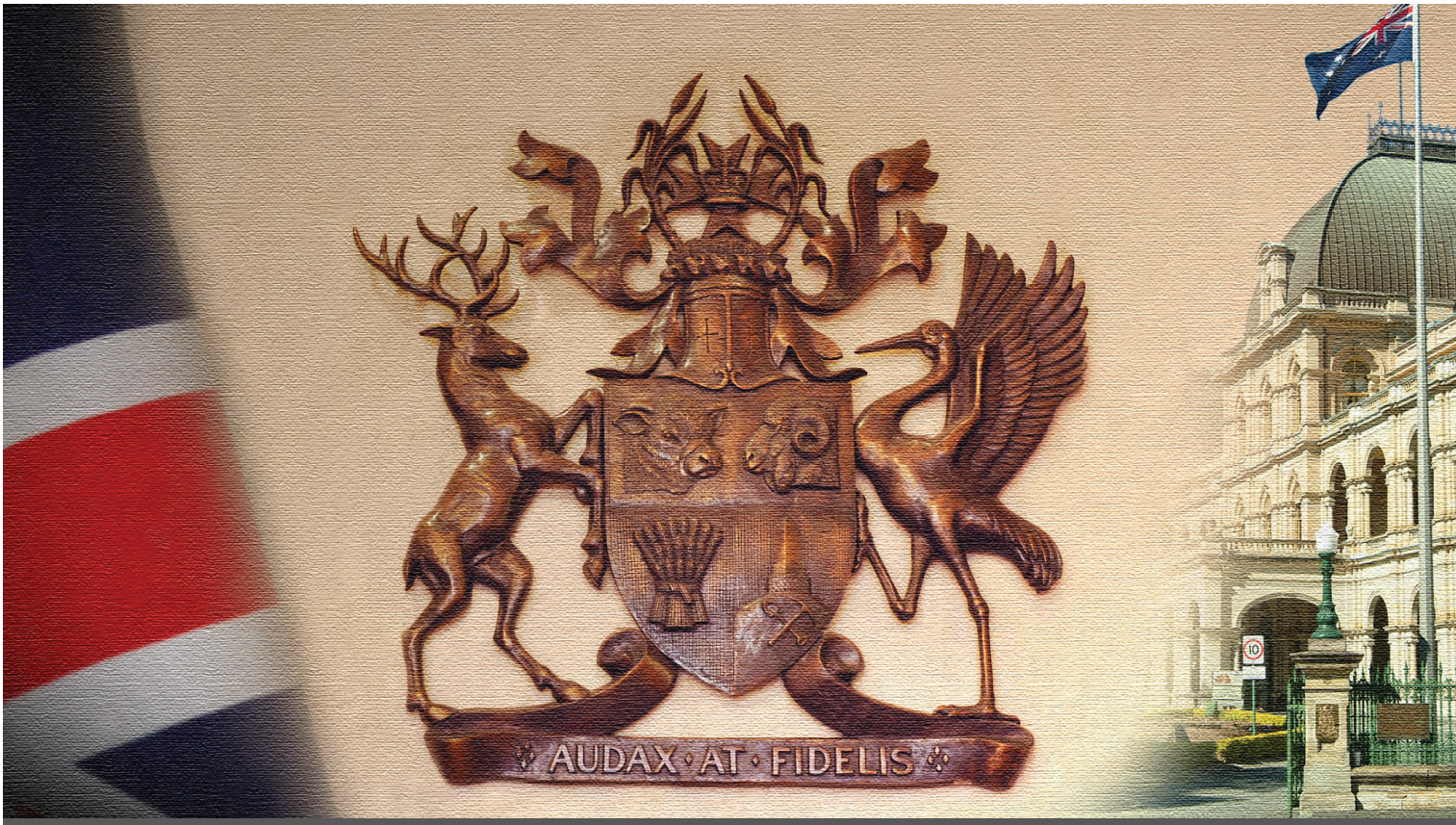
Auditor-General of Queensland



Financial and Assurance audit

Report to Parliament No. 4 for 2011

Information systems governance and security

QUEENSLAND AUDIT OFFICE

Enhancing public sector accountability

Auditor-General of Queensland

Financial and Assurance audit

Report to Parliament No. 4 for 2011

Information systems governance and security

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, 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

Auditor-General of Queensland

June 2011

The Honourable R J Mickel MP
Speaker of the Legislative Assembly
Parliament House
BRISBANE QLD 4000

Dear Mr Speaker

This report is prepared under Part 3 Division 3 of the *Auditor-General Act 2009*, and is titled Information systems governance and security. It is number four in the series of Auditor-General Reports to Parliament for 2011.

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

Yours sincerely

Glenn Poole
Auditor-General

QUEENSLAND AUDIT OFFICE
Level 14, 53 Albert St, 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

Contents

Executive summary

Introduction

This is the second report on the management and control of information and communication technology. It builds on the results of audits reported in *Auditor-General Report to Parliament No. 7 for 2010 – Information systems governance and control, including the Queensland Health Implementation of Continuity Project*.

This year's audit program included examination of the effectiveness of the arrangements that have been established to address the information and communication technology portfolio relating to the Toward Q2 through ICT strategy. Audits were performed at 14 public sector entities to determine whether there were systems and frameworks in place to enable effective management of IT at an agency level.

Major IT programs and a number of key IT projects were audited to see whether processes were in place to ensure the programs and projects were being managed effectively to obtain benefits and outcomes for the Queensland community.

The status of the implementation of recommendations from IT network security audits performed in prior years were followed up. Whole-of-government information security processes were examined.

Assessments were made on whether departments and shared service providers had adequate IT disaster recovery processes and procedures in place to deal with key systems failures in the event of disaster.

Why is appropriate management of IT important?

The cost to the Queensland Government for Information and Communication Technology has been estimated at $1.5b per year[1], representing approximately five per cent of the State Budget. It is therefore essential that strong information and communication technology management and control processes operate effectively across the sector and that the value delivered from this investment is maximised.

Key findings

Management of whole-of-government and agency IT could be improved.

The Queensland Government's Toward Q2 through ICT strategy is a major step in the management of IT at the whole-of-government level. The overall governance framework for the strategy is not effective and could be strengthened.

[1] Queensland Government ICT Market Overview 2008-09, Longhaus.

Frameworks and processes need to be further developed to ensure a greater focus on benefits, accountability and on the subcommittees engaged in the management of the strategy in delivering the strategic objectives and outcomes. Planning for the benefits to be achieved from implementing the Toward Q2 through ICT strategy needs to be further enhanced to enable performance to be reported against the intended benefits and outcomes.

To deliver the targets outlined in the Toward Q2 through ICT strategy, it is essential that rigorous management arrangements are in place at the agencies. Too often, focus is on information technology strategies, policies and budgets, and not recognising that without good management, these actions are unlikely to be translated into the desired results.

The level of maturity of IT management and control at the public sector agencies audited varied. Processes were found to be either developing or defined and documented at most entities audited and the agencies showed commitment to improving the maturity levels of their IT management processes. The linkages between the overall management and control of IT across all the agencies audited needed improvement.

IT programs and projects could be more effectively managed.

Over the past several years, Queensland Government entities have undertaken large programs of IT work that have not achieved the full range of intended benefits or outcomes. The audit of major IT program management found that in many instances there is currently no clearly identified business owner for the whole-of-government programs, that is, the departments who will gain value from the successful implementation of the program. This has resulted in a lack of overall commitment at the individual agency level in the implementation of the technology being produced through these programs. A business owner, or a body to actively represent the business owners, needs to be appointed for whole-of-government solutions to ensure that the systems are kept updated and benefits continue to flow from these investments.

A sponsoring group to oversee whole-of-government programs is needed to ensure that there is a strong commitment to the transformational change required across agencies to realise the benefits. Risk management processes should be improved to include management of strategic risks and consistency of risk management practices across programs and projects.

The audit also found that project management mechanisms did not operate effectively throughout the life of either the New Queensland Drivers Licence project or the Land Tenure Ledger redevelopment project. Both projects experienced significant delays and cost more than originally budgeted. The initial project planning was not adequate for the New Queensland Drivers Licence project and key project documentation was not in place or not updated for either of the two projects. Benefits realisation frameworks and plans were not in place for these projects and consequently, benefits have not been clearly identified, measured and monitored.

Effective management and control is essential to ensure that the implementation of such projects exploit the systems' capabilities to deliver tangible value to the Queensland community.

Information security within agencies could be improved.

Effective information security requires the appropriate leadership, organisational structures and processes to safeguard information. Good information security requires senior management commitment, a security culture, promotion of good security practices and compliance with policy.

Network security should be improved across the Queensland Government to reduce risks such as the manipulation of systems. While 60 per cent of the issues raised in the audits undertaken in 2009 have been resolved, implementing audit recommendations does not appear to have been given a high priority.

Given the threats to security due to the Internet and constant technological advancement, agencies need to give more attention to IT network security. Agency management should continue to review and monitor the administration of network and server security controls. The security of networks and servers supporting financial processing applications and other applications should be proactively managed.

The oversight of information security at a whole-of-government level relies on individual agencies to adopt Queensland Government guidance with agency self assessment and reporting. The results of the audits of IT network security confirm the non-compliance identified through the agency self assessment process and the need for further action by the agencies.

Information technology disaster recovery plans are at various stages of maturity

Disaster recovery planning across the public sector agencies audited is at various stages of maturity. The recent natural disasters have provided some opportunities for testing disaster recovery plans and have highlighted weaknesses that can be used by agencies to improve IT disaster readiness.

While most agencies audited have disaster recovery plans in place, either at an agency level or at a system level, many do not keep the plans up to date and tested. Some agencies have not carried out appropriate risk assessment and business impact analysis to identify the critical systems, data, management and people required for the recovery process.

The disaster recovery arrangements are not clearly detailed in operating level agreements between agencies and the Shared Service Agency. CITEC has some documentation on procedures to be followed in the event of a disaster but there is significant reliance on the knowledge of staff to prioritise key processes when a disaster occurs. CorpTech has performed business impact analysis but it is not extensive enough to develop an end-to-end IT disaster recovery plan for the shared services environment.

There is no documented whole-of-government business continuity management strategy to manage the continuity risks relating to the shared services IT systems.

Stakeholders' responses

Responses provided by the respective entities in relation to the issues raised in this report are provided in Section 5.2.

1 | IT management

Summary

Background

Effective management of IT requires an appropriate framework of leadership, responsibilities and accountabilities to ensure that processes and standards are in place to direct and control the investment in IT so that the agencies' strategies and objectives are achieved.

Audits were conducted of IT management at the whole-of-government level as well as IT management at the 13 departments and the Brisbane City Council.

Key findings

- **Whole-of-government IT management** – The development of the Toward Q2 through ICT strategy has brought together initiatives across agencies and has enabled greater visibility of the Queensland Government's information and communication technology agenda. Existing frameworks and processes require significant changes to foster improved governance and to use benefits management to drive the selection, review and update of the Toward Q2 through ICT strategy.
- **Agency IT management** – Three main areas of IT governance were audited: IT risk management, organisational frameworks and strategic planning processes. Overall, it was found that the management processes were at various levels of maturity within each of the agencies audited. Most of the processes were both defined and documented or at developing stages.

1.1 Whole-of-government IT management

1.1.1 Audit overview

On 9 September 2009, the Premier released the Queensland Government's strategy for Government information and communication technology, the *Toward Q2 through ICT 2009-2014* strategy. A key aim of this strategy is to achieve efficiencies by enabling the Queensland Government to perform successfully as a single enterprise. An extract from the Toward Q2 through ICT strategy detailing the focus areas, priorities and targets is included in Section 5.1.

Among the actions taken to implement the strategy across government:

- A portfolio management approach is used to deliver the strategy implementation plan. Under this approach, the optimal mix and sequencing of the projects proposed under the Toward Q2 through ICT strategy is considered to achieve the government's overall goals.
- A management structure with ten sub-committees has been established to monitor and control progress of the Toward Q2 through ICT portfolio of initiatives.
- A portfolio management office has been established within the Department of Public Works Information and Communication Technology Policy and Coordination Office to coordinate whole-of-government information about government IT activities and to develop frameworks to assist agencies in improving IT management and benefits management processes.

1.1.2 Audit conclusion

The development of the Toward Q2 through ICT strategy is a significant step in adopting a whole-of-government approach to information and communication technology service delivery. It has enabled greater visibility to agencies and the industry, of the whole-of-government information and communication technology activities.

This first strategy, and the experience gained in its implementation, can now be used to revise the strategy. Greater alignment between the initiatives within the strategy and the set targets would enhance the capacity to achieve the desired outcomes.

Frameworks and management processes need to be further developed to ensure a greater focus on benefits, accountability and on subcommittees delivering to strategic objectives and outcomes. Planning for the benefits to be achieved from this portfolio should be strengthened to enable performance to be reported against benefits and outcomes.

The Portfolio Management Office has been instrumental in implementing methodologies and delivering outputs that enable senior executives and Cabinet to have an overall view of information and communication technology activity across the sector. The Portfolio Management Office has developed frameworks to assist agencies in improving IT management and benefits management processes. It is these types of activities that ensure that the Queensland Government's investment in information and communication technology initiatives are optimised in terms of monitoring delivery of benefits and managing risks versus returns.

However the continuation of this office or alternative arrangements to manage the portfolio beyond the current funding approval of June 2011 was unclear as at March 2011. Management has since advised that funding has been allocated until June 2012. However, the whole-of-government ICT strategy and portfolio is a long term initiative and the Department of Public Works needs to adopt a long term approach to managing this portfolio.

The establishment of the various committees to manage individual initiatives within the strategy has created opportunities for greater collaboration across the public sector by emphasising the importance of developing whole-of-government rather than agency focused information and communication technology initiatives.

The processes appear to have now matured to a level where the number of committees could be rationalised. In addition, the reorganisation of the committee structure with reference to established methodologies and the power to govern the whole-of-government portfolio, programs and interagency projects could enhance their effectiveness.

1.1.3 Audit scope

The scope of this audit was to evaluate the effectiveness of the management arrangements that have been established to address the Toward Q2 through ICT strategy.

References used in the development of audit criteria include:

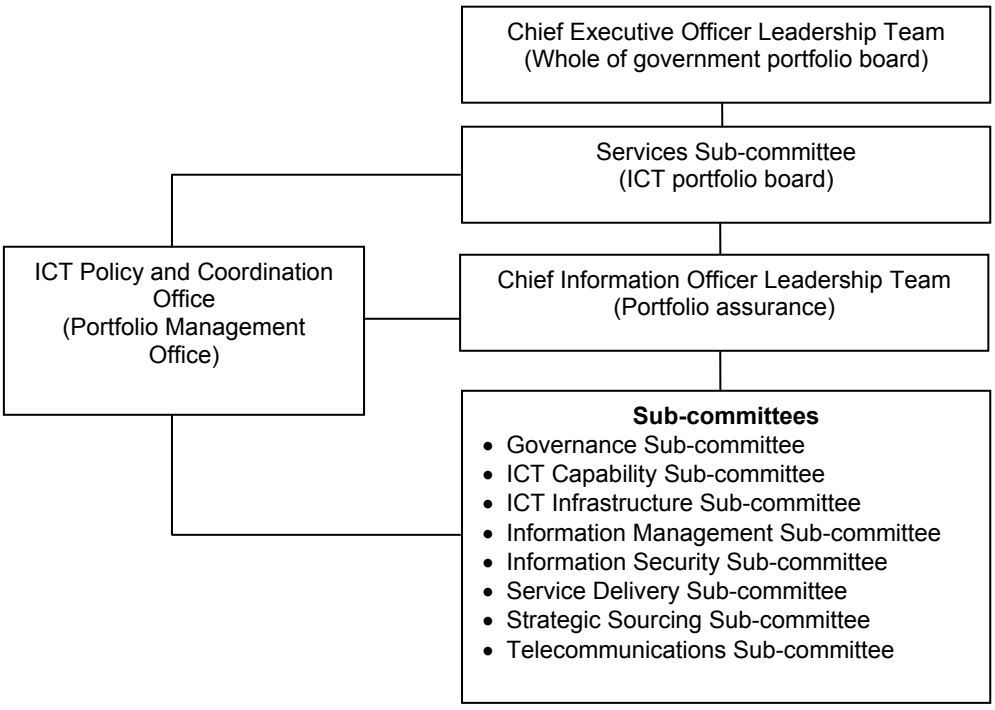
- *Queensland Government Portfolio Management Methodology.*
- *ISO/IEC 38500:2008 Corporate governance of information technology.*

1.1.4 Audit findings

The portfolio board for the Toward Q2 through ICT strategy

Figure 1A shows the structure in place to manage implementation of the strategy.

Figure 1A – Toward Q2 through ICT strategy management structure



The CEO Leadership Team Services Sub-committee was assigned the responsibility for being accountable for the delivery of benefits and outcomes of the Toward Q2 through ICT strategy and projects. This responsibility was communicated to Cabinet through a progress report on the portfolio. However, the terms of reference for the CEO Leadership Team Services Sub-committee did not reflect this role.

One of the ten sub-committees involved in monitoring the Toward Q2 through ICT portfolio, the Services Sub-committee, has an advisory role but was not actively involved in managing the Toward Q2 through ICT portfolio.

Between December 2009 and December 2010, 13 meetings of the Services Sub-committee were held but no material decisions relating to the Toward Q2 through ICT portfolio were made by the Sub-committee during that time. The Services Sub-committee did not have the necessary powers to exercise effective governance over the portfolio such as changing the progress or discontinuing initiatives in response to an assessment of their capacity to deliver benefits to the operations of the Queensland Government.

The overall governance framework for the strategy was not effective and could be strengthened.

Strategic focus is required for sub-committees

As there is no effective portfolio board that is responsible for the delivery of benefits and outcomes, the management structure consists of a set of sub-committees only responsible for the implementation of specific activities. This could result in actions being delivered, but strategic objectives not being achieved. There is an increased risk that initiatives that are completed may not provide strategic value or that opportunities for completing other strategic initiatives may be missed.

Many of the sub-committees were assigned actions that contributed to the same objective. Consequently, there was no clarity about ownership and accountability for the achievement of the strategic objectives.

For example, actions relating to the priority “Delivering savings” were allocated to five sub-committees and the Information and Communication Technology Division of the Department of Public Works. The target assigned to this priority was “By 2013, the government will reduce the per-unit cost of business as usual information and communication technology expenditure by 15 per cent.” However, the sub-committees’ collective accountability for achieving this target was not defined.

Within the current structure, the key benefits of sub-committee involvement for agencies is the sharing of information and increasing awareness of the new or changed policies being developed by the Department of Public Works. More benefit could be achieved if the sub-committees included a mechanism to encourage the implementation of policies and the measurement of the benefits realised for the Queensland Government by implementing these policies.

Risk management practices require improvement

Risk management is vital for effective project, program and portfolio management. There was no evidence of strategic risks being identified in relation to whether the initiatives being undertaken as part of the Toward Q2 through ICT would achieve their objectives.

The risk register of the Toward Q2 through ICT portfolio focused on the risk of delivery of actions. There was no process to assess the risk if the initiatives fail to contribute to overall strategic value of the Toward Q2 through ICT strategy.

The management structure implemented limits the ability of sub-committees to manage strategic risks as the sub-committees are not owners of any of the Toward Q2 through ICT strategic objectives.

Stronger alignment is required between actions and targets

The audit of Toward Q2 through ICT implementation plan showed that actions within the plan defined the deliverables to be achieved. However, these actions and deliverables were not linked to the specific targets outlined in the strategy so it was unclear how the actions identified in the implementation plan would help achieve the targets defined in the strategy.

Measurable benefits, resource requirements and costs of implementation were not identified at the time the strategy and implementation plan were approved. These matters were investigated after the commencement of the implementation phase of the strategy.

There is insufficient data available to support an analysis of benefits for internal performance reporting by sub-committees relating to the Towards Q2 through ICT portfolio.

Portfolio Management Office

A Portfolio Management Office was created to support the Toward Q2 through ICT portfolio. The portfolio of projects is scheduled to be finalised by December 2014. However, as at March 2011 the Portfolio Management Office was funded until June 2011. Management has since advised that funding has been allocated until June 2012.

The Portfolio Management Office has played a key role in supporting the Toward Q2 through ICT portfolio. This is evident from the work that has been done to assist initiative owners in understanding reporting requirements, and the regular completion and communication of performance reports. These performance reports are important in communicating progress being made for each initiative and making recommendations for initiatives that require changes to schedules.

The Queensland Government's vision of the whole-of-government approach to information and communication technology to maximise benefits and savings requires a fully functional Portfolio Management Office.

Benefits management is not well developed

Portfolios exist to achieve strategic objectives measured by benefits that have been realised from implementation of the selected initiatives. While work was progressing to define benefits, this work was not performed at the commencement of the Toward Q2 through ICT portfolio. The benefits management strategy was endorsed 13 months after the portfolio commenced.

The audit found initiative proposals did not contain sufficient documentation of benefits to demonstrate how the initiatives contribute to the achievement of the strategic benefits. There is no register that provides an overview of the total benefits the portfolio is expected to achieve. At the time of the audit, performance measures were defined for only six of the 58 initiatives.

A framework has been developed by the Portfolio Management Office to improve the consistency of benefits management across the sector.

1.2 Agency IT management

1.2.1 Audit overview

Effective management of IT requires process and structures that ensure that organisations deploy their IT investments appropriately for the resulting activities such as programs, projects or operations to achieve the desired results. The creation and application of this management framework is the responsibility of executive management and is an integral part of overall management of the organisation. The management framework consists of the leadership and organisational structures that ensure IT contributes to the organisation's strategies and objectives.

The audit examined whether there were systems and frameworks in place to enable effective management of IT.

1.2.2 Audit conclusion

Overall, the audit found that the level of maturity of IT management and control of the public sector entities audited varied. It is noted that linkages between overall management and control of IT needs improvement across all of the entities audited. The number of entities within categories of maturity levels is shown in Figure 1B.

Figure 1B – Overall assessment of IT management processes

IT management processes are defined and documented	New or developing IT management processes	IT management processes not operating effectively
9	3	2

After assessing three key management areas, it was found that IT management processes at two departments were not operating effectively. In the case of the one department, in approximately two years since the machinery of government changes in 2009, the IT management processes of the amalgamated departments have not been consolidated. The outdated frameworks of the former departments do not depict current practices.

Processes are either developing or defined and documented at the Brisbane City Council and the other 11 departments audited. Senior management at all entities showed commitment to improving the maturity levels of the IT management processes.

Audits of IT management processes at the Department of Education and Training have been undertaken and reported to Parliament for the past three years. A concerted effort has been made by the Department of Education and Training to address the majority of the recommendations from previous audits. There has been significant improvement since the first audit in 2009.

1.2.3 Audit scope

The scope of the audit was to examine the effectiveness of:

- IT management frameworks including organisational structures, processes, leadership, roles and responsibilities.
- IT strategic planning processes including definition, measurement and monitoring of key performance indicators.
- IT risk management to ensure that investment in IT is aligned and delivered in accordance with organisational strategies and objectives.

The public sector entities audited are shown in Figure 1C. The Brisbane City Council was included with the 13 departments due to the size and complexity of its IT management.

Figure 1C – Entities audited

Entities	
Brisbane City Council	Treasury Department
Department of Communities	Queensland Health
Department of Justice and Attorney-General	Department of Employment, Economic Development and Innovation
Department of Community Safety	Department of Environment and Resource Management
Queensland Police Service	Department of the Premier and Cabinet
Department of Local Government and Planning	Department of Transport and Main Roads
Department of Public Works	Department of Education and Training

1.2.4 Audit findings

IT management framework

The IT management framework enables the alignment of IT with organisational strategies and objectives, the delivery of value from the use of IT, the management of risks and resources and the measurement of performance. The framework should define leadership, accountability, roles and responsibilities, information requirements, organisational structures, and practices to avoid breakdowns in internal control and oversight.

Figure 1D shows the level of maturity of IT management frameworks in the 14 entities audited.

Figure 1D – Status of IT management frameworks

IT management framework is defined	Developing IT management framework	Action required to properly develop IT management framework
7	5	2

The audit found seven entities had defined IT management frameworks with five other entities in the process of developing their IT management framework. Entities with defined frameworks have documented and communicated IT management structures and there is senior management involvement in IT strategic decision making. The organisation of IT in these entities is well-developed, documented, communicated and aligned with IT strategy. Strategies are defined and updated in line with changing business strategies and objectives.

Action is required at two entities to develop the IT management framework. Examples of the issues identified at these entities include:

- Lack of control and coordination of IT functions.
- The Information Steering Committee either not existing or not effectively governing IT functions.
- Effective reporting practices not being in place over those responsible for managing IT functions.

Without an effective framework, IT may not be appropriately aligned with the business objectives and processes may not be in place to ensure IT business risks are managed.

IT strategic planning process

An IT strategic plan includes the documentation of all key benefits, costs and risks associated with planned IT investments and operations. The IT strategic plan must contain sufficient information and performance metrics to allow planning of activities and monitoring of progress against the plan.

The development of an IT strategic plan is a significant undertaking that requires contributions by all business areas requiring IT services. This plan needs to be supported by senior management and updated to reflect changing business requirements annually. IT strategic planning is a requirement of *Information Standard 2 ICT Resources Strategic Planning*, issued by the Queensland Government Chief Information Office. Although this standard is only applicable to Queensland government departments, the Brisbane City Council was assessed against this standard in terms of better practice.

Figure 1E – Status of strategic planning process

IT strategic planning processes are defined	IT strategic planning processes in place but some improvement needed	Significant improvement to IT strategic planning processes required
7	4	3

As Figure 1E shows, seven entities have IT strategic planning processes with defined key performance indicators and effective reporting mechanisms. The other seven entities need to improve their IT strategic planning processes in the following areas:

- Plans not aligning with corporate plans, making it unclear how IT would be used to contribute to the achievement of the agency's strategic objectives.
- Plans not including significant IT programs, projects and initiatives which would contribute to strategic objectives.
- Plans in draft or out of date.
- Plans not defining key performance indicators, key risks and the management of these risks.
- The timeframes to complete IT projects only defined at the individual project level and not being defined in the IT strategic plans.

The lack of a formal, updated and monitored IT strategic plan may result in a disparity between service delivery and business needs. IT initiatives may not be aligned with the business priorities and plans, or support whole-of-government IT directions. Information required for informed decisions on investing in IT may not be provided to those responsible for approving IT initiatives.

Benefits management

Benefits management drives the development of the IT strategy and facilitates prioritisation of initiatives so they are undertaken based on the value that they deliver to the agency. It needs to be carried out from the proposal to the post-implementation stage. The achievement of benefits needs to be progressively reviewed to ensure that the investment in IT achieves the intended outcomes.

If a benefits realisation process is not in place, full business benefits from IT initiatives may not be attained.

As shown in Figure 1F, 12 of the 14 entities do not have benefits realisation processes in place or the process is in such an early stage of development that it cannot be used to drive the delivery of IT strategy.

Figure 1F – Status of benefits realisation processes

Benefits management processes documented	Developing benefits realisation processes	Benefits realisation processes not in place
2	5	7

The seven entities without benefits realisation processes did not have in place:

- A benefits management strategy to guide the implementation of benefits management.
- A benefits realisation plan documenting a structured process for the department to manage and demonstrate the progressive achievement of the benefits from IT investment and operations.
- Formal benefit reviews conducted during or at the conclusion of IT investment programs to assess benefit achievement against the benefits realisation plan.

Lack of progressive review of benefit achievement may result in resources continuing to be applied to investments that will no longer deliver the intended outcomes.

IT risk management processes

An IT risk management framework should be designed and implemented so that risks are identified, reported and managed in a consistent manner throughout the organisation. This will assist in ensuring that key risks are not missed or the impact of risks is not underestimated.

Effective IT risk management raises the awareness of potential risks and demonstrates a proper level of due diligence. Figure 1G shows the status of IT risk management processes at the 14 entities audited.

Figure 1G – Status of IT risk management processes

Effective risk management processes	Risk management processes in place but requires some improvement	Risk management processes need significant improvement
4	5	5

Nine of the entities audited either have effective risk management processes in place or show only some areas of improvement. Five entities need significant improvement to risk management processes. Issues identified at these entities include the lack of an overarching IT strategic risk register, the IT risk management framework and risk registers not being documented. Minimum consideration is given to operational, program and project risks as part of the IT risk management process.

Weaknesses in risk management processes may result in appropriate risk treatment and mitigation procedures not being undertaken. Accountability for strategic and corporate IT risk may not be identified and communicated when IT risks have not been documented and escalated appropriately.

2 | Program and project management

Summary

Background

Program management is the coordinated organisation, direction and implementation of a group of projects and activities that together achieve the outcomes and realise benefits that are of strategic importance. The projects in the program should be managed in a coordinated way to obtain benefits and a level of control not available from managing the projects individually. Programs should be designed to deliver both outcomes and benefits. The audit examined three major programs: ICT Consolidation Program; Identity, Directory and Email Services Program; and Corporate Solutions Program.

Two significant projects were examined, being the New Queensland Drivers Licence project and the Land Tenure Ledger redevelopment project. The status of the Queensland Health payroll project and the OneSchool project have also been reviewed by audit.

Key findings

- **Program management** – The whole-of-government programs are significantly delayed with the result that these programs are not contributing effectively to the savings target of the Toward Q2 through ICT strategy.
- **Project management** – IT project management across these two projects could be improved. The audit found that project management mechanisms did not operate effectively throughout the life of both the New Queensland Drivers Licence project and Land Tenure Ledger redevelopment project.
- **Status of Queensland Health's payroll project** – Some project governance issues continue to be experienced with the Queensland Health payroll project. Salary overpayments and emergency cash payments to employees have continued though at a reduced level in recent pay cycles.
- **Status of the Department of Education and Training's OneSchool project** - Management of the OneSchool project has improved over time with all previous audit recommendations being implemented.

2.1 IT program management

2.1.1 Audit overview

A program consists of several inter-related projects with each project designed to deliver a specific capability. Effective program management entails the coordination of a number of projects and oversees the realisation of the benefit from the investment such as ensuring the right capabilities are delivered and are integrated into the organisation.

The management controls of three programs for implementation across the public sector were audited in 2010. The programs, ICT Consolidation Program; Identity, Directory and Email Services Program and Corporate Solutions Program, were initiated with the expectation of significant financial savings and other benefits to government.

This audit was a follow up of the audit of program management included in *Auditor-General Report to Parliament No. 7 for 2010 – Information systems governance and control, including the Queensland Health Implementation of Continuity Project*.

2.1.2 Audit conclusion

The management of IT programs designed to provide benefits across all or a number of departments is currently not fully effective. These programs are the responsibility of the department assigned to undertake their development and delivery, in the case of these three programs audited, the Department of Public Works.

There is currently no clearly identified business owner for the programs, that is, the departments that will gain value from the successful implementation of the program.

This has resulted in a lack of overall commitment in the implementation of the technology being produced through these programs. A business owner, or a body to actively represent the business owners, needs to be appointed for whole-of-government solutions to ensure that the systems are kept updated and benefits continue to flow from these investments.

There is no sponsoring group to oversee whole-of-government programs to ensure that there is a strong commitment to the transformational change required across agencies to realise the benefits.

There is no clear accountability for delivery of outcomes and benefits after technology solutions are implemented. Benefits realisation should be measured and monitored after the programs are delivered.

2.1.3 Audit scope

The objectives of the audit were to determine whether appropriate management controls were implemented over three major programs. The focus was to ascertain whether processes existed to ensure corresponding benefits were realised from the major investments.

The following programs were examined:

- ICT Consolidation Program.
- Identity, Directory and Email Services Program.
- Corporate Solutions Program.

2.1.4 Audit findings

These significant whole-of-government programs were established to achieve different outcomes. Since the audits of these programs were last reported, further delays occurred in implementing the technology. Lengthy delays in program delivery results in programs being exposed to significant changes in operating environments over time.

For example, the original business case for the Identity, Directory and Email Services could not have anticipated events such as the machinery of government changes in 2009 and the 2011 floods having a significant impact on the capacity of agencies to fund project activity to migrate to the Identity, Directory and Email Services solution. These events have affected the take-up of the Identity, Directory and Email Services solution with only four agencies now expected to migrate to the solution within the required timeframe with other agencies deferring their migrations following reevaluation of their individual priorities.

At the time of the audit, only one department had committed to CITEC's fully managed service under the ICT Consolidation Program. Negotiations are underway with three other agencies to use selected aspects of CITEC's fully managed service.

Details of the audit of the individual programs are discussed in the following sections.

2.1.5 Programs audited

ICT Consolidation Program

The ICT Consolidation Program was formed in September 2009 after a review of the former Technology Transformation Program that began in July 2008 with funding of $44m. This program is a key enabler to achieving consolidation of the Queensland Government's central business district data centres, networks and infrastructure services.

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

A key objective of the ICT Consolidation Program has been to deliver savings by implementing infrastructure for the whole-of-government consolidation of information and communication technology infrastructure. To date, a Tier 3 data centre and an interim network to access that data centre has been made available.

Consolidation of network, security and storage services cannot occur until the infrastructure to enable these activities has been delivered. The planning for this migration activity has been hindered by the lack of a service catalogue and price book to outline the costs to agencies for using this infrastructure.

The level of technology consolidation achieved will depend on activities undertaken following this program's closure, expected to be in September 2011. Ongoing partnerships between CITEC and agencies will need to continue so that the Queensland Government's investment in the infrastructure delivers benefits through effective use of the technology by agencies.

While attempts were made to promote the notion of a sponsoring group or business owners, it was not implemented effectively at the time of this audit.

In addition, benefits analysis was still progressing. The ICT Consolidation Program may deliver an enhanced level of technology that provides resilience and redundancy at a lower cost, given the economies of scale. However, whether this will result in lower costs for agencies will depend on the price charged by CITEC compared to the cost of agencies previously operating their own technology. There were concerns that agencies had not captured and reported the true cost of their existing IT operations.

Information and communication technology consolidation strategies and roadmaps had been agreed with all 13 departments however the agreements did not require commitments for specific deliverables from either CITEC or the departments. There was a general expectation that the departments would support whole-of-government information and communication technology consolidation. While CITEC has been conducting detailed migration planning with four agencies, audit identified that the consolidation strategies of the remaining departments were not supported by schedules outlining when CITEC would deliver the infrastructure and the related pricing. Therefore, these departments have not been able to effectively plan for consolidation activities. Similarly, timeframes and deliverables for departments to prepare for consolidation activities were lacking.

Identity, Directory and Email Services Program

The Identity, Directory and Email Services Program set out to deliver a whole-of-government email, identity management and authentication service to be managed and operated by CITEC upon which multiple whole-of-government services can be provisioned. The first service to be provisioned is a whole-of-government email services based upon the Microsoft Exchange platform. Originally, it was expected that this program would be one of the largest email consolidations implemented by government in Australia. It was intended that the Identity Management platform would provide a single unique identifier for every government employee.

A business case for the Identity, Directory and Email Services Program completed by the Department of Public Works in October 2007 identified that estimated savings of $123m could be achieved over ten years when compared with the cost of agencies operating on separate platforms.

At the time of the audit, the actual spend on the Identity, Directory and Email Services Program was $34.2m. While this is below the $89.1m forecasted for this stage of the program, the program has not collected any revenue and is not expected to commence receiving revenue from agencies until the 2011-12 financial year. The original business case forecast that $56.6m revenue would be received by 30 June 2011.

There have been a number of changes to the expected completion date of the Identity, Directory and Email Services Program since the program began in December 2007.

A 12 month delay of the detailed level design phase has affected the program's schedule. The build and test phase of the program is now in progress while system integration testing is being finalised. This delay has affected delivery of the subsequent phases.

The program was originally expected to be delivered by December 2009. This was later changed to June 2011 and subsequently changed to December 2012. Due to a reduction in agency take-up of the Identity, Directory and Email Services service within the required timeframe, further migration activities will need to occur following closure of the Identity, Directory and Email Services program. These migration activities should continue to be governed after the close of the current program as part of CITEC's 'business as usual' operations.

IT programs that last as long as the Identity, Directory and Email Services Program are at risk of being exposed to major unplanned changes in their operating environments and these can significantly affect the outcome of the program. The original business case did not anticipate the following events that have affected delivery of the program:

- Significant machinery of government changes resulting in 22 departments being reduced to 13. This meant that the program had to be replanned based on the new arrangements.
- Contract negotiations taking longer than anticipated.
- The solution taking longer to develop than originally anticipated due to the complexity of integration between the identity management and email solutions.
- The 2011 floods having a significant impact on the capacity of agencies to fund project activity to migrate to the Identity, Directory and Email Services solution following reevaluation of agency priorities. Only four agencies are now expected to migrate to the Identity, Directory and Email Services solution within the required timeframe. Other agencies have deferred their migrations following reevaluation of their priorities.

The Identity, Directory and Email Services program has attempted to promote the need for a sponsoring group that would be responsible for obtaining strong commitment to the transformational change required across agencies. This group would be responsible for ensuring that benefits from the Queensland Government's expected investment in the Identity, Directory and Email Services Program are realised. The CEO Leadership Team Services Sub-committee was assigned the role of monitoring the program however, this group did not have the power to manage the Identity, Directory and Email Services Program. The Department of Public Works is currently reviewing options for assigning sponsoring group responsibilities.

A revised benefits map for the program has been developed, however the benefit profiles and measures have not been revised. A key issue for the Identity, Directory and Email Services Program will be the timing of benefits with agencies deferring their migration.

As at April 2011. the program was expected to deliver services for 20,000 users by December 2012. This is approximately 25 per cent of the number of users that were expected to be migrated by that date. This will result in the program incurring further losses until the number of departments taking up the solution increases. It is estimated that the program will need to deliver services to approximately 81,000 users to break even.

Corporate Solutions Program

The Corporate Solutions Program (formerly Shared Services Solution) was established in August 2005 to design and build a whole-of-government finance and human resource solution. The original vision of a single solution proved difficult to achieve. The strategy changed to having a reduced number of systems. *Auditor-General Report to Parliament No. 7 for 2010 – Information systems governance and control, including the Queensland Health Implementation of Continuity Project* highlighted deficiencies with the model adopted for the most recent implementation.

In response to the problems faced during the implementation of the Queensland Health payroll, the Queensland Government engaged PricewaterhouseCoopers to review the shared services operating model. The proposed PricewaterhouseCoopers operating model supports a multi-instance approach for finance and human resource/payroll applications across three clusters, being Queensland Health, Department of Education and Training and the rest of government.

The Corporate Solutions Program has continued to progress delivery of its priorities through implementation of the Department of Community Safety human resource systems, which is in the detailed planning phase, and the Department of Public Works finance system, which is being rescoped as a result of initial planning.

Some six years on, CorpTech currently supports eight finance and 13 payroll systems. Some of these systems present a risk to business continuity of departmental processes due to the age of some legacy systems. Audit was advised that in the short to medium term, the program would focus on ensuring business system continuity through the management of risks to system failures and returning systems into mainstream vendor support.

There have been weaknesses with the management of the Corporate Solutions Program under different delivery models from its beginning. A review of the original Shared Services Solution program in 2007 identified problems with the management of the program that resulted in the adoption of a prime contractor model. This model was implemented, but was inadequately governed which contributed to desired outcomes not being achieved, the size of the program being underestimated, and ultimately the flawed implementation of Queensland Health's payroll system.

Both Auditor-General Report to Parliament No. 7 for 2010 and the PricewaterhouseCoopers report identified the need for management of shared services to be improved to ensure that there is clear accountability for delivery of outcomes and benefits.

Whilst consolidation was a key driver of the Corporate Solutions Program, the delays experienced have increased the risk exposure of existing systems. Therefore, projects now undertaken are focussed on addressing the risk associated with legacy systems that are no longer being covered by mainstream vendor support. It is important that risks relating to ageing systems be promptly addressed. Should these risks materialise, it could affect the continuity of key back office processes such as processing payroll for some Queensland Government public servants.

However, if further activities address only this risk and projects do not contribute to the reduction in the number of systems, there will continue to be high costs to support systems in future years.

Standardisation of systems cannot be effectively delivered without standardisation of business processes. This was identified in the PricewaterhouseCoopers review of shared services, and a recommendation was made for business process standardisation to be included in the Corporate Solutions Program. This is a key requirement to enhance the effectiveness of the program. Systems that have been deployed to date have not adequately addressed the need to automate existing manual controls. There remain instances even in the newer environments where key controls continue to be undertaken manually.

2.2 IT project management

2.2.1 Audit overview

The role of effective IT project management is to provide a decision making framework that is logical, robust and repeatable to govern an organisation's investment in IT. This framework outlines the relationships between all involved in the project, describes the project information flow to all stakeholders and ensures reviews and approvals at appropriate stages of the project.

Project management not only provides a framework for the organisation of responsibilities and decision making, it ensures that the project implementation and execution will be completed efficiently. Under an effective project management framework, the key project decision makers are clearly identified prior to the commencement of the project. The establishment of appropriate project management mechanisms decreases the probability of poor controls during the life of the project.

A series of information systems audits undertaken since 2005 have consistently highlighted the importance of good project management and identified deficiencies in implementation across agencies. Since 2005, there have been eight Auditor-General Reports to Parliament that included the results of audits of information and communication technology projects.

This audit in 2010-11 examined two projects, which had not previously been reported to Parliament, being the New Queensland Drivers Licence project and the Land Tenure Ledger redevelopment project.

2.2.2 Audit conclusion

The audit found that project management mechanisms did not operate effectively throughout the life of either the New Queensland Drivers Licence project or the Land Tenure Ledger redevelopment project. Both projects experienced significant delays and cost more than originally budgeted.

The initial project planning was not adequate for the New Queensland Drivers Licence project and key project documentation was not in place or not updated for either of the two projects. Benefits realisation frameworks and plans were not in place for these projects and consequently, benefits have not been clearly identified, measured and monitored.

Recent changes to the governance of the New Queensland Drivers Licence project demonstrate a more effective system implementation process and the project is on track to rollout a new driver licence across the State by December 2011.

Effective management and control is essential to ensure that the implementation of such projects exploit the systems' capabilities to deliver tangible value to the Queensland Government and to the community.

2.2.3 Audit scope

This audit reviewed project management for two projects:

- New Queensland Drivers Licence project at the Department of Transport and Main Roads. The New Queensland Drivers Licence project is introducing smartcard driver licences that replace the existing laminated cards. The new driver licence stores a digital photograph and signature and an embedded computer chip and has greater security capacity than the current laminated cards. Apart from the licence, the project deliverables include related infrastructure such as hardware, software and office fit outs and new business processes for the new system.
- Land Tenure Ledger redevelopment project at the Department of Environment and Resource Management. The Land Tenure Ledger redevelopment project was established to provide the Department of Environment and Resource Management with a replacement for its legacy system which is more than 15 years old and based on obsolete and unsupported technology.

These projects were chosen for audit because they are significant systems implementation projects that provide critical government services.

2.2.4 Overall audit findings

Key project management tools were not in place for both projects

The business case for the New Queensland Drivers Licence project was not maintained after it was approved in 2006 nor does it appear to have been available to the staff involved in the project. The business case was approved based on opportunities for benefits outside the provision of a secure driver licence rather than specific and measurable benefits.

The opportunities for benefits were identified well before any detailed analysis and design of the technology required for their delivery was undertaken. In addition, the opportunities for benefits were not subject to scrutiny or assessment by the third parties required to use the solutions to achieve those benefits. Key project management documentation critical to managing the project such as a complete project plan and project initiation document did not exist and formal project quality plans, logs and reviews were only available for a recent review of pre-implementation risks. A benefits realisation plan was not in place for the project.

In the case of the Land Tenure Ledger redevelopment project, the original business case was developed in 2007, a year after the project was initiated. An up to date project and stage plans to direct project activity were not in place. The project plan in use at the time of the audit was last updated in November 2007. Similarly, the Phase 2 stage plan was last updated in February 2008. These plans referenced key staff, timelines, deliverables and risks that had since substantially changed. Although there were four project scope changes in 2007, two scope changes in 2008 and three changes in 2009, the business case, was only updated three years later in September 2010.

A benefits realisation plan was not in place for the Land Tenure Ledger redevelopment project. The business case records some benefits but does not contain sufficient detail to enable it to be used for benefits management. In addition, the achievement of the benefits stated in the original business case in 2007 is not tracked and monitored.

Both projects experienced significant delays

Both projects took longer than originally budgeted to be completed.

The New Queensland Drivers Licence project was initiated in August 2003 after Cabinet consideration in May 2002 of replacement options for the existing laminated licences. Upon completion of the business case and Cabinet approval to proceed with the project in May 2006, the rollout of the new driver licence was planned to be completed by June 2009. In 2007 the Cabinet Budget Review Committee was informed that a suitable public private partnership proponent could not be identified and there was to be a seven month delay with the rollout to commence in mid 2009. The rollout completion date changed to late 2010.

There has been substantial activity on the project in the last 12 months to two years with the procurement of the services and equipment necessary to introduce the new licence, user acceptance testing, internal trials, completion of training packages and planning of a staged implementation of the system. It is now anticipated that the rollout will be completed by late 2011. A pilot implementation began in November 2010.

The Land Tenure Ledger redevelopment project was established in November 2005 with the system to be redeveloped inhouse and to be completed by 2009. The area of land tenure is subject to evolving legislation and several legislative changes were required to be taken into account throughout the life of the project. These legislative as well as other scope changes have contributed to project delays of at least two years from the original anticipated go-live date.

Both projects cost more than originally budgeted

The rollout of the New Queensland Drivers Licence project cost increased significantly from the original budget. The final cost of the project including capital and operational expenditure is expected to be $148.3m by the time the rollout to the Department of Transport and Main Roads centres is completed.

In April 2007, the Cabinet Budget Review Committee approved approximately $5.4m over a two year period to redevelop the Land Tenure Ledger redevelopment project as an inhouse development. At that stage it was envisaged that the project would be completed by 2009. Additional funding was approved and the project has now been completed. The total cost of the finalised project was $8.75m.

2.3 Status of Queensland Health's payroll project

In March 2010, Queensland Health went live with a new rostering and payroll solution. Significant system and business process issues were experienced that impacted on the timely and accurate payment of Queensland Health employees. The details of key issues resulting from the new system implementation were reported in *Auditor-General Report to Parliament No. 7 for 2010 – Information systems governance and control, including the Queensland Health Implementation of Continuity Project*.

Queensland Health engaged Ernst & Young to provide advice on the future direction of the payroll solution. Ernst & Young's report recommended reconfiguration and reimplementation of the solution over a three year period. A follow up audit has been performed on the progress Queensland Health has made in stabilising the rostering and payroll solution.

Overall, Queensland Health is progressing the improvement of the payroll and rostering systems. The new payroll operating model has been implemented. A key aspect of the new payroll operating model relates to each payroll processing centre (or payroll hub) processing mainly the transactions within the specific districts. The aim of the new payroll processing model is a more localised payroll process with opportunities to build good customer relationships with Queensland Health staff.

It is expected that the new model will contribute to improved client satisfaction. However, the actual benefits of the new model have yet to be formally measured. The new payroll operating model may assist with improving client satisfaction but requires higher staffing costs. Under the Lattice payroll system, the ratio of the number of payroll staff to process transactions to Queensland Health employees was approximately 1:160. Under the current system, the ratio is approximately 1:90. The strategic direction of the payroll should continue to be reassessed and complexities addressed over time to decrease the number of staff required to process payroll transactions.

There have been improvements made to reduce the number of unprocessed payroll transactions. More rigour around processing has shown a decline in unprocessed transactions. At the initial reporting stages of the new payroll system in April 2010, approximately 44,000 outstanding adjustments were recorded at the end of each pay cycle. On 2 June 2010, there were 42,088 outstanding adjustments and an initial target was set by Queensland Health to reduce this number to below 20,000 by August 2010, which was achieved on 11 August 2010 when the number was 16,644.

The average number of transactions processed per day is approximately 4,000 and with the current pay cycle and cut-off periods, Queensland Health states there will always be a backlog of two to three days of processing for the current period, being approximately 8,000 to 12,000 adjustments.

Since October 2010, the backlog of outstanding adjustments has stabilised and consistently been within Queensland Health's two to three day expectation. This is considered by Queensland Health to represent a 'business as usual' situation and is comparable to the previous payroll system in terms of outstanding adjustments.

Program and project management structures have been progressively implemented in accordance with good practice standards. However, there needs to be more rigour in delivering to scope and ensuring investments are directly related to benefits expected to be realised.

Simultaneous programs are being undertaken by different business areas within Queensland Health as part of the improvement program which has an overall budget of $208.6m.

The accuracy and stability of the payroll system is progressing. Issues continue to be identified and system changes continue to be made to improve accuracy and stability. At the time of the audit, Queensland Health was implementing systems and processes to improve issue recording, monitoring and reporting.

A follow up of prior audits reported in *Auditor General Report to Parliament No. 13 for 2010 – Results of audits at 31 October 2010* has been performed. Two of the 11 issues raised are fully resolved. Nine issues are being addressed by Queensland Health.

Salary overpayments and emergency cash payments have been made to employees since the system went live in March 2010 as a consequence of significant system and business process control issues related to the implementation of the new SAP HR payroll and rostering system. Details of outstanding overpayments and cash payments are provided in Figure 2A.

Figure 2A – Outstanding overpayments and cash payments

Type of payment	Date	Total value outstanding $M	Total number of instances
Salary overpayments	At 30 June 2010	$13.994	16,475
	At 29 May 2011	$43.333	47,069
Emergency cash payments	At 30 June 2010	$5.700	5,917
	At 29 May 2011	$9.246	10,180

Note: the above figures exclude instances of overpayments or cash payments up to $200.

Salary overpayments to employees have continued to occur during the current year, with audit being advised that the primary causes for these continuing overpayments being late employee roster changes after processing for the pay period had closed, processing errors and rounding amounts. As at 31 March 2011, Queensland Health had written off overpayments of $200 or less totalling approximately $1.3m.

Following an order of the Queensland Industrial Relations Commission in June 2010, Queensland Health gave an undertaking to affected employees that action to recover overpayments would not commence until the system was stabilised. With the stabilisation of the new system earlier this year, Queensland Health has now established the Employee Overpayments Recovery Program to manage the recovery of overpayments and interim cash payments and to reduce the occurrence of future overpayments. Affected employees will be notified by Queensland Health of their identified overpayments and the process of recovery by 30 June 2011. A call centre is being established to support staff wishing to clarify, negotiate or contest their overpayment.

The impact of salary overpayments incurred by Queensland Health on the auditor's opinion to be issued for the Department's 2010-11 financial statements will be further assessed at year end.

2.4 Status of the Department of Education and Training's OneSchool project

The OneSchool system is a web based system that provides functionality relating to student management and school resource management. When completed, it will provide school financial management functions.

In mid-2008, a high level audit was performed of the OneSchool project against better practice project management principles. The audit highlighted that the OneSchool's management framework could be enhanced through improving controls relating to scope, time, cost and quality. Seven issues including 18 audit recommendations were raised during the audit. The follow up audit in 2009 identified that 11 recommendations remained outstanding. During the 2010 follow up audit, it was determined that all of the recommendations have been implemented.

As part of the follow up audit, it was noted that the implementation of OneSchool Release 3 would mark the end of the program with the systems being transferred to the Department of Education and Training's Information Technology Branch for ongoing support. At the time of the audit, the project costs were approximately $66.8m and the annual maintenance cost of OneSchool is estimated at $7m.

Release 3 will deliver additional functions including asset and facilities management, improved student information and financial management through implementation of the Agresso Business World Finance system and its integration with previous OneSchool releases. The Department of Education and Training has entered into a fixed price contract to replace the current financial management systems with the Agresso financial application. The purchasing cost of Agresso is approximately $7.2m.

The implementation of Release 3 was scheduled to commence on 15 December 2010 with all schools to be changed over to the new finance system within a 29 day time frame. This was contingent upon a full readiness agreement signoff by school principals.

The Release 3 roll out strategy has changed to a phased approach with two schools selected for the pilot implementation. Based on the results of the pilot, the system will be progressively implemented in all schools over the 2011 calendar year.

The Department of Education and Training recently engaged Ernst & Young to perform a pre-deployment assessment of the potential risks and issues associated with the delay and planned phased deployment of OneSchool during 2011. Ernst & Young's report highlighted that further planning, organisational change management and operational readiness planning and support are required. The report identified that the majority of the organisational change activities are the responsibility of school principals. Indicative feedback from schools involved in the March and April implementation was that principals are fulfilling their duties as change agents.

Audit was informed that further detailed deployment planning is underway to address the risks and issues identified in the Ernst & Young report. A road map for the future upkeep, maintenance and upgrades of OneSchool and a best practice deployment checklist was being developed. The Department of Education and Training is planning an independent review against this checklist following the initial pilot.

Significant effort has been spent on developing the system rollout guides with pre-deployment, deployment and post deployment activities. A comprehensive support and change guide has been documented to assist schools to assess the difference between current processes and new processes. It was noted some good online help information relating to financial procedures. Indicative feedback from schools in the March and April implementations was that the training materials and web help were useful and satisfied their needs.

3 | Information security

Summary

Background

The Queensland Government holds and processes extensive amounts of information in the conduct of its business. This involves government's financial information and both public and personal records. The scale of information processing creates a need for adequate assurance of the protection of the Queensland Government's information repositories and systems at both the whole-of-government and agency level through appropriate security processes.

Key findings

- **Whole-of-government information security** – A whole-of-government approach that relies on individual agencies to adopt Queensland Government guidance with agency self assessment is not providing effective risk management for the protection of Queensland Government information. The extent of information security risk is not well understood at the whole-of-government level. There is no formal role at the whole-of-government level to coordinate information security and to oversee how the Queensland Government's information security objectives will be achieved.
- **IT network security** – Agency network security controls have been audited in the financial years 2009 to 2011. Most agencies audited have scope for improving the protection of information and their computer networks. It is evident that some agencies audited in 2011 have similar weaknesses in network security as those identified in *Auditor-General Report to Parliament No. 4 for 2009 – Results of audits at 31 May 2009*. This indicates that both whole-of-government and agency IT security processes need to be improved.
- **Online payment security management** – This audit identified that several of the controls commonly deployed in government information systems were in place. However, the security and fraud risks for the online payment service are not being actively managed, although there are some preliminary steps taken in this direction.
- **Computing server operating systems security management** – Security audits of servers that contain financial information has shown that improvements recommended in the past two audit periods have been implemented. Consequently, the reliability of the computer servers and their application software controls has improved generally within the scope of systems audited.

3.1 Whole-of-government information security governance

3.1.1 Audit overview

Effective information security requires the appropriate leadership, organisational structures and processes to safeguard information. Good information security requires senior management commitment, a security culture, promotion of good security practices and compliance with policy.

An Information Security Sub-committee has been established under the Toward Q2 through ICT Portfolio Management Office. It is an advisory committee that has representation from most Government departments. The Sub-committee has endorsed a revised Information Standard for security including several supporting guidelines.

3.1.2 Audit conclusion

Whole-of-government information security could be more effective. The oversight of information security at a whole-of-government level relies on individual agencies to adopt Queensland Government guidance with agency self assessment and reporting.

Agency self assessment reports on alignment to the Government Enterprise Architecture were developed for 2009 and 2010. Among other issues, this report raised concerns about compliance with the information standards for security and information custodianship. This report was provided to the Chief Information Officer Leadership Team rather than the Information Security Sub-committee. No action was taken by the Chief Information Officer Leadership Team to further assess or correct the concerns regarding information security. The Information Security Sub-committee as an advisory committee does not have appropriate authority to initiate information security activity due to its limited terms of reference.

The results of the audits of IT network security outlined in Section 3.2 of this report confirm the non-compliance identified through the agency self assessment process and the need for further action by the agencies.

3.1.3 Audit findings

The extent of information security risk is not well understood at the whole-of-government level. While the Chief Information Officer Leadership Team received reports raising information protection concerns, the residual risk is not defined, so information protection concerns are usually noted rather than being the catalyst for taking corrective actions.

The effectiveness of the Information Security Sub-committee in terms of its information security role is diminished due to its limited terms of reference. This sub-committee has primarily focused on an operational level response to one Auditor-General's report on network security rather than pursuing the broader responsibility for the appropriate protection of information across government.

Agency network security controls have been audited in the financial years 2009 to 2011. Most agencies under review had scope for improving the protection of information and their computer networks.

The Queensland Government Chief Information Officer relies on agencies to self assess and to report their alignment to Government Information Standards. Audit sighted alignment reports from 2008, 2009 and 2010 that progressively raised concerns about the incomplete adoption of mandatory *Information Standard 18 Information Security* principles.

The Information Security Sub-committee's initial action plan had a stated goal of a whole-of-government response to the control limitations reported in *Auditor-General Report to Parliament No. 4 for 2009 – Results of audits at 31 May 2009*. The Information Security Sub-committee reported the completion of 25 of 31 actions from this draft action plan in December 2010.

Many of these actions related to the publication of information security related guidance rather than improved security outcomes. For example, the network security audits undertaken indicate that agencies under review for the first time evidenced similar control weaknesses to those reported in 2009. These agencies had not adopted the guidance from the Information Security Sub-committee, Auditor-General Report to Parliament No. 4 for 2009 or previous Queensland Government Chief Information Office security standards and guidelines.

3.2 IT network security

3.2.1 Audit overview

For efficient and effective service delivery, the Queensland Government is reliant on internal IT systems. A current strategy is to deliver more Government services through online services. In this environment, it is critical that computer networks continue to operate reliably and that the information assets and government processes accessed through these networks are protected against theft, misuse, disruption and unauthorised access.

The results of an audit of network security at eight agencies was reported in the *Auditor-General Report to Parliament No. 4 for 2009 – Results of audits at 31 May 2009* tabled in Parliament on 30 June 2009. *Auditor-General Report to Parliament No. 7 for 2010 – Information systems governance and control, including the Queensland Health Implementation of Continuity Project* reported on the slow progress of the improvements recommended in 2009 and the network security controls at Queensland Health.

In 2011, the scope of the audit was expanded to include seven additional agencies. The network environments audited are shown in Figure 3A.

Figure 3A – Network environments audited

Agencies where network environments audited	
2009 and 2010 audits	**2011 audits**
Department of Justice and Attorney-General	Department of Communities (agency network)
Department of Communities (Recreation network)	Department of Education and Training
Department of Public Works – Shared Service Agency and CITEC (only the component of network supporting shared services Finance and HR systems)	Department of Public Works (agency network)
Department of Public Works – CITEC (only the component of network supporting shared services Finance and HR systems)	QIC Limited
Department of Transport and Main Roads	Queensland Treasury Corporation
Department of Community Safety	The Public Trustee of Queensland
Queensland Health	Treasury Department
Queensland Police Service and the Public Safety Network Management Centre	

3.2.2 Audit conclusion

Except for three agencies, network security should be improved across the Queensland Government to reduce risks such as the manipulation of systems and unauthorised access to information, including client details. While 60 per cent of the issues have been resolved from the 2009 audit, implementing audit recommendations does not appear to have been given a high priority.

A high assurance of the security of government networks cannot be obtained until the majority of security improvements are implemented and operational. At the time of the audit, no serious security incidents have been reported by the agencies in the follow up audit. However, half of the additional agencies audited identified that there had been some form of network security compromise in the previous two years. The majority of agencies must move to a more robust level of control to obtain an acceptable risk level.

It is apparent that the additional agencies audited this year had not implemented measures in their agencies to address the weaknesses reported to Parliament in 2009. If the issues had been addressed, it is likely some security compromises may not have occurred.

Given the threats to security due to the Internet and constant technological advancement, agencies need to give more attention to IT network security. All agencies are encouraged to confirm that the security controls for their networks are functioning as required.

3.2.3 Audit findings

The 2009 audit disclosed that while a significant number of security technologies and associated controls have been deployed, the resilience of network security controls need to be strengthened at all agencies audited. The 2009 audit found that the strength of the overall network security environment varied across the eight agencies and there is a clear indication that an ongoing focus on continuous improvement towards good practice security standards is required.

Progress on the resolution of the issues reported in Auditor-General Report to Parliament No. 4 for 2009 and Auditor-General Report to Parliament No. 7 for 2010 has been audited. The follow up audit disclosed that varying degrees of action has been taken to improve network security relating to all of the networks audited in the prior years.

At the time of the 2010 audit, 55 per cent of the issues were resolved. While management formally accepted the need to improve their security controls, the implementation does not appear to be given a high priority in some agencies. The implementation of many remaining audit recommendations missed the original implementation timeframes by an average of 12 months or more. The follow up audit in 2011 shows that with the exception of two of the original eight agencies audited, the security control maturity level is still consistent with that of medium size business rather than a more complex State Government department holding and processing sensitive information.

Half of the agencies have not completed the mitigation of risks associated with the operation of their gateway to the Internet. In addition, half of the agencies have not developed the capability to reliably detect surreptitious entry into their networks or online services. Detective controls are essential, as perfect preventive controls are cost prohibitive. Early detection allows damage minimisation steps to be initiated. Urgent action is needed to address these issues.

In September 2009, following the tabling of Auditor-General Report to Parliament No. 4 for 2009, the Queensland Government Chief Information Office proposed the implementation of a scheme for the central reporting of information and information and communication technology security incidents and the establishment of an incident response capability. *Information Standard 18 – Information Security* has been updated to make it mandatory for agencies to report incidents to this registry.

As this scheme began operation in January 2011, it will now be possible to determine the frequency and significance of security incidents across government. Such performance metrics should enable more effective management of network security.

A list of the issues found in the seven new networks audited is included in Figure 3B.

Figure 3B – Key issues

Issues	Number of network environments
Inadequate controls over firewalls and Internet gateway	6
Intrusion detection not implemented or insufficient security monitoring	5
Security levels required from third party suppliers not clearly defined	3
Security weaknesses due to network design	2
Inadequate vulnerability management and security configuration processes	5
Network security policy guidelines not documented	1
Inadequate network disaster recovery infrastructure or planning	1
Formal processes for security incident and problem management not in place	4
Inadequate communication of IT security precautions to staff	4
Irregular reviews of remote user access privileges	3
Insufficient logging to ensure staff are accountable for network usage	5
Networks with one or more systems not implementing government authentication policy	5
Ineffective use of encryption	6

Issues	Number of network environments
Network susceptible to the forgery of emails	5
Network design did not align to information sensitivity	4

The audits of network security in further agencies in 2011 identified that, while a significant number of security technologies and associated controls had been deployed, the resilience of network security controls need to be strengthened in a similar manner recommended to the agencies that were included in the 2009 audit.

In 2006 the Queensland Government Chief Information Office published the Network Management Position Paper as a component of a information and communication technology management tool known as the Government Enterprise Architecture. This position paper required agencies to have a Level 4 'Control Maturity' out of a scale from one to five for 'online services' (externally facing) networks by December 2008 and for all agency networks by December 2010.

Each of the 16 network security environments was assessed against the capability maturity model of the network management position paper in conjunction with international information and communication technology auditing standards. Three of the agencies audited had attained the Level 4 benchmark.

The results are shown in Figure 3C.

Figure 3C – Network security control maturity

Level	Description	Number of network environments
5	Optimised. Network security is diligently managed and fully supportive of the business objectives.	0
4	Managed. Network security is closely monitored and corrected as necessary.	3
3	Defined. Network security technical and operational controls are documented and implemented.	6
2	Reactive. Network security largely depends on skilled technicians.	7
1	Adhoc. Security is applied on a case by case basis.	0
0	Nonexistent. No effective controls.	0

Most of the agencies with network security with a Level 2 or Level 3 control rating could readily progress to the next level of control maturity particularly where information and communication technology governance issues are addressed. All agencies should improve network security control maturity to a level that is appropriate for their role within government service delivery and the protection of personal and State records. In many cases this will be the 'managed' level reflecting a reasonable balance between costs and risks.

3.3 Online payment security management

3.3.1 Audit overview

Queensland Government has added online services as a method of payment in addition to the traditional methods of over the counter and telephone payments. The Toward Q2 through ICT strategy sets a target of enabling Queenslanders by 2012 to conduct 50 per cent of all government service interactions online (excluding services that require face-to-face delivery).

In the 2010 financial year, 31 per cent of the revenue collected by Smart Service Queensland was processed online. It is anticipated that this will increase as more agencies provide online services.

There is an inherent risk to any online service due to diverse interests of other users of the Internet. The increased focus by organised crime and professional hackers on Internet based payment systems over the last ten years has significantly increased the threat and altered the likelihood of payment systems being compromised.

Implementing adequate controls to mitigate the risks associated with online payments is critical to ensuring that users can have confidence in using these services.

3.3.2 Audit conclusion

This audit identified that several of the controls commonly deployed in government information systems were in place. However, the security and fraud risks for the online payment service are not being actively managed, although there are some preliminary steps taken in this direction.

Although there has been no known breach of the current system, it is recognised that the control environment needs to be enhanced to mitigate the growing threats to a payment system connected to the Internet. Proactive oversight of the management of security and fraud risks for online payment systems is required.

A first step should be to plan for compliance with the industry standard, being the Payment Card Industry Data Security Standard. This is the worldwide information security standard defined by the Payment Card Industry Security Standards Council. The standard was created to help payment card industry organisations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise.

A second and equally important step is the development and implementation of a security plan for the online systems.

3.3.3 Audit scope

The objective of the audit was to assess the adequacy of preventative and detective security controls implemented for the payment systems managed by CITEC and Smart Service Queensland.

Examples of the type of Queensland Government services that use the online payment service provided by Smart Service Queensland include the Queensland Government Information Service and online Right to Information applications.

The audit did not include the payment systems used by the Department of Transport and Main Roads for driver licence renewal and vehicle and vessel registration renewal.

3.3.4 Audit findings

The findings identified from the audit of the online payments environment are similar to those identified from audits of other computer server operating environments previously audited.

The key findings include:

- There is insufficient evidence of risk identification and security planning for the online payment systems and the current threats from the Internet.
- The detection of possible security weaknesses in the software can be more robust.

- Services agreements with providers of technical and financial services that support the online payments do not clearly specify appropriate levels of security.
- Whilst there are various layers of security logging, the monitoring level is not rigorous enough to reliably detect all fraudulent misuse of the online payment systems.
- The database being used does not log who has accessed the records.

3.4 Computing server operating systems security management

3.4.1 Audit overview

A computing server's operating system includes a large range of features to protect access to computing resources. Operating system software uses computer accounts to separate users from each other and to limit their scope for any potential misuse of a system.

The audit examined how computing servers protect both information records and application software. An insecure operating system security configuration could allow a user to bypass software controls and to gain unauthorised access to sensitive information or conduct unauthorised transactions.

The configuration and operation of these controls on several key Queensland Government computing servers was examined.

3.4.2 Audit conclusion

There is scope for improvement for the accountability of use of server operating system security accounts and for agencies to move to higher levels of security for Internet application servers. Agency management should continue to review and monitor the administration of server operating systems and server security controls.

The security of servers supporting financial processing applications and servers delivering web applications should be proactively managed. Each agency should be cognisant of the potential impacts on other parts of government when assessing and mitigating these risks.

A follow up audit of computer servers at CITEC showed that the security configuration of the operating system software has now moved towards a high security level for a subset of internal financial processing systems.

3.4.3 Audit scope

The objective of the audits was to assess the adequacy of preventative and detective security controls implemented by the operating system software. The operating system security of the following computing server environments were examined during the audit:

- The Shared Services Solution and the Integrated Consolidation Environment supporting SAP based financial, payroll and human resource records and the FAMMIS environment supporting Queensland Health's SAP based financial records. These servers are operated by CITEC under the direction of CorpTech.
- The QBuild Ellipse environment supporting financial, payroll and human resource records. These servers are operated by CITEC and an external third party provider.

- The server supporting the Queensland Police Service's payroll processing and human resource records operated by the Queensland Police Service.
- Online payment system servers operated by CITEC for services delivered by both CITEC and Smart Services Queensland.
- Internet servers supporting web applications and Internet infrastructure in several agencies were examined during the audit of the information technology network security discussed in Section 3.2.

3.4.4 Audit findings

The key findings include:

- The configuration of operating system security controls for a subset of internal financial processing systems was previously set to a moderate level rather than high security level. The security configuration of the operating system software has now moved towards a high security level.
- The management of operating system accounts and their associated technical authentication policies could be improved for two financial information processing environments. The accountability for access or use of a number of these accounts was diminished.
- A number of computer servers were not configured to a high level of security as recommended by their respective vendors when deployed for Internet applications.
- Scope remained to increase the resilience of the security of a small number of key government servers.
- One environment relied on an external third party and the services agreement did not sufficiently define the Queensland Government's security requirements for the system.
- All server operating systems relied on the protection of the network as a part of their security arrangements. Audit has reviewed the security of several of these networks with the results presented in Section 3.2 of this report.

.

4 | IT disaster recovery planning

Summary

Background

IT disaster recovery planning is a major component of overall business continuity planning. It refers to the strategies and processes implemented to address the risks of loss of IT systems, services and data in the event of a significant disruption or disaster.

Tested IT disaster recovery plans and adequately resourced risk mitigation strategies are essential in ensuring critical computer services can be recovered within the required timeframe in the event of a disaster.

Key findings

- **Shared services IT disaster recovery planning** – Disaster recovery arrangements are not clearly defined in operating level agreements between agencies and the Shared Service Agency and in some of the agencies' service level agreements with third parties. At a whole-of-government level, a documented analysis has not been undertaken of which critical systems are to be prioritised by CITEC and individual agencies for recovery in the event of a disaster.
- **Agency IT disaster recovery planning** – At the agency level, disaster recovery planning requires further management attention. While most agencies audited have disaster recovery plans in place, either at an agency level or at a system level, many of these agencies did not keep the plans up to date and tested. Some agencies have not carried out appropriate risk assessment and business impact analysis to identify the critical systems, data, and staff required for the recovery process.

4.1 Shared services IT disaster recovery planning

4.1.1 Audit overview

There is an increased focus to deliver efficiency savings through the consolidation of IT systems. This has included the centralisation of IT infrastructure to CITEC.

The weaknesses in disaster recovery processes for systems supported through Shared Services were reported in *Auditor-General Report to Parliament No. 8 for 2010 – Results of audits at 31 May 2010*. The report identified that there is insufficient documentation of key processes relating to how services will be recovered, the timeframes for recovery and whether these timeframes are acceptable to client agencies.

This audit examined the IT disaster recovery planning within the Shared Services environment.

4.1.2 Audit conclusion

The audit found disaster recovery planning is not focused on a documented understanding of the whole-of-government priorities in relation to IT systems. There is reliance on making decisions about priorities during or immediately after a disaster. This type of decision making can be risky as key staff or sound information may not be available.

The disaster recovery arrangements are not clearly detailed in operating level agreements between agencies and the Shared Service Agency. CITEC has some documentation on procedures to be followed in the event of a disaster but there is significant reliance on the knowledge of staff to prioritise key processes when a disaster occurs. CorpTech has performed business impact analysis but it is not extensive enough to develop an end-to-end IT disaster recovery plan for the shared services environment.

There is no documented whole-of-government business continuity management strategy to manage the continuity risks relating to the shared services IT systems.

4.1.3 Audit scope

This audit examined operating level agreements with the Shared Service Agency and other service level agreements with third party suppliers to determine whether agencies had taken mitigating actions to manage risks associated with the outsourcing of IT services.

The operating level agreements for the agencies included in Figure 4A were audited.

Figure 4A – Agencies audited

Agencies audited	
Department of Communities	Department of the Premier and Cabinet
Department of Community Safety	Department of Public Works
Department of Education and Training	Department of Transport and Main Roads
Department of Employment, Economic Development and Innovation	Queensland Health
Department of Environment and Resource Management	Queensland Police Service
Department of Justice and Attorney-General	Treasury Department
Department of Local Government and Planning	

4.1.4 Audit findings

There is no whole-of-government IT business continuity management strategy

There is no business continuity management strategy for IT systems managed through whole-of-government activities. As a result, the continuity risks relating to whole-of-government IT systems or environments are not clearly understood.

At a whole-of-government level, a documented analysis of which critical systems need to be prioritised by CITEC and individual agencies for recovery in the event of a disaster has not been performed. Audit was advised that the priority listing would be developed by the Crisis Management Team and the Business Recovery Team when a disruptive event occurred and key government stakeholders will be consulted in this process.

In 2005, CorpTech performed a business impact analysis, identifying CorpTech's time critical business processes that support the delivery of finance and human resource applications. It assesses the maximum acceptable outage for each of the critical activities as identified by CorpTech managers and operational personnel. However, the business impact analysis does not consider the maximum outage accepted by clients using CorpTech's applications. The business impact analysis does not define the recovery time objective (that is, the earliest point in time at which systems must resume after a disaster) and recovery point objective (that is, the acceptable data loss in the event of disruption of operations) of these systems.

Service level agreements do not address IT disaster recovery planning

Queensland Government service delivery depends on multiple agencies to provide an 'end-to-end' service. End-to-end disaster recovery planning for Shared Service Agency clients includes a minimum of five service level agreements as well as other service level agreements with external service providers.

The disaster recovery arrangements are not clearly detailed in operating level agreements between all agencies audited and the Shared Service Agency. The standard operating level agreements state that both parties would maintain the business continuity process for the agreed services. However, the operating level agreements do not identify which business processes provided by the Shared Service Agency are considered critical by each agency and the priority in which the systems will be recovered.

The recovery time and the recovery point objectives for services provided by the Shared Service Agency have not been established in these agreements. If a disaster occurs, timely recovery of services may not eventuate for critical SAP Finance and Aurion human resource system platforms.

There are service level agreements in place with other third party service providers. For example, CITEC and the Public Safety Network Management Centre provide critical IT related services and facilities management services to a number of agencies.

These agencies have not been assured of the timeframes for the recovery of the critical services provided by the Public Safety Network Management Centre or CITEC in the event of a disaster. These agencies' operations may be exposed to unacceptable delays if the roles and responsibilities for disaster recovery are not clearly defined with third party service providers. CITEC advised that, in general, agencies have not informed CITEC of their recovery requirements.

An end-to-end review is recommended for disaster recovery management so that roles and responsibilities for managing the risks are clearly defined. As part of this review, specific assurance should be obtained in relation to any disaster recovery roles or responsibilities assigned to each agency.

The absence of signed service level agreements increases the risk that services stated in the agreement may not be enforced. The audit found at least two agencies had service level agreements with CITEC that had not been signed by representatives of either party.

4.2 Agency IT disaster recovery planning

4.2.1 Audit overview

Business continuity and IT recovery planning usually gain importance following a major disaster. For example, the natural disasters across Queensland in early 2011 had an impact on the continuity of government business. In Brisbane, the main impact of the floods on government IT systems was caused by loss of power to some buildings, however this is only one of the numerous threats to IT systems. It should not be assumed that any recent disaster recovery success would guarantee protection of critical infrastructure and staff against other scenarios, such as fire, cyclone or deliberate attack.

The audit examined IT disaster recovery readiness to ascertain whether there were systems, frameworks and adequate testing in place to enable the recovery of critical systems within the appropriate timeframes. It should be noted that the audit was planned and the majority of the audit fieldwork was completed prior to the natural disasters that occurred in early 2011.

4.2.2 Audit conclusion

Disaster recovery planning across the public sector agencies audited is at various stages of maturity. The recent natural disasters have provided some opportunities for testing disaster recovery plans and have highlighted weaknesses that can be used by agencies to improve IT disaster readiness.

While most agencies audited had disaster recovery plans in place, either at an agency level or at a system level, many of these agencies did not keep these plans up to date and tested to ensure the plans are effective. The audit found that the larger and more complex the agency, the more difficult the task to effectively plan for disaster recovery.

Even with disaster recovery plans in place, some agencies have not carried out appropriate risk assessment and business impact analysis to identify the critical systems, data, management and people required for the recovery process.

The audit found that disaster recovery arrangements have been poorly defined in operating level agreements between agencies and the Shared Service Agency and in agencies' service level agreements with third parties.

The following better practice guides may assist agencies in developing disaster recovery plans, recovery frameworks, procedures and processes:

- *ISO/IEC 24762:2008 – Guidelines for Information and Communications Technology Disaster Recovery Services.*
- *Business Continuity Management – Building Resilience in Public Sector Entities – Better Practice Guide*, June 2009, Australian National Audit Office.

4.2.3 Audit scope

The scope of the audit was to evaluate the preparedness of Queensland public sector agencies to respond to disruption in IT services. Figure 4B shows the agencies audited:

Figure 4B – Agencies audited

Agencies audited	
Brisbane City Council	Department of Local Government and Planning
Department of Communities	Department of the Premier and Cabinet
Department of Community Safety	Department of Public Works
Department of Education and Training	Department of Transport and Main Roads
Department of Employment, Economic Development and Innovation	Queensland Health
Department of Environment and Resource Management	Queensland Police Service
Department of Justice and Attorney-General	Treasury Department

The audit process assessed whether appropriate IT disaster recovery practices were implemented which were consistent with practices outlined in international standards, and Queensland Government Information standards.

The main references used in the development of audit criteria include:

- *Queensland Government Information Standard 18 – Information Security.*
- *ISO/IEC 27002:2006 – Information technology – Security techniques – Code of practice for information security management.*

4.2.4 Audit findings

Comprehensive disaster recovery plans are not in place

The importance of ensuring the continued operation or the rapid recovery of systems increases as IT systems and the information they contain have become critical to organisations. As a result, preparation for continuation or recovery of systems needs to be taken seriously. This involves a significant investment of time and money to ensure minimal losses in the event of a disruption.

Three agencies do not have an IT disaster recovery plan in place or are still developing plans for critical business systems. Another three agencies did not have a whole of agency IT disaster recovery plan and only had plans at the business unit level.

Risk assessments and business impact analysis was not conducted

The audit examined the extent to which agencies have analysed the business impact of an outage in IT services. Whether agencies have prioritised the key services and the accepted timeframes in which those services must be recovered to support business processes was audited.

Performing risk assessments and analysing business impact determines critical business functions and the priority for the recovery of these functions. It enables identification of information systems, data, and people needed for the recovery process. It forms the basis for the development of the business continuity and the IT disaster recovery plan.

Five of the 14 agencies audited have not or have only partially completed risk assessment and business impact analysis activities. Without appropriate risk assessment and business impact analysis, critical IT resources may not be prioritised and appropriate disaster recovery capability may not be implemented for those resources and functions. An agency wide risk assessment and business impact analysis process should be performed and documented, including a comprehensive list of disaster recovery related risks. Mitigating measures should be documented to address all business and IT risks identified in the risk assessment.

Recovery times and defined restoration priorities not accurately estimated could lead to unplanned escalation of recovery times for key IT services.

Disaster recovery plans were not reviewed and tested

Disaster recovery plans should be reviewed and tested at least annually to ensure agencies are able to respond to disasters within accepted timeframes for key business functions.

While some agencies have long standing disaster recovery plans in place, plans for eight agencies have not been reviewed or updated for extended periods. The IT disaster recovery capability of these agencies may be seriously affected if plans are not updated and tested on a regular basis or when major changes to infrastructure occur.

Information in the IT disaster recovery plan may be outdated if it is not regularly updated. Without the plan being formally tested, there cannot be reasonable assurance that critical systems will be recovered within acceptable timeframes in the event of a disaster.

5 | Appendices

5.1 Extract from *Toward Q2 through ICT* 2009-2014 (September 2009)

Toward Q2 through ICT outlines the Queensland Government's information and communication technology priorities and targets to help create more accessible, efficient and effective services for the benefit of all Queenslanders.

Toward Q2 through ICT is a five year plan that supports the Queensland Government's 2020 vision for the State, *Toward Q2: Tomorrow's Queensland*. The strategy identifies priorities for action within four key focus areas, and sets targets to be met in delivering the strategy.

The whole-of-government strategy focuses on four areas.

Focus area 1 - Accessible government

Outcome – Delivering easy to access customer centric services and information for all Queenslanders through ICT innovation, and using ICT to develop new ways for Queenslanders to engage with government.

Priority	Target
Improving government service delivery	By 2014, Queenslanders will be able to access government information and services through single entry points across multiple channels. By 2012, Queenslanders will be able to conduct 50 per cent of all government service interactions online (excluding services that require face to face delivery). By 2010, the government will develop a whole-of-government broadband development plan by working with the ICT industry to ensure government service delivery is able to maximise the benefits of the National Broadband Network rollout.
Engaging online with Queenslanders	By 2010, Queenslanders will be able to contribute to contemporary policy debates through the use of new and emerging technologies. By 2011, the government will ensure all major community consultation activities are available online.
Improving information management and access	By 2011, the government will develop an action plan to maximise the use of existing online and ICT infrastructure to support the release of information under the right to information reforms, and where necessary provide investment guidance. By 2011, the government will enhance its capabilities in record keeping across the sector through training, further policy development and compliance monitoring. By 2010, the government will develop and commence implementation of an information management framework to maximise the use and value of information, and improve business outcomes and services to Queenslanders.

Focus area 2 – Efficient government

Outcome – Adopting a 'one government' ICT approach across government agencies to improve service delivery and information access, and reduce the cost of government operations.

Priority	Target
Adopting a 'one government' approach to ICT investment and development	By 2010, the government will implement a leadership framework for ICT within the Queensland Government, through the development of an agency Chief Information Officer charter. By 2011, the government will require all agencies to work collaboratively to deliver an ICT management framework and to prioritise and implement 'one government' ICT outcomes to deliver efficiencies. The ICT management framework will include: ● A process for prioritising and assigning lead agency responsibilities for strategic 'one government' ICT-related agendas such as core infrastructure and multi-agency applications, policy development, and research and development. ● A 'share before buy before build' focus, and the ongoing use of the Queensland Government Enterprise Architecture as a key planning, policy-setting and assessment mechanism. ● Whole-of-government infrastructure and service provisioning.
Delivering savings	By 2013, the government will reduce the per-unit cost of business-as-usual ICT expenditure by 15 per cent.
Building our ICT capability	By 2010, the government will develop and commence implementing an ICT capability framework to improve the capacity, capability and sourcing of the government's ICT professional resource base. The ICT capability framework will include: ● Workforce planning tools (to identify and address gaps between future labour supply and demand). ● Development of a Queensland Government ICT skills framework to help ensure the ICT workforce has the capability and leadership skills to meet future demand.

Focus area 3 – Effective government

Outcome –Supporting front-line service delivery through the provision of leadership in whole-of-government ICT directions, successful ICT governance and early engagement with industry.

Priority	Target
Delivering successful projects	By 2011, the government will implement a whole-of-government best practice delivery framework for the procurement and delivery of successful outcomes through ICT-enabled solutions. The delivery framework will include: ● Whole-of-government implementation of standardised Project, Program and Benefits Management Methodologies. ● Integrated and standardised best practice procurement method to enable timely delivery. ● Industry linkages that optimise project resourcing, areas of expertise, and the application of government methodologies. ● Education, training and engagement of project managers and key business stakeholders. ● Effective post-implementation review mechanisms to share lessons learned, and promote successful outcomes.
Providing whole-of-government leadership in ICT delivery	By 2010, the government will review whole-of-government governance processes and implement enhancements to create a cohesive Chief Information Officers' Leadership Team responsible for oversight and delivery of the ICT management framework. By 2010, the government will develop and implement a priority setting, assessment and monitoring process for mandated elements of the Queensland Government Enterprise Architecture.
Engaging early with industry	By 2010, on all ICT projects worth $2 million of more, or of a high complexity, the government will collaborate with industry subject matter experts in concept, feasibility, design and project approach stages. By 2011, the government will present an annual portfolio forward plan and analysis to industry to allow active engagement and consideration of appropriate participation.

Focus area 4 – A strong industry/government partnership

Outcome – Developing a mature industry/government relationship where ICT is deployed to help solve contemporary changes facing Queensland and to deliver efficiencies to the Queensland taxpayer.

Priority	Target
Improving government service delivery	By 2010, the Queensland Government will work with industry to develop a shared code of practice and an industry engagement framework which includes: ● A review of procurement processes and practices to streamline them ● Mechanisms to improve the engagement of, and collaboration with industry in research and development, and strategic opportunities ● A centralised register of industry expertise and government partnerships/experience.
Creating opportunities to solve contemporary problems	By 2010, the Queensland Government will develop, jointly with industry, strategies to engage industry in discussions concerning significant community issues, for example, the National Broadband Network, e-health and e-learning. By 2010, the Queensland Government will deliver its Green ICT Strategy to reduce the environmental footprint of ICT equipment within the government, and help 'green' government operations through the innovative use of ICT. By 2012, the Queensland Government will be utilising ICT to support alternative work locations for 10 per cent of the core public service workforce – contributing to improved government performance and reduced travel and congestion.
Creating enhanced business opportunities for local industry	By 2010, the government will implement a simplified procurement process for low risk projects under $2 million. By 2009, the government will implement its 'share before buy before build' direction. By 2010, the government will undertake a targeted review of business-as-usual ICT and examine delivery options (including local industry options) as part of this review.

5.2 Stakeholders' responses

Department of Public Works

The Director-General provided the following response:

The Department of Public Works (DPW) is responsible for providing a range of government wide information and communications technology services.

Over the past two financial years, the Department has taken the lead in improving whole-of-Government ICT policy, governance and service delivery through the auspices of the ICT Division of the Department. With the cooperation of agencies, there have been many notable achievements over this period including the –

- *Release of the Government's ICT Strategy 'Towards Q2 through ICT.'*
- *Establishment of a CIO Executive Leadership Team and relevant governance sub-committee structure to oversee the implementation of the strategy.*
- *Commissioning of the government's second primary tier III data centre at Springfield.*
- *Development and release of a Queensland Government Portfolio, Program and Project Management methodology for governance of ICT programs.*
- *Establishment of a Portfolio Management Office within the ICT Policy and Co-ordination Office.*

- *Progression of major ICT Programs such as the ICT Consolidation Program (ICTC), Identity Directory and Email Services (IDES) Program and the Corporate Services Program (CSP), all of which are building significant future ICT capability for whole-of-Government.*
- *Development of an ICT Capability Framework to identify the in demand roles and develop programs for future ICT skill requirements for Government agencies to aid retention and attraction of staff.*

Significant action has been taken by DPW to prioritise and address the matters raised in previous audits especially in the area of program governance and security.

Current developments such as the Foundation Infrastructure Project to be delivered as part of the ICT Consolidation Program will further enhance the capability and security of Government's ICT environment.

5.2.1 Whole-of-government IT management (Section 1.1)

Department of Public Works

The Director-General provided the following response:

To support the delivery of the Government's five-year strategy for government ICT outlined in the Toward Q2 through ICT Strategy, DPW has established and manages the ongoing operation of the whole-of-Government ICT Portfolio governance arrangements. The ICT Portfolio approach requires cross-agency involvement, collaboration and commitment at all levels, embedding the 'one government' vision.

The Department agrees with the Queensland Audit Office's (QAO) assessment regarding the value of the Portfolio Management Office and has allocated funding to continue the Office through to 30 June 2012.

The Department and all agencies are making a major commitment to the success of the Towards Q2 through ICT strategy through the CIO Leadership Team and the eight sub-committees. The sub-committees include ICT Governance, Information Management, Information Security, ICT Infrastructure, Strategic Sourcing, ICT Capability, Service Delivery and Telecommunications. Each of the subcommittees is chaired by a Chief Information Officer (CIO) from one of the core departments with membership including other CIO's and senior officers. Similarly, the CIO Leadership Team comprises all CIO's and the members of the executive management team from DPW's ICT Division. This is an unprecedented investment in the future of Government ICT and is acknowledged as a leading governance model within Australian governments.

Under this model a strategic objective may involve a number of actions which are allocated to sub-committees on the basis of the sub-committee's skill sets, knowledge and specialist areas. For example, cost efficiency might be achieved through process improvement, procurement optimisation, technology shifts, changes in security practices, and a better deployment of skilled resources. Each of these requires specialist knowledge to execute which supports the existence of the specialist sub-committees. The CIO Leadership Team has provided strategic oversight while leveraging the specialist capabilities of the sub-committees

Through this model, the Towards Q2 through ICT implementation plan has achieved the completion of 30 actions for 2010 out of a scheduled 33 actions. These actions contribute to the strategies of Accessible Government, Efficient Government, Effective Government and Strong Industry/Government Partnership.

Cabinet reviews the progress of the Towards Q2 through ICT strategy on a 6 monthly basis. This includes an annual refresh of the strategy which considers the value and feasibility of implementation of each of the initiatives. In addition, for each calendar year, Cabinet considers the outcomes achieved as a result of having implemented the initiatives.

The next annual review of the ICT Portfolio initiatives and Towards Q2 through ICT implementation plan will be conducted by DPW by September 2011.

A review of the ICT Portfolio Governance Structure commenced in April 2011 and will be completed as part of this review.

A program of improvements to the risk and benefits management processes for the portfolio will continue to be further developed and implemented by the ICT Portfolio and Coordination Office.

5.2.2 IT program management (Section 2.1)

Department of Public Works

The Director-General provided the following response:

The Department believes that Program Management for the audited programs is in accordance with the Queensland Government Methodology and that recent improvements in Program Management have not been adequately acknowledged. In addition it is the Department's view that DPW responsibility and accountability for program delivery exists alongside agency responsibility for implementation.

The Department would also argue that it is not reasonable or feasible for the lead program management agency to be accountable for benefits realisation as benefits will accrue over time and often well after the program is completed, and that these benefits and return on investment will be realised across all areas of government.

The Queensland Government Portfolio, Program and Project Methodology provides for governance arrangements that can adequately deal with benefits recognition across multiple agencies. Benefits Management, which has until recently been treated separately from the application of the Queensland Government Portfolio, Program and Project methods is now being integrated, and a revised communication with agencies is underway.

A project focusing on improving Senior Executives' knowledge, awareness and understanding of their role and responsibility in the governance of IT programs and projects is now nearing completion. To date, 208 senior executives and senior level officers from nine of thirteen agencies have taken part in the education sessions.

The work being undertaken in Benefits Management is part of a broader program refocussing on portfolio management which specifically addresses strategic ICT investment decision making at the business (services) layer.

The level of take up of the program is evidence of strong commitment to improvement in the sector.

ICT Consolidation Program (ICTC)

The Department believes that the governance of the ICTC program works well for the implementation of the ICTC key deliverables and is in accordance with the Queensland Government Methodology. The ICTC Program Board has independent agency membership managing the program deliverables and progress. The program is tracking within budget.

The Audit appears to understate the commitment of agencies to the program. The ICTC program has been liaising with all agencies regarding their migration to a whole-of-Government consolidated infrastructure environment. All 13 departments have signed technology consolidation strategy roadmaps.

Agency consolidation strategies relate to migration to the whole-of-Government environment at a point of technology upgrade or refresh. It is unrealistic to expect that all agencies can immediately migrate from their existing legacy environments to a whole-of-Government consolidated environment. Indeed technical limitations relating to hardware and decisions relating to the timing of these upgrades or refresh activities will always be impacted by budget and other priority changes affecting the agency.

CITEC is continuing to work with agencies on progressing their migration activities.

Delivery of a consolidated network, security and storage service requires the design and delivery of critical foundation infrastructure. An extensive tender process was undertaken to establish appropriate technology to facilitate the whole-of-Government infrastructure environment. Until final designs and associated costs of the infrastructure tenders were completed, it was not possible to finalise the revised service catalogue and price book.

A draft of the revised service catalogue and price book based upon this foundation infrastructure was published on 31 March 2011, and was distributed to departments for review and comment. Following the review, the final service catalogue and price book was endorsed by the Program Governance Board on 8 June 2011 and has since been published.

The program has generated considerable ICT consolidation across government, including the signing of all agencies roadmaps and strategies, closure of 4 metropolitan data centres and 12 agency data sites, delivery of proven application rationalisation methodology and foundation infrastructure procured and implementation progressing ahead of schedule.

In addition, an independent review of the ICTC program's proposed benefits has identified potential savings of $29.6 million over five years and a reduction of 24.5 thousand tonnes of CO2 over the same time period.

IDES

With the support of DPW the IDES Program will implement a fully functional identity management and authentication platform as a whole-of-Government ICT utility service, managed and operated by CITEC in June 2011.

The Department recognises that the IDES program is a large and complex program of work providing one of the largest identity management platforms and email consolidations implemented by a government in Australia. The Department has improved program governance with the establishment of a program structure in accordance with the Queensland Government Portfolio, Program and Project Methodology.

While it is recognised that this Project was delayed early in its implementation timeframe, the department is taking care to ensure that IDES is not rushed into production.

Email forms an integral component of workflow practices of all government agencies and any disruption to the email service has a significant impact on agency service delivery and productivity. As a consequence, the IDES Program has undertaken extensive system integration and user acceptance testing prior to 'go-live' to ensure that the solution operates as intended and meets the business requirements of Government. In addition, the first two agencies to adopt the IDES solution, CITEC and DPW, will act as 'pilot agencies' to ensure that any system modifications and enhancements can be identified and addressed prior to roll out across other government agencies.

The program is now on track to complete the delivery of the Identity Management capability by June 2011 with CITEC and DPW to be transitioned to the new IDES solution in June and July 2011. The Project remains within the original Project Budget.

Commitment from agencies to migrate to the IDES system has grown from a firm commitment of 25,000 seats at the start of this calendar year to a total of 53,000 by 2013. Further consultation is occurring with agencies to reach the original forecast total of 81,000 seats.

Corporate Solutions Program

The Department is concerned that the coverage of the Corporate Solutions Program by Audit does not sufficiently recognise the progress that has been made since Auditor-General Report to Parliament No 7 for 2010. Instead it reiterates historical issues surrounding the program that date back to 2007.

As recommended by the PricewaterhouseCoopers Shared Services Review, the Department has developed a Strategic Implementation Roadmap for Corporate Solutions within the rest-of-Government over a two-year planning horizon. It is due to be submitted for Cabinet Budget Review Committee's consideration in July 2011.

While the Audit Report suggests that consolidation was a key driver for the program, the Department is clear that the Corporate Solutions Program, supporting the Shared Service Initiative, has been and continues to be guided by three strategic drivers.

- ***Business System Continuity/System Risk Mitigation:*** *Maintain human resource, payroll and financial systems in vendor-supported environments. This ensures ongoing stability and reliability of human resource, payroll and financial systems.*
- ***Consolidation:*** *Consolidate the number of systems with the longer-term goal to operate a single SAP environment. Reducing the total number of system environments and different products will provide improved efficiency and effectiveness. This enables DPW to cost-effectively manage system support risks while reducing operating costs for shared service providers and agencies.*
- ***Business Process Reform:*** *Reform and standardise end-to-end business processes to maximise efficiencies in standard corporate processes.*

The proposed two-year Strategic Implementation Roadmap is focused on 'must do' actions that are essential ensuring service continuity in the rest-of-Government human resource, payroll and financial systems. The key objective is to move agencies that are on obsolete and unsupported versions of human resource, payroll and financial systems to vendor-supported versions. Particular consideration has been given to the number, age and complexity of agency systems as well as the underlying technology infrastructure upon which these systems operate.

System consolidations and further migrations will continue to occur around the existing machinery-of-Government programs of work.

The department understands the importance of critical business process standardisation and reform. The creation of the new entity Queensland Shared Services will provide further opportunities to negotiate business process standardisation initiatives with client departments, some of which will not be necessarily systems dependent.

5.2.3 IT project management (Section 2.2)

Department of Environment and Resource Management

The Director-General provided the following response:

- *The LTLr project was initially established in November 2005 with the system to be developed in-house for completion by 2009.*
- *The land tenure function is subject to evolving legislation and several legislative changes directly impacting the development of the system were required to be taken into account throughout the life of the project.*
- *The LTLr system was successfully deployed into production on 14 March 2011 and management is addressing any outstanding recommendations.*

Department of Transport and Main Roads

The Director-General provided the following response:

Since commencing the rollout of the New Queensland Drivers Licence (NQDL) and associated products in Toowoomba late last year, to date, some 14 Customer Service Centres have successfully issued around 38,000 new cards. The department is on track to have the remainder of its Customer Service Centres fitted and issuing licences by the end of 2011 where the bulk of transactions occur. Regional and remote police stations and QGAP offices that issue the new licences will be operating by June 2012. The department is also investigating a mobile licence issuing solution.

You correctly note that TMR has changed the way projects utilising information technology are implemented. In the department, our focus is on improving business processes, realising business case benefits and strong governance and project management. We have strengthened our governance and sought greater confidence through the use of external reviewers.

The Queensland Audit Office (QAO) report states that "The business case was approved based on opportunities for benefits outside the provision of a secure driver's licence rather than specific and measurable benefits." This was the case in the early days of the project, but government policy and direction changed over-time to respond to the external environment.

As demonstration of this point:

- *The value proposition and key benefit identified in the Business Case for the NQDL project, approved by Cabinet in May 2006, was to significantly reduce the risk of licence and identity fraud. The new NQDL cards have been designed for their primary purpose of delivering legislated licences and industry authorities which will effectively achieve that benefit. These benefits are being delivered.*

- *Various potential future commercial opportunities identified as part of the original approved Business Case in 2006 were predicated on an assumption that the NQDL would be delivered via a Public Private Partnership (PPP). Under a PPP the commercial opportunities would be driven and realised by the private sector partners. As you appreciate, the delivery of a project by PPP will have a different capital and operating cost profile, as it was expected that the PPP proponent would be able to offset costs by revenues from other third party sources. In September 2007, the Cabinet Budget Review Committee decided the proposed PPP to deliver the NQDL project was not a viable proposition and the project would need to be delivered by TMR through traditional procurement arrangements. The project is being delivered this way and required an alternate capital and operating cost profile to the PPP. The project remains on budget.*

Since then, the NQDL project has focussed on realising the primary benefit of the project, which is replacement of easily forged driver licences and industry authority cards with a secure product that significantly reduces the risk of licence and identity fraud, thereby ensuring the integrity of the government's licensing system and saving costs to the private sector and the community from identity fraud.

5.2.4 Status of Queensland Health's payroll project (Section 2.3)

Queensland Health

The Director-General provided the following response:

The findings and recommendations highlighted in your report in relation to the improvement of Queensland Health's payroll and rostering system are noted. Queensland Health has made significant progress in stabilising and improving the current system and has completed the implementation of the localised payroll operating model. Queensland Health is committed to monitoring the success and progress of the localised payroll model and it will continue to make incremental improvements to the model including the ratio of payroll staff to the number of transactions. This will also be done in the context of the National Health and Hospital's reform and how this impacts local payroll service delivery and staffing levels.

Queensland Health also notes QAO's recognition of the good progress being made to implement program and project management structures in line with good practice. Further to this, Queensland Health will establish a portfolio management approach to provide overarching monitoring and governance of all payroll related activities and budget, to ensure alignment between program/project outcomes and investment.

Queensland Health is in the process of establishing the processes and systems to monitor, recover and prevent overpayments from occurring. We feel that it is important to understand that the Department has not commenced the recovery of overpayments based on an Order from the Queensland Industrial Commission and agreement with employees to not commence this process until the system was considered stable. Significant work is also underway to prevent overpayments from occurring with a particular emphasis on the ability to make prior period pay adjustments, which is the biggest cause of overpayments occurring.

The department is also establishing regular meetings with QAO to keep it informed about progress and to seek input into the future planning for payroll services and for the implementation of the payroll portfolio management approach. QAO's willingness to provide time and advice in the establishment of the portfolio approach is greatly appreciated.

In relation to the IT related matters it is acknowledged that this audit activity was undertaken at a point in time, however Queensland Health continues to improve its information system management and controls and improvements have progressed since that time.

5.2.5 Status of the Department of Education and Training's OneSchool project (Section 2.4)

Department of Education and Training

The Director-General provided the following response:

I appreciate that you have noted in the report the concerted effort the Department has made to address the recommendations from your previous years' report and that there has been a significant improvement since the first audit in 2009.

5.2.6 Whole-of-government information security (Section 3.1)

Department of Public Works

The Director-General provided the following response:

The Department acknowledges the need to continue to enhance the security governance in order to address ongoing security challenges.

The Department has developed a 31 point action plan that addressed the information security issues raised in a prior Auditor-Generals report. Governance of the 31 actions was allocated to the Queensland Government Information Security Sub-Committee (ISSC). 29 actions have been completed and all 31 actions are expected to be completed as of the 30 June 2011.

In November 2010, the Queensland Government Chief Information Officer (QGCIO) approved version 5.0 of Information Standard 18 – Information Security (IS18). Version 5 addresses the recommendations of the Auditor-General's No. 4 Report of 2009 and includes detailed implementation advice and reporting requirements. The revised IS18 in itself completed eight of the actions within the action plan and also contributed to the completion of six others. IS18 aligns with international best practice, is nationally recognised as a quality framework for the management of information security.

Under this standard, agencies must report incident data to QGCTO (on a monthly basis) which will enable aggregation of security incidents for analysis response and reporting to the Information Security Sub-Committee.

The ICT Policy and Coordination Office, Queensland Government Chief Technology Office and the Public Sector ICT Development Office within the Department of Public Works along with the Department of Justice and Attorney General continue to develop the security program of work to meet changing security challenges.

A review of the governance approach, including the role of the sub-committee, will be undertaken by DPW from July 2011. In addition a review of agency implementation issues and recommendations for whole-of-government approach will be undertaken by DPW 2011-12.

5.2.7 Online payment security management (Section 3.3)

Department of Public Works

The Director-General provided the following response:

The Department recognises that the control environment needs to continue to be enhanced to keep pace with the growing threats to payment systems connected to the internet and the department is undertaking steps to ensure an efficient and secure system. It should be recognised that with the controls that are in place, there has been no known breach of the current system.

The controls that are in place include the checking of all current payment system source code by a security code testing tool or outsourced provider. All payment applications are checked quarterly using the most recent test suite from the vendor.

The Audit recommends that the Department undertakes planning to achieve compliance against the Payment Card Industry Data Security Standard. This work is well underway. The Department is undertaking steps to address security and fraud risks and as a result Smart Service Queensland has reviewed the architecture supporting online payments and is currently working with Queensland Treasury and the Commonwealth Bank of Australia to utilise an external service that meets the Payment Card Industry Data Security Standard.

Following decisions on future directions, CITEC & Smart Service Queensland will review all audit findings to ensure that continuing systems have a detailed security assessment in accordance with the audit recommendations for the payment systems based on the current and projected threat environment.

CITEC will review the risks relating to the current level of logging of access to the servers processing financial payments, make recommendations and implement recommendations where appropriate.

5.2.8 Computing server operating systems security management (Section 3.4)

Department of Public Works

The Director-General provided the following response:

The Department is pleased to note that the Audit recognises that the security configuration of the operating system software has now moved towards a high security level for a number of internal financial processing systems operated by CITEC. This is a positive result reflecting the priority that has been given to addressing known audit issues. As a result, CITEC has resolved technical issues related to accounts and authentication. CorpTech are in the process of finalising remaining technical issues.

CITEC has addressed all of the network security issues raised in the 2009-10 audit. There are no outstanding audit findings in this area for CITEC.

In addition, the Foundation Infrastructure Project to be delivered by CITEC as part of the ICT Consolidation Program will add additional capability for security incident and event management on the whole-of-government network.

DPW will continue to review and monitor the administration of server operating systems and server security controls.

5.2.9 Shared services IT disaster recovery planning (Section 4.1)

Department of Public Works

The Director-General provided the following response:

The Department feels that while the Audit identifies issues related to the processes to be followed in the event of a disaster, there has been inadequate acknowledgement of the major improvements in the disaster recovery capability for ICT systems that the department has initiated and managed over recent years.

The Department through CITEC as the primary technology infrastructure service provider to the Queensland Government delivers whole-of-government and agency specific ICT services including ICT services for the Shared Services Systems.

Technology services that the Department provides through CITEC are a critical element in the operations of key government agencies.

In early 2007, DPW developed a ten-year whole-of-Government Data Centre Strategy. The strategy has been reinforced by Toward Q2 through ICT and includes the use of the Polaris Data Centre and the CITEC Data Centre at 317 Edward Street to enhance availability, integrity, security and confidentiality of Queensland Government ICT systems and assets. Polaris became operational in 2009.

This two data centre capability allows for resilient and fully redundant support for mission-critical systems in the event of unplanned outages.

Where it is required by agencies, CITEC has the capability to support 24 hour a day 7 days a week computer system operations, disaster recovery and business continuity, reducing risks, and costs and environmental impacts on services. This was particularly highlighted by the flood disaster in the Brisbane Central Business District in January 2011 when departmental data centre facilities were at risk from flood inundation and loss of power. During this event, CITEC services remained unaffected and CITEC were able to reallocate additional capacity as urgent needs arose.

In addition, the Foundation Infrastructure Project currently being implemented as part of the ICTC Program will provide a consolidated robust infrastructure on which to run the government's critical information systems.

CITEC has a documented Business Continuity Plan. CITEC has also ensured that it has implemented disaster recovery technology in accordance with the services it is contracted to supply to agencies. However, as commonly found in complex technology areas, there is significant reliance on the knowledge of staff to prioritise key processes in the event of service disruptions. This has been the case during major service disruptions in the past and has allowed the specific nature of a disaster event to be considered in the recovery strategy by the key CITEC staff involved in the recovery effort.

By December 2011, the Department will have developed a Business Continuity Management Framework which will include the requirement for SLAs to clearly articulate metrics and testing requirements for disaster recovery. This will clarify the general layered structure of the shared service environment, agency interdependencies and associated roles and responsibilities.

5.3 What is an information systems audit?

Information systems are critical in all areas of government business, not just for the traditional uses of payment of employees and suppliers but as a repository of private and public information. Computerised systems are pervasive through government and virtually all citizens are reliant on the accuracy and reliability of information generated by and stored within computerised information systems.

Using computers to record information, changes the way in which that information is processed and stored. This affects the procedures used by a public sector entity to achieve adequate internal control. An information systems audit examines controls within an organisation's IT environment and evaluates evidence of its information systems, practices, and operations. The evaluation of evidence obtained determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organisation's objectives.

An information systems audit is different from a financial and assurance audit. While a financial audit's purpose is to evaluate whether an organisation is adhering to standard accounting practices, the purpose of an information systems audit is to evaluate the system's internal control design and effectiveness. This includes, but is not limited to, information systems security, development processes and IT governance. An information systems audit focuses on determining risks that are relevant to information, and in assessing controls to mitigate these risks. By implementing controls, the effect of risks can be minimised.

5.4 Acronyms

CEO	Chief Executive Officer
CIO	Chief Information Officer
ICT	Information and Communication Technology
NQDL	New Queensland Drivers Licence
QAO	Queensland Audit Office

5.5 Glossary

Accountability

Responsibility on public sector agencies to achieve their objectives, about the reliability of financial reporting, effectiveness and efficiency of operations, compliance with applicable laws, and reporting to interested parties.

Auditor's opinion

Positive written expression within a specified framework indicating the auditor's overall conclusion on the financial report based on audit evidence obtained.

Disaster recovery plan

Also referred to as a business continuity plan. It describes how an organisation is to deal with potential disasters. A disaster recovery plan consists of the precautions taken so that the effects of a disaster will be minimised and the organisation will be able to either maintain or quickly resume mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention.

Effectiveness

The achievement of objectives or other intended effects of activities at a program or entity level.

Efficiency

The use of resources such that output is optimised for any given set of resource inputs, or input is minimised for any given quantity and quality of output.

Governance

The role of persons charged with the oversight, control and direction of an entity.

Independent auditor's report

Issued as a result of an audit and contains a clear expression of the auditor's opinion on the entity's financial report.

Information technology governance

Information technology governance is the framework that ensures that processes and standards are in place to direct and control the investment in information technology.

Program management

Program management is the coordinated organisation, direction and implementation of a group of projects and activities that together achieve the outcomes and realise benefits that are of strategic importance.

Qualified opinion

Type of modified auditor's opinion expressed when, except for the effect of a disagreement with those charged with governance, a conflict between applicable financial reporting frameworks or a limitation on scope that is considered material to an element of the financial report, the rest of the financial report can be relied upon.

5.6 References

Auditor-General Act 2009

Business Continuity Management – Building Resilience in Public Sector Entities – Better Practice Guide, June 2009, Australian National Audit Office

ISO/IEC 27002:2006 – Information technology – Security techniques – Code of practice for information security management

ISO/IEC 24762:2008 – Guidelines for Information and Communications Technology Disaster Recovery Services

ISO/IEC 38500:2008 – Corporate governance of information technology

Payment Card Industry Data Security Standard v2, October 2010, Payment Card Industry Security Standards Council

Queensland Government ICT Market Overview 2008-09, Longhaus

Queensland Government Information Standard 2 – ICT Resources Strategic Planning

Queensland Government Information Standard 18 – Information Security

Toward Q2 through ICT 2009-2014, September 2009.

6 | Auditor-General Reports to Parliament

6.1 Tabled in 2011

Report No.	Subject	Date tabled in Legislative Assembly
1	*Auditor-General Report to Parliament No. 1 for 2011* *Management of offenders subject to supervision in the community* Performance Management Systems audit	25 February 2011
2	*Auditor-General Report to Parliament No. 2 for 2011* *Results of local government audits* Financial and Assurance audit	22 March 2011
3	*Auditor-General Report to Parliament No. 3 for 2011* *Follow-up of administration of grants and funding to community organisations by local governments in Queensland* Performance Management Systems audit	9 June 2011
4	*Auditor-General Report to Parliament No. 4 for 2011* *Information systems governance and security* Financial and Assurance audit	21 June 2011

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