Auditor-General of Queensland

Report 5 : 2012

June 2012

Results of audits:

Internal control systems

QUEENSLAND AUDIT OFFICE

Enhancing public sector accountability

Auditor-General of Queensland

Results of audits:

Internal control systems

QUEENSLAND

Prepared under Part 3 Division 3 of the
Auditor-General Act 2009

Queensland Audit Office
Level 14, 53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002

Phone	07 3149 6000
Fax	07 3149 6011
Email	enquiries@qao.qld.gov.au
Web	www.qao.qld.gov.au

This report has been produced using paper stock manufactured to ISO 14001 environmental standards. Hanno Art Silk is totally chlorine free and acid free, has pulp sourced from sustainably managed forests and meets ISO 9706 archival standards. It was proudly printed in Queensland by Goprint meeting ISO 14001 environmental and ISO 9001 quality standards.

ISSN 1834-1128

Publications are available at www.qao.qld.gov.au or by phone on 07 3149 6000.

Auditor-General of Queensland

June 2012

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

Dear Madam Speaker

This interim report, titled *Results of audits: Internal control systems*, is prepared under section 62 of the *Auditor-General Act 2009.*

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

Yours sincerely

Andrew Greaves
Auditor-General

Contents

Summary

This interim report to Parliament is prepared under section 62 of the *Auditor-General Act 2009*. It summarises results from the interim phase of the 2011-12 financial audits of departments, statutory bodies and government owned corporations.

It contains the results of audits where areas of control were emphasised during the audit process. These areas were examined in greater detail due to their importance at this point in time.

Effectiveness of financial controls

The Accountable Officer or Chief Executive Officer is responsible for establishing and effectively maintaining adequate financial control throughout the financial year.

Control weaknesses have been identified in 25 (13 per cent) of the 196 departments, government owned corporations and statutory bodies audited, with 221 significant control issues reported to those charged with the governance of these entities, primarily entity boards and chief executives, or their equivalents.

Weaknesses in internal financial control increase the risk of error, both intentional and unintentional. The number of control issues identified during our audits demonstrates that significant scope remains for improvement in this area of fundamental governance responsibility.

Effectiveness of fraud controls

Auditor-General Report to Parliament No 5 for 2011, *Results of audits at 31 May 2011*, commented that the focus across the public sector on maintaining basic financial controls was declining, with issues raised showing an increase in the number of departments failing to maintain adequate financial controls. There were aspects that needed to be urgently addressed to ensure such fundamental controls are working as required.

Fraud occurs where the conditions are right for it to occur. Internal control structures within departments have recently been experiencing increased stress due to transfers of functions and staff both within departments, and as part of machinery of government changes, the loss of experienced and key staff through voluntary separation programs, and the need to do more with less as required by budget savings.

Our assessment of the effectiveness of entity fraud prevention strategies identified 11 departments as not having at least two of the six basic elements (discussed further in Section 3.2) operating at a level to minimise the risk of fraud occurring. The internal control issues identified during our audits, such as lack of criminal history checking, controls over preventing duplicate payments, missing reports and documentation, and inadequate monitoring and checking that controls were operating effectively, also contribute to an environment where fraud can occur and remain undetected.

IT governance

Audits of the governance of two major IT programs—Identity Management and Email Services (IDES) and Information and Communication Technology Consolidation (ICTC)—in 2010 and 2011 recommended improvements to the management of these key IT infrastructure programs.

We have found that benchmarks for benefits and pricing for both the IDES and ICTC programs were not put in place at the start of the programs, making it difficult to establish whether the current pricing is reasonable and that the expected benefits will be realised.

Auditor-General Report to Parliament No 4 for 2011, *Information systems governance and security*, reported on the lack of overall commitment in the implementation of the technology being produced through these programs. Little action has occurred to gain this commitment.

Without effective oversight, both IDES and ICTC are not likely to realise the original benefits expected by government.

Recommendations

1. **All public sector entities should document their internal financial control framework and systemically assess its effectiveness.**
2. **Departments should establish fraud control plans targeted to their specific fraud risks.**
3. **Departments should establish guidance for staff as to what procurement methods should be employed for the different types of expenditure processed, following a risk assessment that includes consideration of fraud risk and the cost-effectiveness of control.**
4. **Departments should regularly review their financial delegations with a view to limiting them to only those employees who require it as part of their normal roles and responsibilities.**
5. **Departments should review their recordkeeping activities especially over electronic financial transactions, to maintain appropriate documentation trails.**
6. **Departments should provide specific fraud training to staff, customised to their particular fraud risks.**
7. **Departments should establish detailed analytical review or data mining procedures as a fraud detection countermeasure function of either internal audit or their finance function.**
8. **Accountability for the IDES and ICTC programs should be assigned to a system owner or sponsoring group able to make decisions on the future of these programs.**

Comments received

In accordance with section 64 of the *Auditor-General Act 2009*, a copy of this report was provided to the Department of the Premier and Cabinet, Queensland Treasury and Trade and Department of Science, Information Technology, Innovation and the Arts with a request for comments.

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

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

1 | Context

1.1 Internal controls

Internal controls are processes (including elements such as policies, procedures and systems) that are established, operated and monitored by management of an entity to provide reasonable assurance to them and to their governing body about the achievement of the entity's objectives.

Among other things, effective systems of internal control enable:

- preparation of accurate financial records
- delivery of reliable, accurate and timely external and internal reports
- adaption to changes in the business and operating environment
- compliance with applicable laws and regulations
- appropriate safeguarding of assets
- prevention or detection of fraud, corruption and other irregularities.

The chief executive officer and the executive management team are responsible for establishing and maintaining internal controls. They set the tone and provide funding to implement the controls. They also evaluate the effectiveness of controls on an ongoing basis.

Internal controls cannot guarantee that there is no error or fraud. They can, however, reduce the risk of error and fraud occurring in the first place, and can help to detect fraud and error where it has occurred.

Fraud has significant consequences for entities and stakeholders, as well as for public confidence. A strong control environment where written policies and procedures are enforced, internal controls are appropriately implemented and employees are educated about fraud and its consequences is one of the best deterrents and methods of curtailing fraud.

1.2 Legislative requirements

Section 61 of the *Financial Accountability Act 2009* states that Accountable Officers are to ensure the operations of the department are carried out efficiently, effectively and economically and are to establish and maintain appropriate systems of internal controls.

Section 8 of the *Financial and Performance Management Standard 2009* requires departments to establish cost-effective internal control structures.

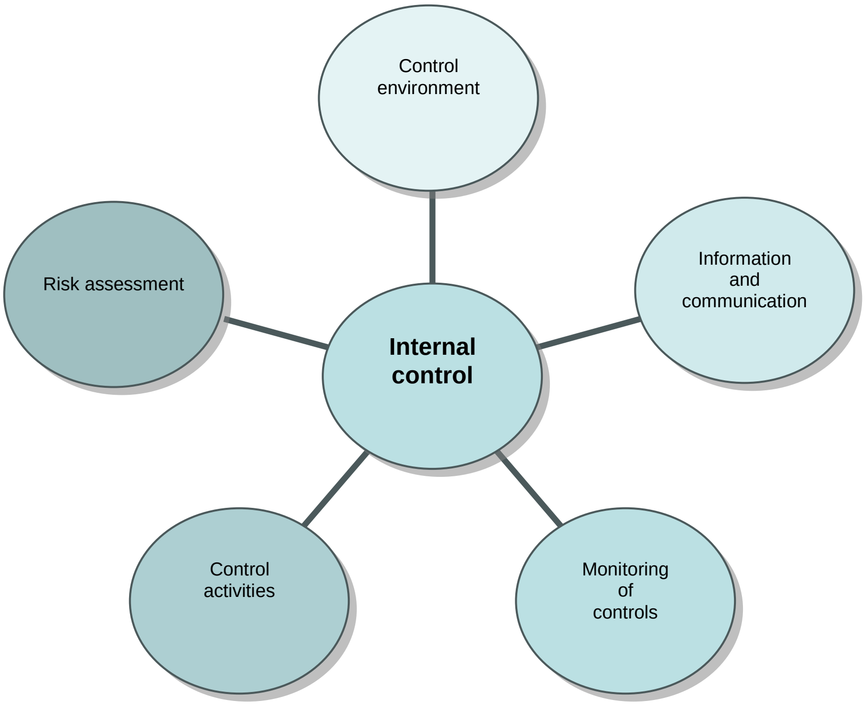
These requirements make the Director-General of a department and the Chief Finance Officer responsible for maintaining appropriate financial internal controls of the department. Each year, under s.77(2) of the Financial Accountability Act, the Chief Finance Officer is required to provide to the Director-General, as the Accountable Officer, a statement of whether the financial internal controls of the department were operating efficiently, effectively and economically.

1.3 COSO internal control framework

The Committee of Sponsoring Organisations (COSO) of the Treadway Commission released its *Internal Control – Integrated Framework* in 1992. Since that time the framework has gained broad acceptance and is widely used around the world and is recognised as a leading framework for the design, implementation and evaluation of the effectiveness of internal control. COSO sponsors and disseminates frameworks and guidance based on in-depth research, analysis and best practices.

The COSO framework recognises that internal control is an ongoing process. Embedded within the processes are policies and procedures reflecting management's statement of what should be done. Figure 1A sets out COSO's five directly related components of internal control.

Figure 1A
Components of an internal control framework



Source: Victorian Auditor-General's Office

In Figure 1A:

- The **control environment** provides discipline, process and structure. Senior management demonstrates the tone from the top regarding the importance of internal control and expected standards of conduct. Management structures, reporting lines and appropriate responsibilities are established.
- **Risk assessment** involves a dynamic and iterative process for identifying and analysing risks to achieving the entity's objectives, forming a basis for determining how risks should be managed.
- **Control activities** are the actions established by policies and procedures to help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
- **Information and communication** involves communicating control responsibilities throughout the entity and providing information in a form and timeframe that allows officers to discharge their responsibilities.
- **Monitoring** of controls involves observing the internal controls in practice and assessing their effectiveness.

When these components are present in a system of internal control and when they operate together, there is an expectation that business and operating risks will be reduced to an acceptable level.

1.4 Audit responsibility

Because internal controls operate both at a financial transaction and account balance level to produce reliable financial information, and to maintain compliance with prescribed requirements, they are examined as part of the audit of each entity's financial statements.

Typically this occurs during the financial year, in what is described as the interim phase of the financial audit. Any weaknesses in internal control that are identified are assessed by the auditor to establish whether and how they affect the risk of error and fraud.

Significant weaknesses or breakdowns in internal control are reported to executive management and to the governing body for their attention and corrective action.

1.5 Structure of the report

The report is structured as follows:

- Section 2 discusses the significant control issues identified and reported to management during the interim phase of 2011-12 financial audits.
- Section 3 addresses fraud risks and how well departments are managing these risks.
- Section 4 identifies significant IT governance issues.
- Appendix A contains departmental responses.

2 | Effectiveness of financial controls

Summary

Background

Internal controls include the systems, policies and activities established by public sector entities to ensure the effectiveness and efficiency of their operations, reliability of financial reporting, and compliance with applicable legislation. As part of the financial audit assessment is made of key internal controls over the reliability of financial reporting. Any weaknesses identified are raised with management for corrective action. This section discusses the significant control issues identified during the 2011-12 interim audits.

Key findings

- Five entities had incomplete ICT strategic plans, disaster recovery plans, or strategic asset management plans or a lack of documented and approved ICT policies and procedures.
- Seven entities had inadequate controls for monitoring risks and their treatment, or managing the risks to IT systems.
- Twenty-one entities had control weaknesses raised in relation to the accounting systems and processes that pose significant risk, and require corrective action as a matter of high priority.
- Thirteen entities had information and communication issues, with 43 of the 85 issues raised about information security controls.
- Significant monitoring and review issues were raised at eight entities, including inadequate monitoring and review of reports and processes across non-current assets, expenditure and payables, employee expenses and benefits, and information systems.

Key recommendation

1. **All public sector entities should document their internal financial control framework and systemically assess its effectiveness.**

2.1 Control issues

Each public sector entity is responsible for developing measures for managing risks to which their operations are exposed. These measures include maintaining an adequate system of internal control to ensure that financial records and other information are complete and accurate, assets are safeguarded, and errors and other irregularities are prevented or detected.

Elements of the entity's internal control framework are assessed during an audit to determine if the controls put in place are operating and whether they are effective. The extent of compliance with legislative requirements is also assessed.

Where significant issues are identified, they are discussed with management and summarised in reports to the entity. Significant control issues were identified in 25 (13 per cent) out of the 196 public sector entities audited. In total, 221 significant control issues were identified during the interim audit and reported to management.

Figure 2A summarises by type of entity the number of significant control weaknesses reported to date.

Figure 2A
Significant control weaknesses reported

Category	2011-12	
	Number of entities	Number of issues
Departments	16	178
Statutory bodies	4	14
Government owned corporations	5	29
Total	**25**	**221**

The 221 reported issues have been analysed against the relevant components of the internal control framework.

2.2 Control environment

Planning and accountability documents outline the goals, strategies and policies for implementing an organisation's vision, managing finances, ensuring information system security and the sustainable management of infrastructure. Policies and plans assist management to reinforce relevant legislation and best practices.

Areas of concern identified during our audits included incomplete ICT strategic plans, disaster recovery plans or strategic asset management plans and lack of documented and approved ICT policies and procedures.

Lack of comprehensive documented and approved information systems policies and plans can result in unauthorised information system access, increasing the risk of unauthorised or inappropriate access to financial systems and data, and the processing of unauthorised transactions.

The number of significant **control environment** weaknesses reported by category is summarised in Figure 2B.

Figure 2B
Significant control environment weaknesses reported

Category	2011-12	
	Number of entities	Number of issues
Departments	3	3
Statutory bodies	1	2
Government owned corporations	1	2
Total	**5**	**7**

2.3 Risk management

An organisation faces risks that may be difficult to quantify or control. It is important to identify and manage these risks and formulate responses to deal with them if the risks eventuate. A commitment to risk management contributes to sound management practice and increases community confidence. The issues of concern raised with entities related to monitoring risks and their treatment, and managing the risks to IT systems.

Figure 2C shows the entities with significant **risk management** issues by category.

Figure 2C
Significant risk management weaknesses

Category	2011-12	
	Number of entities	Number of issues
Departments	5	10
Statutory bodies	2	2
Government owned corporations	0	0
Total	**7**	**12**

2.4 Control activities

Control activities are the procedures established to protect assets, ensure reliable accounting records, promote efficiency and encourage adherence to the organisation's policies. Effective controls can provide early warning of weaknesses or susceptibility to error, support for timely reporting and the early identification of irregularities.

Twenty-one entities had significant weaknesses in control activities associated with their accounting and supporting systems and processes. These pose a business or financial risk and need corrective action as a matter of high priority. The major issues were:

- inadequate segregation of key duties across expenditure and payables, employee expenses and benefits, and revenue and receivables. This increases the risk of users having access to two or more functions within a process that may lead to inappropriate activities such as fraudulent payments or misappropriation
- inadequate expenditure approvals, with instances of duplicate vendors and duplicate payments identified

- inadequate control over approval of employee movements, such as appointments to positions and employees starting and leaving, and criminal history checks not performed
- missing reports and supporting documentation
- lack of control over dealing with discrepancies in inventory.

Figure 2D shows the number of significant **control activity** issues reported by category.

Figure 2D
Significant control activity weaknesses

Category	2011-12	
	Number of entities	Number of issues
Departments	14	89
Statutory bodies	3	6
Government owned corporations	4	9
Total	**21**	**104**

2.5 Information and communication

Information and communication activities communicate control responsibilities throughout the entity, and provide information in a form and timeframe that allows officers to discharge their responsibilities.

Figure 2E shows the number of significant **information and communication** issues reported by category.

Figure 2E
Significant information and communication weaknesses

Category	2011-12	
	Number of entities	Number of issues
Departments	8	64
Statutory bodies	0	0
Government owned corporations	5	21
Total	**13**	**85**

Information security control weaknesses account for 43 of the 85 issues identified to date. These controls operate to restrict access to systems, data and programs to authorised users, and to properly align their access rights with their authority and responsibility. Without adequate controls, it is difficult to safeguard information against unauthorised use, disclosure or modification, and damage or loss, and the integrity of the data cannot be guaranteed.

Prior audits have identified significant weaknesses in the management of IT risks within departments, identifying weaknesses in network security.

This year, we followed up also on those areas identified in Report to Parliament No. 7 for 2010 and Report to Parliament No. 4 for 2011 to determine if there had been any significant progress in addressing the IT risks that we had raised previously.

We found that half of the departments audited in 2010 and 2011 had not adequately progressed audit recommendations to improve their controls over computer networks. The number of security incidents identified in these years correlates closely with those departments with the higher numbers of issues and delays in remediation.

Auditor-General Report to Parliament No. 4 for 2011 identified that there was no whole of government IT business continuity management strategy to prioritise system recovery in the event of a disaster. In December 2011, the Queensland Government Chief Information Office produced a draft whole of government business continuity management and disaster recovery implementation framework.

However, the framework is still under consultation and responsibilities for restoring systems are yet to be conveyed and agreed. The framework depends on departments providing the Queensland Government Chief Information Office with documentation identifying their critical applications, services dependent on those applications and their impact on government and non-government infrastructure and services. From documentation received so far from departments, the Queensland Government Chief Information Office created a prioritised list of critical systems but this list is incomplete.

2.6 Monitoring and review

Monitoring of controls involves observing the internal controls in practice and assessing their effectiveness. Areas of concern identified related to ongoing monitoring activities which should occur in the course of an entity's operations, such as inadequate monitoring and review of reports and processes across non-current assets, expenditure and payables, employee expenses and benefits, and information systems. Such weaknesses mean that unauthorised or inappropriate transactions are less likely to be detected.

Figure 2E shows the number of significant **monitoring and review** issues reported by category.

Figure 2E
Significant monitoring and review weaknesses

Category	2011-12	
	Number of entities	Number of issues
Departments	7	12
Statutory bodies	1	1
Government owned corporations	0	0
Total	**8**	**13**

Recommendation

1. **All public sector entities should document their internal financial control framework and systemically assess its effectiveness.**

3 | Effectiveness of fraud controls

Summary

Background

Fraud is an ever-present and ongoing risk in the management of public sector assets. We examined the strategies that departments have to prevent and detect fraud.

Key findings

- Nine of the 13 departments did not have fraud control plans to identify the key risks that needed to be monitored on an ongoing basis.
- Seven of the 13 departments had not provided guidance to employees on procurement methods to be used to minimise fraud for the various types of expenses.
- Around 17 000 departmental staff have a financial delegation, with between 4 per cent and 48 per cent of staff within individual departments having a financial delegation.
- All departments had performed a recent review of their vendor master file to identify duplicate and redundant vendors.
- No specific training was provided to employees in fraud control and prevention.
- Nine of the 13 departments did not perform detailed analytical review or data mining procedures to highlight irregular or unusual transactions.

Key recommendations

2. **Departments should establish fraud control plans targeted to their specific fraud risks.**
3. **Departments should establish guidance for staff as to what procurement methods should be employed for the different types of expenditure processed, following a risk assessment that includes consideration of fraud risk and the cost-effectiveness of control.**
4. **Departments should regularly review their financial delegations with a view to limiting them to only those employees who require it as part of their normal roles and responsibilities.**
5. **Departments should review their recordkeeping activities, especially over electronic financial transactions, to maintain appropriate documentation trails.**
6. **Departments should provide specific fraud training to staff, customised to their particular fraud risks.**
7. **Departments should establish detailed analytical review or data mining procedures as a fraud detection countermeasure function of either internal audit or their finance function.**

3.1 Managing fraud risk

An ongoing theme raised in previous Auditor-General Reports to Parliament has been the risk of fraud. Most recently*, Auditor-General Report to Parliament No. 5 for 2011 – Results of audits at 31 May 2011* warned that inadequate controls over vendor information can expose departments to significant losses though fraudulent manipulation of this information.

While cost–benefit considerations are part of the determination of what level of internal control should be established within an entity's financial management framework, fraud represents an ever-present and ongoing risk in the management of public sector assets.

The importance of an effective system of internal controls as both a preventative and detective countermeasure to the incidence of fraud was highlighted in Auditor-General Report to Parliament No. 4 for 2008. Internal controls are responsible for detecting around half of frauds and this has been confirmed recently in the New Zealand Comptroller and Auditor-General's 2011 Public Sector Fraud Awareness Survey.

The effectiveness of internal control structures within departments is being increasingly challenged because of:

- regular transfers of functions and staff both within departments, and as part of machinery of government changes—there have been four significant restructures in the past six years increasing the risk that lines of responsibility, authority and accountability become blurred thereby weakening the control environment
- the loss of experienced and key staff through voluntary separation programs—during the current financial year in excess of 4 200 non front-line departmental staff have accepted a voluntary separation package leading to a heightened risk of loss of corporate knowledge and experience in the 'back office' where most internal financial control activities operate
- the need to do more with less as required by budget savings—increasing the risk that resources will be diverted from necessary internal control monitoring measures, such as internal audit.

In this environment, it was considered timely to examine the strategies that departments had in place to prevent and detect fraud. The audit assessed the effectiveness of both fraud prevention and detection elements at the 13 departments as they existed before the recent machinery of government changes.

3.2 Effectiveness of prevention strategies

Fraud prevention strategies are designed to prevent fraud from occurring in the first instance. Prevention of fraud should be an integral part of the organisation and is more than management establishing a set of policies, plans and procedures to be complied with by a department. It involves the way controls are designed and implemented, the behaviour, knowledge and skills of staff, and how well staff and risks are being managed.

In this context the audit assessed the following prevention criteria:

- adequacy of fraud control policies and plans
- whether procurement methods were linked to fraud risk
- control over financial delegations
- monitoring and review of vendor masterfiles
- control over payment documentation
- provision of specific training on fraud prevention.

Our assessment of the effectiveness of fraud prevention strategies identified 11 departments as not having at least two of these six basic elements at a level to prevent fraud. Nearly all departments need to develop a fraud control plan and specific training over fraud control and prevention. All departments have, however, performed a review of their vendor master files during early 2012, in response to the alleged Queensland Health fraud.

3.2.1 Policies and plans

Fraud control policies and plans set out management's commitment and response to fraud risk management.

To be effective, fraud risk management policies need to be established and supported by management, should spell out management's expectation, and be monitored in order to ensure that they achieve the desired outcome. We found that all departments have fraud control policies in place and these policies were recently updated or updated continuously for risks.

Fraud control plans support fraud policies. Robust fraud control plans set out departments' strategies for the prevention, detection and investigation of fraud and clearly identify:

- the consequence and likelihood of potential fraud risks occurring in the department
- an assessment of fraud risks after considering the effectiveness of existing internal controls in preventing fraud
- an action plan to reduce fraud risk to an acceptable level.

Nine of the 13 departments did not adequately address one or more of the above criteria in their fraud control plans.

Recommendation

2. Departments should establish fraud control plans targeted to their specific fraud risks.

3.2.2 Procurement and payment methods

For the Queensland public sector, the organisational structures of some of the largest government departments are characterised by multiple lines of authority, complex financial delegations and remote transaction processing.

In this context, we found that the potential fraud risk associated with different procurement and payment methods has not been adequately assessed by departments.

Departments most commonly purchase and pay for goods and services either by a corporate credit card, by direct invoice or using a purchase order based payment. The direct invoice method involves the purchase of an item and financial approval after the date of purchase, while for the purchase order method, financial approval of purchases is made before a purchase occurs. Corporate credit cards are usually limited to low value, low risk or infrequent transactions to limit the risk of misuse.

Seven departments do not provide adequate guidance to staff as to what type of procurement method should be employed to minimise fraud risk for various types of expenditure.

The direct invoice method is the most common, with five departments using direct invoices for 50 per cent or more of all payments. While this method may be more cost effective, it is also the most risky in terms of fraud, as direct invoice payments typically rely on a signature of one person with an appropriate financial delegation. A well controlled procurement environment is characterised by the separation of duties between initiating the purchase, certifying goods or services received and authorising the payment—the principle is that more than one set of eyes should be involved.

Recommendation

3. **Departments should establish guidance for staff as to what procurement methods should be employed for the different types of expenditure processed, following a risk assessment that includes consideration of fraud risk and the cost-effectiveness of control.**

3.2.3 Approval of expenditure

Around 17 000 departmental staff have the delegated responsibility to authorise departmental expenditure. This ranges between 4 per cent and 48 per cent of staff in the individual departments. The more staff with the ability to authorise expenditure, the greater the risk of inappropriate payments and the more difficult it is to maintain controls to ensure payments are appropriately and correctly authorised.

As a preventative countermeasure to fraud, management should regularly re-assess those departmental staff with a financial delegation and limit expenditure delegations to those employees who require it as part of their normal roles and responsibilities.

Recommendation

4. **Departments should regularly review their financial delegations with a view to limiting them to only those employees who require it as part of their normal roles and responsibilities.**

3.2.4 Monitoring and review

Poor control over vendor information can result in duplicate and erroneous payments and significant losses and fraud where there has been manipulation of vendor information.

Auditor-General Report to Parliament No. 5 for 2011 reported that the management and monitoring of creation and changes to the vendor master file for the departments audited required significant improvement. None of the departments then audited had implemented monitoring and detective controls for vendor creation or changes.

All departments have now performed a review of their vendor master file during early 2012, in response to the alleged Queensland Health fraud. As a preventative countermeasure to fraud, the regular review of accounts payable systems of duplicate, redundant or inappropriate vendors reduces the risk that these can be used to defraud the public sector.

3.2.5 Recordkeeping controls for financial records

Effective management of records facilitates sound decision-making and the management of corporate information, and is necessary to meet legal and accountability requirements. It also provides an ‘audit trail’ to support and substantiate the accuracy and validity of transactions.

An increasingly higher proportion of electronic invoices from suppliers and customers are being used as the supporting basis for the payment of goods and services. Where documentation on which payments are made is not retained in an original format or is electronically stored, there is a heightened risk for departments of duplicate payments, alteration of documentation and other fraudulent practices through electronic means.

More guidance is needed for departmental staff on recordkeeping requirements for public records. Management also needs to review the quality of recordkeeping activities relating to business transactions processed through a shared service provider, particularly that of digitised documents.

We audited the processing of financial records supporting financial transactions to determine whether there was an appropriate audit trail between each entity and Queensland Shared Services, and whether paper and electronic records were appropriately stored to allow timely access in compliance with the *Public Records Act 2002*. We found:

- limited review and analysis of the risks associated with processing transactions through a shared service provider, including departments’ responsibility for complying with relevant legislation relating to the retention and disposal of public records
- limited training and awareness programs provided to staff about recordkeeping requirements, increasing the risk that these requirements are not understood or adhered to
- inconsistent practices for processing and retaining paper or electronic documents between the entity and the service provider, increasing the risk of fraudulent or duplicate payments due to multiple paper and electronic copies of supporting documents
- inconsistent practices for the capture and retention of emails, with some entities relying on users to manage and store emails relating to business transactions and some emails with scanned documents not retained once the transaction is processed.

Recommendation

5. **Departments should review their recordkeeping activities, especially over electronic financial transactions, to maintain appropriate documentation trails.**

3.2.6 Trained and experienced staff

Employees play a significant role in the prevention and detection of fraud. Given the size of the public sector, an inconsistent level of fraud awareness experience and knowledge of employees represents a source of risk for management. Without specific fraud awareness training, employees are less likely to identify the early warning signs of fraud and will not be equipped to respond appropriately.

No departments had specific fraud training which was customised to the particular circumstances of their department. Seven departments conducted code of conduct training which covers, at a high level, fraud and misconduct, and only one department advised new staff of the department's fraud management policy as part of employee induction.

The recent Voluntary Separation Program has resulted in over 4 200 staff exiting all departments, including from work units which are integral to the internal control activities of the entities. Anecdotal evidence indicates that the recipients of this program include the more senior staff members within departments nearing retirement age, which has resulted in a significant loss of corporate knowledge and experience, particularly around the importance of and need for implementing appropriate internal controls.

Effective and ongoing employee training, particularly for those employees who are responsible for performing internal control procedures, would improve the prevention as well as the detection and response to fraud.

Recommendation

6. **Departments should provide specific fraud training to staff, customised to their particular fraud risks.**

3.3 Effectiveness of detection strategies

Fraud detection strategies are strategies to discover fraud as soon as possible after it has occurred. Monitoring and detection by management act as a strong deterrent to those intending to defraud the public sector. Monitoring strategies need to be widely promoted to departmental staff to foster a culture whereby there is zero tolerance to fraud.

Nine of the 13 departments had not established detailed analytical review or data mining procedures as a fraud detection countermeasure function.

3.3.1 Continuous data analysis and monitoring

Detailed data analytics or data mining as a detection countermeasure to fraud is an area for improvement for departments.

Nine of the 13 departments do not utilise detailed analytical reviews or data mining of transactions by either their finance areas or internal audit. This type of monitoring is best carried out as a live review on a continuous basis, so that irregular or unusual transactions or trends can be identified and investigated in a timely manner.

One department processes three million financial transactions per month, and such volumes emphasise the need to highlight unusual or irregular transactions to management on a regular and ongoing basis, such as transactions that have bypassed normal processing controls.

Continuous data analysis together with management review and questioning of budgetary outcomes, particularly at a cost centre level, would provide a powerful detective capability for departments as well as a strong deterrent.

Internal audit is also well placed to examine on an ongoing basis emergency procurements or transactions where 'work around arrangements' have been imbedded to compensate for computer system deficiencies.

There is also potential for a greater role for audit committees in examining losses occurring and complaints from whistleblowers to identify any systemic issues in their department.

Recommendation

7. **Departments should establish detailed analytical review or data mining procedures as a fraud detection countermeasure function of either internal audit or their finance function.**

4 | IT governance

Summary

Background

We followed up on those areas identified in previous reports to Parliament involving the management of IT programs to determine if there had been any significant progress in addressing the IT risks previously raised.

Key findings

- The take up by departments of both IDES and ICTC is currently far lower than was originally planned.
- Benchmarks for benefits and pricing were not put in place at the start of the programs, making it difficult to establish whether the current pricing is reasonable and that the expected benefits will be realised.

Key recommendation

8. **Accountability for the IDES and ICTC programs should be assigned to a system owner or sponsoring group able to make decisions on the future of these programs.**

4.1 Managing IT program risks

IT is a strategic asset and a significant investment for the public sector representing approximately five per cent of the State Budget. The sector relies on IT systems for efficient and effective service delivery. These systems support key capabilities such as financial processing, payroll processing and core business activities.

At both a whole of government and departmental level, IT systems need to operate reliably, the information in those systems needs to be protected against theft, misuse, disruption and unauthorised access, and management should ensure processes are in place to identify and assess risks and potential threats.

Even before key systems are in place and relied on by the public sector, departmental management have an obligation to ensure that the systems they develop and implement deliver the outcomes expected on time, in budget and meeting the needs of users.

Prior audits have identified significant weaknesses in the management of IT program risks across the sector and within departments.

This year, our audits followed up on those areas identified in Report to Parliament No. 7 for 2010 and Report to Parliament No. 4 for 2011 to determine if there had been any significant progress in addressing the IT risks that we had previously raised.

We found that benchmarks for benefits and pricing for both the IDES and ICTC programs were not put in place at the start of the programs, making it difficult to establish whether the current pricing is reasonable and that the expected benefits will be realised.

Without effective oversight, both IDES and ICTC are not likely to realise the original benefits expected by government.

4.2 Whole of government IT programs

Auditor-General Report No. 4 for 2011 and Auditor General Report No. 7 for 2010 recommended improvements to the management of two key IT infrastructure programs—Identity Management and Email Services (IDES) and Information and Communication Technology Consolidation (ICTC).

There was no effective whole of government sponsoring group in place during the development of these programs. Consequently it was not clear who was accountable for ensuring that departments participate in the programs, that plans for migration were assessed and schedules developed and agreed, or that expected benefits were realised.

While these programs are now substantially complete, there remains the need to identify and monitor their overall benefits.

The audit found that the take up by departments of both IDES and ICTC is currently far lower than was originally planned for. Benchmarks for benefits and for pricing were not put in place at the start of the programs, making it difficult to establish whether the current pricing is reasonable and that the expected benefits will be realised.

In the absence of effective oversight, both IDES and ICTC are not likely to realise the original benefits expected by government.

4.2.1 IDES

IDES was intended to deliver email and identity management services for all departments to be managed and operated by CITEC, the service provider for whole of government ICT infrastructure. The program was meant to be one of the largest email consolidations implemented by government in Australia and it was intended that the Identity Management platform would provide a single unique identifier for every employee.

It was originally expected to be available for use by 2009 and that financial savings of $123 million compared with the cost of departments operating on separate platforms would be delivered over 10 years. These benefits were based on there being 23 000 users by 2009 and 82 000 users by 2010 at a cost of $22.50 per mail box per month.

IDES was not available until 2011 and it is now expected that only 11 000 users will be migrated by August 2012.

By the time IDES was available to use, departments were reluctant to take up the services due to changes to funding available due to the 2011 floods, the global financial crisis and budget cuts which had occurred over the four year period it took to develop the program. Departments also considered the price of $22.50 per mail box to be too high, compared to the costs of their current systems.

To reduce the cost to departments of using IDES, the Government approved an alternate pricing structure of $12.31 per mail box. This new price excludes recovery of the cost of development of the asset and its depreciation, and seeks only to recover operating costs.

No benchmarking had been performed by CITEC for the delivery of email services across government so it remains unclear that the new IDES program pricing model will deliver a lower overall cost to government for providing email services.

The costs to design, build and implement IDES were funded from a $45.3 million loan facility. These costs were to be recovered from departments using IDES and the loan repaid from this revenue. In the absence of a full cost recovery pricing model, it is not apparent how future capital requirements will be funded.

Under the new pricing structure, indicative modelling by CITEC shows that the operating costs of IDES over the next two years will be greater than revenue. This would result in an operating loss (excluding depreciation) of $10.4 million over the 2011-12 and 2012-13 financial years before achieving a break-even position for 2013-14. The model forecasts significant financial returns for CITEC after 2013-14.

These forecasts, however, are based on an uptake of 80 000 mail boxes by June 2014. On current estimates, IDES is already 9 000 users behind in 2011-12, and apart from the Department of Public Works and Housing, there are no departments committed to definite up-take.

For IDES to break even by 2013-14, 29 000 users must be migrated in 2012-13 and a further 40 000 users in 2013-14. It is not evident that the capacity exists both within CITEC and within departments to migrate this volume of users, as the migration of the first 11 000 users will take 12 months to complete. As the take up of IDES is slower than expected, it is probable that losses above forecast levels will occur.

4.2.2 ICTC

The purpose of the ICTC program was to deliver savings by implementing infrastructure to enable the consolidation of central business district data centres, networks and infrastructure services.

The ICTC program was expected to cost approximately $43m by the program completion date of September 2011. These costs did not include the cost to departments of migrating to the new services, or the cost of subsidising the lease costs for the Polaris data centre while it is not fully utilised.

In 2009-10 we reported that consolidation of network, security and storage services could not occur until the infrastructure to enable these activities had been delivered. The planning for this migration activity had been hindered by the lack of a service catalogue and price book to outline the costs to departments of using this infrastructure.

The ICTC program did not have a business case against which the success of the program could be assessed and we recommended that a cost–benefit analysis be performed on a department by department basis.

While ICTC reported a number of achievements in the draft program closure report in February 2012, it did not report against baseline data that could be used for comparison, and performance measures for its objectives were not quantifiable. It remains unclear therefore that ICTC has successfully delivered the stated objectives.

The draft program closure report states now that ICTC is expected to generate savings of $29.6 million over five years. However, the report did not reconcile or explain why the savings figure differed from the benefits of $40.9 million expected when funding was approved.

The expected cost savings were based on a consultant's report in March 2011. However, no review of the inputs to the benefits model has been undertaken subsequently to ensure the assumptions used in March 2011 remained valid. The following factors will affect the estimated savings:

- ICTC was to be depreciated over five years, but it is now likely to be depreciated over four years, so savings should now be measured over four years rather than five years.
- The benefits for ICTC depend on how it compares to each department renewing their own infrastructure. While ICTC may offer superior infrastructure, the current infrastructure of departments may be meeting their business requirements at a lower cost.
- The unused capacity in the network infrastructure since ICTC began is expected to cost CITEC $18 million over the next five years. This cost will reduce any financial benefits realised through ICTC and subsequent consolidation activity over that period.
- The consultant's review was performed while the infrastructure was being developed, when the price to be charged had not been communicated by CITEC. Changes to this key variable would impact on the expected financial benefits.
- The ability to accurately estimate the level of benefits achieved is limited due to the absence of reliable baseline data of costs departments presently incur to support their own IT infrastructure. While some departments are migrating part of their IT environments to CITEC, the benefits of partial migration are limited as the overheads of servicing existing environments still remains with the departments.

CITEC through consultation with the departments has developed consolidation strategies for each department. These strategies outline the planned activities for each department and provide a roadmap on the timing of a department migrating to ICTC. These were completed in 2010. However, due to delays in the delivery of ICTC, the timeframes in these documents require revision.

We recommended in 2010-11 that clear commitment be obtained both from departments and CITEC for joint consolidation schedule plans for deliverables and milestones. Only one migration plan has been completed; however, the relevant department has not approved its execution.

It is acknowledged that the consolidation strategies and roadmaps outline the intent of departments to use ICTC. However, the development of departmental migration plans that satisfy their business requirements is necessary to obtain commitment for the timing of migration. This is critical to ensure that there is some level of certainty over the timing of benefits.

Recommendation

8. Accountability for the IDES and ICTC programs should be assigned to a system owner or sponsoring group able to make decisions on the future of these programs.

Appendices

Appendix A

Auditor-General Act 2009 (Section 64) – Comments received

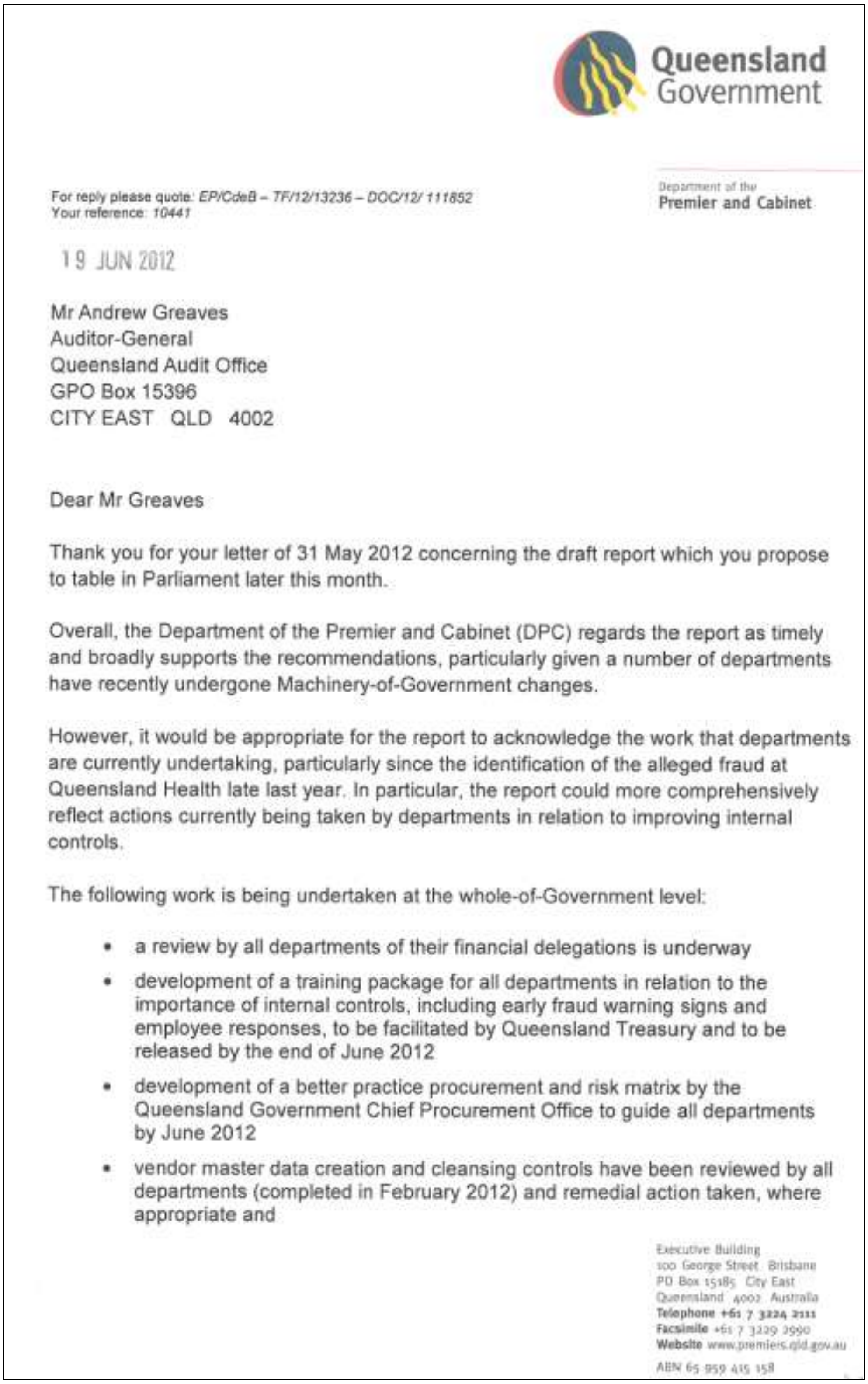
Introduction

In accordance with section 64 of the *Auditor-General Act 2009*, a copy of this report was provided to the Department of the Premier and Cabinet, Queensland Treasury and Trade and Department of Science, Information Technology, Innovation and the Arts with a request for comments.

Responsibility for the accuracy, fairness and balance of the comments rests with the head of each agency.

Comments received

Response provided by the Director-General, Department of the Premier and Cabinet on 19 June 2012.



Queensland Government

For reply please quote: *EP/CdeB – TF/12/13236 – DOC/12/ 111852*
Your reference: *10441*

Department of the
Premier and Cabinet

19 JUN 2012

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

Dear Mr Greaves

Thank you for your letter of 31 May 2012 concerning the draft report which you propose to table in Parliament later this month.

Overall, the Department of the Premier and Cabinet (DPC) regards the report as timely and broadly supports the recommendations, particularly given a number of departments have recently undergone Machinery-of-Government changes.

However, it would be appropriate for the report to acknowledge the work that departments are currently undertaking, particularly since the identification of the alleged fraud at Queensland Health late last year. In particular, the report could more comprehensively reflect actions currently being taken by departments in relation to improving internal controls.

The following work is being undertaken at the whole-of-Government level:

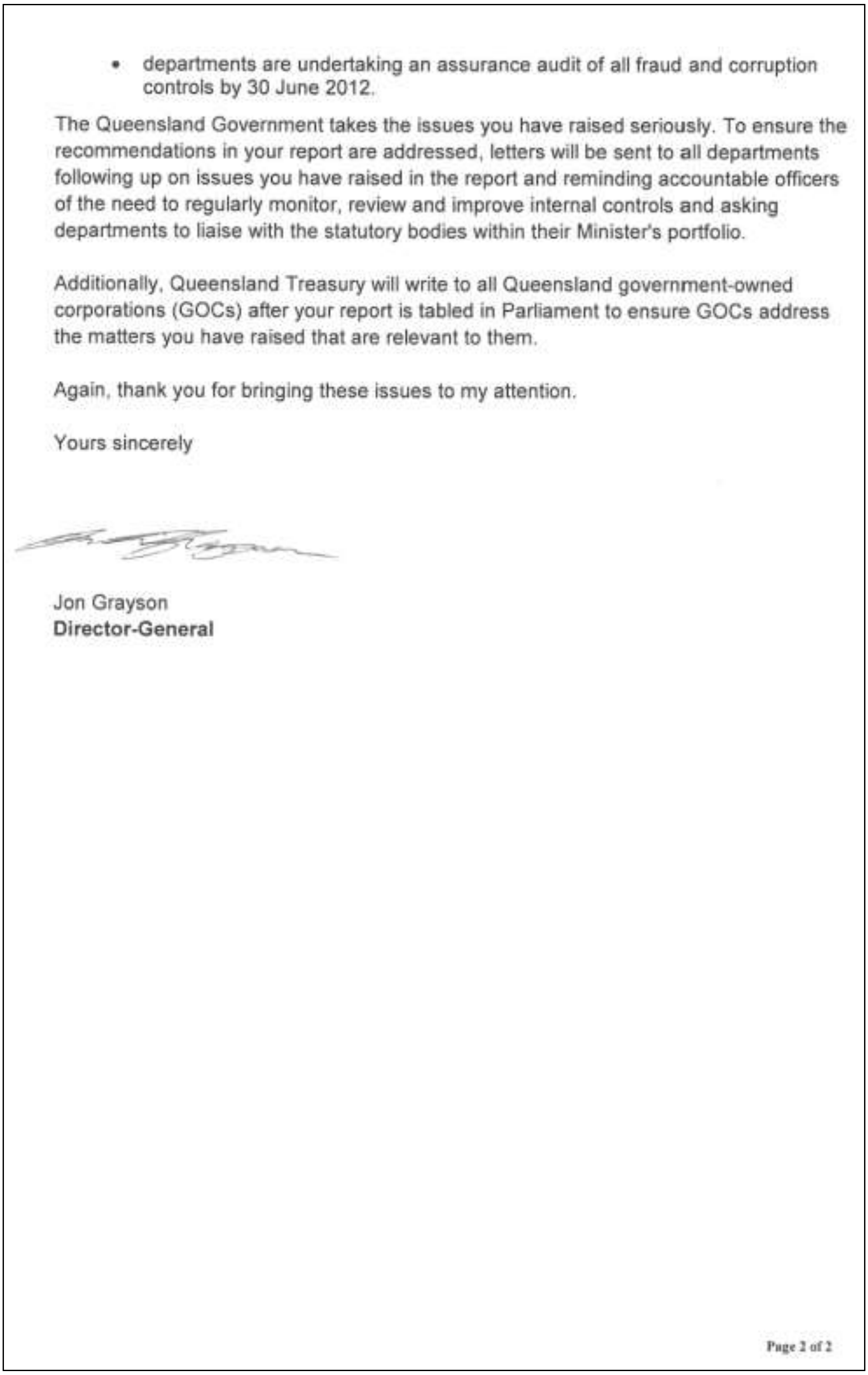
- a review by all departments of their financial delegations is underway
- development of a training package for all departments in relation to the importance of internal controls, including early fraud warning signs and employee responses, to be facilitated by Queensland Treasury and to be released by the end of June 2012
- development of a better practice procurement and risk matrix by the Queensland Government Chief Procurement Office to guide all departments by June 2012
- vendor master data creation and cleansing controls have been reviewed by all departments (completed in February 2012) and remedial action taken, where appropriate and

Executive Building
100 George Street Brisbane
PO Box 15185 City East
Queensland 4002 Australia
Telephone +61 7 3224 2111
Facsimile +61 7 3229 2990
Website www.premiers.qld.gov.au

ABN 65 959 415 158

Comments received

Response provided by the Director-General, Department of the Premier and Cabinet on 19 June 2012.



- departments are undertaking an assurance audit of all fraud and corruption controls by 30 June 2012.

The Queensland Government takes the issues you have raised seriously. To ensure the recommendations in your report are addressed, letters will be sent to all departments following up on issues you have raised in the report and reminding accountable officers of the need to regularly monitor, review and improve internal controls and asking departments to liaise with the statutory bodies within their Minister's portfolio.

Additionally, Queensland Treasury will write to all Queensland government-owned corporations (GOCs) after your report is tabled in Parliament to ensure GOCs address the matters you have raised that are relevant to them.

Again, thank you for bringing these issues to my attention.

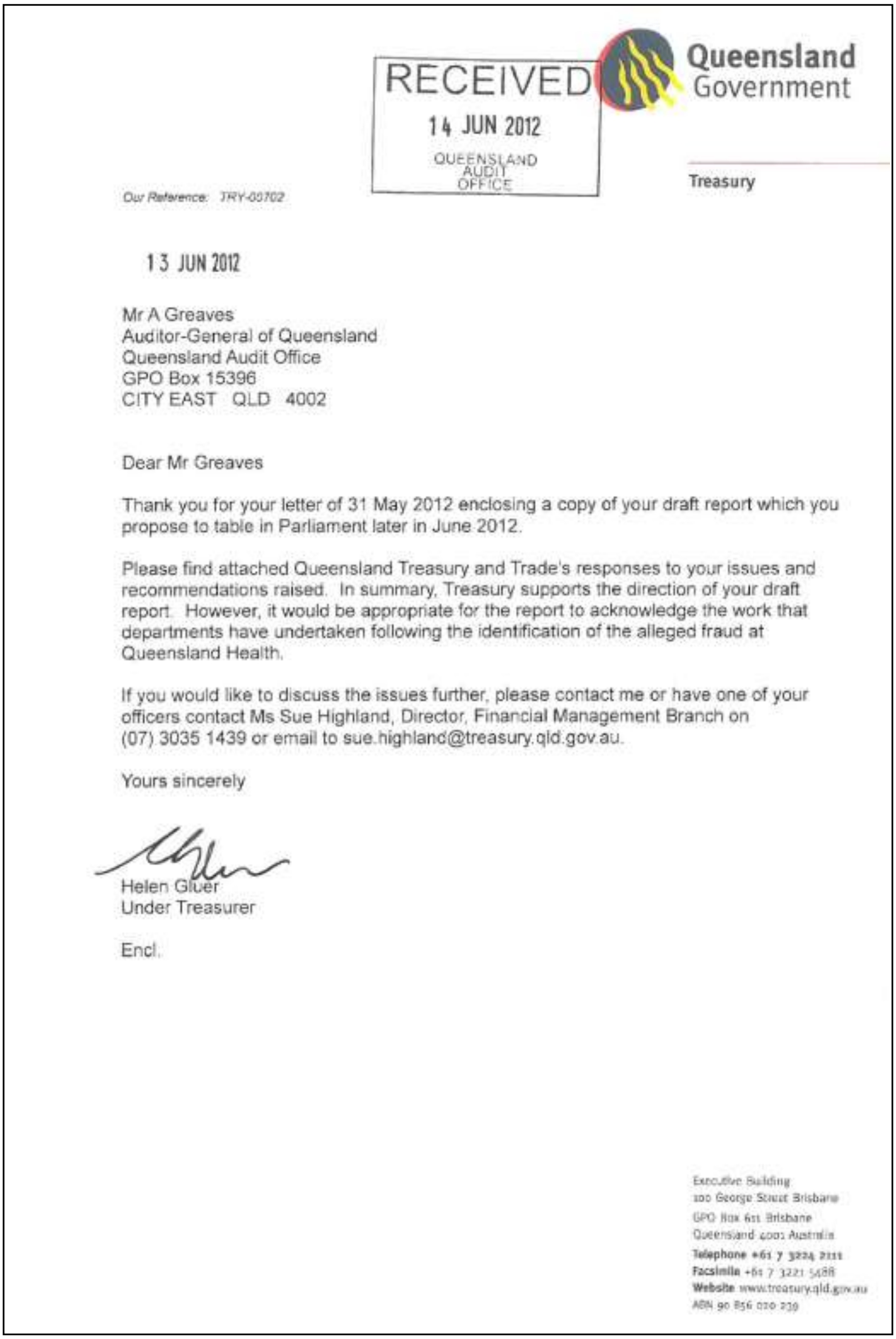
Yours sincerely

Jon Grayson
Director-General

Page 2 of 2

Comments received

Response provided by the Under Treasurer, Queensland Treasury and Trade on 13 June 2012.



Queensland
Government

Treasury

Our Reference: TRY-03702

13 JUN 2012

Mr A Greaves
Auditor-General of Queensland
Queensland Audit Office
GPO Box 15396
CITY EAST QLD 4002

Dear Mr Greaves

Thank you for your letter of 31 May 2012 enclosing a copy of your draft report which you propose to table in Parliament later in June 2012.

Please find attached Queensland Treasury and Trade's responses to your issues and recommendations raised. In summary, Treasury supports the direction of your draft report. However, it would be appropriate for the report to acknowledge the work that departments have undertaken following the identification of the alleged fraud at Queensland Health.

If you would like to discuss the issues further, please contact me or have one of your officers contact Ms Sue Highland, Director, Financial Management Branch on (07) 3035 1439 or email to sue.highland@treasury.qld.gov.au.

Yours sincerely

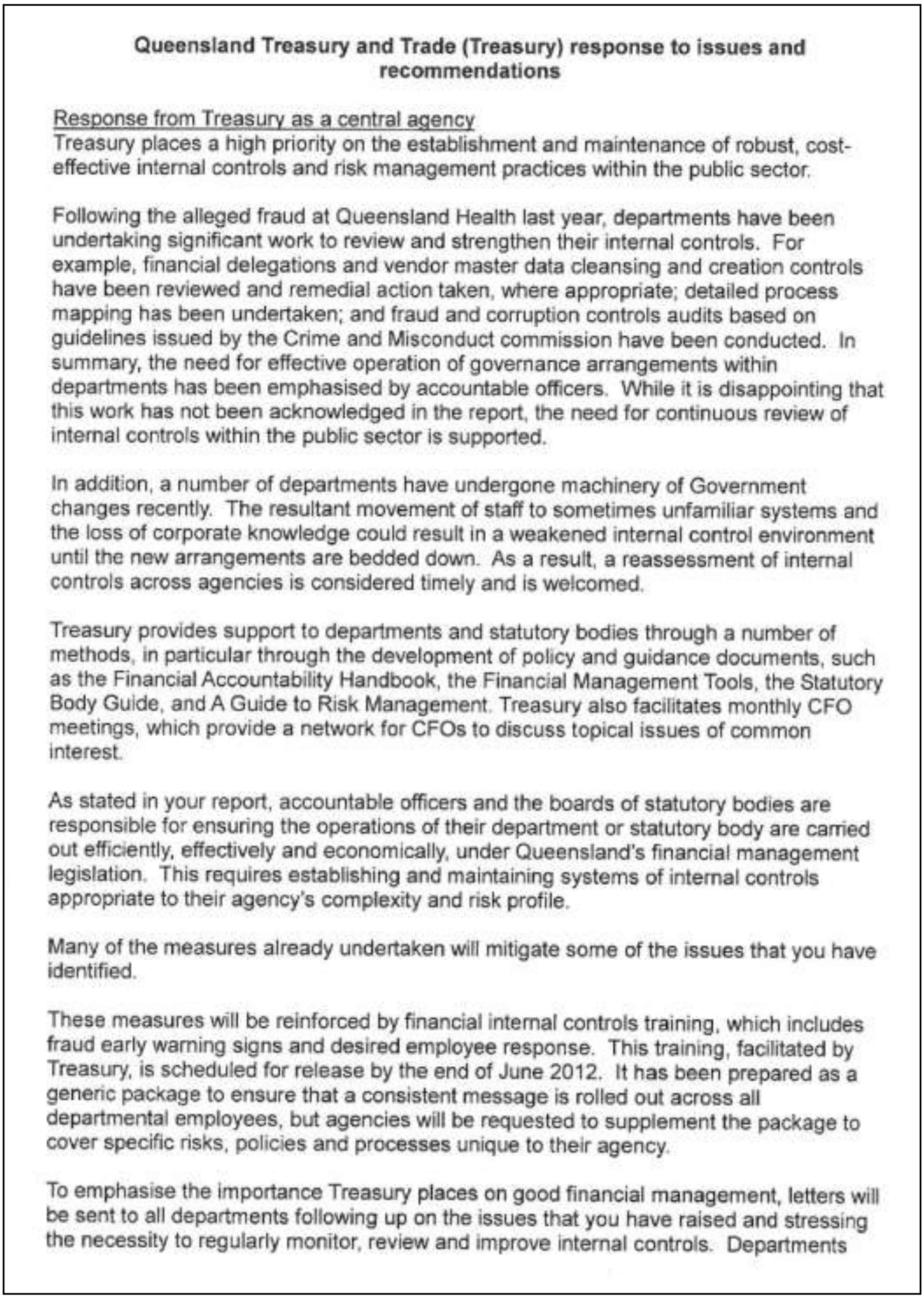
Helen Gluer
Under Treasurer

Encl.

Executive Building
100 George Street Brisbane
GPO Box 611 Brisbane
Queensland 4001 Australia
Telephone +61 7 3224 2111
Facsimile +61 7 3221 5488
Website www.treasury.qld.gov.au
ABN 90 856 020 239

Comments received

Response provided by the Under Treasurer, Queensland Treasury and Trade on 13 June 2012.



Queensland Treasury and Trade (Treasury) response to issues and recommendations

Response from Treasury as a central agency

Treasury places a high priority on the establishment and maintenance of robust, cost-effective internal controls and risk management practices within the public sector.

Following the alleged fraud at Queensland Health last year, departments have been undertaking significant work to review and strengthen their internal controls. For example, financial delegations and vendor master data cleansing and creation controls have been reviewed and remedial action taken, where appropriate; detailed process mapping has been undertaken; and fraud and corruption controls audits based on guidelines issued by the Crime and Misconduct commission have been conducted. In summary, the need for effective operation of governance arrangements within departments has been emphasised by accountable officers. While it is disappointing that this work has not been acknowledged in the report, the need for continuous review of internal controls within the public sector is supported.

In addition, a number of departments have undergone machinery of Government changes recently. The resultant movement of staff to sometimes unfamiliar systems and the loss of corporate knowledge could result in a weakened internal control environment until the new arrangements are bedded down. As a result, a reassessment of internal controls across agencies is considered timely and is welcomed.

Treasury provides support to departments and statutory bodies through a number of methods, in particular through the development of policy and guidance documents, such as the Financial Accountability Handbook, the Financial Management Tools, the Statutory Body Guide, and A Guide to Risk Management. Treasury also facilitates monthly CFO meetings, which provide a network for CFOs to discuss topical issues of common interest.

As stated in your report, accountable officers and the boards of statutory bodies are responsible for ensuring the operations of their department or statutory body are carried out efficiently, effectively and economically, under Queensland's financial management legislation. This requires establishing and maintaining systems of internal controls appropriate to their agency's complexity and risk profile.

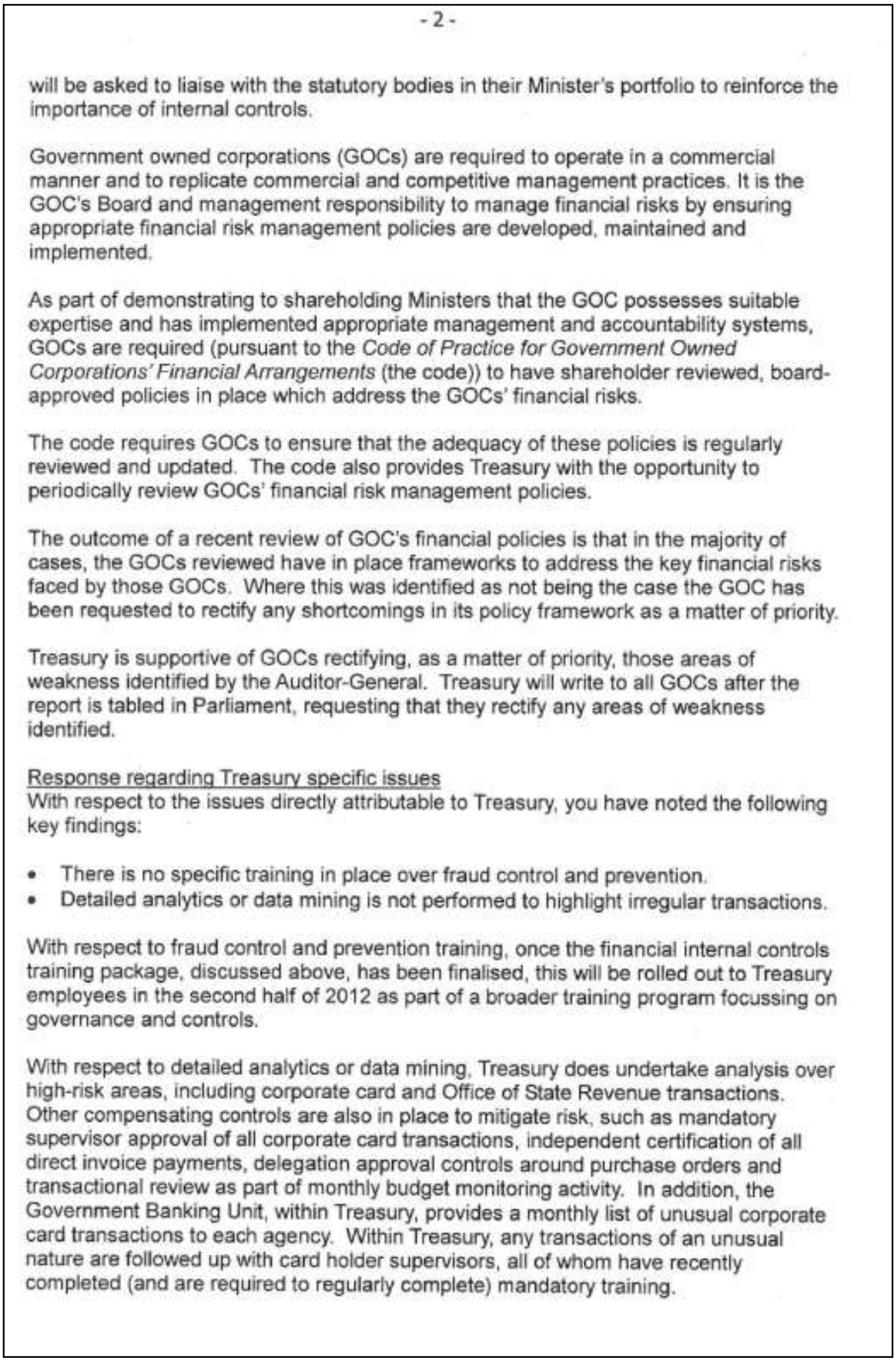
Many of the measures already undertaken will mitigate some of the issues that you have identified.

These measures will be reinforced by financial internal controls training, which includes fraud early warning signs and desired employee response. This training, facilitated by Treasury, is scheduled for release by the end of June 2012. It has been prepared as a generic package to ensure that a consistent message is rolled out across all departmental employees, but agencies will be requested to supplement the package to cover specific risks, policies and processes unique to their agency.

To emphasise the importance Treasury places on good financial management, letters will be sent to all departments following up on the issues that you have raised and stressing the necessity to regularly monitor, review and improve internal controls. Departments

Comments received

Response provided by the Under Treasurer, Queensland Treasury and Trade on 13 June 2012.



will be asked to liaise with the statutory bodies in their Minister's portfolio to reinforce the importance of internal controls.

Government owned corporations (GOCs) are required to operate in a commercial manner and to replicate commercial and competitive management practices. It is the GOC's Board and management responsibility to manage financial risks by ensuring appropriate financial risk management policies are developed, maintained and implemented.

As part of demonstrating to shareholding Ministers that the GOC possesses suitable expertise and has implemented appropriate management and accountability systems, GOCs are required (pursuant to the *Code of Practice for Government Owned Corporations' Financial Arrangements* (the code)) to have shareholder reviewed, board-approved policies in place which address the GOCs' financial risks.

The code requires GOCs to ensure that the adequacy of these policies is regularly reviewed and updated. The code also provides Treasury with the opportunity to periodically review GOCs' financial risk management policies.

The outcome of a recent review of GOC's financial policies is that in the majority of cases, the GOCs reviewed have in place frameworks to address the key financial risks faced by those GOCs. Where this was identified as not being the case the GOC has been requested to rectify any shortcomings in its policy framework as a matter of priority.

Treasury is supportive of GOCs rectifying, as a matter of priority, those areas of weakness identified by the Auditor-General. Treasury will write to all GOCs after the report is tabled in Parliament, requesting that they rectify any areas of weakness identified.

Response regarding Treasury specific issues
With respect to the issues directly attributable to Treasury, you have noted the following key findings:

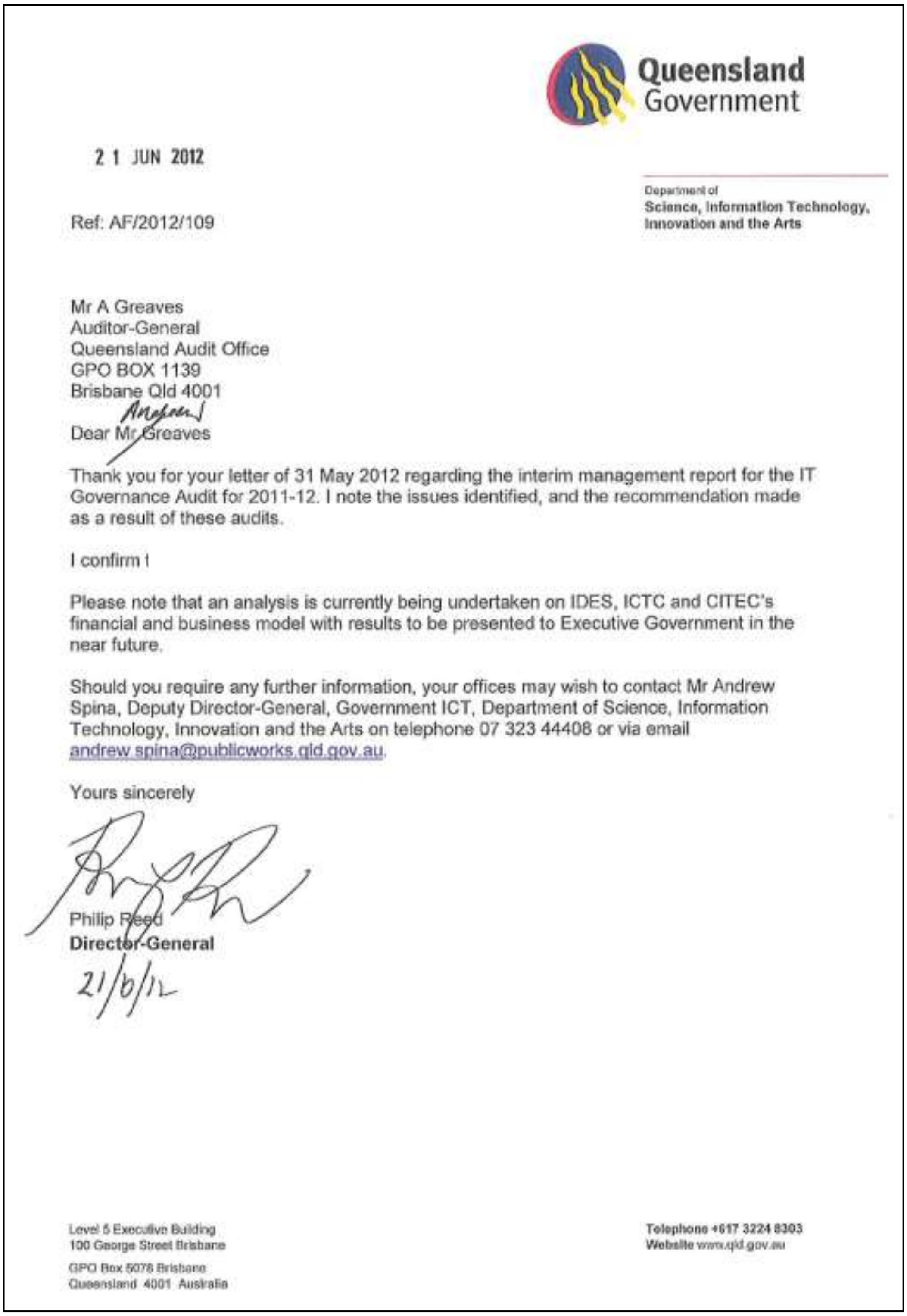
- There is no specific training in place over fraud control and prevention.
- Detailed analytics or data mining is not performed to highlight irregular transactions.

With respect to fraud control and prevention training, once the financial internal controls training package, discussed above, has been finalised, this will be rolled out to Treasury employees in the second half of 2012 as part of a broader training program focussing on governance and controls.

With respect to detailed analytics or data mining, Treasury does undertake analysis over high-risk areas, including corporate card and Office of State Revenue transactions. Other compensating controls are also in place to mitigate risk, such as mandatory supervisor approval of all corporate card transactions, independent certification of all direct invoice payments, delegation approval controls around purchase orders and transactional review as part of monthly budget monitoring activity. In addition, the Government Banking Unit, within Treasury, provides a monthly list of unusual corporate card transactions to each agency. Within Treasury, any transactions of an unusual nature are followed up with card holder supervisors, all of whom have recently completed (and are required to regularly complete) mandatory training.

Comments received

Response provided by the Director-General, Department of Science, Information Technology, Innovation and the Arts on 22 June 2012.



Queensland Government

Department of
Science, Information Technology,
Innovation and the Arts

21 JUN 2012

Ref: AF/2012/109

Mr A Greaves
Auditor-General
Queensland Audit Office
GPO BOX 1139
Brisbane Qld 4001

Dear ~~Mr Greaves~~ Andrew

Thank you for your letter of 31 May 2012 regarding the interim management report for the IT Governance Audit for 2011-12. I note the issues identified, and the recommendation made as a result of these audits.

I confirm t

Please note that an analysis is currently being undertaken on IDES, ICTC and CITEC's financial and business model with results to be presented to Executive Government in the near future.

Should you require any further information, your offices may wish to contact Mr Andrew Spina, Deputy Director-General, Government ICT, Department of Science, Information Technology, Innovation and the Arts on telephone 07 323 44408 or via email andrew.spina@publicworks.qld.gov.au.

Yours sincerely

Philip Reed
Director-General
21/6/12

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

Telephone +617 3224 8303
Website www.qld.gov.au

Auditor-General Reports to Parliament

Tabled in 2012

Report No.	Title	Date tabled in Legislative Assembly
1	Improving student attendance	May 2012
2	Results of audits: Local government financial statements for 2010-11	May 2012
3	Results of audits: Education sector financial statements for 2011	June 2012
4	Managing employee unplanned absence	June 2012
5	Results of audits: Internal control systems	June 2012

Publications are available at *www.qao.qld.gov.au* or by phone on 07 3149 6000.