Queensland Audit Office

Traffic management systems

Report to Parliament 5 : 2013–14

Queensland Audit Office

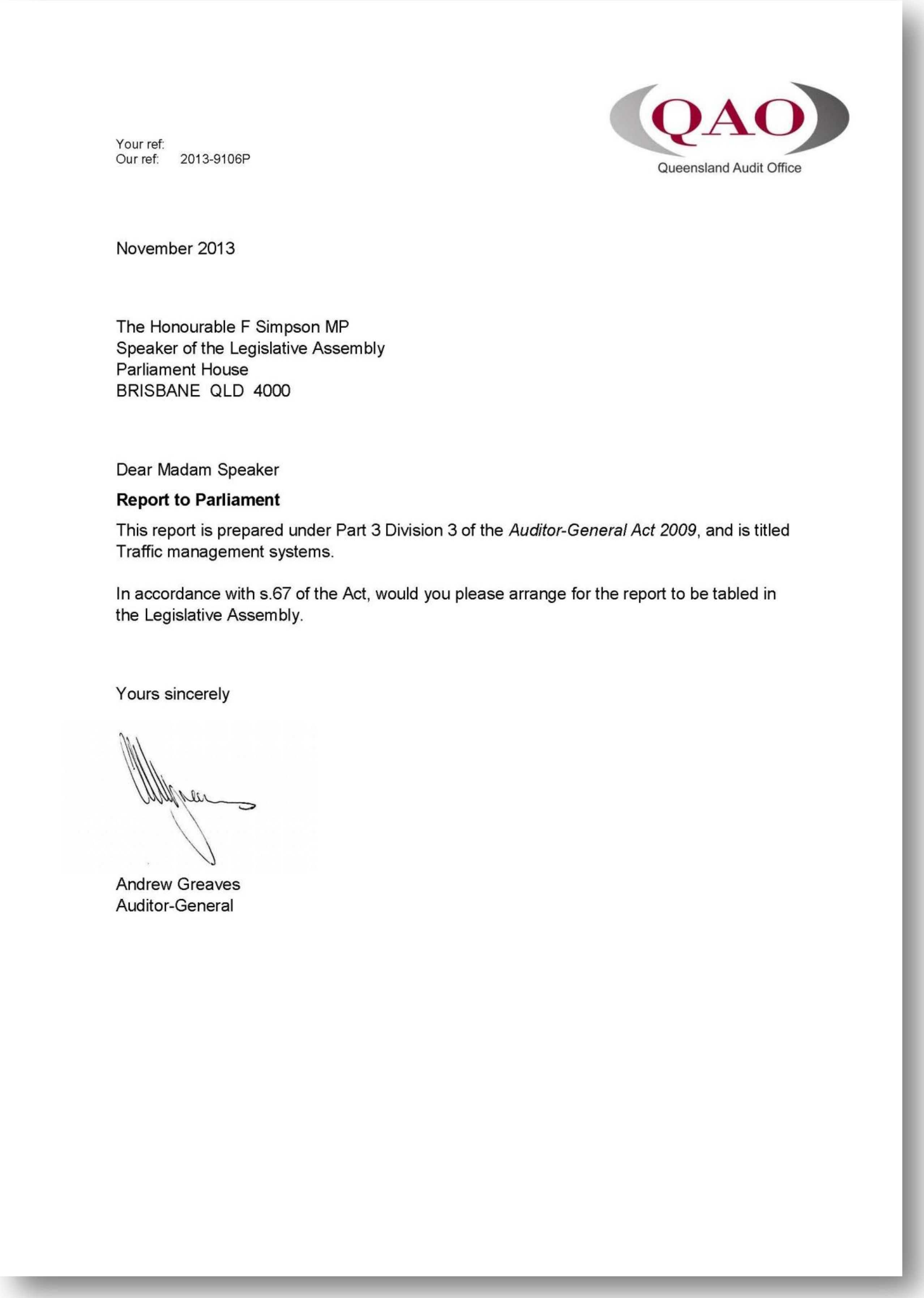
Location	Level 14, 53 Albert Street, Brisbane Qld 4000
PO Box	15396, City East Qld 4002
Telephone	(07) 3149 6000
Email	qao@qao.qld.gov.au
Online	www.qao.qld.gov.au

QUEENSLAND

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

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

ISSN 1834-1128



QAO
Queensland Audit Office

Your ref:
Our ref: 2013-9106P

November 2013

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

Dear Madam Speaker

Report to Parliament

This report is prepared under Part 3 Division 3 of the *Auditor-General Act 2009*, and is titled Traffic management systems.

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

Yours sincerely

Andrew Greaves
Auditor-General

Contents

Summary

With Queensland hosting the G20 Leaders Summit in November 2014, there is a heightened risk of cyber intrusions and opportunistic attacks to government information technology systems. Infrastructure critical to the safe and efficient operation of the road network is managed using information technology known as intelligent transport systems (ITS). The Department of Transport and Main Roads (TMR) and Brisbane City Council (BCC) use separate ITS to manage traffic for roads under their control. This setup requires the operation of multiple systems and duplicate staff, policies, processes, governance mechanisms, and communications technologies even though TMR and BCC have formed an alliance—the Brisbane Metropolitan Traffic Management Centre—for coordinated incident response using a common incident response and traveller information systems.

While robust engineering controls are built into such critical infrastructure systems, their overall coordination and operations rely on the use of common information technologies and connection to the internet, corporate networks and portable devices. This reliance increases the threat of security breaches and malicious damage.

If these systems become unavailable due to intentional or accidental damage or natural disaster, road safety and road network capacity could be negatively impacted. Unauthorised access with malicious intent has the greatest potential to cause serious traffic disruption on a wide scale which, at best, would diminish trust in public institutions and could cause appreciable economic loss. In either scenario, it would be important that the systems are able to be restored quickly and efficiently.

In this audit, we examined whether the ITS operated by TMR and BCC are secure and how well they can be recovered in the event of a security incident. As part of the audit, we carried out our own security penetration tests to seek to identify and exploit any security vulnerabilities that could allow others to gain unauthorised access to the systems. We also assessed whether using two ITS is cost effective.

Conclusions

The systems to manage traffic critical infrastructure in the Brisbane metropolitan area were demonstrably not as secure as they should have been, and they were susceptible to targeted attacks. Our ability to successfully penetrate some components of the system meant the risk of unauthorised access was unacceptably high at that time. This result should serve as a timely reminder to all entities that operate critical infrastructure, such as rail, water and electricity networks, to check and re-check their security arrangements.

Both TMR and BCC are capable of responding to security incidents if and when detected, provided key staff members are available. The level of response planning, however, is not yet sufficient for high profile events. Plans to drive the response across all relevant entities are not complete and have not been tested thoroughly; any response will be partly reactive and less efficient than a planned and rehearsed one.

TMR and BCC recognise and acknowledge the criticality of these issues and have accepted all the recommendations relating to security and response capability. Since the audit was conducted, they have undertaken a risk assessment and have projects underway to improve their security arrangements.

Our analysis of whether it is cost effective to run two ITS showed that switching to a single system would not reduce the total cost of ownership to TMR or BCC; it also would not increase their costs. As it would be a cost neutral change, it becomes more relevant to consider the wider economic and social benefits that could be achieved through a single intelligent transport system and, in particular, whether it would afford the opportunity to manage and reduce the effect of traffic congestion.

Such wider considerations require the two levels of government to step aside from their individual, entity-based points of view to adopt a more holistic view of these issues. Given the current forecast of growth in traffic and road tunnels, the economic advantages to the state of reduced congestion significantly outweigh narrower, entity-based considerations of cost.

Key findings

Security of traffic systems

Traffic systems had not been adequately secured to withstand targeted physical and software-based attacks. We breached physical security without being detected and gathered information about key staff and technologies used to manage ITS, to plan our penetration tests.

We were able to penetrate some parts of the ITS where sufficient security measures to counteract information technology security attacks had not been deployed. Neither entity had performed a comprehensive security risk assessment of the ITS environment and did not fully appreciate the risks to ITS, nor the controls required to prevent exploitation of security weaknesses.

The general lack of security awareness by staff was a significant factor in why we were able to breach security controls. Staff members did not respond appropriately when exposed to techniques which were aimed at gaining unauthorised access to the systems.

Continuity of traffic systems

TMR and BCC have the ability to respond effectively to security incidents and major disasters. This response, however, relies heavily on the availability of key staff. The capability of both entities is supported by backup technology and alternate operating sites, but a lack of complete plans to resume business and information technology functions mean that key staff members, familiar with traffic operations and systems, are necessary to recover systems promptly.

Where continuity plans existed, they were not tested thoroughly. Tests conducted involved either a 'desktop' review or recovery of the information technology components only. End to end exercises that invoked the business continuity plan, disaster recovery site and backup systems were not performed. As a result, there is no assurance that the existing capability can recover ITS within acceptable time frames during high profile events.

Cost effectiveness of multiple traffic systems

Migration to a single intelligent transport system has the potential to generate greater economic benefits through improved traffic management capabilities, while creating a better travel experience for road users. With the Bureau of Infrastructure, Transport and Regional Economics predicting congestion costs expected to reach $3 billion per annum in 2020, even small reductions in congestion and improvements to the efficient use of existing road infrastructure would deliver significant savings to the south-east Queensland economy.

While the current model is both cost neutral and capable of delivering effective congestion and incident management, the choice to strategically manage two ITS has resulted in missed opportunities for economies of scale and innovation in traffic management. The fundamental challenges to improved effectiveness and reduced costs result from the existence of two separate organisations, with different strategies, staff, systems, and hardware, managing one road network. To mitigate these challenges would require a closer alignment of TMR and BCC, of which a single intelligent transport system would only be one aspect.

Recommendations

It is recommended that the Department of Transport and Main Roads and Brisbane City Council:

1. **perform risk assessments and develop security plans for the intelligent transport systems environment**
2. **implement comprehensive staff security awareness programs**
3. **operate intelligent transport systems security using good practice standards such as Queensland Government Information Standard 18: Information security**
4. **review the access control permissions to the intelligent transport systems network and applications environment**
5. **establish and test formal processes to maintain business continuity for the end to end intelligent transport system environment**
6. **jointly develop a long term strategy for intelligent transport systems, including a full feasibility study of intelligent transport systems options**
7. **implement common approaches to shared challenges through establishing coordinated governance, joint service level agreement and key performance indicators for intelligent transport systems management across the Department of Transport and Main Roads and Brisbane City Council**
8. **introduce systems to record, report and monitor the cost of the information technology components of intelligent transport systems.**

Reference to agency comments

In accordance with section 64 of the *Auditor-General Act 2009*, a copy of this report was provided to TMR and BCC with a request for comments.

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

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

1 Context

1.1 Background

Intelligent transport systems (ITS) are advanced engineering applications that provide services relating to different modes of transport and traffic management. They enable various users to be better informed and to make safer, more coordinated, and 'smarter' use of transport networks. These systems extend beyond traffic management to incident management, traveller information and a range of emerging, vehicle-based safety applications.

ITS are broadly known as Supervisory Control and Data Acquisition (SCADA) systems, which are designed for operations and safety. Safety features and complexities of engineering systems have contributed to the perception that ITS are also secure. However, these systems are now connected to the internet and use commercially available technologies that have introduced new security risks and threats.

In June 2010, an anti-virus security company reported the first detection of malicious software (malware) that attacks SCADA systems running on Microsoft Windows. The malware is called Stuxnet and was initially found on 14 systems internationally. In August 2013, a security research company in the United States created a mock water utility system; it received 74 security attacks from more than 16 countries. Ten of the attacks were deemed to have the ability to take complete control of the mock system.

The emerging security threats and the significance of the G20 Summit to be held in Queensland in November 2014 highlight the need to strengthen ITS security. In addition, with the focus on improving the efficiency and effectiveness of government, there is a need to determine the cost effectiveness of systems where all costs of a given system or project are evaluated and compared over its economic life.

1.2 Roles and responsibilities

In Brisbane, there are two separate organisations that operate and manage ITS using two different sets of systems.

The Department of Transport and Main Roads (TMR) and Brisbane City Council (BCC) are responsible for managing traffic on roads under their control. While TMR and BCC have separate units for road operations and congestion reduction respectively, they have created an alliance agreement to form the Brisbane Metropolitan Traffic Management Centre (BMTMC) for monitoring traffic flows and responding to traffic incidents.

TMR uses an intelligent transport system developed and maintained by a controlled entity of TMR. BCC uses a third party provided traffic signals system as well as other internally developed systems to manage road signs and to collect information for road operations. For improved coordination, TMR and BCC have signed a memorandum of understanding for specified groups of traffic signals to be on one system, regardless of who owns those signals.

1.2.1 Department of Transport and Main Roads

TMR manages traffic systems for roads owned by the state and all local governments, except those owned by BCC. The main objective of TMR's road operations unit is to plan an integrated, reliable and cost effective transport system for the state. Its responsibilities include:

- planning and making investments in cost effective transport infrastructure and services
- addressing traffic congestion throughout the state
- developing and implementing ITS policies and plans.

In 1992, a division of TMR began developing a new intelligent transport system called STREAMS. The division was incorporated in 2002 to form a controlled entity of TMR.

TMR owns the physical infrastructure supporting traffic management systems, but has a service contract with the controlled entity to develop and maintain STREAMS.

1.2.2 Brisbane City Council

BCC manages road operations for roads under its control through the congestion reduction unit (CRU). The role of the CRU is to improve the day to day performance of the BCC road network. The CRU responsibilities include:

- managing unplanned incidents through the BMTMC
- coordinating planned incidents and special events
- identifying and mitigating congestion hot spots in the road network
- managing all aspects of traffic signal operations
- managing and operating ITS
- monitoring and evaluating road network performance.

Brisbane Metropolitan Traffic Management Centre

The BMTMC was established in late 2006 as an alliance between BCC and TMR. BCC hosts the BMTMC and both BCC and TMR provide the systems it uses. The BMTMC provides real time traffic and incident management, road network monitoring and traveller information services for the greater Brisbane area on behalf of the alliance partner. The BMTMC, located in BCC, operates its own technology environment to access both BCC and TMR systems.

1.3 Intelligent transport systems

There are two primary software solutions in Australia for traffic systems, both used in managing Brisbane metropolitan traffic:

- SCATS—used by BCC for managing traffic signals in conjunction with seven peripheral systems
- STREAMS—an integrated system used by TMR for traffic signal, motorway and incident management.

The peripheral traffic management systems used by BCC provide the following functions:

- display variable message signs
- display variable speed limit signs
- business intelligence
- record and monitor closed circuit television
- gather Bluetooth data to measure travel times of motorists

In addition to STREAMS, TMR has separate systems for recording and monitoring closed circuit television, and storing Bluetooth data. TMR is also responsible for managing the traveller information website. Both TMR and BCC use common traveller information and incident management systems.

Unlike other local governments in Queensland, TMR and BCC have historically operated two sets of systems to manage traffic in the Brisbane metropolitan region. In 1968, TMR implemented the first computer-controlled, coordinated traffic signals system in Australia. The system has evolved to become STREAMS. Meanwhile, BCC developed its own system to coordinate traffic signals.

1.4 Single intelligent transport systems project

In 2003, BCC decided to find a suitable replacement for its traffic management system to address risks relating to internally developed systems. As a result, the single intelligent transport system project was established.

In 2006, the then Minister for Transport and Main Roads allocated $6 million for TMR and BCC to undertake a pilot project to converge their ITS into a single environment. The new system was to be based on an enhanced version of STREAMS, at no cost to BCC.

In May 2007, TMR and BCC signed a memorandum of understanding to have a single intelligent transport system with the aim of managing the Brisbane metropolitan road network as a single network, independent of asset ownership. The total cost of the pilot project to TMR was $8.5 million. The pilot project took longer than originally planned. There were delays in BCC finalising the technical aspects of its requirements and TMR underestimated the time required to enhance STREAMS to meet BCC's requirements.

In 2010, BCC decided to implement SCATS as its traffic signal management system. While an expert industry report subsequently concluded that the STREAMS enhancement met the stated requirements of BCC, the project did not achieve its objective of progressing STREAMS to be used as a single intelligent transport system platform for Queensland. One benefit of the project was the improved cooperation between TMR and BCC. In particular, they established a memorandum of understanding to allocate intersections and traffic signals at the boundaries of TMR and BCC traffic signal networks to either TMR or BCC. As a result, STREAMS operates 28 intersections owned by BCC and SCATS operates 12 intersections owned by TMR. In addition, TMR and BCC agreed to use TMR's incident management systems and the traveller information phone and web services across Brisbane through the BMTMC. Both entities also agreed to share travel time data and to establish traffic response unit service embedded as part of the BMTMC operation.

While collaboration amongst road operators has improved, the total cost of owning two systems had not been determined until the analysis was carried out for this report.

1.5 Total cost of ownership

The total cost of ownership is used to quantify the financial effect of deploying and using a system over its life cycle or a predefined period. The costs usually include direct and indirect costs of computer hardware and software, other operating expenses and long term expenses such as system replacement, future upgrades and decommissioning. Figure 1B describes the categories for total cost of ownership analysis.

Figure 1B
ITS total cost of ownership

Category	Description
Software	Costs associated with all software for an organisation including ongoing licensing costs and acquisition costs
Field infrastructure	Costs associated with ITS field infrastructure including closed circuit televisions, variable speed limit signs, intersections and others
Hardware	Costs associated with ITS infrastructure including desktops, servers, networks and peripherals
Management	Labour associated with managing ITS assets and setting the direction of ITS operations, including network management, application management and systems research, planning and others
Development	Labour associated with the update of applications using a software development lifecycle approach including development staff, testing staff, documentation staff and others
Utilities	Costs associated with electricity, internet access and others
Support labour	Labour associated with the provision of service for day to day ITS operations, including helpdesk effort (Tier 1), maintenance labour, ITS training and others

Source: Queensland Audit Office

1.6 Security standards and good practice

1.6.1 Information security standards

Queensland legislation does not define standards for compliance with security of control systems. However, a number of international standards exist that outline good practices for securing any systems of business value. These include:

- AS/NZS ISO 31000:2009, *Risk management—Principles and guidelines*
- ISO/IEC 27001:2013, *Information technology—Security techniques—Information security management systems—Requirements*
- ISO/IEC 27002:2013, *Information technology—Security techniques—Code of practice for information security management*
- ISO/IEC 27005:2008, *Information technology—Security techniques—Information security risk management.*

The IT Security Expert Advisory Group of the Australian Government's Trusted Information Sharing Network for Critical Infrastructure Resilience has developed the following good practice guides for use by operators of national critical infrastructure. These include:

- generic SCADA risk management framework
- SCADA architecture principles
- knowing your SCADA network
- hardening of SCADA ICT systems
- implementing gateways
- monitoring of SCADA networks.

1.6.2 Business continuity standards

The joint Australian/New Zealand Standard AS/NZS 5050:2010 *Business continuity—Managing disruption-related risk* provides a framework for assessing, treating and monitoring the risks associated with business disruption.

1.7 Audit objective, method and cost

The objective of the audit was to examine whether the systems used to operate and manage traffic control infrastructure were secure and cost effective. The audit examined whether:

- controls to prevent, detect and respond to security breaches were effective
- business continuity management was effective and there was established emergency response capability
- systems used to deliver traffic management services for council-controlled roads and state-controlled roads were cost effective.

In addition to the standard audit testing methods, we used the following specialised methods for robust analysis of the results:

- security penetration tests to simulate attacks on ITS from external and internal threats which included:
  - analysing the system and vulnerabilities
  - exploiting identified vulnerabilities to breach system controls
  - social engineering to manipulate staff to provide unauthorised access or information that would assist in carrying out future security attacks
- financial modelling to assess the total cost of ITS ownership for TMR and BCC
- facilitating workshops with TMR, BCC and TMR's controlled entity to:
  - examine the use that ITS provide to the road user
  - examine whether those uses will be best achieved using two separate ITS
  - explore potential benefits and risks in using a single intelligent transport system
  - examine a plausible alternative architecture for a single intelligent transport system including preliminary analysis on the operating and conversion costs based on information provided by TMR, BCC and TMR's controlled entity.

The cost of the audit was $420 000.

1.8 Structure of the report

The findings in this report are structured as follows:

- Chapter 2 examines the security of traffic systems
- Chapter 3 examines the continuity of traffic systems
- Chapter 4 examines the cost effectiveness of ITS
- Appendix A contains responses received
- Appendix B details the audit approach.

2 Security of traffic systems

In brief

Background

Traffic management systems do not just manage traffic signals; they include features that enable complex planning and improved technology integration. Consequently, a robust control environment needs to be in place to protect the information assets that are required to deliver traffic outcomes.

We examined the control designs of Brisbane's traffic management systems and performed penetration testing to assess their security.

Conclusions

The intelligent transport systems (ITS) environments were not secure and we were successful in our penetration testing at both the Department of Transport and Main Roads (TMR) and Brisbane City Council (BCC).

The entities audited did not actively monitor and manage information technology security risks and did not have comprehensive staff security awareness programs. Had they done so, breaching the security controls would have been less likely.

Both TMR and BCC have accepted all findings relating to ITS security and are currently addressing the control weaknesses. TMR and BCC are developing a desired security posture and plan for ITS which includes detail on how they will implement the controls.

Key findings

- The level of management oversight to actively manage ITS security risks was insufficient. As a result, neither entity took a comprehensive planned approach to design and monitor the overall ITS control environment.
- Comprehensive staff awareness programs for information security were not implemented.
- Information technology security policies, procedures and best practices were not applied completely or effectively to the ITS environment.
- Technology to secure the ITS environment was deployed but not configured to achieve the full benefits of managing risks within separate system components.

Recommendations

It is recommended that the Department of Transport and Main Roads and Brisbane City Council:

1. **perform risk assessments and develop security plans for the intelligent transport systems environment**
2. **implement comprehensive staff security awareness programs**
3. **operate intelligent transport systems security using good practice standards such as Queensland Government Information Standard 18: Information security**
4. **review the access control permissions to the intelligent transport systems network and applications environment.**

2.1 Background

The increase in computer and internet connectivity provides benefits in terms of more efficient business operations, but it increases the risk of system security being breached. There have been incidents where the security of engineering systems was breached because of their connectivity to the internet or other networks. Security breaches have also occurred when the systems were not connected to other computer networks; these breaches were through physically connecting external devices to the systems.

The 2003 SoBig virus, spread via email, affected the train signalling systems at CSX Corp in the eastern United States. The incident resulted in delays for both transport and commuter trains. In 2005, Chrysler reportedly shut down thirteen manufacturing plants due to the Zotob internet worm. Even though Chrysler's manufacturing control network was separated from its corporate systems and the internet, the worm spread into the control network via an infected laptop. The 2010 Stuxnet malicious software (malware) infected fourteen nuclear plant systems. The malware targeted engineering systems and was initially spread via USB devices. These incidents highlight the importance of using a comprehensive approach to secure the ITS environment.

A security plan clearly sets out the overall approach, from planning to implementation of secure systems environments. A security plan comprises technical and non-technical policies, procedures and controls to protect from both internal and external threats. This chapter examines whether the controls to prevent, detect and respond to security breaches of the ITS for the Brisbane metropolitan region were effective.

2.2 Conclusions

The traffic management systems for the Brisbane metropolitan area were not secure. If the systems were specifically targeted, hackers could access the system and potentially cause traffic congestion, public inconvenience and affect emergency response times. Such attacks could also cause appreciable economic consequences in terms of lost productivity.

Poor security controls and awareness, including understanding of the consequences of poor control, led to a sub-optimal security environment. This was exacerbated by a lack of risk assessments to formulate relevant security plans for ITS environments.

In this audit, we have demonstrated that the technology interconnectivity and integration of various traffic operators have introduced security risks and threats: to ITS and to the overall business of traffic operations. Since the audit, all of the audited entities have developed plans to address the key risk areas.

2.3 Findings

In designing information security controls, attention has to be given to the three fundamental components of business operations—'people', 'process' and 'technology'. This is a well-known business concept and can be applied effectively in managing information technology security.

While all three components are equally important and operate in conjunction with each other, a well-controlled component can mitigate control weakness in other areas; for example, security conscious personnel can mitigate weakness in technology controls.

Our penetration testing took place over a three-week period and was conducted with all entities being fully informed of the tests. Carefully planned attacks over a longer period could have been successful in compromising the systems while such technical security vulnerabilities exist. For this reason, in addition to staff training and awareness, processes to identify and address new and emerging security risks and threats are required to ensure a robust control environment. Systems security is like a chain—one weak link can disrupt the integrity of the whole chain.

Therefore, controls should be implemented in all aspects of the business operations, having regard to the components of people, process and technology. In this section, we discuss the key issues in the area of security risk assessment and planning and security of the information technology environment. We also highlight some better practice principles as a starting point to help other entities assess their own security risks and the corresponding controls needed to mitigate the risks.

2.3.1 Security risk assessment and planning

Security risk assessment

The entities audited did not actively monitor and manage information technology security risks. They mainly focused on meeting operational outcomes and optimising their use of existing infrastructure assets. There was a perception that the safety controls within the Supervisory Control and Data Acquisition (SCADA) systems also made those systems secure; therefore, management oversight on system security did not receive the required level of attention.

Security roles, responsibilities, performance indicators and standards for external operation partners were not formally defined. Security plans or organisational security postures that could be used to manage and monitor information technology risks were not established.

Security plan

While all entities audited deployed several security controls, a holistic view of all the controls with respect to specific risks was not defined and documented. In the absence of this key planning document, it is difficult to identify and prioritise gaps in the chain of controls, including implementing suitable controls within the people, process and technology aspects of the SCADA systems.

2.3.2 People

Senior management support and leadership are required to help influence and set examples for desirable behaviours that promote a security culture within the organisation. To operate a robust control environment, technical staff members operating the information technology environment need to be skilled in security governance, risk management and security operations. In addition, staff awareness programs are required so that each staff member can discharge his or her duties in taking precautions to prevent, detect and respond to security incidents and threats.

Staff security awareness

There was a general lack of staff awareness of current and emerging security risks, including awareness of social engineering techniques. These techniques are often used to manipulate staff to give away access to systems or confidential information. Social engineers perpetrate their scams by using psychological manipulation and they rely on the natural human desire to be helpful.

Our testing confirmed that social engineering techniques were the easiest and most effective means to gain access to systems. We were able to bypass physical security multiple times without being detected.

Social engineering techniques of which entities should be aware are provided in the case study at Figure 2A.

Figure 2A
Social engineering case study

Bypassing security using social engineering techniques

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. It is a type of confidence trick for the purpose of information gathering, fraud or system access.

The following are examples of social engineering exploits that are used to gain unauthorised system access:

- Piggyback rides: Someone appears as a legitimate employee and walks into a secure building by following a person who has access. This technique is one of the most common ways to enter into an organisation. When social engineering perpetrators breach physical security controls, they can deploy devices that enable them to gain unauthorised access to the systems or collect more information about the organisation and key staff members. This information can later be used in planning an attack.
- Use of portable device (USB device): USB devices that have been infected with a virus or malicious software can be delivered to the target teams. The USB devices may look legitimate and can even be embedded with an organisation's logo and branding. When the users use the USB devices on their computers, the malicious files in the USB drives traverse through the internal network and can connect to a remote system set up by a hacker. This can provide the hacker with access to the target systems. The hacker can then use other techniques, such as password guessing, to gain full control of the system.
- Phishing: An email is sent or a phone call is made where the person claims to be someone in authority or a trusted organisation to trick users into revealing passwords or sensitive information.
- Click this link scams: Email or use of social networking sites (such as Facebook or Twitter) is used to entice users to click on a link such as a great offer, picture and so on. The link often looks legitimate but diverts the user to a harmful website designed to steal sensitive information or infect the computer.
- Fake e-cards or attachment: An email is sent that looks as if its attachment contains an electronic greeting card or job offer from a trusted 'friend'. The attachment contains a harmful program to infect the computer.
- Fake security alert: This is typically a warning from a trusted source like the organisation's information technology security provider or Microsoft that the computer is at risk of being infected or hacked. It usually provides a link or attachment that is supposed to fix the 'problem' but will actually infect the computer.

Source: adapted from Open Web Application Security Project community

2.3.3 Process

Securing business operations is not a 'set and forget' activity. Processes to manage evolving security threats and vulnerabilities require constant review and update; therefore, it is important to establish security practices to protect the systems over time. Policies and procedures provide a baseline to establish security management. Access to systems and regular reporting and monitoring of security-related events are also critical to managing security.

Information technology security policies, procedures and standards

The audited entities have corporate information technology security policies and procedures, but these were not always completely or effectively applied to the system environment. We found that corporate policies relating to remote access management, use of portable devices, patch management and anti-virus management were not reliably applied to the systems being audited.

Access management

Access controls use the concept of least privileged access to ensure that only authorised users can access the system and users' access is restricted to the level that is required to perform their duties and responsibilities.

None of the systems we audited had a documented, approved process to determine and record the users' access levels for the specified system. In addition, exit procedures for terminating employees and annual user access reviews were not operating effectively. Around 18 per cent of user accounts, in each of the main traffic systems, did not relate to current employees.

Information technology security reporting

Poor controls around reporting and monitoring meant that unauthorised or covert actions were unlikely to be detected. This can lead to delays in identifying security breaches and their sources and increased the risk of harm to business operations.

The inability to detect unauthorised access arose because:

- key security incidents were not always logged
- security incidents that were logged were not reviewed
- automated intrusion detection systems were not always implemented to monitor security
- roles and responsibilities for monitoring and reporting security incidents were not articulated.

2.3.4 Technology

Information technology security consists of a number of controls to provide the desired level of protection. In this section, we examine the security zones, a key control within the network design that enables system components to be on separate networks. Security zoning is used as an efficiency mechanism, as it can be costly to secure every component of a system. We also examined controls in place for when the systems are connected to the internet, other networks or portable devices.

Security zones

The entities we audited designed their networks to provide for security zones. This design enables different levels of security to be implemented, according to the requirements of separate system components. In addition, the design enables any security breaches to be contained within the infected zones.

The entities, however, did not achieve the full benefit of using security zones, as they did not implement restrictive network level access controls; therefore, security incidents in one part of the system could spread to other system components.

In addition, some of the external service providers' access to the network was not restricted to specific zones, ensuring that they only had the required level of access. This means that the security of the systems under review also relied on the security of the service providers’ information technology environments and staff.

Connectivity to the internet, other networks and portable devices

The risk of operational interruption from malicious software is high if an organisation is targeted by skilled adversaries. This occurs when the entity does not remove unnecessary connections and services to restrict access to systems. While network firewalls and email and web filters reduce the likelihood of malicious software incidents, they cannot block all new instances of malicious software. In addition, outdated and vulnerable software on workstations and mobile devices can open the path for unauthorised access.

Access controls

We examined user access controls separately for each application within the system network. Access to one entity's system at the application layer demonstrated good control design and was implemented through the use of digital security certificates. Only users with a valid security certificate installed on their workstations could access the application. All other applications examined for this entity required a username and password and access controls varied in strength. Password policies of some systems did not support good practice password setting, including length and complexity. The user account was not automatically locked after a number of failed logon attempts.

2.4 Principles of better practice

Entities need to do their own risk assessment to assess security risks and the corresponding controls needed to mitigate the risks. The controls outlined in Figure 2B are not prescriptive or all-inclusive but highlight some essential elements to improve the security of critical infrastructure and other operational systems.

Figure 2B
Key controls for security management

Principle	Key controls
Security risk assessment	• Establish organisational risk appetite for security risks and a security posture • Perform a security risk assessment to identify security risks and potential effect on the business in terms of likelihood, consequences and controls to mitigate the risks • Implement ongoing security risk management processes to ensure security remains current • Implement an information technology security plan based on security risk assessment
People	• Implement security awareness training and an ongoing security refresher program to ensure staff members understand: – current and emerging security risks – how to respond when faced with social engineering tactics to breach physical and system security or to obtain sensitive information – applicable policies, procedures, standards and best practices on information technology security • Introduce job and role specific security training on the application of security principles, security roles and responsibilities and response to suspected system security breach
Process	• Implement corporate information technology security policies and procedures such as remote access, use of portable devices, anti-virus management, system change and patch management, backup and restoration, incident response • Implement system-specific policies, procedures or standards • Implement access management process to grant, modify or remove access to system; users should only have access to functions they are authorised to perform in accordance with their duties and responsibilities • Implement physical security policies and procedures • Establish security risk oversight, monitoring, response and report of unusual activities in the system • Establish system backup and disaster recovery plan to recover system and data in the event of disaster

Principle	Key controls
	• Perform routine assessment of applications, networks and any other connected network to identify any security concerns
Technology	• Evaluate current network architecture and assess all connections to the systems and the corresponding security requirements—this includes connection to the internet, wireless network, portable devices, business partners, vendors and regulatory agencies—and disconnect unnecessary connections, disable unnecessary services and implement strong controls over any access that can be used as a backdoor to the system • Segment the network into zones, depending on security requirements and establish controls between security zones • Implement firewalls and virtual private network with alert mechanisms for abnormal behaviours in the network; assess the security access rules for appropriateness on a regular basis • Establish access controls and authentication mechanisms, including those for remote access • Maintain an anti-virus software and apply security patches for all layers of technology; for example, applications, databases, network and server operating systems • Implement intrusion detection software to detect malicious or suspicious network activities

Source: Queensland Audit Office and Queensland Government Information Standard 18: Information security

2.5 Recommendations

It is recommended that the Department of Transport and Main Roads and Brisbane City Council:

1. **perform risk assessments and develop security plans for the intelligent transport systems environment**
2. **implement comprehensive staff security awareness programs**
3. **operate intelligent transport systems security using good practice standards such as Queensland Government Information Standard 18: Information security**
4. **review the access control permissions to the intelligent transport systems network and applications environment.**

3 Continuity of traffic systems

In brief

Background

Key functions of Intelligent transport systems (ITS) include road operation and managing safe and efficient traffic flow. These services can be affected by disasters that cause physical damage to ITS infrastructure or to buildings housing the ITS infrastructure and road operations staff. They can also be affected by computer-based attacks, more commonly known as cybercrime, through the ITS technology networks.

Upcoming high profile events, such as the G20 and Commonwealth Games, increase the likelihood that ITS will be targeted through these types of attacks. It is therefore critical that processes are in place to recover ITS quickly from a security incident or disaster.

This chapter outlines the capabilities of the Department of Transport and Main Roads (TMR) and Brisbane City Council (BCC) to respond and recover ITS from natural or other disasters that affect the physical, human or information technology resources associated with ITS.

Conclusions

TMR and BCC have the technical capability to respond to security incidents and disasters when they are detected; however, untested and incomplete plans increase the risk that traffic operations will not be recovered from incidents within reasonable time frames if technical staff is not available. This risk is heightened during significant and high profile events.

Key findings

- TMR and BCC have access to experienced and technically competent staff members who can respond to system related events that are detected.
- The business continuity plans of TMR and BCC do not address both the business recovery and technical recovery of the ITS environment. Where plans are in place, they have not been tested rigorously.

Recommendations summary

It is recommended that the Department of Transport and Main Roads and Brisbane City Council:

5. **establish and test formal processes to maintain business continuity for the end to end intelligent transport systems environment.**

3.1 Background

The Brisbane Metropolitan Traffic Management Centre (BMTMC) is an alliance between the Brisbane City Council (BCC) and the Department of Transport and Main Roads (TMR). The BMTMC was formed to detect and respond to traffic incidents on roads controlled by TMR and BCC.

Intelligent transport systems (ITS) are the main systems that BMTMC uses to manage road traffic and public transport on a day to day basis; for example, BMTMC staff members coordinate the response to clear traffic congestion and update variable message boards by the roadside to warn motorists of traffic incidents. The safety and efficiency of the road network depends, therefore, on the continuity of traffic management operations and ITS.

Continuous operations can be planned by identifying likely disruptive scenarios—such as natural disasters or power failures—and creating a plan for managing the effects. A business continuity plan describes how designated response teams will communicate to employees, where they will go and how they will keep doing their jobs in the case of a disaster. Information technology (IT) disaster recovery planning is a subset of business continuity planning that deals with the recovery of IT systems supporting critical business functions. It describes the technological contingencies in place and provides instructions for manual system recovery, should the backup systems fail to operate.

The Australian/New Zealand Standard AS/NZS 5050: 2010 *Business continuity—Managing disruption-related risk* recommends that organisations plan both their response to the initial incident and the recovery of normal operations. These plans should be tested regularly so that staff members are capable of providing a prompt response during an incident or disaster.

3.2 Conclusions

TMR and BCC have the requisite capabilities in place to respond to disasters and security incidents that are detected. The capabilities include skilled staff, backup technology and alternate operating locations. It is likely that, in the event of a disaster, systems will not be recovered within an acceptable time frame because TMR and BCC have not fully tested the business and technical recovery of ITS.

3.3 Findings

3.3.1 Business continuity plan

Business continuity and IT disaster recovery plans provide instructions to recover business processes and IT systems in the event of a security incident or disaster. In the context of traffic management, this includes recovery procedures for operations facilities and IT systems.

Because TMR and BCC use separate staff, locations, processes and IT systems, they need separate business continuity and IT disaster recovery plans that address their individual circumstances. The BMTMC, as the responsible party for traffic management and a user of the TMR and BCC IT systems, requires a business continuity plan that will address how traffic management operations will continue during a disruptive event; therefore, three sets of business continuity plans are required for traffic operations.

Response capability

TMR and BCC have access to highly skilled technical staff members who can provide a response to system related events. Backup technology and alternate operating sites are also in place; therefore, both entities are able to respond to a system related incident if it is detected.

Plan

TMR and BCC do not have comprehensive business continuity plans that address all aspects of recovery (both technical and operational) for the end to end ITS environment. BCC has addressed key aspects of business continuity planning within its documented business continuity plan. These include plan activation and deactivation criteria, continuity process descriptions and communication protocols in the event of a disaster; however, aspects of IT disaster recovery, such as the contingent technology currently in place or the steps required for recovery of ITS, have not been documented.

Conversely, TMR has technically-focused recovery plans that are sufficient for recovery of the ITS environment, but plans for recovery of business functions are incomplete. As a result, recovery can be performed at both TMR and BCC but it is heavily reliant on the backup systems to operate as required in the event of an incident or a disaster and on the knowledge and experience of staff.

The BMTMC maintains a business continuity plan to re-establish operations in the event of a disaster affecting the primary operating site. This plan covers many attributes required by industry standards; however, the roles and responsibilities of staff involved in the recovery process are not clearly defined. In the absence of thorough training, staff members will not know what to do during a disaster which will delay the recovery effort.

Testing

TMR and BCC indicated they have tested their ITS recovery plans but they did not record evidence of this testing; therefore, we were not able to determine the success of tests, the speed of recovery, the nature of any lessons learned and refinement of plans after the tests.

The BMTMC plan was last tested through a desktop exercise in August 2012. This test did not include an inspection of the proposed recovery sites. It is therefore unclear whether the secondary sites will meet the operational needs of the BMTMC when the plan is activated.

Recovery sites

TMR, BCC and the BMTMC have established alternate sites where they can continue operations in the event of a disaster. The BMTMC has made arrangements for its traffic management and network coordination functions to be re-established at locations outside the inner city. However, some of TMR's primary and secondary sites do not provide sufficient distance if a major disaster was to occur at one of the sites.

3.4 Recommendations

It is recommended that the Department of Transport and Main Roads and Brisbane City Council:

5. **establish and test formal processes to maintain business continuity for the end to end intelligent transport systems environment.**

4 Cost effectiveness of traffic systems

In brief

Background

The Department of Transport and Main Roads (TMR) and the Brisbane City Council (BCC) operate two sets of intelligent transport systems (ITS) for managing traffic in the Brisbane metropolitan area. All other councils within Queensland use one system for traffic management—TMR's ITS.

We assessed whether the current arrangement of using separate ITS at TMR and BCC is effective in terms of cost and service delivery. We did this by evaluating the total cost of ownership to both entities using separate ITS and compared it with a scenario where a single intelligent transport system is used. In addition, we identified qualitative benefits of a single intelligent transport system for Queensland.

Conclusions

While the potential savings are modest and the return on investment is marginal, there are social, environmental and economic benefits for road users and the state in using a single intelligent transport system. Key benefits include a unified and coordinated strategy for incidents and congestion management, innovation in ITS and prioritising emergency vehicles across the entire road network.

Key findings

- TMR and BCC have managed the existing two-system model so that it is effective in both cost and service delivery to each entity; however, lack of alignment between TMR and BCC technology strategies is limiting the opportunities to improve traffic outcomes and to develop long term strategies for ITS.
- Both entities face common challenges and have a shared goal of reducing congestion and providing a better travel experience to the road user. While the road operations alliance group and the Brisbane Metropolitan Traffic Management Centre (BMTMC) board exist as forums for sharing ideas and business needs, both entities and road users can benefit from further collaboration initiatives relating to long term strategies for traffic management systems.
- TMR and BCC do not have processes in place to assess total cost of ownership of ITS; therefore, TMR and BCC cannot quantify the return on total investment in the information technology component of ITS.

Recommendations summary

It is recommended that the Department of Transport and Main Roads and Brisbane City Council:

6. **jointly develop a long term strategy for intelligent transport systems, including a full feasibility study of intelligent transport systems options**
7. **implement common approaches to shared challenges through establishing coordinated governance, joint service level agreement and key performance indicators for intelligent transport systems management across the Department of Transport and Main Roads and Brisbane City Council**
8. **introduce systems to record, report and monitor the cost of the information technology components of intelligent transport systems.**

4.1 Background

Intelligent transport systems (ITS) enable safer, coordinated and efficient use of road networks. They also enable a wide range of information to be provided to road users through roadside message signs and the internet. In Brisbane, the Department of Transport and Main Roads (TMR) uses the STREAMS platform while Brisbane City Council (BCC) uses SCATS for traffic signal management, along with systems for other traffic management functions developed in house.

When assessing whether the current arrangement of TMR and BCC using separate ('as is') ITS is cost effective, we evaluated the total cost of ownership of both entities using separate ITS and compared it with a hypothetical scenario where both entities would be on one intelligent transport system ('to be'). Although there are other potential candidates, we chose STREAMS as the hypothetical 'to be' single intelligent transport system, due to the availability of technical expertise and existing costing information.

We engaged TMR and BCC in workshops where we progressively built a common understanding of a single intelligent transport system capability. We confirmed with TMR and BCC that the single intelligent transport system being discussed would provide at least the utilities to the road user that are available in the current ITS. In addition, we used these workshops to identify risks and opportunities, and to agree upon costs for a transition project and ongoing operation of a single intelligent transport system. Our preliminary analysis, however, does not replace the need for full feasibility analysis of future ITS options and costs, should TMR and BCC decide to implement a single intelligent transport system.

4.2 Conclusions

Despite creating only modest savings in annual operating costs, a single intelligent transport system across Queensland has the potential to improve traffic management capabilities. Using a single intelligent transport system for the state could provide opportunities for BCC to implement current and innovative solutions rather than maintaining legacy systems that rely on specific systems-based skills. It could also enable BCC and TMR to develop a coordinated long term ITS strategy in Queensland.

The shared responsibility for road network management was a fundamental challenge to developing long term strategies for ITS. To overcome these challenges would require closer collaboration between TMR and BCC, of which a single intelligent transport system is only one aspect.

4.3 Findings

4.3.1 Cost neutrality

Given the minimal net savings, the alternative of a single intelligent transport system based on STREAMS is cost neutral when compared with the current arrangements of using two separate ITS.

The ITS costs for Queensland is estimated at $510 million for the next ten years, adjusted for current inflation rates. Figure 4A shows the 'as is' annual cost information provided by TMR and BCC. The analysis also shows the effect of the investment decision for the ITS: the ITS software and hardware costs of $58 million (11 per cent of total cost of ownership) drive $322 million of ITS field infrastructure costs (63 per cent of total cost of ownership).

Figure 4A
Estimated ‘as is’ total cost of ownership of ITS for Queensland

Category	2013–14 $	2013–14 to 2022–23 $
Hardware	998 000	11 125 000
Field infrastructure (hardware)	28 867 000	321 946 000
Software	4 216 000	46 992 000
Management	1 612 000	17 973 000
Support labour	2 870 000	32 004 000
Development	2 051 000	22 876 000
Utilities	5 102 000	56 897 000
Total costs	**45 716 000**	**509 813 000**

Source: Queensland Audit Office using data from TMR and BCC

In investigating the costs of a single intelligent transport system, we divided the ten-year timespan into a transition period—assumed to be two years—and the remaining eight years of single system operation. We also considered best and worst case scenarios, based on possible variations in project costs and in operating costs of the single intelligent transport system. These estimates have been included in our analysis to provide a more complete understanding of the cost effectiveness of the 'as is' case in comparison to the hypothetical 'to be' scenario.

The analysis shows that there would be an increase in ITS cost during the transition phase (2013–14 to 2015–16), due to the project costs associated with the transition and temporary duplication of systems during the two-year transition period. The estimated ITS costs during the transition period range from $97 million to $100 million for the two-year period. Figure 4B shows ITS cost during this transition period.

Figure 4B
ITS costs (net present value) during the transition period 2013–14 to 2015–16

Category	Single system (best case) $	Single system (worst case) $
Ongoing costs	91 735 155	91 735 155
Project costs	5 426 667	8 071 184
Total costs	**97 161 822**	**99 806 339**

Source: Queensland Audit Office using data from TMR and BCC

The estimated ongoing operating costs of the single system, after the transition period, allowed a comparison with existing operating costs to give a range of expected ongoing annual savings. It is estimated that the intelligent transport system costs after the two-year transition period range from $338 million to $342 million.

Figure 4C shows the costs and savings of a single intelligent transport system after the transition period (2016–17 to 2022–23).

Figure 4C
Intelligent transport system costs (net present value) and savings on a single intelligent transport system after transition period 2016–17 to 2022–23

Category	'as is' $	Single system (best case) $	Single system (worst case) $
Ongoing costs	344 950 000 (A)	337 850 437 (B)	342 490 761 (C)
Total costs		7 099 563 (A - B)	2 459 239 (A - C)
Total savings / year		**887,445**	**307,404**

Source: Queensland Audit Office using data from TMR and BCC

Taking into account the transition costs, the outcome would range from net savings of $877 742 to net additional costs of $6.4 million over the period 2013–14 to 2022–23. This is only a marginal cost saving when considered against the total cost of ownership. Figure 4D provides a comparison of costs in terms of net present value of the 'as is' and 'to be' systems.

Figure 4D
Total net savings (net present value) for ten-year period (2013–14 to 2022–23)

Category	'as is' $	Single system (best case) $	Single system (worst case) $
Ongoing costs 2013–14 to 2022–23	435 890 000		
Ongoing costs 2013–14 to 2015–16		97 161 821	99 806 338
Ongoing costs 2016–17 to 2022–23		337 850 437	342 490 761
Total costs	435 890 000 (A)	435 012 258 (B)	442 297 099 (C)
Total savings / (costs)		**$877,742 (A - B)**	**($6,407,099) (A - C)**

Source: Queensland Audit Office using data from TMR and BCC

4.3.2 Benefits to the road user

There is consensus amongst TMR and BCC that a single intelligent transport system across the state would provide improved traffic management capabilities. Figure 4E outlines the key benefits that were identified during workshops we facilitated between TMR and BCC.

Figure 4E
Qualitative benefits of a single intelligent transport system

Use	Benefits
Traffic management and response to incidents through BMTMC	Improved efficiency through reduced complexity and the risk of error from using multiple systems when managing traffic flows and traffic incidents, planned (e.g. road works) and unplanned (e.g. accidents)
Efficient use of road infrastructure	A unified and coordinated strategy for congestion management, particularly at network locations of mutual dependency regardless of whether the road is controlled by BCC or TMR
Vehicle prioritisation (e.g. emergency services, buses, VIPs)	A common view of the road network allowing end to end prioritising of emergency vehicles
Integrating with other systems (e.g. SCADA, other ITS)	Reducing the complexity and number of interfaces required when integrating with other critical systems (for example SCADA system for tunnel management), which also allows the consolidation of tender requirements on third parties
Providing information to the government (e.g. road network planning)	A holistic view of traffic outcomes, including management and reporting of traffic data, to assess the success of congestion strategies across Queensland regardless of the road owners
Providing data to third parties (e.g. Google, global positioning system providers)	Provision of a common and consistent data set from a single source

Source: Queensland Audit Office using data from TMR and BCC

4.3.3 Organisational alignment and collaboration opportunities

While roads controlled by TMR include those of extended and high traffic road networks (for example, freeways and motorways) and BCC's roads are mostly arterial and suburban roads, both TMR and BCC face many common challenges in managing their road networks. This includes managing suppliers for traffic operation and field maintenance; managing private roads, tunnel and motorway operators; establishing policies, procedures and business continuity planning; and coordinating with the Queensland Police Service and RACQ.

Despite this, there are two differing traffic operation strategies through two distinct management cultures and structures. TMR focuses on maximising value through ITS investment and innovation while BCC has a cost minimisation strategy.

The current arrangement is not an optimal response to the task of managing Queensland's road network and limits the potential for improvements in effectiveness and cost reductions. Duplication of efforts occurs in managing common challenges on their road networks. These efforts could be used to focus in specific areas where each of these organisations excels.

BCC and TMR can benefit from ITS innovation, if both entities are using one platform, whether STREAMS or any other best practice system that is adopted. This will also address some of the risks of in house developed systems and heavy reliance on limited but critical ITS personnel. Similarly, both TMR and BCC can benefit from coordinating the strategy, selection, procurement and maintenance of ITS field infrastructure for efficiency and economies of scale.

By working together on a common vision, TMR and BCC can improve the way they discover opportunities for innovation and improvement of current services. During our workshops, both parties engaged as a group in identifying better ways to use infrastructure in the provision of services. There was evidence that both parties understood there is one common goal to provide a better travel experience for the road user. The pursuit of these opportunities, however, requires that TMR and BCC overcome the challenges of working as separate entities, with different areas of focus and governance.

4.3.4 Total cost of ownership

TMR and BCC have annual asset management planning processes to determine funding required for traffic services. While these processes are important in determining resource requirements, neither TMR nor BCC could provide total life cycle costs to implement, use and maintain traffic systems and the related information technology infrastructure.

Without this information, TMR and BCC cannot quantify the return on total investment in the information technology components of ITS nor assess options for a long term ITS strategy.

4.4 Recommendations

It is recommended that the Department of Transport and Main Roads and Brisbane City Council:

6. **jointly develop a long term strategy for intelligent transport systems, including a full feasibility study of intelligent transport systems options**
7. **implement common approaches to shared challenges through establishing coordinated governance, joint service level agreement and key performance indicators for intelligent transport systems management across the Department of Transport and Main Roads and Brisbane City Council**
8. **introduce systems to record, report and monitor the cost of the information technology components of intelligent transport systems.**

Appendices

Appendix A—Comments

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

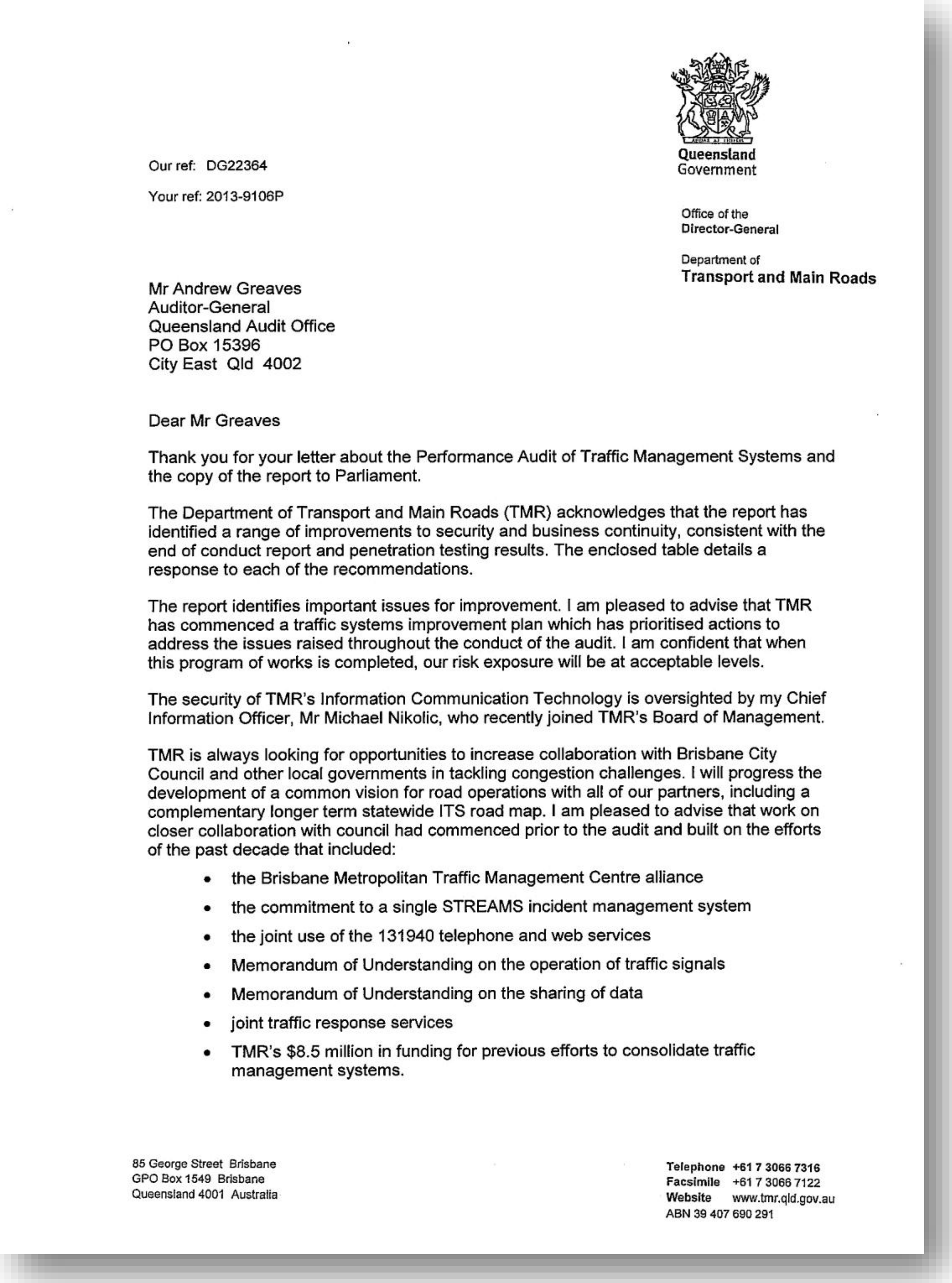
Introduction

In accordance with section 64 of the *Auditor-General Act 2009* a copy of this report was provided to the Department of Transport and Main Roads and Brisbane City Council with a request for comment.

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

Comments received

Response provided by the Director-General, Department of Transport and Main Roads on 12 November 2013.



Queensland
Government

Our ref: DG22364

Your ref: 2013-9106P

Office of the
Director-General

Department of
Transport and Main Roads

Mr Andrew Greaves
Auditor-General
Queensland Audit Office
PO Box 15396
City East Qld 4002

Dear Mr Greaves

Thank you for your letter about the Performance Audit of Traffic Management Systems and the copy of the report to Parliament.

The Department of Transport and Main Roads (TMR) acknowledges that the report has identified a range of improvements to security and business continuity, consistent with the end of conduct report and penetration testing results. The enclosed table details a response to each of the recommendations.

The report identifies important issues for improvement. I am pleased to advise that TMR has commenced a traffic systems improvement plan which has prioritised actions to address the issues raised throughout the conduct of the audit. I am confident that when this program of works is completed, our risk exposure will be at acceptable levels.

The security of TMR's Information Communication Technology is oversighted by my Chief Information Officer, Mr Michael Nikolic, who recently joined TMR's Board of Management.

TMR is always looking for opportunities to increase collaboration with Brisbane City Council and other local governments in tackling congestion challenges. I will progress the development of a common vision for road operations with all of our partners, including a complementary longer term statewide ITS road map. I am pleased to advise that work on closer collaboration with council had commenced prior to the audit and built on the efforts of the past decade that included:

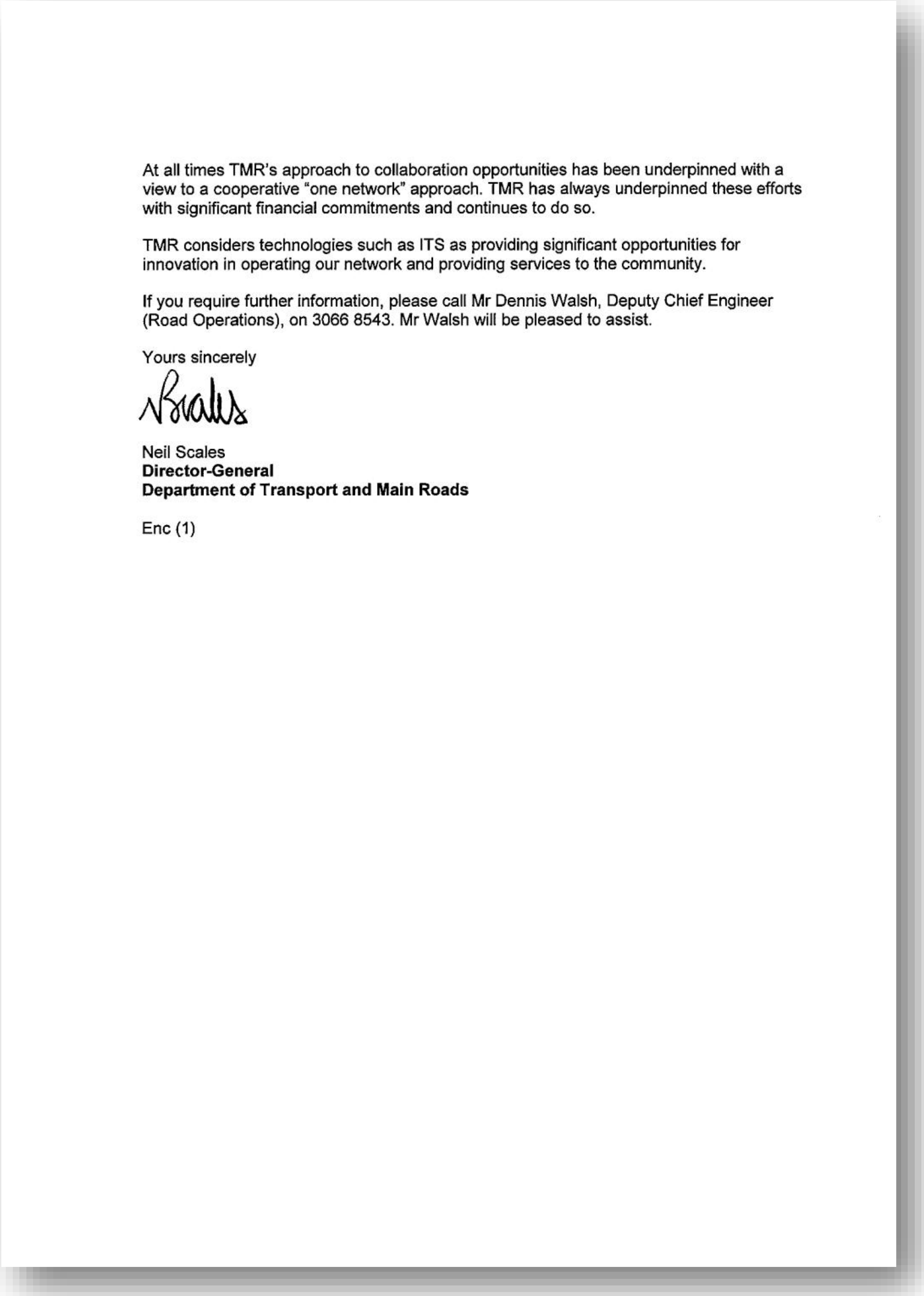
- the Brisbane Metropolitan Traffic Management Centre alliance
- the commitment to a single STREAMS incident management system
- the joint use of the 131940 telephone and web services
- Memorandum of Understanding on the operation of traffic signals
- Memorandum of Understanding on the sharing of data
- joint traffic response services
- TMR's $8.5 million in funding for previous efforts to consolidate traffic management systems.

85 George Street Brisbane
GPO Box 1549 Brisbane
Queensland 4001 Australia

Telephone +61 7 3066 7316
Facsimile +61 7 3066 7122
Website www.tmr.qld.gov.au
ABN 39 407 690 291

Comments received

Response provided by the Director-General, Department of Transport and Main Roads on 12 November 2013.



At all times TMR's approach to collaboration opportunities has been underpinned with a view to a cooperative "one network" approach. TMR has always underpinned these efforts with significant financial commitments and continues to do so.

TMR considers technologies such as ITS as providing significant opportunities for innovation in operating our network and providing services to the community.

If you require further information, please call Mr Dennis Walsh, Deputy Chief Engineer (Road Operations), on 3066 8543. Mr Walsh will be pleased to assist.

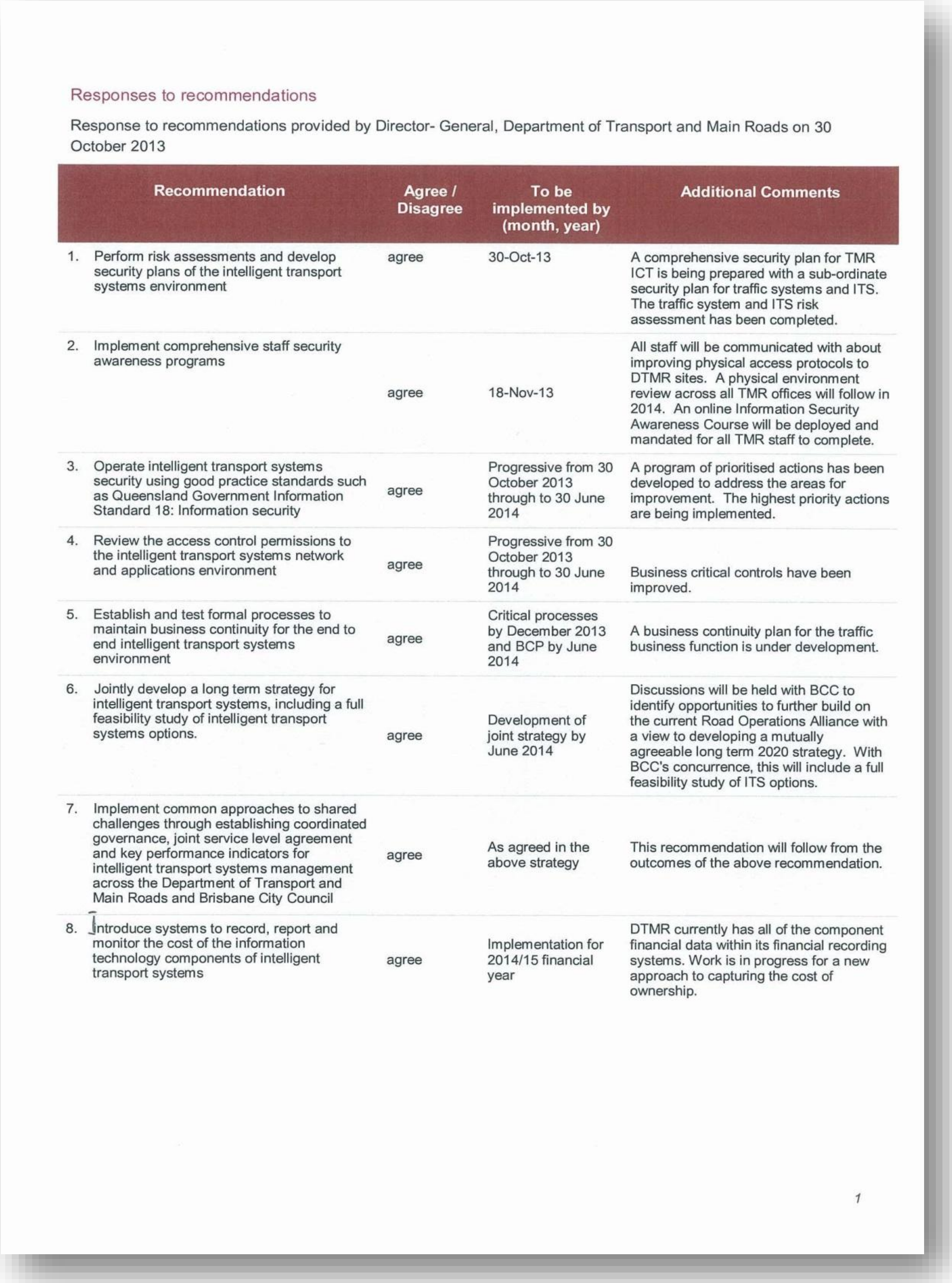
Yours sincerely

Neil Scales
Director-General
Department of Transport and Main Roads

Enc (1)

Responses to recommendations

Response to recommendations provided by the Director-General, Department of Transport and Main Roads on 12 November 2013.



Responses to recommendations

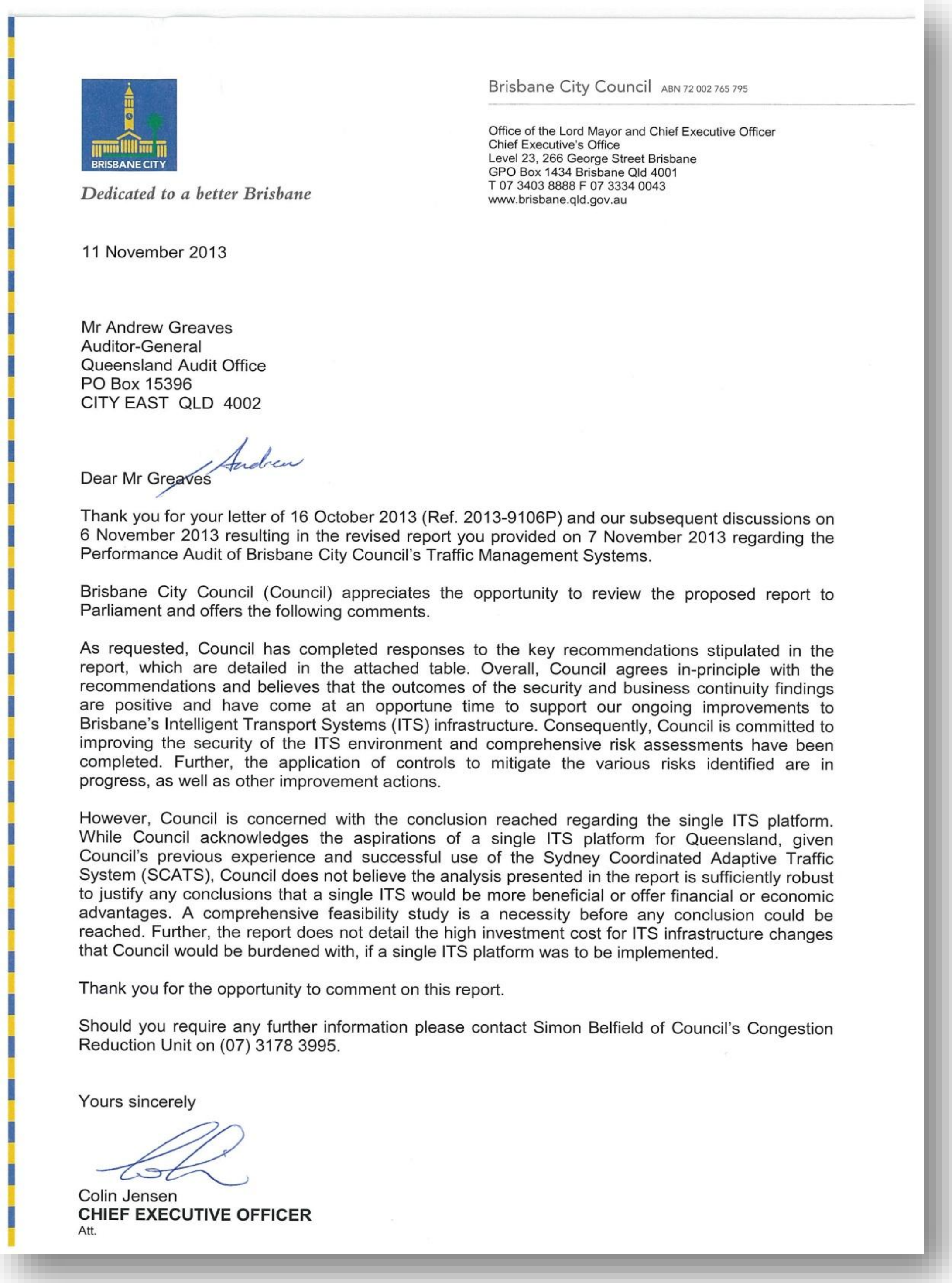
Response to recommendations provided by Director- General, Department of Transport and Main Roads on 30 October 2013

Recommendation	Agree / Disagree	To be implemented by (month, year)	Additional Comments
1. Perform risk assessments and develop security plans of the intelligent transport systems environment	agree	30-Oct-13	A comprehensive security plan for TMR ICT is being prepared with a sub-ordinate security plan for traffic systems and ITS. The traffic system and ITS risk assessment has been completed.
2. Implement comprehensive staff security awareness programs	agree	18-Nov-13	All staff will be communicated with about improving physical access protocols to DTMR sites. A physical environment review across all TMR offices will follow in 2014. An online Information Security Awareness Course will be deployed and mandated for all TMR staff to complete.
3. Operate intelligent transport systems security using good practice standards such as Queensland Government Information Standard 18: Information security	agree	Progressive from 30 October 2013 through to 30 June 2014	A program of prioritised actions has been developed to address the areas for improvement. The highest priority actions are being implemented.
4. Review the access control permissions to the intelligent transport systems network and applications environment	agree	Progressive from 30 October 2013 through to 30 June 2014	Business critical controls have been improved.
5. Establish and test formal processes to maintain business continuity for the end to end intelligent transport systems environment	agree	Critical processes by December 2013 and BCP by June 2014	A business continuity plan for the traffic business function is under development.
6. Jointly develop a long term strategy for intelligent transport systems, including a full feasibility study of intelligent transport systems options.	agree	Development of joint strategy by June 2014	Discussions will be held with BCC to identify opportunities to further build on the current Road Operations Alliance with a view to developing a mutually agreeable long term 2020 strategy. With BCC's concurrence, this will include a full feasibility study of ITS options.
7. Implement common approaches to shared challenges through establishing coordinated governance, joint service level agreement and key performance indicators for intelligent transport systems management across the Department of Transport and Main Roads and Brisbane City Council	agree	As agreed in the above strategy	This recommendation will follow from the outcomes of the above recommendation.
8. Introduce systems to record, report and monitor the cost of the information technology components of intelligent transport systems	agree	Implementation for 2014/15 financial year	DTMR currently has all of the component financial data within its financial recording systems. Work is in progress for a new approach to capturing the cost of ownership.

1

Comments received

Response provided by the Chief Executive Officer, Brisbane City Council on 11 November 2013.



BRISBANE CITY

Dedicated to a better Brisbane

Brisbane City Council ABN 72 002 765 795

Office of the Lord Mayor and Chief Executive Officer
Chief Executive's Office
Level 23, 266 George Street Brisbane
GPO Box 1434 Brisbane Qld 4001
T 07 3403 8888 F 07 3334 0043
www.brisbane.qld.gov.au

11 November 2013

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

Dear Mr ~~Greaves~~ Andrew

Thank you for your letter of 16 October 2013 (Ref. 2013-9106P) and our subsequent discussions on 6 November 2013 resulting in the revised report you provided on 7 November 2013 regarding the Performance Audit of Brisbane City Council's Traffic Management Systems.

Brisbane City Council (Council) appreciates the opportunity to review the proposed report to Parliament and offers the following comments.

As requested, Council has completed responses to the key recommendations stipulated in the report, which are detailed in the attached table. Overall, Council agrees in-principle with the recommendations and believes that the outcomes of the security and business continuity findings are positive and have come at an opportune time to support our ongoing improvements to Brisbane's Intelligent Transport Systems (ITS) infrastructure. Consequently, Council is committed to improving the security of the ITS environment and comprehensive risk assessments have been completed. Further, the application of controls to mitigate the various risks identified are in progress, as well as other improvement actions.

However, Council is concerned with the conclusion reached regarding the single ITS platform. While Council acknowledges the aspirations of a single ITS platform for Queensland, given Council's previous experience and successful use of the Sydney Coordinated Adaptive Traffic System (SCATS), Council does not believe the analysis presented in the report is sufficiently robust to justify any conclusions that a single ITS would be more beneficial or offer financial or economic advantages. A comprehensive feasibility study is a necessity before any conclusion could be reached. Further, the report does not detail the high investment cost for ITS infrastructure changes that Council would be burdened with, if a single ITS platform was to be implemented.

Thank you for the opportunity to comment on this report.

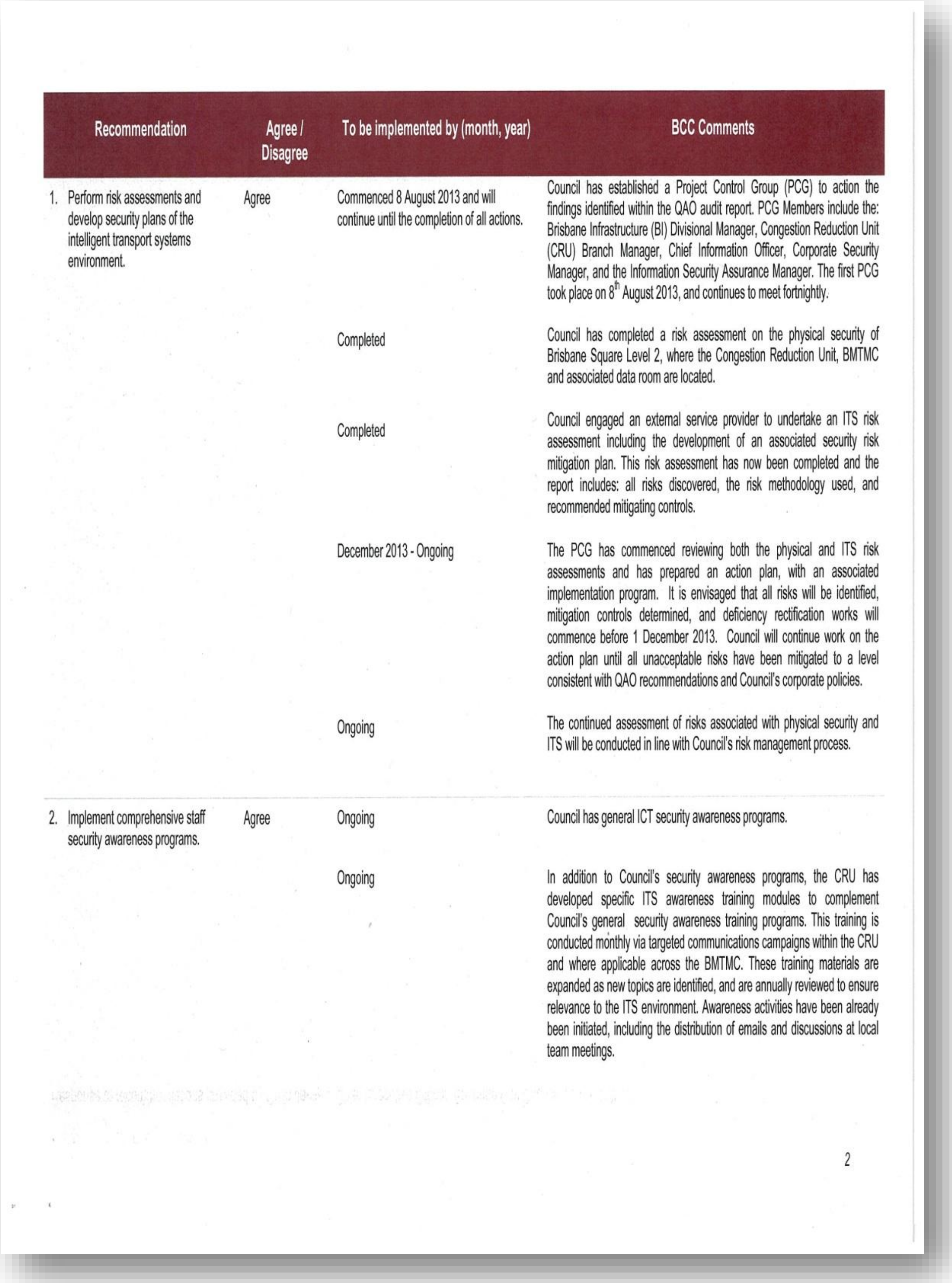
Should you require any further information please contact Simon Belfield of Council's Congestion Reduction Unit on (07) 3178 3995.

Yours sincerely

Colin Jensen
CHIEF EXECUTIVE OFFICER
Att.

Responses to recommendations

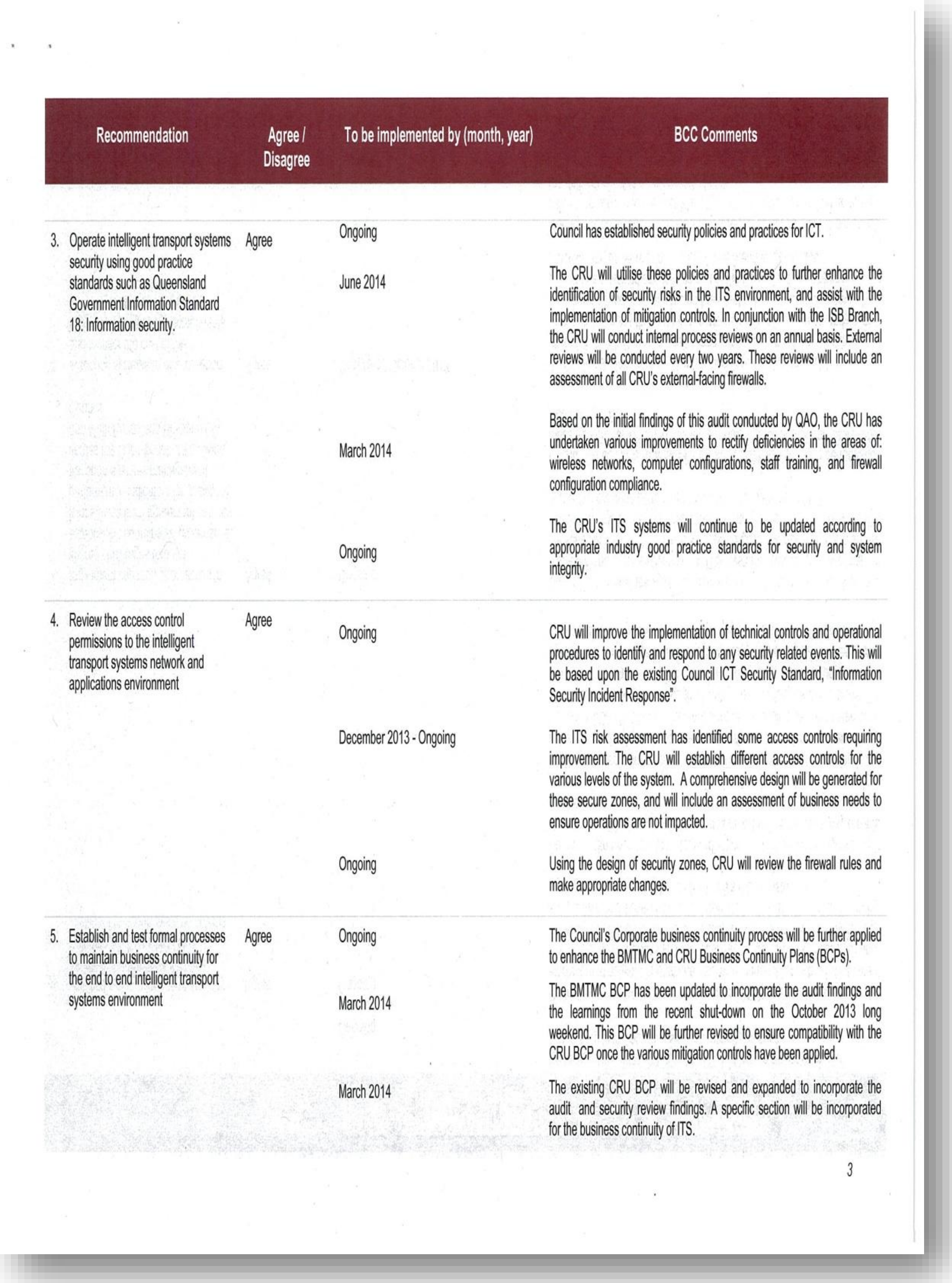
Response to recommendations provided by the Chief Executive Officer, Brisbane City Council on 11 November 2013.



Recommendation	Agree / Disagree	To be implemented by (month, year)	BCC Comments
1. Perform risk assessments and develop security plans of the intelligent transport systems environment.	Agree	Commenced 8 August 2013 and will continue until the completion of all actions.	Council has established a Project Control Group (PCG) to action the findings identified within the QAO audit report. PCG Members include the: Brisbane Infrastructure (BI) Divisional Manager, Congestion Reduction Unit (CRU) Branch Manager, Chief Information Officer, Corporate Security Manager, and the Information Security Assurance Manager. The first PCG took place on 8th August 2013, and continues to meet fortnightly.
		Completed	Council has completed a risk assessment on the physical security of Brisbane Square Level 2, where the Congestion Reduction Unit, BMTMC and associated data room are located.
		Completed	Council engaged an external service provider to undertake an ITS risk assessment including the development of an associated security risk mitigation plan. This risk assessment has now been completed and the report includes: all risks discovered, the risk methodology used, and recommended mitigating controls.
		December 2013 - Ongoing	The PCG has commenced reviewing both the physical and ITS risk assessments and has prepared an action plan, with an associated implementation program. It is envisaged that all risks will be identified, mitigation controls determined, and deficiency rectification works will commence before 1 December 2013. Council will continue work on the action plan until all unacceptable risks have been mitigated to a level consistent with QAO recommendations and Council's corporate policies.
		Ongoing	The continued assessment of risks associated with physical security and ITS will be conducted in line with Council's risk management process.
2. Implement comprehensive staff security awareness programs.	Agree	Ongoing	Council has general ICT security awareness programs.
		Ongoing	In addition to Council's security awareness programs, the CRU has developed specific ITS awareness training modules to complement Council's general security awareness training programs. This training is conducted monthly via targeted communications campaigns within the CRU and where applicable across the BMTMC. These training materials are expanded as new topics are identified, and are annually reviewed to ensure relevance to the ITS environment. Awareness activities have been already been initiated, including the distribution of emails and discussions at local team meetings.

Responses to recommendations

Response to recommendations provided by the Chief Executive Officer, Brisbane City Council on 11 November 2013.

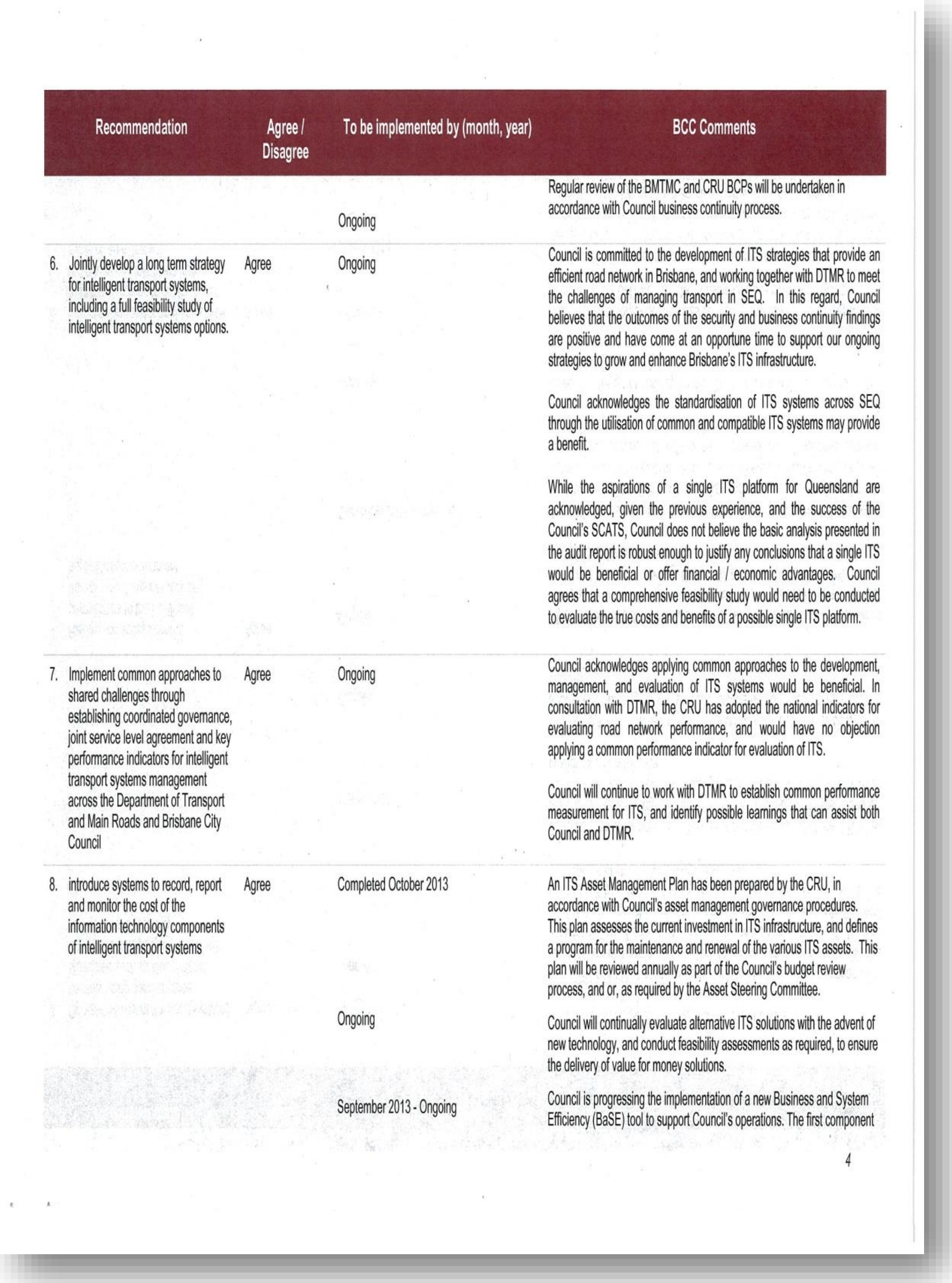


Recommendation	Agree / Disagree	To be implemented by (month, year)	BCC Comments
3. Operate intelligent transport systems security using good practice standards such as Queensland Government Information Standard 18: Information security.	Agree	Ongoing	Council has established security policies and practices for ICT.
		June 2014	The CRU will utilise these policies and practices to further enhance the identification of security risks in the ITS environment, and assist with the implementation of mitigation controls. In conjunction with the ISB Branch, the CRU will conduct internal process reviews on an annual basis. External reviews will be conducted every two years. These reviews will include an assessment of all CRU's external-facing firewalls.
		March 2014	Based on the initial findings of this audit conducted by QAO, the CRU has undertaken various improvements to rectify deficiencies in the areas of: wireless networks, computer configurations, staff training, and firewall configuration compliance.
		Ongoing	The CRU's ITS systems will continue to be updated according to appropriate industry good practice standards for security and system integrity.
4. Review the access control permissions to the intelligent transport systems network and applications environment	Agree	Ongoing	CRU will improve the implementation of technical controls and operational procedures to identify and respond to any security related events. This will be based upon the existing Council ICT Security Standard, "Information Security Incident Response".
		December 2013 - Ongoing	The ITS risk assessment has identified some access controls requiring improvement. The CRU will establish different access controls for the various levels of the system. A comprehensive design will be generated for these secure zones, and will include an assessment of business needs to ensure operations are not impacted.
		Ongoing	Using the design of security zones, CRU will review the firewall rules and make appropriate changes.
5. Establish and test formal processes to maintain business continuity for the end to end intelligent transport systems environment	Agree	Ongoing	The Council's Corporate business continuity process will be further applied to enhance the BMTMC and CRU Business Continuity Plans (BCPs).
		March 2014	The BMTMC BCP has been updated to incorporate the audit findings and the learnings from the recent shut-down on the October 2013 long weekend. This BCP will be further revised to ensure compatibility with the CRU BCP once the various mitigation controls have been applied.
		March 2014	The existing CRU BCP will be revised and expanded to incorporate the audit and security review findings. A specific section will be incorporated for the business continuity of ITS.

3

Responses to recommendations

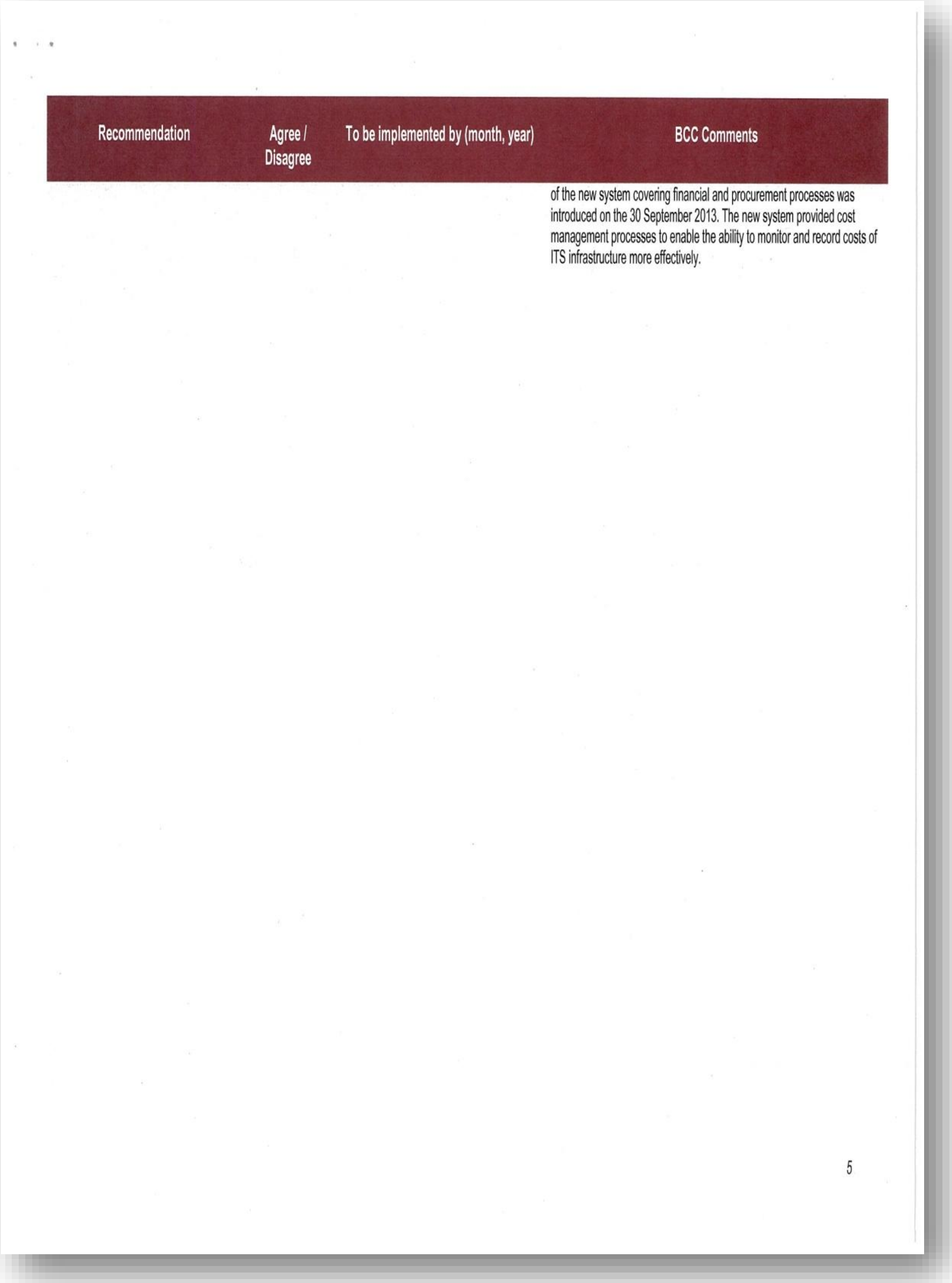
Response to recommendations provided by the Chief Executive Officer, Brisbane City Council on 11 November 2013.



Recommendation	Agree / Disagree	To be implemented by (month, year)	BCC Comments
		Ongoing	Regular review of the BMTMC and CRU BCPs will be undertaken in accordance with Council business continuity process.
6. Jointly develop a long term strategy for intelligent transport systems, including a full feasibility study of intelligent transport systems options.	Agree	Ongoing	Council is committed to the development of ITS strategies that provide an efficient road network in Brisbane, and working together with DTMR to meet the challenges of managing transport in SEQ. In this regard, Council believes that the outcomes of the security and business continuity findings are positive and have come at an opportune time to support our ongoing strategies to grow and enhance Brisbane's ITS infrastructure. Council acknowledges the standardisation of ITS systems across SEQ through the utilisation of common and compatible ITS systems may provide a benefit. While the aspirations of a single ITS platform for Queensland are acknowledged, given the previous experience, and the success of the Council's SCATS, Council does not believe the basic analysis presented in the audit report is robust enough to justify any conclusions that a single ITS would be beneficial or offer financial / economic advantages. Council agrees that a comprehensive feasibility study would need to be conducted to evaluate the true costs and benefits of a possible single ITS platform.
7. Implement common approaches to shared challenges through establishing coordinated governance, joint service level agreement and key performance indicators for intelligent transport systems management across the Department of Transport and Main Roads and Brisbane City Council	Agree	Ongoing	Council acknowledges applying common approaches to the development, management, and evaluation of ITS systems would be beneficial. In consultation with DTMR, the CRU has adopted the national indicators for evaluating road network performance, and would have no objection applying a common performance indicator for evaluation of ITS. Council will continue to work with DTMR to establish common performance measurement for ITS, and identify possible learnings that can assist both Council and DTMR.
8. introduce systems to record, report and monitor the cost of the information technology components of intelligent transport systems	Agree	Completed October 2013 Ongoing September 2013 - Ongoing	An ITS Asset Management Plan has been prepared by the CRU, in accordance with Council's asset management governance procedures. This plan assesses the current investment in ITS infrastructure, and defines a program for the maintenance and renewal of the various ITS assets. This plan will be reviewed annually as part of the Council's budget review process, and or, as required by the Asset Steering Committee. Council will continually evaluate alternative ITS solutions with the advent of new technology, and conduct feasibility assessments as required, to ensure the delivery of value for money solutions. Council is progressing the implementation of a new Business and System Efficiency (BaSE) tool to support Council's operations. The first component

Responses to recommendations

Response to recommendations provided by the Chief Executive Officer, Brisbane City Council on 11 November 2013.



Recommendation	Agree / Disagree	To be implemented by (month, year)	BCC Comments
			of the new system covering financial and procurement processes was introduced on the 30 September 2013. The new system provided cost management processes to enable the ability to monitor and record costs of ITS infrastructure more effectively.

5

Appendix B—Audit details

Audit objective

The objective of this audit was to determine whether the systems used to operate and manage traffic control infrastructure are secure and cost effective. In conducting the audit, we examined whether:

- controls to prevent, detect and respond to security breaches were effective
- business continuity management was effective and there was established emergency response capability
- systems used to deliver traffic management services for roads controlled by council and state were cost effective.

Reasons for the audit

The audit was conducted for the following reasons:

- The urgency for secure critical infrastructure systems. There are lessons to be learned from a number of security breaches on these systems worldwide.
- The heightened security risks and cyber-attacks for the G20 Summit. Security research shows an increase in cyber-attacks on the G20 host and participating countries leading to the G20 Summit. As the host of the 2014 Summit, the Queensland government needs to have secured information technology environments and be able to recover from information technology security incidents when the need arises.
- Currently, there are two sets of intelligent transport systems (ITS) to manage traffic in Brisbane. The current economic climate and increased government focus on efficiency necessitates the evaluation of ITS costs and the benefit of using a single intelligent transport system.

Performance audit approach

The audit was conducted between May 2013 and August 2013.

Figure B1
Audit approach

Audit area	Approach
Traffic system security	• Interview key staff of the Department of Transport and Main Roads (TMR), Brisbane City Council (BCC), Brisbane Metropolitan Traffic Management Centre (BMTMC) and TMR's controlled entity • Evaluate the security and control designs of the ITS environments • Conduct security penetration tests to identify and exploit security vulnerabilities—the tests include the use of social engineering techniques to manipulate staff members to provide access or information that can be used to plan penetration tests
Business continuity	• Perform desktop review on the information technology disaster recovery plan and business continuity plan • Evaluate the capabilities and tests to respond to incidents and disasters
ITS costs	• Perform financial modelling to assess the total cost of ownership to TMR and BCC for ITS for the period of 2013–2014 to 2022–23 • Facilitate a number of workshops with TMR and BCC to: – examine the utility provided by ITS to the road user – determine plausible options, benefits and costs for a single intelligent transport system – conduct preliminary analysis on the operating costs and conversion costs of a single intelligent transport system based on information provided by TMR and BCC

Source: Queensland Audit Office

Use of experts

Experts were used and consulted throughout the audit.

Figure B2
Experts used

Expert	Purpose
Information technology security consultants	Conduct security and penetration tests on ITS environments
ITS consultants	Provide expert opinion and advice on ITS
System and engineering experts from TMR, BCC and TMR's controlled entity	Provide the costs and use information of each components of ITS Provide expert opinion on the benefits and costs of a single intelligent transport system
Total cost of ownership consultants	Perform total cost of ownership calculation on TMR and BCC ITS

Source: Queensland Audit Office

Auditor-General
Reports to Parliament

Tabled in 2013–14

Report number	Title of report	Date tabled in Legislative Assembly
1	Right of private practice in Queensland public hospitals	July 2013
2	Supply of specialist subject teachers in secondary schools	October 2013
3	Follow up - Acquisition and public access to the Museum, Art Gallery and Library collections	October 2013
4	Follow up - Management of offenders subject to supervision in the community	October 2013
5	Traffic management systems	November 2013

Reports to Parliament are available at www.qao.qld.gov.au