls for risk management activities, deficiencies identified indicate that all are not implemented effectively.</p> <p>Agencies have identified risks from all parts of their business. A number of deficiencies were noted in the identification and recording of financial and financial reporting risks.</p> <p>Not all agencies are measuring the performance of risk treatment plans against set criteria or implementation dates.</p> <p>Fifty per cent of agencies have conducted independent reviews of elements of the risk management framework.</p>

Finding	Status
<p><b>Accountability and corporate governance</b></p> <p>It is recommended that:</p> <ul style="list-style-type: none"> <li>agencies strengthen their governance arrangements to ensure proper accountability</li> <li>agencies consider setting up a risk management committee (whether combined with the audit committee or not) to oversee the risk management framework, systems, controls and procedures and provide assurance on their efficiency and relevance</li> <li>agencies clarify the roles and responsibilities in relation to managing risk, as well as risk ownership across all levels and functions of the organisation</li> <li>central agencies provide clear guidelines on the role and responsibilities of the risk management committee.</li> </ul>	<p><b>PARTLY COMPLETED</b></p> <p>All agencies in the audit established appropriate governance arrangements to ensure appropriate accountability for risk.</p> <p>All agencies in the review have established audit and risk committees. One agency had established a risk committee in addition to an audit and risk committee.</p> <p>Sixteen agencies had policies in place that outlined the roles and responsibilities for managing risk and assigned owners to risks in their risk registers.</p> <p>Central agencies have established guidelines for the roles and responsibilities for audit committees which includes guidance for risk oversight.</p>

Source: Queensland Audit Office

## Appendix C—Entity acronyms

---

### Budget departments:

- Department of Agriculture, Fisheries and Forestry (DAFF)
- Department of Aboriginal and Torres Strait Islander and Multicultural Affairs (DATSIMA)
- Department of Communities, Child Safety and Disability Services (DCCSDS)
- Department of Education, Training and Employment (DETE)
- 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 Justice and Attorney-General (DJAG)
- Department of Local Government, Community Recovery and Resilience (DLGCRR)
- Department of Natural Resources and Mines (DNRM)
- Department of National Parks, Recreation, Sport and Racing (DNPRSR)
- Department of Premier and Cabinet (DPC)
- Department of Science, Information Technology, Innovation and the Arts (DSITIA)
- Department of State Development, Infrastructure and Planning (DSDIP)
- Department of Tourism, Major Events, Small Business and the Commonwealth Games (DTESB)
- Department of Transport and Main Roads (DTMR)
- Queensland Police Service (QPS)
- Queensland Treasury and Trade (QTT)
- Public Safety Business Agency (PSBA)
- Queensland Fire and Emergency services (QFES).

### Small department:

- Public Trustee of Queensland (PTQ).\*

### Statutory bodies:

- Queensland Rail (QRAIL) \*
- Queensland Treasury Corporation (QTC) \*
- WorkCover Queensland (WCQ).\*

### Government owned corporations:

- Queensland Investment Corporation (QIC). \*

\* These entities were included in the risk management (Chapter 3) and financial delegation (Chapter 4) area of emphasis audits in addition to the listed budget departments.

|



# Auditor-General Reports to Parliament

## Reports tabled in 2014–15

Number	Title	Date tabled in Legislative Assembly
1.	Results of audit: Internal control systems 2013–14	July 2014

[www.qao.qld.gov.au](http://www.qao.qld.gov.au)