Queensland Audit Office
better public services

Security of critical water infrastructure

Report 19: 2016–17

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

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

ISSN 1834-1128

Your ref:
Our ref: 2016-P9155

Queensland Audit Office
better public services

June 2017

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

Dear Mr Speaker

Report to Parliament

This report is prepared under Part 3 Division 3 of the *Auditor-General Act 2009*, and is titled *Security of critical water infrastructure* (Report 19: 2016–17).

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

Yours sincerely

Anthony Close
Auditor-General (acting)

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

Phone 07 3149 6000
Email qao@qao.qld.gov.au
Web *www.qao.qld.gov.au*

Contents

Summary

Reliable drinking water and wastewater services are essential to all Queenslanders. Water service providers generally use computer systems to control operations of water treatment plants, and related facilities and assets. The security of these control systems is therefore important in maintaining continuity of service.

It is common practice for organisations to secure their financial systems, but this is not always the case for computer systems controlling operational infrastructure. Yet failure or security breaches in these control systems can have major consequences for the health of citizens, the environment, and the businesses that rely on these services.

Owners of critical water infrastructure are responsible for protecting these control systems from potential attacks. These threats may be through acts of terrorism, or carried out by curious and technically competent individuals, or by trusted insiders with malicious intent to harm. Staff can also compromise security by making simple technical errors. Recent security threats and incident reports show that, as the security industry advances, so do the hackers and cyber criminals. Attackers can easily access malicious software online to use in attempts to breach control systems. This software is becoming harder to control as it has become more resilient to the solutions developed to protect control systems.

Reported incidents also show that some critical infrastructure breaches and cyber threats come from inside the entities, or from 'lone wolf' attackers. The increased incidence of these types of attacks means that owners of control systems must continually assess and improve the defences that they have built within their control environment.

In this audit, we assessed whether a selection of entities responsible for critical water infrastructure have processes in place to protect their water control systems. We carried out our own tests, known as penetration tests, to identify and exploit security vulnerabilities. We also assessed whether these entities could detect the security breaches and restore the systems in the event of an attack.

Audit conclusions

The water control systems were not as secure as they should have been at the time of our audit testing. The age of many of these control systems, combined with more recent integration with corporate networks, had resulted in higher risks that had not always been recognised and tested by the entities themselves. Security controls did not sufficiently protect them from internal or external information technology-related attacks. Information security is like a chain—it is only as strong as the weakest link. All entities were susceptible to security breaches or hacking attacks because of weaknesses in processes and controls.

At the time of our testing, attacks could disrupt water and wastewater treatment services. They could also disrupt other services that relied on the entities' information technology environments. There was a risk to public health and appreciable economic loss in terms of lost productivity, not only to water service providers but also to citizens and businesses. A sewage spill could also have a significant impact on the environment.

We acknowledge the efforts of the critical infrastructure owners since our testing to mitigate the risk of security incidents, including cyber attacks, on their systems to minimise the impact of such events.

All entities we audited had the capability to respond to information security incidents if they detected them. However, they were not well prepared to respond to cyber attacks. They had not planned or tested their response and recovery from a malicious or cyber incident. These can occur without notice and can affect availability and integrity of multiple systems.

The entities audited reported that they could operate smaller plants or parts of their larger water treatment plants manually in the event of disruption to computer systems, but they had not demonstrated this capability. Only one entity had documented its manual operating procedures, and none had ever tested running their whole plants manually. This places a high reliance on individual knowledge, experience and physical presence to continue water services in the event of an attack.

The results of this audit serve as a timely reminder for any public sector entity managing critical infrastructure. Entities should assess and strengthen defences to protect their systems from information technology and cyber threats, and ensure that manual operation of critical infrastructure is documented and well tested.

Audit findings

The entities we audited needed to improve their processes for managing information technology risks and business continuity planning for water control systems.

Managing control system risks

Water service providers needed to:

- identify risks of information technology security breaches
- implement controls to protect their systems
- monitor and review the effectiveness of the controls.

While entities we audited have taken steps in recent years to improve their information technology security, the results of this audit shows that management needs to do more. The entities need to do more in terms of oversight, leadership, and direction.

- Roles and responsibilities—several Queensland Government departments deal with counter-terrorism and response, but no central agency is responsible for supporting critical water infrastructure owners to protect these systems from security events resulting from information technology risks. The entities we audited understand they are accountable for protecting these systems from adverse events. They have established teams to manage corporate systems and water control systems. But they have not clearly defined roles and responsibilities, or held individuals accountable for their respective control environments.
- Security of critical infrastructure guidelines—the Australian Government guidelines for protecting critical infrastructure systems require the state government to assist critical infrastructure owners to implement security controls. However, Queensland has not yet established this assistance for water control systems.
- Identifying security risks—entities were not aware of some of the security risks for water control systems that related to information technology. This is because they did not critically assess each of the assets relating to water control systems and the need to protect them from physical and technical security breaches.
- Designing network controls—entities did not design their networks to provide adequate protection for control systems. They did not have adequate controls to secure the servers and workstations that connect users with the control systems. We understand that management cannot always keep water control systems up to date with technical controls, due to operational reasons and costs. However, we expect that entities will assess the risk of not implementing network security controls that compensate for vulnerabilities within water control systems.

- Communication—all entities have processes for obtaining and communicating relevant information about the security of information technology. However, they have not developed key performance indicators to measure the improvement in their security. In addition, the entities can improve their communication to staff about how to respond to security risks and issues.
- Security reviews—all entities have undertaken security reviews and penetration tests (tests of a computer system to find vulnerabilities that an attacker could exploit). However, they did not promptly address all the security issues raised by those reviews and tests. They limited the scope of penetration tests to cover mainly corporate networks and business systems—they did not include water control systems as targets for penetration tests.

Continuity of water systems

We assessed the ability of the entities to respond to, and fully recover from, security breaches relating to water control systems.

While all entities we audited have business continuity and resilience programs, they need to extend these to include all components of water control systems. None of the entities has comprehensive end-to-end processes for responding to a major security incident that would result in multiple systems failure.

All entities have disaster recovery plans for information technology and business continuity plans that they can invoke in the event of information technology systems failure. Both the information technology and operational technology teams know their components of the systems well and can respond to specific system outages in their own area. However, none of the entities has integrated information technology disaster recovery plans for all their information technology systems, including systems that external service providers may manage.

All entities advised that they could manually operate their smaller plants or parts of the larger drinking water and wastewater plants, if required. This would be a challenging task, depending on the skills, experience, and availability of critical staff. Therefore, all the entities need to ensure they are continually training staff and maintaining on-site manuals for individual components of water infrastructure. We note that each entity operates small sections of the plants manually during regular maintenance.

Recommendations

We recommend that the Department of Energy and Water Supply:

1. integrate information technology risks and cyber threats into the existing risk management framework for drinking water services and in the Queensland water and sewage service provider performance reports. (Chapter 2)
2. facilitate information sharing about adopting standards for securing information technology amongst entities that manage water control systems. (Chapter 2)

We recommend that the entities we audited:

3. improve oversight, identification and monitoring of information technology risks and cyber threats to water control systems. (Chapter 2)

   This should include:

   - clearly articulating and assigning roles and responsibilities for all parties, including any external service providers in securing the systems
   - maintaining a complete and up-to-date list of assets for water control systems and assessing the risk exposure of each asset
   - developing and implementing a security plan for water control systems based on risk assessments
   - implementing appropriate user access and authentication policies
   - using a phased approach to implementing the Australian Government's 'essential eight' security controls based on each entity's risk assessment
   - establishing performance indicators for security and periodically testing these controls to monitor the maturity and strength of defences built into the information technology control environment
   - improving understanding of how to manage information technology risks and how they relate to other forms of operational risks.

4. establish enterprise-wide incident response plans, business continuity, and disaster recovery processes for information technology. (Chapter 3)

   This should include:

   - testing the capability to respond to wide-scale information technology security incidents either through scenario testing or through desktop exercises
   - training staff to identify, assess, and have a coordinated response to information technology security breaches
   - adopting appropriate business continuity plans that include processes for reporting incidents to stakeholders and building on lessons learned
   - updating and testing information technology disaster recovery and business continuity plans to include processes to recover from a wide-scale information technology security breach
   - considering the impact of multiple system failures on business continuity planning and how entities can operate water and wastewater plants manually, if required.

Reference to comments

In accordance with section 64 of the *Auditor-General Act 2009,* we provided a copy of this report to the entities we audited. The entities have accepted all our recommendations.

We received comments from the Minister for Main Roads, Road Safety and Ports and Minister for Energy, Biofuels and Water Supply; the Department of Energy and Water Supply; and the Department of the Premier and Cabinet. Their responses are in Appendix A.

Report structure

Chapter	
Chapter 1	provides the background to the audit and the context needed to understand the audit findings and conclusions.
Chapter 2	examines whether water service providers have established effective security processes and controls for managing information technology risks.
Chapter 3	assesses whether water service providers have the capability to detect, respond and recover in the event of an attack.
Appendices	Appendix A contains responses received from agencies Appendix B describes the audit methodology Appendix C contains The Australian Signals Directorate—essential eight controls Appendix D explains information technology security assessments.

Report cost

This audit report cost $350 000 to produce.

1. Context

Queensland's water service providers protect the quality of drinking water by operating treatment plants that remove contaminants from the water. Some water service providers also treat and dispose of wastewater.

Because of the critical importance of clean drinking water to the community, it is vital that water service providers identify and manage the risks associated with this infrastructure. Entities cannot always prevent attackers from attempting to break into these systems, but they can strengthen their systems with appropriate controls to detect and recover from breaches.

Water service providers in Queensland

Water service providers monitor and control water transport, treatment and distribution. These include:

- the water distribution network for drinking water, reservoirs, and pump stations
- the collection and treatment of wastewater.

Water service providers in Queensland include:

- bulk water service providers and water authorities (Seqwater and Sunwater)
- drinking water service providers (primarily local governments).

Figure 1A describes the roles of these providers.

Figure 1A
Roles of water service providers

Entity	Roles
Queensland Bulk Water Supply Authority (trading as Seqwater)	sells and distributes bulk water to the following entities for South East Queensland: ▪ Queensland Urban Utilities covers Brisbane, Ipswich, Lockyer Valley, Scenic Rim, and Somerset ▪ Unitywater covers Sunshine Coast and Moreton Bay ▪ City of Gold Coast, Logan City Council, and Redland City Council.
Sunwater	sells and distributes bulk water to entities outside South East Queensland.
Local governments	sell and distribute water to households and manage wastewater.

Source: Queensland Audit Office.

Water control systems

Over 50 years ago, operators controlled water infrastructures manually—people walked around each facility, turning pumps on and off. Supervisory Control and Data Acquisition systems were first introduced in the 1960s to monitor and control water infrastructure remotely. In this report, we refer to Supervisory Control and Data Acquisition systems as water control systems.

Today, new technologies enable the systems to automate processes, collect and store information, produce analytics, and report real-time operational data. Further advances in wireless and digitally connected systems enable operators to access multiple sites remotely through the internet on any device, including a mobile phone. The entities we audited use water control systems to enable operators and facility personnel to monitor and control the water treatment plants locally and remotely.

Threats to water control systems

Attackers have been known to target water control systems to endanger public health and safety. This has resulted in overflows of untreated sewage, reductions in water pressure, or shutdowns in the distribution of water.

Water service providers sometimes connect their control systems to other networks and the internet. The risk of unauthorised access increases when systems are connected to other networks that may not be secure. However, security breaches can also occur when the operators do not connect the control systems to other networks. These breaches can occur through social engineering techniques and/or distributing malicious software (malware) via portable (USB) drives.

Examples of reported security incidents affecting control systems include the following:

- In April 2017, someone breached radio signals to trigger all emergency alarm systems used by the City of Dallas for tornado warnings and other emergencies. This person kept the alarms in action for 95 minutes.
- In March 2016, Verizon's security research reported the hacking of an unnamed water processing plant through unpatched web vulnerabilities in its internet-facing customer payment portal.
- In December 2015, there were attacks against three Ukrainian electrical distribution sub-stations where destructive malware was used in a broad and sophisticated cyber attack. This attack resulted in approximately 225 000 customers losing power for three hours.
- In August 2013, a security research company in the United States created a mock water utility system and received 74 security attacks from more than 16 countries. Ten of them were able to take complete control of the mock system.
- In 2011, infiltration of a water treatment and delivery plant in the US resulted in damage to a water pump through manipulation of water control systems.
- In 2010, an Iranian nuclear facility was infected with Stuxnet. Stuxnet is a malware detected in control systems running on Microsoft Windows. It had entered the facility's systems through an infected USB drive. According to published reports, Stuxnet ruined almost one fifth of Iran's nuclear centrifuges.
- In 2000, a security breach caused sewage overflow in Maroochy Shire. This incident was an act of revenge from a contractor who implemented the system. He changed the system control remotely causing approximately 800,000 litres of raw sewage to overflow into local rivers and parks.

Responsibilities for security of water systems

Several Australian Government entities play a role in setting guidelines and strategies for securing critical infrastructure, and assisting critical infrastructure owners when a security breach occurs. Water service providers own critical water infrastructure and are responsible for securing their own water assets.

Australian Government

Nationally, CERT Australia—the Computer Emergency Response Team—and the Australian Signals Directorate play advisory roles for the water service providers. CERT Australia advises on cybersecurity threats to owners and operators of Australia's critical infrastructure. The Australian Signals Directorate provides advice to mitigate targeted cyber or information technology intrusions. The Australian Signals Directorate 'essential eight' are well-regarded strategies for preventing up to 85 per cent of cyber security intrusions and are mandatory for the Australian Government.

Both CERT Australia and Australian Signals Directorate are partner agencies of the Australian Cybersecurity Centre. The Australian Government established the Australian Cybersecurity Centre in 2014 to combine cybersecurity capabilities across Australian governments.

In January 2017, the Australian Government established the Critical Infrastructure Centre to provide a coordinated approach to securing critical infrastructure. This centre also provides security advice to government about foreign-owned critical infrastructure. This is a new unit and is currently establishing its roles and approach to carry out its functions.

State government

At the state level, the Department of Energy and Water Supply regulates the water service providers' compliance with the *Water Supply (Safety and Reliability) Act 2008*. The safety of water supply in the legislation relates to making sure there is a supply of water, rather than providing information technology security. The legislation does not require the Department of Energy and Water Supply to provide guidance on information technology security for critical water infrastructure.

The responsibilities for setting information technology strategy and policies for Queensland Government departments sit with the Queensland Government Chief Information Officer. In February 2016, the Queensland Government Chief Information Officer also established a cybersecurity unit to expand whole-of-government protection against cyber threats.

However, the Queensland Government Chief Information Officer is not responsible for developing security policies, standards, or guidelines for critical infrastructure systems.

Water service providers

Each entity that owns critical water infrastructure is responsible for securing its own water assets. The entities we audited generally had two teams responsible for the security of water systems—information technology services and water operations. Each of the teams is responsible for securing its respective part of the water and wastewater systems. Figure1B details the roles and responsibilities of these teams.

Figure 1B
Water service provider responsibilities for securing water control systems by business unit

Business unit	Roles
Information technology services	Responsible for the information technology and security of computers, storage, and networking devices. This team may report to the chief financial officer, the general manager responsible for assets, or the director for organisational services.
Water operations	Responsible for installing and maintaining hardware and software for the water control systems and field devices. These are also known as operational technology. This team typically reports to the general manager of water operations.

Source: Queensland Audit Office.

Security standards and good practice

Queensland legislation does not define standards for the security of control systems.

However, the Information Technology Security Expert Advisory Group of the Australian Commonwealth Government's Trusted Information Sharing Network for Critical Infrastructure Resilience has developed some good practice guides. The following guides are available for use by operators of national critical infrastructure:

- *Generic Supervisory Control and Data Acquisition Risk Management Framework*
- *Supervisory Control and Data Acquisition Architecture Principles*
- *Knowing Your Supervisory Control and Data Acquisition Network*
- *Hardening of Supervisory Control and Data Acquisition ICT Systems*
- *Implementing Gateways*
- *Monitoring of Supervisory Control and Data Acquisition Networks.*

In addition to the Trusted Information Sharing Network guidelines, the Australian Signals Directorate published 35 strategies to mitigate targeted cyber intrusions. The Australian Signals Directorate also mandated the 'essential eight' from these strategies for Australian Commonwealth Government agencies. The Australian Signals Directorate has made these mandatory, based on research showing that these mitigate 85 per cent of the cyber intrusions investigated by the Australian Signals Directorate.

Many international standards also outline good practices for securing systems of value. These include:

- National Institute of Standards and Technology 2014, *Framework for improving critical infrastructure cybersecurity*
- The Committee of Sponsoring organisations of the Treadway Commission*, Internal Control—Integrated Framework*
- 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 27005:2012, *Information technology—Security techniques—Information security risk management*
- ISO/IEC 27031:2011, *Information technology—Security techniques—Guidelines for information and communications technology readiness for business continuity*
- National Institute of Standards and Technology 2008, *Technical guide to information security testing and assessment*
- Australian Signals Directorate, Australian Cyber Security Centre 2017*, Strategies to Mitigate Cyber Security Incidents*
- The 2015 *National Guidelines for Protecting Critical Infrastructure from Terrorism*—focuses on potential disruptions of infrastructure systems by terrorists
- The Critical Infrastructure Resilience Policy and Strategy
- The National Strategy for Disaster Resilience—provides a wider context for the work of the critical infrastructure centre
- AS/NZS 5050:2010, *Business continuity—Managing disruption-related risks.*

2. Managing control system risks

Chapter in brief

Water infrastructure owners need to actively protect control systems so they can operate as intended. In an effective control environment, management:

- sets an appropriate tone at the top about the importance of security and controls
- is clear about governance, roles and responsibilities
- establishes appropriate security policies and procedures
- develops robust risk management processes
- designs, implements, and monitors controls.

In this chapter, we assess the governance and oversight processes that the owners of water control systems use to manage information technology risks. We also assess whether the entities we audited have designed network architecture and implemented adequate security controls across the information technology environment to protect water control systems.

Main findings

- While several Queensland Government departments deal with counter-terrorism and response, no central agency is responsible for supporting critical water infrastructure owners to protect these systems from security events resulting from information technology risks.
- All entities we audited have appropriate information security policies, procedures, and organisation structures to manage water control systems. However, they have not clearly defined the roles and responsibilities for securing the information technology systems.
- All entities we audited have governance structures and frameworks in place to manage risks. However, they have not identified information technology security risks relating to all aspects of water control systems.
- All entities we audited need to strengthen the design of their information technology networks and tighten the controls relating to physical security, user access management and technical configuration of network devices, workstations, and servers.
- None of the entities audited had security plans or established security requirements for their water control systems. As a result, these entities did not measure and monitor key performance indicators relating to the strength of their controls.
- Each entity had staff awareness and training for security of information technology. However, none of the entities audited had comprehensive programs to educate staff about ways to prevent an intruder physically entering facilities and gaining access to systems.
- All entities audited undertook internal audits and security assessments. However, they did not always address risks promptly. In addition, there was inadequate monitoring of system activities to detect any covert misuse of these systems.

Introduction

The infrastructure for water supply consists of elements that pump, divert, transport, store, treat, and deliver safe drinking water. Entities that also manage wastewater have infrastructure to collect, pump, treat, and dispose of wastewater. These functions rely on industrial control systems that monitor and control the treatment, supply, distribution and, in the case of wastewater, appropriate disposal.

Entities are increasingly connecting control systems to corporate computer networks and to the internet. This opens them to internal and external threats. Therefore, critical infrastructure owners need to have a robust control environment in place to protect these systems so that they can continue to operate as intended.

Implementing optimal level of security requires owners of water control systems to:

- establish a control environment with management setting the tone from the top, with security policies, procedures and organisational structures and holding individuals accountable for their control environment
- implement risk management frameworks that enable management to identify risks and to develop a security plan for water control systems
- build security controls into the design of the information technology networks and computer systems to protect them from both internal and external unauthorised users
- obtain, use, and communicate relevant information on how the control environment functions
- monitor control activities and communicate control deficiencies for corrective actions.

In this chapter, we assess whether the water control systems we audited are secure and whether the owners of water control systems have adequate oversight in managing information technology risks and cyber threats. In addition, we examine and test entities' computer networks and the technical and process controls.

Audit conclusions

The water control systems we audited were not as secure as they should have been. This is because these entities did not identify some of the key risks and, therefore, did not have control processes in place to mitigate those risks.

While each entity had appropriate security policies, procedures and organisational structures in place, none of the entities has developed security plans for their water control systems. In addition, there is no state level support for the owners of water control systems about how to manage and report information technology risks.

Entities we audited can improve the way they are designing their networks or implementing controls to strengthen their defences against harmful attacks. In addition, the entities we audited did not always recognise the importance of the physical security of their offices when designing the security of their information systems.

One of the entities needs significant improvements in all areas of the control activities, from physical security of office buildings, to the design of the information technology systems and their connectivity to the critical infrastructure systems. The other entities had done work to strengthen their information technology security over recent years. All entities we audited had either planned or were planning projects that would address information technology security risks.

It is unlikely, at the time of testing, that the entities we audited would have promptly detected unauthorised access or covert misuse of the water control system because they did not always monitor activities within the computer network. Since our audit, these entities have reported to us that they have taken steps to improve their processes to monitor security incidents.

Establishing the control environment

All critical infrastructure owners we audited have established elements of a control environment, with appropriate information security policies and procedures, organisation structures, and management oversight committees.

Whole-of-government guidance and monitoring

There is a wide policy platform for information security across government and individual public sector entities. According to the Australian national guidelines for protecting critical infrastructure, state and territory governments and their agencies have a role in assisting owners of critical infrastructure with prevention, response, and recovery planning in their jurisdictions. It also states that critical infrastructure owners are responsible and accountable for protecting these systems.

Several departments, business units, and committees within Queensland Government deal with counter-terrorism and response activities. However, no central agency is responsible for setting policy and guidelines to protect critical infrastructure assets from security events resulting from information technology risks. The Australian Government has guidance material for protecting critical infrastructure, but the water service providers we audited are either not aware of, or are not implementing, key aspects of those guidelines.

The Department of Energy and Water Supply (DEWS) administers the *Water Supply (Safety and Reliability) Act 2008* and requires water service providers to develop a management plan for water quality. Within this plan, water service providers document hazards and hazardous events that may affect the quality of water.

DEWS provides a definition of a hazard in their guidelines. It has defined a hazard as 'a biological, chemical, physical or radiological agent that has potential to cause harm'. This definition does not include information technology or cyber threats that have the potential to affect the water control systems and cause them to stop operating as intended. As a result, DEWS does not provide guidance on how to secure critical infrastructure. Neither does DEWS require water service providers to implement security measures to protect the water control systems from information technology risks or cyber threats.

As the regulator for multiple critical water infrastructure entities, DEWS is in a good position to monitor that water service providers manage information technology risks. In addition, DEWS can encourage owners of water control systems to use standards and guidelines available nationally and internationally to design and implement security for their information technology environment.

Management oversight—owners of critical water infrastructure

A survey of six hundred corporate board directors and professionals from the National Association of Corporate Directors (NACD) in December 2016, reported that only 19 per cent believe their boards have a high level of understanding of cyber security risks. To improve the maturity of oversight for information technology risks, executive management needs to prioritise and consider information technology risks at an enterprise level.

In addition, those charged with governance need to seek answers about key aspects of information technology security risks that can have a significant impact on the entity. Figure 2A shows some of the key questions for senior management to consider.

Figure 2A
Key questions for senior management

Source: Queensland Audit Office.

Information security policies

While each of the entities had appropriate information security policies and procedures in place, we identified improvement opportunities for the entities in the following areas:

- One entity did not define security requirements for water control systems within their organisational level policies.
- One entity did not have service provider roles included in approved security policies.
- One entity did not comply with key aspects of its security policy to secure and monitor its water control systems.

Organisation structure

At each of the entities we audited, two teams had to work together to secure the water control systems: the information services team and the operations team.

Generally, operations teams manage the water control systems and information technology services teams manage the corporate networks and internet. This arrangement, involving separate teams to manage information technology and operational technology, is common for control systems. However, there is a trend for information technology and operational technology to converge and integrate to optimise business processes, and that has implications for how teams work together.

As the technologies converge, the teams need to collaborate and establish shared standards and processes to manage both information technology and operational technology. Lack of integration of the two teams increases the risk to the security of control systems. We found some indications of this risk materialising in all the entities we audited.

We found that:

- Those charged with governance have not clearly articulated the roles and responsibilities of the two teams in designing and implementing security for control systems.
- Operations teams have not documented the requirements for the security and availability of the corporate networks that are essential for protecting and operating control systems.
- Information technology teams do not always understand the impact of the corporate network on the security and availability of the water control systems.

One of the ways to improve the understanding of each team's roles is to document the information technology and operational technology environments and their respective roles and responsibilities. Those charged with governance need to notice the difference in the cultures of both teams and encourage collaboration and the mutual understanding of risks and their implications.

Identifying and assessing information technology risks

Risk management is the ongoing process of identifying, assessing and responding to risk. Entities we audited have identified several strategic level risks. However, two entities have not explicitly included information technology risks or cyber threats within their strategic risk registers. Therefore, they have not assessed the strategic impact of these risks materialising. One entity included cyber security risk in the strategic risk register but had not correctly recorded its own assessment of the maturity of the mitigating controls.

While these entities covered some of the risk areas for their corporate and business systems, they did not analyse those risks for water control systems. Figure 2B highlights examples of the areas of control that entities did not always apply to water control systems.

Figure 2B
Examples of gaps in risk treatments for water control systems

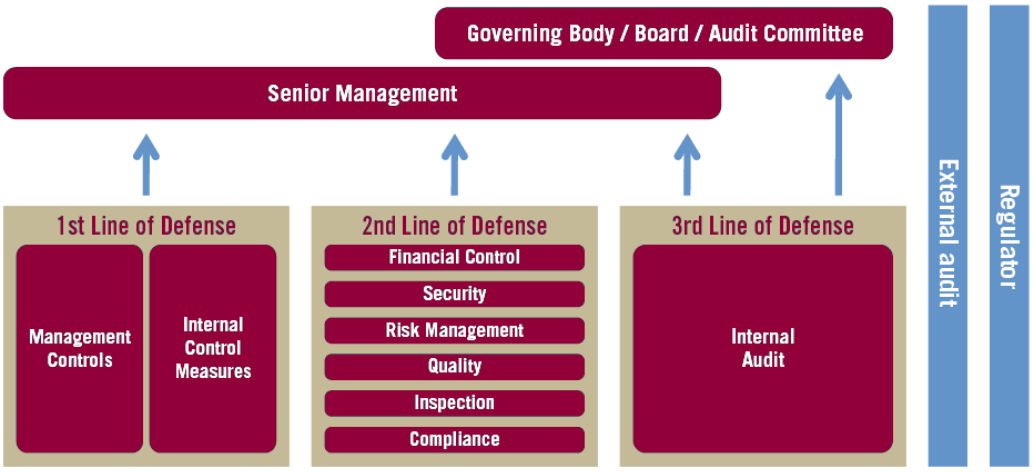
Areas of controls	Risk treatments	Gap in risk treatment for water control system
Governance	ICT governance frameworks are in place and consist of policies and procedures for information technology security.	Some entities did not define security requirements for water control systems. As a result, they did not apply information technology policies and procedures to water control systems.
Information security plan	Align security strategy with business strategic requirements.	ICT security strategy for water control systems is either in draft form, or does not exist. Critical systems and threats are not always documented. This limits the ability to formulate effective information security plans.
User access reviews	Perform user access review regularly on finance systems. This is to determine validity of users and appropriateness of access level.	Entities do not always review user access levels for water control systems.
Information classification controls	Review corporate information systems classification and realign controls.	Entities do not always apply information classification controls to critical infrastructure systems.

Note: ICT—information and communications technology.

Source: Queensland Audit Office.

To understand why all the entities we audited had gaps in identifying risks for water control systems, we mapped their processes to the Institute of Internal Auditors' risk management model. Many organisations use this model effectively as an integrated approach for managing risks. It constitutes three lines of defence as illustrated in Figure 2C.

Figure 2C
Three lines of defence model in risk management



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

Source: The IIA position paper: The three lines of defence in effective risk management and control, January 2013.

We found that all entities we audited could improve their practices of identifying and assessing risks in all three lines of defence.

Identifying and assessing risks as part of the first line of defence

As a first step, the entities need to identify their assets that connect with water control systems, and then to determine the threats and vulnerabilities related to those assets. These are key inputs in them assessing the impact and likelihood of security risks for each combination of assets. This process helps managers to prioritise and focus on the most important risks.

The next step is to design and implement only those controls that are required because of the risks. This also means that management cannot exclude some controls or put them on long-term plans simply because they are not convenient or are too costly.

If management decides not to implement some controls over a period, then they need to evaluate the risks they are accepting until they implement the controls. As managers implement controls to mitigate risks, they are implementing their first line of defence.

Identifying and assessing risks as part of second and third lines of defence

The entities we audited engaged external consultants as part of their second line of defence to review and provide recommendations to management for mitigating some of the risks. However, the entities did not promptly address some of the key risks that security reviews and audits identified. This indicates that entities need to improve their understanding of the consequences if security risks materialise. All entities have internal audits as their third line of defence to identify information technology risks.

Implementing control activities for information security

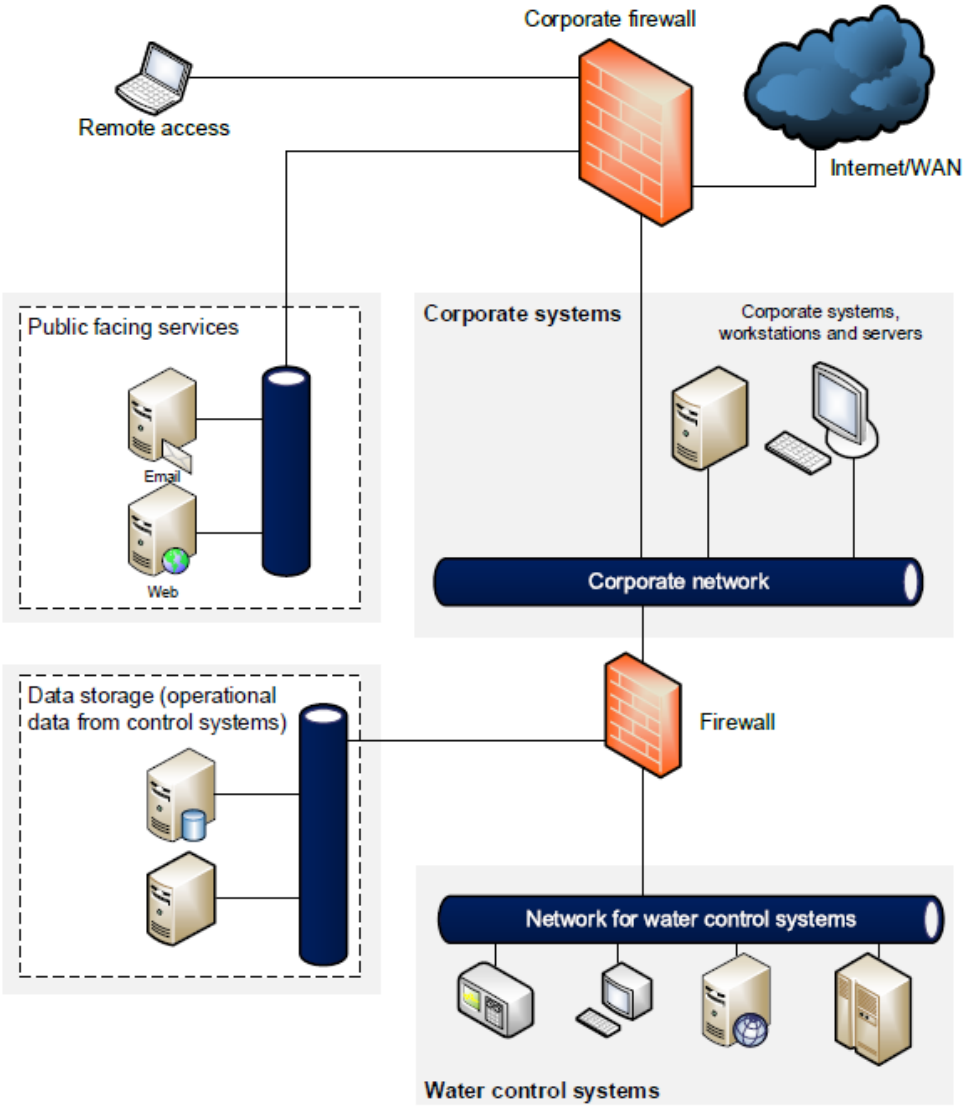
A sound security design within the computer network architecture is a crucial control. Entities can implement and configure security devices at various points within the network. In addition, entities can implement process controls, such as physical security and user access management, as well as technical controls to protect their servers and workstations from unauthorised access.

Information technology network architecture

Entities had not designed and implemented some of the network access controls effectively. This resulted in varying levels of separation within their corporate computer systems from the water control systems. Therefore, a security breach of their corporate network could potentially breach the security of the water control systems.

The Australian Government's Trusted Information Sharing Network guidelines recommend separate zones for control systems. In Figure 2D we illustrate how entities can organise their information technology networks to achieve this type of separation. It shows that entities can use security devices, such as firewalls, to separate various networks within the organisation. This illustration is a conceptual view of an information technology environment. Critical infrastructure owners need to assess their own environments and determine controls to suit their business.

Figure 2D
Example of network separation



Source: adapted from TISN Guidelines.

For the network design in Figure 2D to operate effectively, technical security controls within the devices on the network need to be implemented, as well as those connecting with the network.

Figure 2E highlights some of the essential practices that entities need to assess when designing controls for information technology networks. These can increase the effectiveness of separating the corporate network from control systems.

Figure 2E
Good practices—security of the information technology network

Controls that increase the effectiveness of information technology network security
Implement network segmentation to keep the control systems separate from other networks, including corporate systems and the internet. If a rule is relaxed for purposes of fixing issues, promptly tighten this after use.
Diligently manage user access controls, and regularly review and update network security.
Implement network access controls and system logging to detect unauthorised access and transfers of data from internal networks.
Use secure remote access methods and ensure external connections do not have full access to critical infrastructure systems.
Record logs of all connections to the control system networks. The lack of logs of network connections makes it harder, slower, and more expensive to investigate a security breach.
Use strong passwords, change default passwords and use more than two pieces of information to verify user identity, i.e. user name, password, and a security token for remote access.
Only enable network connections in public areas or meeting rooms when required.
Encrypt data that travels through the network. Connections without encryption can help a hacker to move from a basic compromise on the computer network to full access to key systems.
Enable the encryption services available within the radio communications devices.
Maintain awareness of vulnerabilities, implement security per vendor recommendations and decommission end-of-life systems as a priority.

Source: Queensland Audit Office.

Process and technical controls

While entities we audited had implemented security controls, the controls were not sufficient to protect water control systems from unauthorised access or targeted attacks. In this section, we discuss the strength of defences in the areas of physical security, access controls, servers and workstations, and staff awareness and training.

- **Physical security—**all entities audited had implemented different levels of physical security at their offices, public facilities, and water treatment sites. In conducting our audit tests, we tested security by attempting to gain unauthorised physical access into buildings. Not all offices had adequate controls to stop a member of the public from gaining access to the offices. As a result, we faced varying degrees of success in bypassing the physical security barriers to reach computers at each of the entities.

  Staff did not challenge people within the offices without a visitor or staff identification. We were also able to circumvent most procedural controls to gain access into buildings. Delays in detecting unauthorised physical access can increase the amount of damage done by intruders, and therefore the cost to recover from a physical security breach.

- **Access controls—**all entities we audited have developed access controls for water control systems but these are only partially effective. For example, entities used generic user identifiers and former staff still had access at the time of the audit. Some systems did not have strong password controls. These issues reduce the assurance that only authorised people can access the water processing interfaces.

- **Servers and workstations—**while all entities audited had implemented several security controls, they did not implement some of the controls within their servers and workstations.

  Entities had informal processes to assess the risks from security flaws in the software of the water control systems. They did not have risk-based plans to continuously review these and keep the software up to date with the recommendations of the software vendor.

  Controls for managing malicious software were ineffective as some computers had out-of-date software, while others did not have anti-virus installed. Where controls for malicious software are not effective, there is an increased risk of outages or the unauthorised manipulation of systems and related processes.

  Entities did not always address the security risks of lost or mobile workstations. We also found that entities did not enable encryption or implemented controls to make sure that users could only access authorised internet sites from some unsupervised computers. Lack of these technical controls increases the risk of unauthorised access to systems and data.

The Australian Signals Directorate recommends that entities implement a package of the essential eight controls as a baseline; this will make it harder for attackers to compromise systems. The Australian Signals Directorate's essential eight are provided in Appendix C.

Monitoring control environment

Control reviews

All entities audited undertook internal audit assessments and engaged external consultants to review and report on their control environments for information technology. In addition, they undertook various methods to test the strength of their controls. This included penetration testing, which is the practice of testing a system to find vulnerabilities that an attacker could exploit.

However, none of the entities moved quickly to fix the issues or mitigate risks that these reviews identified. The entities either incorporated the results of the assessments into longer-term programs of work or adopted a piecemeal approach to address some of the findings. In addition, the entities could not demonstrate that they improved their control environments after each penetration test. This is mainly because senior management did not prioritise information technology security risks for water control systems. In addition, the entities did not adopt a holistic approach for evaluating the overall information technology environment. In Appendix D, we have outlined various methods that entities can consider when developing plans for evaluating their control environment for information technology.

In addition, these entities have some monitoring tools that alert information technology staff to unusual events. However, none of the entities have a clear policy for recording, retaining or protecting security-related event logs.

Some water control systems did not generate activity logs; some systems retained logs for one day; while others retained logs for a few hours. In addition, the entities did not always monitor access logs for user activities within the network. Therefore, it is unlikely these entities would have detected unauthorised access or covert misuse of water control systems.

Information security reporting

All entities we audited have established processes for reporting on information security controls to managers and governance bodies. Two of these entities had ongoing security programs and projects. However, none of these entities defined and implemented key performance indicators to measure improvements in their control environment as they implement risk mitigation strategies.

We also noted there is a risk that staff could unwittingly help a security breach to occur. While each entity had awareness programs for the security of information technology, they did not have effective programs to ensure staff members were aware of intruder threats from breaching physical security. If staff members are not careful, they can allow unauthorised persons to gain physical access to office buildings. The entities we audited did not train their staff to challenge those that are in their building facilities and do not display identification.

We conducted an email campaign requesting a random sample of users to provide us with their user identification and passwords. Although about 20 per cent of users clicked on the emails and we attained some credentials, the information technology teams were quick to identify and block malicious sources of emails. A sound communication program can reduce the risk of users clicking on malicious links in emails by increasing awareness of staff in good control practices

3. Continuity of water systems

Chapter in brief

The two main functions of water control systems at the entities audited are:

- operating treatment and distribution plants for water and wastewater
- monitoring drinking water quality.

Computer-based attacks or malicious software can affect these services. High profile events increase the likelihood of these types of attacks.

In case of an attack, entities managing water control systems must respond quickly and efficiently to minimise the amount of damage to water and wastewater facilities and services.

This chapter outlines the capabilities of the entities we audited to detect, respond, and recover from wide-scale security incidents related to information technology.

Main findings

- Water service providers audited have processes to control and regularly test drinking water quality. This means they can detect and start responding to water quality issues within a reasonable timeframe.
- These entities have documented response and disaster recovery plans for information technology. They have tested these plans. But these plans do not cover all components of water control systems. Nor do they cover how they will respond to wide-scale information technology security incidents that result in multiple system failures.
- These entities reported that they could run their smaller plants or parts of their larger water and wastewater plants manually should the need arise, but only one entity has documented the manual procedures. They have tested running sections of the plants manually during regular maintenance, but none of the entities has tested the process for running the whole plant manually.
- Not all entities conduct regular competency training for site staff to run the plants manually.

Introduction

Entities can plan to operate continuously by identifying likely disruptive scenarios—such as natural disasters, power failures or cyber threats—and create plans to manage the effects. These plans are called disaster recovery plans.

New, diverse and more damaging attacks are emerging in relation to computer systems. It is imperative that entities respond efficiently and effectively to minimise the amount of damage and cost that may result from such a disruptive event.

The Australian/New Zealand Standard AS/NZS 5050: 2010 *Business continuity—Managing disruption-related risk* recommends that organisations' plans should cover not only their initial response to the incident, but also the steps necessary to recover systems and return to normal operations. Regular testing and review of these plans is equally important to ensure that team members have the knowledge and skills necessary to recover systems as required. Entities need comprehensive disaster recovery plans to fully restore information systems after initial recovery from an attack.

In this chapter, we assess whether the entities we audited have systems and processes in place to detect, respond, and recover from security incidents relating to information technology.

Audit conclusions

All entities audited either have, or can access, the capability to respond to a breach of information security. To recover the water control systems, they depend on the capabilities and availability of their internal operations and technology teams and the vendors of the water control systems.

Their disaster recovery plans and testing do not cover all aspects of the water control systems. They fall short of providing assurance that they would be able to recover these systems within a timely manner. The plans do not include information on how they will identify, respond, and recover from a harmful incident involving the water control systems.

We acknowledge that some entities have used these plans to recover their systems after a natural disaster. However, they have not planned for a wide-scale security incident that can occur without notice and affects multiple computer systems at the same time. Nor do the plans consider the scenario where the entities need to operate the plants manually. While all entities audited have operated sections of a plant manually during maintenance, they have never tested running the whole plant manually. Only one entity has documentation to manage such an event.

Detecting water quality issues

It is likely that the entities we audited will detect issues with the quality of drinking water within a reasonable timeframe. This is because they control the quality of drinking water using two approaches. Firstly, the water service providers program the control systems to release the appropriate levels of chemicals, such as chlorine, into drinking water. Secondly, the entities perform chemical tests on the water outputs daily. In addition, there is a time lapse of at least one day before the treated water reaches households. This gives water service providers time to address any water quality issues that they detect.

One of the entities we audited leads the way in implementing innovative solutions to monitor the quality of drinking water. These innovations have the potential to improve the speed with which water service providers can detect changes in water quality. Case study 3A shows this.

Figure 3A
Case study on improving water quality monitoring

Innovation in monitoring water quality
The audited entity is improving the speed of detecting water quality issues by: ▪ collaborating with a university to define what the water is normally made up of in terms of various chemicals and compounds i.e. its baseline composition. The entity plans to compare the results of water testing performed daily during major events to determine whether there are changes in the concentration of known or unknown compounds ▪ implementing systems and processes that record the water distribution system through a geographical information system. The entity uses this system to analyse and display chlorine residuals to identify priority areas for the disinfection program ▪ implementing online water quality analysers to continuously monitor parameters such as pH, chlorine etc. to identify contamination in the drinking water These projects have many potential benefits for efficient monitoring of water quality.

Source: Queensland Audit Office.

Responding to security incidents

Even when an entity has established a strong control environment, persistent attackers with advanced capabilities can breach security. For this reason, it is important to implement and test incident response plans. In addition, entities need to train staff to use the plans, so they have an agreed and coordinated approach for responding to incidents.

The entities we audited have developed documentation for emergency and incident management. They have also conducted some testing of their response capability. However, these entities have not:

- assessed the impact that a sustained information technology security incident would have on operations
- established processes on how information technology and water operations teams would coordinate their activities when responding to wide-scale information technology security breaches and major system outages
- documented the end-to-end processes and procedures for responding to information technology security incidents across information technology and operations teams
- trained staff to identify, assess and respond to information technology security breaches.

Recovering information systems

A disaster recovery plan for information technology is a set of procedures to recover from a computer systems failure. It includes the systems and the priority for restoring each one. It also includes a list of stakeholders and communication protocols in the event of a disaster.

While all entities have disaster recovery plans for their corporate systems, they do not include recovery of water control systems. Nor have the entities reviewed and updated their plans for disaster recovery, considering wide-scale computer security incidents. As a result, there is no assurance that the entities could restore a fully compromised water control system within a timeframe acceptable to the business.

The water operations teams are responsible for managing their own servers, workstations and control systems. These teams typically know their systems well and have previously responded to incidents related to their own environments. However, without documentation for the recovery of these systems, an effective recovery process will be difficult if teams with specific site knowledge are not available.

In addition, contracts with any external service providers for information technology did not always include:

- roles and responsibilities for the recovery of control systems that may be managed internally or by external service providers
- key performance indicators, such as, maximum acceptable outage and recovery time objectives for water control systems.

Manually operating water and wastewater treatment plants

The water treatment plants and pumps contain additional (redundant) systems, aimed at minimising downtime. In the event of a control systems failure, all entities audited reported to us that manual operation of the smaller plants is possible for a short period. The entities we audited have not determined the periods for which they can run the plants manually.

One of the entities believes that it can manually operate the larger wastewater treatment plants. While such an endeavour would be challenging, this entity believes it has the expertise and training to operate its plants manually. This is because this entity:

- conducts competency training for site staff
- maintains onsite manuals for individual system components.

While all entities audited have operated sections of a large plant manually during maintenance, they have never tested running the whole plant manually.

Appendices

Appendix A—Full responses from agencies

As mandated in Section 64 of the *Auditor-General Act 2009*, the Queensland Audit Office gave a copy of this report with a request for comments to the audited entities.

The head of these agencies are responsible for the accuracy, fairness and balance of their comments.

Comments received from Director-General, Department of Energy and Water Supply

RECEIVED
22 JUN 2017
QUEENSLAND AUDIT OFFICE

Queensland Government

Department of
Energy and Water Supply

1 William Street Brisbane
PO Box 15456 City East
Queensland 4002 Australia
Telephone + 61 7 3137 4296
Website www.dews.qld.gov.au
ABN 91 416 908 913

Our reference: CTS 15856/17

22 JUN 2017

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

Dear Mr Close

Re: Performance audit on security of critical water infrastructure Departmental feedback

Thank you for your letter of 30 May 2017.

Please find attached the completed agency response form as requested. The completed form indicates support for the departmental specific recommendations detailed in the proposed report to parliament on the performance audit on the security of critical water infrastructure undertaken by the Queensland Audit Office.

The water industry in Queensland is unique in Australia. Queensland has 86 registered providers of drinking water services operating over 300 individual supply systems. Forty-four percent of these systems supply to less than 1000 connections. Many of these supply systems are located in very remote, isolated areas and are operated manually. This unique environment has been taken into account when developing the detailed actions as described in the attached form, that will be undertaken by the department to implement the report recommendations.

If you require further information please contact Mrs Toni Stiles, Director – Water Supply Regulation on .

Yours sincerely

Paul Simshauser
Director-General
Department of Energy and Water Supply

Att: QAO departmental response form

Responses to recommendations

Queensland Audit Office
better public services

Department of Energy and Water Supply, Security of critical water infrastructure (Report No. XX: 2016–17)

Response to recommendations provided by Director-General, Department of Energy and Water Supply on 22 June 2017.

Recommendation	Agree / Disagree	Timeframe for implementation (Quarter and year)	Additional comments
We recommend that the Department of Energy and Water Supply: 1. Integrate information technology risks and cyber threats into the existing risk management framework for drinking water services and in the Queensland water and sewage service provider performance reports (Chapter 2)	Agree	Completed by end Q4 2018	Inclusion of information technology and cyber security risks into drinking water quality management plan risk management framework and associated reporting (incidents, audit and annual) Development of appropriate information technology and cyber security related performance key performance indicators for steering committee agreement. Inclusion of agreed KPI's into the annual reporting framework
2. facilitate information sharing about adopting standards for securing information technology amongst entities that manage water control systems. (Chapter 2)	Agree	Completed by end Q4 2018	Use existing networks and stakeholder engagement activities to identify and develop an appropriate standards framework (based on existing documents, such as AS) and identify the entities potentially at risk. Support this work with explanatory information/ guidance resources on DEWS website

1

Comments received from the Minister for Main Roads, Road Safety and Ports, Minister for Energy, Biofuels and Water Supply

Queensland Government

The Honourable Mark Bailey MP
Minister for Main Roads, Road Safety and Ports
Minister for Energy, Biofuels and Water Supply

Our Reference: CTS 15244/17

Level 34, 1 William Street Brisbane 4000
GPO Box 2644 Brisbane
Queensland 4001 Australia
Telephone +61 7 3719 7300
Email energyandwatersupply@ministerial.qld.gov.au
Website www.dews.qld.gov.au

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

Dear Mr Close Anthony,

Re: Performance audit on security of critical water infrastructure departmental feedback

Thank you for your letter regarding the performance audit on security of critical water infrastructure departmental feedback.

Please find attached the completed agency response form as requested. The completed form indicates support for the departmental specific recommendations detailed in the proposed report to parliament on the performance audit on the security of critical water infrastructure undertaken by the Queensland Audit Office.

The water industry in Queensland is unique in Australia. Queensland has 86 registered providers of drinking water services operating over 300 individual supply systems. Of these systems, 44 per cent supply to less than 1000 connections. Many of these supply systems are located in very remote, isolated areas and are operated manually. This unique environment has been taken into account when developing the detailed actions, as described in the attached form that will be undertaken by my department to implement the report recommendations.

Yours sincerely

Mark Bailey MP
Minister for Main Roads, Road Safety and Ports and
Minister for Energy, Biofuels and Water Supply

Att: QAO Departmental response form

Responses to recommendations

Queensland Audit Office
better public services

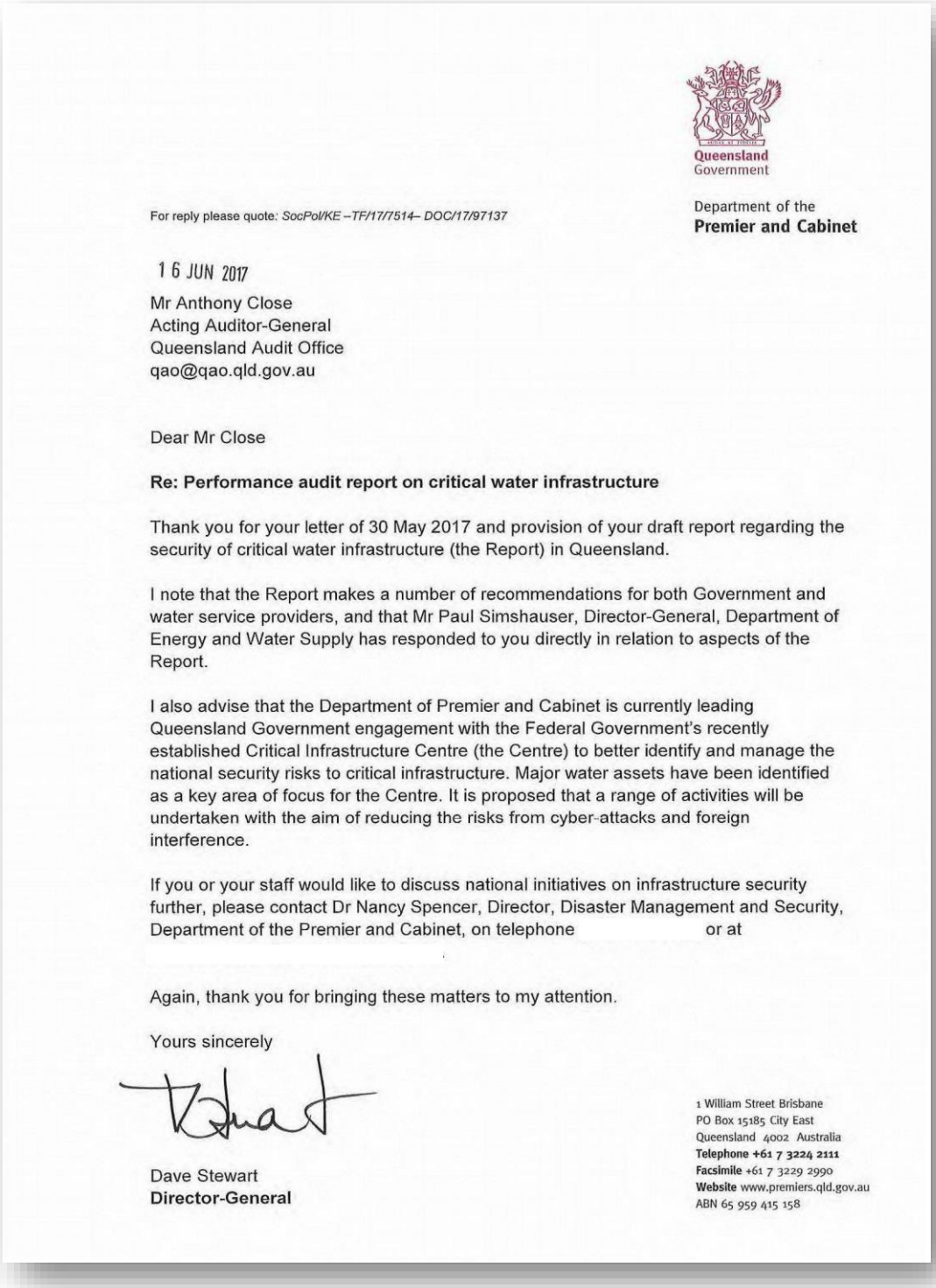
Department of Energy and Water Supply, Security of critical water infrastructure
(Report No. XX: 2016–17)

Response to recommendations provided by Director – Water Supply Regulation, Department of Energy and Water Supply on 31 May 2017.

Recommendation	Agree / Disagree	Timeframe for implementation (Quarter and year)	Additional comments
We recommend that the Department of Energy and Water Supply: 1. integrate information technology risks and cyber threats into the existing risk management framework for drinking water services and in the Queensland water and sewage service provider performance reports (Chapter 2)	Agree	Completed by end Q4 2018	Inclusion of information technology and cyber security risks into drinking water quality management plan risk management framework and associated reporting (incidents, audit and annual) Development of appropriate information technology and cyber security related performance key performance indicators for steering committee agreement. Inclusion of agreed KPI's into the annual reporting framework
2. facilitate information sharing about adopting standards for securing information technology amongst entities that manage water control systems. (Chapter 2)	Agree	Completed by end Q4 2018	Use existing networks and stakeholder engagement activities to identify and develop an appropriate standards framework (based on existing documents, such as AS) and identify the entities potentially at risk. Support this work with explanatory information/ guidance resources on DEWS website

1

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



Queensland Government

Department of the **Premier and Cabinet**

For reply please quote: *SocPol/KE –TF/17/7514– DOC/17/97137*

16 JUN 2017

Mr Anthony Close
Acting Auditor-General
Queensland Audit Office
qao@qao.qld.gov.au

Dear Mr Close

Re: Performance audit report on critical water infrastructure

Thank you for your letter of 30 May 2017 and provision of your draft report regarding the security of critical water infrastructure (the Report) in Queensland.

I note that the Report makes a number of recommendations for both Government and water service providers, and that Mr Paul Simshauser, Director-General, Department of Energy and Water Supply has responded to you directly in relation to aspects of the Report.

I also advise that the Department of Premier and Cabinet is currently leading Queensland Government engagement with the Federal Government's recently established Critical Infrastructure Centre (the Centre) to better identify and manage the national security risks to critical infrastructure. Major water assets have been identified as a key area of focus for the Centre. It is proposed that a range of activities will be undertaken with the aim of reducing the risks from cyber-attacks and foreign interference.

If you or your staff would like to discuss national initiatives on infrastructure security further, please contact Dr Nancy Spencer, Director, Disaster Management and Security, Department of the Premier and Cabinet, on telephone or at

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

Yours sincerely

Dave Stewart
Director-General

1 William Street Brisbane
PO Box 15185 City East
Queensland 4002 Australia
Telephone +61 7 3224 2111
Facsimile +61 7 3229 2990
Website www.premiers.qld.gov.au
ABN 65 959 415 158

Appendix B—Audit objectives and methods

Audit objective

The objective of the audit was to assess whether systems used to operate, manage, monitor water infrastructure are secure, and effective processes are in place to recover from adverse events.

Reason for the audit

We conducted the audit for the following reasons:

- The need for secure critical infrastructure. Recent security threats highlight the need to strengthen systems security for all critical infrastructure. Critical infrastructure owners can adopt some of the learnings from a number of security breaches on these systems worldwide.
- The heightened security risks and cyber attacks leading up to Commonwealth Games. Security research shows an increase in cyber attacks on countries and organisations hosting major events.
- In our previous audit of systems used to manage traffic, we found that the related control systems were not secure and susceptible to targeted attacks. It is time to ascertain whether water control systems have the required level of security.

Performance audit approach

The audit was conducted between August 2016 and May 2017.

Figure B1
Audit approach

Audit area	Approach
Security of water control system	▪ Evaluate the governance and oversight function for security of water control systems from the perspective of the whole of government and the entities we audited ▪ Evaluate the security and control designs of the water control systems ▪ Conduct 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 we can use to plan for a penetration attack.
Business continuity management	▪ 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.

Source: Queensland Audit Office.

Appendix C—The Australian Signals Directorate—essential eight controls

Figure C1
Key controls the Australian Signals Directorate recommends

Control	Description and practical application
Application whitelisting	A whitelist only allows selected applications to run on computers. While this needs to be applied across the board on all computers, entities can take a phased approach, implementing in risky areas first, for example, on computers in meeting rooms.
Patch application	A patch fixes security vulnerabilities in software applications. Entities need to schedule security patches into their maintenance process and assess the risks of not applying any security patches that the vendor is recommending.
Disable untrusted Microsoft Office macros	Microsoft Office applications can use software to automate routine tasks. Entities need to secure or disable these macros as adversaries are increasingly using these to download malware.
User application hardening	Block web browser access to Adobe Flash Player, web ads and untrusted Java code on the internet. These are popular ways to deliver malware to infect computers.
Restrict administrative privileges	These should be restricted to only those that need them. Admin accounts are keys to the kingdom and those that have this type of access should only use it to install software and apply patches. Those users should have separate accounts for their day-to-day operational work.
Patch operating systems	A patch fixes security vulnerabilities in operation systems. Entities need to schedule security patches into their maintenance process and assess the risks of not applying any security patches that the vendor is recommending.
Multi-factor authentication	The user is only granted access after successfully presenting multiple, separate pieces of evidence. Entities can use physical tokens, passphrase and/or biometric data.
Daily backup of important data	Regularly back up all data and store it securely offline. That way your organisation can access data if it suffers a cyber security incident.

Source: Australian Signals Directorate—Essential Eight.

Appendix D—Assessing information technology security

Assessing the security of information technology involves inspecting the environment, policies and security controls. Its main purpose is to determine the strength of the entity's defences in protecting the systems under review. Testing the controls can help in planning for unforeseen gaps in security risks and threats that the entity has not addressed.

Due to the complexities of systems and the continuous evolution of hackers and vulnerabilities, passing security tests is not an indication that flaws do not exist. Nor does it indicate that the system adequately satisfies the security requirements. New hacking techniques are continuously developed and easily accessible online. For this reason, a continuous review and improvement program is essential in protecting key systems from security threats and vulnerabilities.

Evaluating the strength of the information technology control environment

There are a number of techniques to evaluate the control environment. Typically, entities use a combination of these methods when conducting assessments. In this section, we discuss three methods of evaluating information technology controls:

- examining information technology controls
- penetration testing
- red teaming.

Examining detailed information technology controls

This method, when compared with other testing methods, does not provide definite proof that attacks are possible and does not clearly demonstrate the potential impact of an attack. Entities can use this method to assess the applicable threats and potential consequences of a breach.

This type of testing typically involves:

- Examining policies and procedures to assess whether the controls within the documents address potential risks. In addition, the entity needs to assess whether staff members follow the policies and procedures.
- Assessing the network design and mapping these to any existing security plans to determine whether the design is consistent with the plan.
- Testing the security of information technology infrastructure. Examples of this test includes:
    - analysing the firewall configuration and assessing access controls for network traffic
    - testing message transfers to evaluate the type of access across the network
    - assessing network devices, servers and other network infrastructure for security vulnerabilities (vulnerability scanning)
    - confirming security vulnerabilities exist without exploiting them.

It is important to distinguish vulnerability scanning from penetration testing. Vulnerability scanning only reports known vulnerabilities that exist within systems.

Penetration testing

Penetration testing is an authorised simulated attack on a computer system. The penetration tester is given a defined scope and a particular goal. The primary goal of penetration tests is to find vulnerabilities that an adversarial attacker can exploit, and to recommend mitigation strategies.

Reports from this type of test include potential impacts of the vulnerabilities and entities can use these to inform the business security risk assessment. This type of testing shows the risk of not fixing security issues. These are more expensive and riskier than evaluating information technology controls and can affect system availability and data integrity.

Penetration testing consultant

The quality of the penetration test is directly proportional to the kind of expertise that the penetration testing consultants have. Figure D1 includes key questions that entities can consider when selecting a penetration tester.

Figure D1
Selecting a penetration tester

Questions to consider when selecting a penetration tester
Does the supplier's methodology follow or exceed guidelines of the National Institute of Standards and Technology, Open Web Application Security Project, Open Source Security Testing Methodology Manual, and Penetration Testing Execution Standards?
Are the supplier's staff experienced security professionals? Do they hold recognised certifications for penetration testing?
Does the supplier have sufficient technical consultants that work on the security assessments?
How does the supplier present the deliverables? Do they include detailed findings and recommendations for addressing security issues?
Is the supplier a recognised contributor within the security industry?
Has the lead penetration tester done any of the following? ▪ positively demonstrated a clear track record or performance ▪ published research papers ▪ made presentations at various local and international conferences ▪ gained relevant certifications.

Source: Queensland Audit Office.

Red teaming

A red team differs from a penetration test. The red team performs a controlled, simulated attack on an entire organisation. It uses all resources available to gain complete control of an entity's systems.

The objective of the test is to assess the ease with which an entity can be compromised. Unlike a penetration test, the single purpose of red teaming is to gain compromise. To achieve this, the team will attempt but not be limited to the following:

- masquerade as the entity's staff members to obtain or tamper with physical systems
- produce malicious systems that mimic those of the entity to convince employees to use them
- attack external systems to bypass weak security controls

Results and reports of red teaming provide information on the impacts of a compromise. Entities can use it to evaluate the security of people, process and technology of the business. However, as the red team uses the path of least resistance, the results may not provide the breadth and depth of coverage.

Entities can design this exercise so that the red teams can work with an internal team that would defend the red team's attempts to compromise the system. In this scenario, we refer to the internal team as the blue team. A new approach is also emerging, whereby entities can establish a purple team to enhance the collaboration between the red and blue teams. Figure D2 describes each team's characteristics.

Figure D2
Team compositions for penetration tests

Team Name	Description of their function
Red team	An external entity brought in to test the effectiveness of a security program. The entity emulates the behaviours and techniques of likely realistic attackers. This is similar, but not identical to penetration testing.
Blue team	This is the internal security team. Its primary objective is to defend against attempts to compromise the organisation. This is distinguished from security and operations teams as blue teams have a mentality of constant vigilance.
Purple team	The primary goal of this team is to facilitate integration between the red and blue teams and to provide feedback for improving their respective processes. This also assists the blue team to address the security gaps that the red team identifies.

Source: Daniel Miessler, Information Security Practitioner—The difference between red and blue teams.

Auditor-General reports to parliament

Reports tabled in 2016–17

Number	Title	Date tabled in Legislative Assembly
1.	Strategic procurement	September 2016
2.	Forecasting long-term sustainability of local government	October 2016
3.	Follow-up: Monitoring and reporting performance	November 2016
4.	Criminal justice system—prison sentences	November 2016
5.	Energy: 2015–16 results of financial audits	December 2016
6.	Rail and ports: 2015–16 results of financial audits	December 2016
7.	Water: 2015–16 results of financial audits	December 2016
8.	Queensland state government: 2015–16 results of financial audits	December 2016
9.	Hospital and Health Services: 2015–16 results of financial audits	January 2017
10.	Effective and efficient use of high value medical equipment	February 2017
11.	Audit of Aurukun school partnership arrangement	February 2017
12.	Biosecurity Queensland's management of agricultural pests and diseases	March 2017
13.	Local government entities: 2015–16 results of financial audits	April 2017
14.	Criminal justice system—reliability and integration of data	April 2017
15.	Managing performance of teachers in Queensland state schools	April 2017
16.	Government advertising	May 2017
17.	Organisational structure and accountability	May 2017
18.	Universities and grammar schools: 2016 results of financial audits	June 2017
19.	Security of critical water infrastructure	June 2017

www.qao.qld.gov.au/reports-resources/parliament