New South Wales Auditor-General's Report

Performance Audit

Security of Critical IT Infrastructure

Transport for NSW
Roads and Maritime Services
Sydney Water Corporation

audit office
OF NEW SOUTH WALES

The role of the Auditor-General

The roles and responsibilities of the Auditor-General, and hence the Audit Office, are set out in the *Public Finance and Audit Act 1983*.

Our major responsibility is to conduct financial or 'attest' audits of State public sector agencies' financial statements. We also audit the Total State Sector Accounts, a consolidation of all agencies' accounts.

Financial audits are designed to add credibility to financial statements, enhancing their value to end-users. Also, the existence of such audits provides a constant stimulus to agencies to ensure sound financial management.

Following a financial audit the Audit Office issues a variety of reports to agencies and reports periodically to parliament. In combination these reports give opinions on the truth and fairness of financial statements, and comment on agency compliance with certain laws, regulations and government directives. They may comment on financial prudence, probity and waste, and recommend operational improvements.

We also conduct performance audits. These examine whether an agency is carrying out its activities effectively and doing so economically and efficiently and in compliance with relevant laws. Audits may cover all or parts of an agency's operations, or consider particular issues across a number of agencies.

Performance audits are reported separately, with all other audits included in one of the regular volumes of the Auditor-General's Reports to Parliament – Financial Audits.

audit.nsw.gov.au

auditoffice
OF NEW SOUTH WALES

AUDITOR-GENERAL NEW SOUTH WALES

GPO Box 12
Sydney NSW 2001

The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 38E of the *Public Finance and Audit Act 1983*, I present a report titled **Security of Critical IT Infrastructure, Transport for NSW, Roads and Maritime Services, Sydney Water Corporation**

Grant Hehir
Auditor-General
21 January 2015

Contents

Executive summary

Background

Systems used to control critical infrastructure are known as process control systems or operational technology. Previously, these types of systems were isolated from other networks and the security of these systems depended largely on restricting access to their physical infrastructure. However, in the last two decades their interconnectivity with other networks, for operational purposes, has increased the risk of unauthorised users obtaining access to these systems and disrupting reliable operation of critical infrastructure.

To illustrate, in June 2010, an anti-virus security company reported the first detection of malicious software (malware) that attacks process control systems. The malware is called Stuxnet and it has been found on hundreds of systems internationally. In August 2013, a security research company in the United States created a decoy water utility system; it experienced 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. In 2000, a disgruntled former employee compromised a control system and caused the dumping of 800,000 litres of untreated sewage into waterways in Maroochy Shire, Queensland.

This audit examined whether the systems used to operate and manage critical infrastructure in the Sydney metropolitan water supply system and the NSW traffic signal network are secure and, if systems go down, whether there are sound recovery arrangements in place. The audit considered whether:

- controls to prevent, detect and respond to security breaches are effective
- the risk to business continuity is being managed appropriately.

Due to the sensitive nature of this topic area, detailed findings and recommendations have been provided to agencies in separate management letters.

Conclusions

Roads and Maritime Services and Transport for NSW

Roads and Maritime Services (RMS) and Transport for NSW (TfNSW) have deployed many controls to protect traffic management systems. However the systems in place to manage traffic signals are not as secure as they should be. Established controls are only partially effective in detecting and preventing incidents and are unlikely to support the goal of a timely response to limit impacts to traffic management.

A range of risks are adequately managed, however, there are other risks where control improvements are recommended. For example, there is a potential for unauthorised access to sensitive information and systems that could result in traffic disruptions, and even accidents in one particular section of the road network.

Management has designed and tested an emergency response capability for the Traffic Management Centre (TMC) for some disaster scenarios and has recently identified and initiated improvements for responding to IT related disasters.

Until the IT disaster recovery site is fully commissioned, a disaster involving the main data centre would have traffic controllers operating on a regional basis without the benefit of intervention from the TMC in managing traffic coordination, which means higher congestion is likely in the short term.

Sydney Water Corporation

Sydney Water Corporation (SWC) is well equipped to deal with the impact of security incidents. It has developed and tested procedures for security incidents and major outages and has provided relevant training to staff. It has established a back-up operations centre which is tested on a regular basis, and also established redundant systems such as additional control units and backup power supplies for selected key facilities.

Whilst SWC's response capability is good, it is limited by its inability to detect all security breaches. Controls to prevent and detect breaches are not as effective as they could be. Controls have been implemented to limit a number of risks, however, the protection environment requires improvement to defend against targeted attacks. For example, any malicious activity on most of the corporate network is blocked from accessing the process control system environment but control level access is possible from selected low security workstations on the corporate network.

Key recommendations

RMS and TFNSW, by July 2015, should:

1. Extend the Information Security Management System (ISMS) to oversee the security of the complete traffic management environment, including operational level risks.
2. Develop a comprehensive security plan for the whole environment.
3. Improve the identification, assessment and recording of security risks.
4. Improve logging and monitoring of security related events regarding access to applications, operating systems and network access.
5. Improve security zoning to better protect the system from potential threats.

SWC, by July 2015, should:

6. Extend the Information Security Management System (ISMS) to oversee the security of the process control environment, including the management of operational level risks and controls.
7. Develop a comprehensive security plan for the whole environment (building on SWC's SCADA security policy).
8. Document and undertake additional risk mitigation to reduce risks to acceptable levels, and clearly document what levels of risk can be tolerated.
9. Obtain current documentary evidence to indicate that the risks associated with the security of process control systems at Prospect Treatment Plant are mitigated to acceptable levels.
10. Determine the appropriate controls to limit unauthorised access to computer accounts including SCADA application software and computer operating systems.

Other government agencies with critical infrastructure should seek to determine whether there are lessons from this audit that may apply to their area of government services/business. This includes ensuring:

11. The organisation's ISMS covers business processes and technology including systems used to control infrastructure.
12. Compliance with the NSW Government Digital Information Security Policy (DISP). For State Owned Corporations, this requirement should be incorporated into their Statements of Corporate Intent.
13. A comprehensive security plan is maintained for technical systems supporting critical government services where the system requires additional protection above the baseline controls utilised for the remainder of the agency's systems.
14. Management receives and acts on information security/availability risk assessments that define the current and target risk levels.

The Office of Finance and Services, NSW Treasury, should:

15. Ensure lessons learnt in this audit are communicated to all relevant government agencies
16. Undertake regular reviews to ensure that relevant agencies are complying with the Digital Information Security Policy and that the policy is meeting its objectives.

Detailed recommendations are contained in the body of this report.

Response from Transport for NSW and Roads and Maritime Services

NSW GOVERNMENT | Transport for NSW

SO Ref: SO14/23422

Grant Hehir
Auditor-General
Audit Office of NSW
Level 15, 1 Margaret Street
Sydney NSW 2000

Dear Mr Hehir,

Performance Audit: Security of Critical IT Infrastructure – Traffic Management Systems

Thank you for the opportunity to respond to the *Security of Critical IT Infrastructure – Traffic Management Systems* audit dated 17 December 2014.

As the Audit Office is aware, the traffic management systems that were audited form a set of interoperable systems managed across the Transport cluster. Transport notes that the audit identified opportunities to improve management of the security of these systems.

Over the years, agencies that are now part of Transport cluster have spent considerable effort to ensure NSW has safe and reliable traffic management systems. One key system, SCATS, monitors and manages some 4,000 traffic light intersections across NSW. SCATS continues to be developed by Roads and Maritime Services and is now implemented in 27 countries around the world. Another key system is the Electronic Lane Control System which monitors and controls lanes across the Sydney Harbour Bridge.

Transport has undertaken considerable testing to verify that best-practice controls have been appropriately implemented to assure the safety of these systems. Whilst Transport accepts that there is a possibility for unauthorised access to sensitive information and systems, as there is for all inter-connected industrial control systems, we refute the suggestion the result could "*...cause accidents on one particular section of the road network*". Transport has since provided the Audit Office documentation to that effect.

Transport is committed to enacting the improvements that are detailed in our management responses for each item within the Management Letter.

Dave Stewart
Secretary
- 9 JAN 2015

18 Lee Street Chippendale NSW 2008
PO Box K659 Haymarket NSW 1240
T 8202 2200 F 8202 2209
www.transport.nsw.gov.au
ABN 18 804 239 602

Response from Sydney Water Corporation

13 January 2015

Mr Grant Hehir
Auditor-General
Audit Office of NSW
GPO Box 12
SYDNEY NSW 2001

Performance audit report – Security of Critical IT Infrastructure

Dear Mr Hehir,

Sydney Water welcomes the performance audit of our critical IT systems used to deliver water and wastewater services to our customers. Sydney Water considers these operations to be extremely important to ensure safe, reliable products continue to be produced and supplied to customers within our area of operations.

As noted by the auditor, Sydney Water is well equipped to deal with the impact of security incidents. Developed and tested procedures exist for response to security incidents and major outages. Multiple redundancies are also in place to ensure security is maintained such as the operation of a 24/7 monitoring centre with back-up systems and processes for key facilities and control units.

The report provides 11 recommendations that are specific to Sydney Water and our response to each recommendation is detailed in the appendix provided. Sydney Water acknowledges that there is room for improvement in some areas particularly those relating to formal documentation.

Sydney Water disagrees with the implication in the report that there is an issue with the risk management processes used by Degremont at Prospect Water Treatment Plant. Contracts with our partners include stringent clauses requiring them to ensure the security of systems and water supplies. In addition, Sydney Water has previously received documentation from our Build Own Operate Transfer partner confirming the risk management provisions for the plant. We will continue to work closely with all of our partners to ensure appropriate mitigation of any identified risks related to the ongoing security of water supply.

Sydney Water will carefully consider each recommendation provided in the final report and implement appropriate actions to ensure continued security of our water and wastewater operations.

Yours sincerely

Kevin Young
Managing Director

Sydney Water Corporation ABN 49 776 225 038
1 Smith St Parramatta 2150 | PO Box 399 Parramatta 2124 | DX 14 Sydney | T 13 20 92 | www.sydneywater.com.au
Delivering essential and sustainable water services for the benefit of the community

Sydney WATER

Appendix 1

Performance audit report – Security of Critical IT Infrastructure

Recommendation	Expected completion date	Sydney Water's response
Extend the Information Security Management System (ISMS) to oversee the security of the process control environment, including the management of operational level risks and controls.	July 2015	Sydney Water has an existing ISMS covering corporate governance of some IT systems. Sydney Water supports the recommendation to extend the ISMS to incorporate the entire process control environment.
Develop a comprehensive security plan for the whole environment (building on SWC's SCADA security policy).	July 2015	Sydney Water supports this recommendation.
Document and undertake additional risk mitigation to reduce risks to acceptable levels, and clearly document what levels of risk can be tolerated.	July 2015	Agree in principle. Sydney Water conducts extensive risk assessments in line with its Corporate Risk Management Framework. We agree the documentation of some risks requires improvement and have commenced work to appropriately document and report on operational level risks and associated controls.
Obtain current documentary evidence to indicate that the risks associated with the security of process control systems at Prospect Treatment Plant are mitigated to acceptable levels.	July 2015	Sydney Water disagrees with the implication in the report that there is an issue with the risk management processes used by Degremont at Prospect Water Treatment Plant. Contracts with our partners include stringent clauses requiring them to ensure the security of systems and water supplies. In addition, Sydney Water has previously received documentation from our Build Own Operate Transfer partner confirming the risk management provisions for the plant. We will continue to work closely with all of our partners to ensure appropriate mitigation of any identified risks related to the ongoing security of water supply.
Introduce a formalised procedure and approach to the assessment of security alerts and the recording of risk management decisions in response to these alerts. This should include assessing the commodity application and control system vendor software vulnerability notices and recording the risk management decisions.	July 2015	Sydney Water supports this recommendation. Sydney Water currently conducts assessments of security alerts although we acknowledge that improvements can be made including a documented procedure which will include recording of assessments conducted.

Sydney Water Corporation ABN 49 776 225 038
1 Smith St Parramatta 2150 | PO Box 399 Parramatta 2124 | DX 14 Sydney | T 13 20 92 | www.sydneywater.com.au
Delivering essential and sustainable water services for the benefit of the community

Recommendation	Expected completion date	Sydney Water's response
Improve the logging of security related events.	July 2015	Sydney Water agrees in principle and will consider the implementation of this recommendation based on the impacts to system operations.
Investigate closer alignment to the TISN Critical Infrastructure Resilience Good Practice guidelines to more effectively manage threats to the system.	December 2015	Sydney Water supports this recommendation.
Implement Top 4 ASD mitigation guidelines.	December 2015	Sydney Water supports this recommendation.
Consider implementing the ASD top 35 mitigation guidelines for the protection of process control engineering workstations and SCADA servers.	December 2016	Sydney Water agrees in principle and will consider implementation of the ASD top 35 mitigation guidelines on a case by case basis with continued system functionality a determining factor in the adoption of each.
Determine the appropriate controls to limit unauthorised access to computer accounts including SCADA application software and computing operating systems.	July 2015	Sydney Water supports this recommendation.
Enhance monitoring of SCADA security.	December 2015	Sydney Water supports this recommendation.
Key recommendations for other agencies	**Expected completion date**	**Sydney Water's response**
Compliance with the NSW Government Digital Information Security Policy (DISP). For State Owned Corporations (SOCs) this requirement should be incorporated into their Statements of Corporate Intent (SCI).		While Sydney Water does not specifically comply with the requirements in the policy, it does make an effort to act with the same intent as DISP. That said, Sydney Water does not believe the requirement should be incorporated in the SCI, as the policy does not specifically apply to State Owned Corporations.

Sydney Water Corporation ABN 49 776 225 038
1 Smith St Parramatta 2150 | PO Box 399 Parramatta 2124 | DX 14 Sydney | T 13 20 92 | www.sydneywater.com.au
Delivering essential and sustainable water services for the benefit of the community

Introduction

1. Security of critical IT

1.1 The nature of the risk

The failure or disruption of the day-to-day delivery of essential services to the community can cause a significant loss of brand and organisational reputation, and may even attract penalties for non-compliance with regulatory requirements.

Business drivers for integration with enterprise management systems have led to IT systems for critical infrastructure becoming interconnected with corporate networks and directly or indirectly with the internet. This high level of integration can extend to remote access by operational staff, suppliers and external organisations, further increasing the exposure of these systems to network vulnerabilities associated with internet threats.

Recent incidents demonstrate that a targeted cyber-attack can penetrate traditional corporate cyber defences and cause physical harm to critical infrastructure. Traditional threat sources have evolved and now include nation states, with the threats – such as industrial espionage – becoming more sophisticated and covert.[1]

1.2 Audit objective

This audit assessed whether the systems used to operate and manage critical infrastructure are secure and if systems go down, there are sound recovery arrangements. The report answers two questions:

- Are controls to prevent, detect and respond to security breaches effective?
- Is the risk to business continuity being managed appropriately?

See Appendix 1 for more information on the scope of the audit and Appendix 2 for a glossary of terms.

1.3 Systems examined for this audit

We examined the systems utilised by the Transport Management Centre (TMC) with a focus on the Sydney Coordinated Adaptive Traffic System (SCATS) which monitors and/or controls around 4,000 sets of traffic lights from a central server and subordinate regional servers. It is used to synchronise traffic signals and monitor congestion in order to optimise traffic flows. Vehicle detectors at each intersection enable SCATS to adjust signal timings in response to traffic demand. Traffic coordinators can also adjust signal timing in response to incidents and heavy demand through the TMC. Other systems are used to manage traffic incidents and inform the public regarding road conditions.

We examined Sydney Water Corporation's (SWC) supervisory control and data acquisition (SCADA) system. SCADA is a system operating with coded signals over communication channels to monitor and control remote equipment.

SWC utilises SCADA technology to monitor and control the operation of its reservoirs, water and wastewater pumping stations and other infrastructure throughout greater Sydney over a wide area network. It also uses several separate plant SCADA systems to control its water treatment plants and wastewater treatment plants.

[1] (TISN – SCADA for CEOs)

1.4 Relevant standards and guidelines

In assessing performance the audit had regard to compliance with the requirements of the NSW Government Digital Information Security Policy 2012. This includes:

1. An Information Security Management System (ISMS) based on a comprehensive assessment of the risk to digital information and digital information systems covers the process control system. The ISMS must appropriately address all identified risks and must take account of:
    - NSW Treasury Policy & Guidelines Paper TPP09-05 - Internal Audit and Risk Management Policy for the NSW Public Sector
    - AS/NZS ISO 31000 Risk management - Principles and guidelines
    - AS/NZS ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements and AS/NZS ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management and related Standards.
2. Certification to AS/NZS ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements continuously maintained through audits conducted by an Accredited Third Party.

The policy applies to all NSW Government departments, statutory bodies and shared service providers. The policy does not apply to State Owned Corporations; however, it is commended for adoption.

There is a range of information available to agencies on ways to improve security arrangements for their critical IT infrastructure. The IT Security Expert Advisory Group of the Australian Government's Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN) published good practice guides for use by operators of national critical infrastructure. The guidelines include:

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

The Australian Signals Directorate (ASD), previously known as the Defence Signals Directorate, has developed a list of strategies to mitigate targeted cyber intrusions. The list is informed by ASD's experience in operational cyber security, including responding to serious cyber intrusions and performing vulnerability assessments and penetration testing for Australian and State government agencies.

ISO/IEC 22301 (Societal Security – Business Continuity Management Systems – Requirements) is an international standard for business continuity management published jointly by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC). It provides a framework for managing business resilience and related continuity risks.

Key findings for RMS and TfNSW

2. Controls to prevent, detect and respond to security breaches

Findings:

Controls are only partially effective in preventing and detecting security breaches and are unlikely to support the goal of a timely response to limit damage to business systems. A range of risks are adequately managed, however, there are other risks where control improvements are recommended.

Controls have been implemented to limit a number of risks, however, the protection environment requires improvement to defend against targeted attacks. For example, there is a potential for unauthorised access to sensitive information and systems that could result in traffic disruptions, and even accidents in one particular section of the road network.

The risk management process covers the Transport Management Centre (TMC) but does not extend to the whole traffic light environment. A comprehensive security plan/architecture has not yet been developed.

The risk management process covers strategic level risks, such as a computer room fire or unauthorised access scenarios, but does not cover all operational level risks, such as poor password practices, incomplete access logs, inadequate internet filtering and risks associated with the network access controls.

2.1 Oversight and monitoring of the security of process control systems and their environment

The community expects government agencies to maintain high standards for the security of critical infrastructure such as water supply systems and traffic signal networks.

Effective management of these systems requires that:

- the risks be well understood
- agencies demonstrate appropriate management of those risks.

In relation to the traffic signal network, an information security management system (ISMS) is in place which is regularly reviewed by an accredited external provider. An ISMS is an integrated set of policies, plans, procedures and processes for managing information security risks. We found relevant policies and procedures have been developed, implemented and maintained through the ISMS, however, the system is partially effective because it only covers the TMC and not the whole traffic light environment.

We note that the limited scope of the ISMS was not identified in regular reviews by the external provider. This indicates a lack of adequate guidance on the part of agency management when establishing the scope of these reviews. TfNSW has acknowledged that the ISMS is limited in scope and the coverage needs to be reconsidered. It advised that, in conjunction with RMS, it will investigate the best way to ensure that an ISMS covers appropriate components of the Traffic Management System.

A risk management process is in place which documents strategic level risks, such as a computer room fire or unauthorised access scenarios, but not all operational level risks. For example, poor password practices and a lack of internet web filtering had not been included in the risk register. This limits agencies' ability to routinely identify, evaluate and mitigate risks.

The risk management process also lacks a clear basis for determining risks that are tolerable and those that are not. For unacceptable risks there is no obvious timely mitigation program. Risk assessments identify some risks as acceptable on completion of proposed security improvements, but it was uncertain at the time of the audit if these improvements will be implemented. Accordingly, there was little evidence of management being fully informed of current risks for the short or medium term.

We found security logs are collected for a range of technologies, but monitoring needs to be improved. The NSW Government Digital Information Security Policy (DISP) states that access to digital information and digital information systems must be monitored and controlled.

There was no formalised approach in place for the assessment of security alerts from the US or Australian Government or vendor services for software vulnerabilities. Consequently the risk of such vulnerabilities may not have been reliably assessed or actioned when necessary.

TfNSW has acknowledged the inadequacy in the current systems and advised that a Security Monitoring and Assessment (SMA) Program designed to enhance security monitoring capabilities across the transport cluster is being implemented over the next two years. It advised that relevant traffic management systems will be integrated into the SMA program as part of implementation.

From 2013-14 onwards, in accordance with the DISP, TfNSW and RMS are required to report on the adequacy of their information security systems in their annual reports.

Recommendations

By July 2015, TfNSW/RMS should improve the risk management process by:

1. extending the ISMS to oversee the security of the complete traffic management environment, including operational level risks.
2. developing a comprehensive security plan for the whole environment.
3. improving the identification, assessment and recording of security risks.
4. revising the assessment of risk to better reflect current controls, rather than planned but yet to be implemented controls, and clarify the risk levels that can be tolerated.
5. improve logging and monitoring of security related events regarding access to applications, operating systems and network access.
6. introduce a formalised procedure and approach to the assessment of security alerts and the recording of risk management decisions in response to these alerts. This should include assessing the commodity application and control system vendor software vulnerability notices and recording the risk management decisions.

2.2 Network architecture

The current IT network will limit some threats to the system but not others. A comprehensive security plan/architecture has not yet been developed. RMS advises that a security plan outlining controls for RMS systems will be completed as part of the IT security strategy in mid-2015.

Security zones have been created across the network, however, the separation of zones is only partially effective. A security zone is an area within a network occupied by a group of systems and components with similar requirements for the protection of information,

functions and characteristics associated with those requirements. Where information is required to flow between zones, typically a firewall is put in place to provide security and to control information that flows between them. Using a physical security analogy, a low level security zone might have interview and front-desk areas where there is no segregation of staff from clients and the public. A high level security zone, on the other hand, would have additional access controls such as doors with locks and swipe cards to only allow access to staff with the appropriate security clearance.

We found insufficient access control between the network zones. TfNSW advises that, in conjunction with RMS, it is reviewing the security zoning model.

Higher level risks have been identified in risk management plans, such as a shutdown of the Transport Management Centre or unauthorised access to the computer room, but the risks associated with the current zoning arrangements are not specifically identified.

Some controls were not adequately enforced in either the SCATS or the Central Management Computer Systems (CMCS) used for traffic incident management. RMS advised that SCATS will be fixed by 31 December 2014, and the CMCS is scheduled for replacement. It is expected that RMS will go to tender late in 2015 for the start of the project to be Jan 2016 and completion in 2017.

The controls environment is only partially aligned with the levels specified in ISO/IEC 27001 and 27002 and the advice of the TISN Critical Infrastructure Security Guidelines that expand on the ISO standards in terms of operational technology/SCADA systems. This lack of alignment could result in unacceptable risk levels. Examples of some of the TISN controls are contained in Appendix 3.

The Australian Signal Directorate (ASD) has produced a set of guidelines designed to assist government agencies and companies in reducing the risk of targeted cyber intrusions. At least 85 per cent of the cyber intrusions that ASD responds to across government systems involve adversaries using unsophisticated techniques that would have been mitigated by implementing the Top 4 mitigation strategies as a package.

Exhibit - ASD Top 4 mitigation strategies

The top four are:

- application whitelisting of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.
- patch applications for example Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with ‘extreme risk’ vulnerabilities within two days. Use the latest version of applications
- patch operating system vulnerabilities. Patch/mitigate systems with ‘extreme risk’ vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.
- restrict administrative privileges to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.

Recommendations

By July 2015 TfNSW/RMS should:

7. implement the Top 4 ASD mitigation guidelines and consider implementing the remainder of the ASD top 35.
8. improve security zoning to better protect the system from potential threats.

2.3 Operational, technical and physical controls

Some risks are controlled, however, there are other risks relating to the potential for unauthorised access to sensitive information and control systems that need to be better managed. The IT security of some technical components is basic and does not align to the recommendations of the vendor or the TISN Critical Infrastructure Security Guidelines. The system's protection against targeted attacks or new computer viruses is considered low.

We found that:

Application controls

- The implementation of the controls for the separation of access levels for SCATS could be improved to increase the resilience from technical activities that could defeat these controls.
- RMS advised that the password control mechanism for SCATS will be aligned with RMS corporate password policies by December 2014. It also advised it will continue to keep SCATS security up-to-date for future releases. The access control mechanism for traffic control software (including social media and IT system administration utilities) needs to be continually maintained at the highest security level.

Network controls

- There were a number of issues regarding the security of network controls. Detailed findings and recommendations have been provided to the agencies in a separate management letter.

Workstation and Server Controls

- Servers were only receiving anti-virus updates weekly. Together with the lack of internet gateway scanning for malicious software, this reduced the security of the corresponding servers. TfNSW advised that these servers have recently been re-configured to receive anti-virus updates daily.
- Traffic light controllers are highly resistant to standard hacking techniques. The devices in use have been certified to formal Australian Standards that require safety interlocks. These interlocks are used to prevent simultaneous green lights creating a dangerous situation at an intersection. Electromechanical testing done to TSC4 (an RMS standard adopted by the Australian Standards AS2578.2009) ensures that an intersection cannot create an accident, that is green-green or yellow-green.

Physical security controls

- Servers have been physically secured in the data centres. Physical security and related operational procedures of the TMC was sound for the national security threat level at the time of the audit. However, the physical locking mechanism for road side cabinets for traffic controllers needs to be improved. Door-open sensors are in place but monitoring can be improved. A cabinet could be vandalised or otherwise tampered with to disable signals at an intersection. RMS advised it will investigate the suitability of a more secure door locking mechanism and proactively replace current locks during the normal maintenance process for existing controllers. It also advised that the current design for new installations will be corrected to replace the old door lock, and monitoring of door-open sensors will be improved.

Security operations controls

- TMC IT staff had not received training on the appropriate actions to take following a security breach of the traffic systems. IT staff also need to be kept up-to-date with the latest technologies to ensure the systems remain secure at all times. TfNSW advised that this will be addressed through additional training of personnel in the TMC systems unit.

- Operating system software on servers has been recently patched but some other software components had not been patched. TMC IT staff were not aware that TfNSW had organised NSW Government extended support for these components. TfNSW advises that its newly developed Security Monitoring and Assessment Program will introduce tools to ensure compliance with patch management standards across IT systems. This was scheduled to occur in the TMC by 31 December 2014.
- The effectiveness of the control environment depends on sound design and implementation. Standards and good practice guidelines require periodic security assessment and testing but we found that such testing was lacking. We therefore organised an accredited penetration testing service to test the security of one key application and part of the technical infrastructure. The test report provided to RMS/TfNSW identified a number of issues that should be addressed.

Recommendations

By July 2015, improve system security by:

Security Operations Controls

9. improving the access control mechanism for traffic control software including social media and IT system administration utilities (TfNSW/RMS)
10. ensuring and maintaining adequate technical skills through ongoing training for all staff requiring admin user access (TfNSW/RMS)
11. assessing the software vulnerabilities notices and action or record the risk management decisions. (TfNSW/RMS)
12. developing and conducting a program to perform vulnerability assessments and security penetration tests, at least annually, to verify the security of the key components and networks used to access TMC systems and associated workstations. (TfNSW/RMS).
13. assess the risk of the vulnerabilities identified in the security penetration test and develop an appropriate action plan (TfNSW/RMS).

Technical security controls

14. developing a program to improve locks on traffic signal boxes as a part of a periodic maintenance program (RMS)
15. expediting initiatives to replace outdated software. (TfNSW/RMS)

Additional details have been provided to agencies.

3. Managing the risk to business continuity, including an emergency response capability.

Findings:

RMS and TfNSW have designed and tested emergency response capability for the TMC services for some disaster scenarios and have recently identified and initiated improvements for responding to IT related disasters.

Until the IT disaster recovery site is fully commissioned, a disaster at the main data centre will have traffic controllers operating on a regional basis without the benefit of intervention from the TMC in managing traffic coordination and incidents, which means higher congestion is likely in the short term.

3.1 The response capability for system-related incidents

The TMC could adequately respond to an incident that required relocation of the operations room as an isolated incident. However, the TMC could not adequately respond if an incident disabled the main data centre, as a separate disaster recovery site for TMC systems is yet to be fully commissioned. TMC had identified this risk and is progressing the development of the new site, although this has been delayed from its original schedule.

Until the disaster recovery site is complete and tested, a disaster at the main data centre will have traffic controllers running on a regional basis without the benefit of intervention from the TMC. Use of TMC incident management capabilities would be severely impaired which would likely impact on traffic management.

Security incident management is defined in a procedure within the TMC. The roles and responsibilities for responding to an incident have also been defined, however, there is no evidence that staff have received the required training. This means the TMC may not optimally respond to an information or IT security breach. TfNSW advised that TMC systems staff were briefed on the TfNSW security policies and procedures during November 2014.

Recommendations

16. by July 2015, develop a program of testing the disaster recovery capability following the delivery of the TMC IT disaster recovery project (TfNSW/RMS)
17. by January 2015, ensure a program of ongoing training is in place to provide relevant staff with the knowledge to respond to a real or suspected security incident (TfNSW/RMS).

3.2 Plans for system-related incident response and business continuity

A business continuity plan for the TMC has been developed and tested for the TMC operations rooms, however, disaster recovery procedures for the information systems are incomplete and do not include timeframes.

TfNSW advised that annual TMC operations room's business process continuity testing was successfully carried out at the alternative TMC in September 2014, and SCATS disaster recovery system testing was carried out during November 2014. It advised that TMC procedures, including recovery plans, will be reviewed and updated by February 2015.

Recommendation

18. by July 2015, ensure a tested IT disaster recovery plan is in place that meets the maximum acceptable outage timeframes should a disaster occur (TfNSW/RMS).

Key findings for Sydney Water Corporation

4. Controls to prevent, detect and respond to security breaches

Findings:

Controls to prevent and detect security breaches are not as effective as they could be. Whilst SWC's response capability is good, it is limited by its inability to detect all security breaches.

Controls have been implemented to limit a number of risks, however, the protection environment requires improvement to defend against targeted attacks. For example, any malicious activity on most of the corporate network is blocked from accessing the SCADA environment but control level access is possible from selected low security workstations on the corporate network.

SWC's risk management process documents risks and controls at a strategic level but does not cover all operational level risks, such as non-expiring engineering passwords and the potential introduction of USB-based malicious software.

4.1 Oversight and monitoring of the security of process control systems and their environment

SWC has an established Information Security Management System (ISMS), but it only covers the corporate data centre and not the engineering systems. An ISMS is an integrated set of policies, processes and systems for managing IT-related risks. SWC advises that a security roadmap has recently been approved to address this limitation.

SWC is yet to formally document what is an appropriate level of security for SCADA and a comprehensive risk management plan for the system. SWC's risk management process documents risks and controls at a strategic level but does not cover all operational level risks, such as the potential introduction of USB-based malicious software.

A range of common specific risks and their mitigating controls have not been documented, including risks associated with non-expiring engineering passwords. This means the risk management process is inherently limited in its ability to routinely identify, evaluate and mitigate risks.

SWC has not documented all risks and, as such, reports to management do not present a complete picture of current risk levels. Management reports also list a range of controls that are overdue for implementation.

SWC does not currently have a formalised approach to the assessment of security alerts from the US or Australian Government services for process control system software vulnerabilities. SWC indicated that an assessment is conducted for every SCADA related alert from national computer emergency response team (CERT Australia), with emails received on a regular basis by several managers whose job it is to assess impacts. However the assessment process was not defined and the analysis documentation that was provided to support this assertion was limited to a minority of the security advisories released by the US Government. Our review indicated that assessments were ad-hoc and it is not possible to provide assurance that corresponding risks are reliably assessed.

We can provide limited assurance regarding the adequacy of security of process control systems at Prospect Treatment Plant (operated by a contracted company, Degremont), which produces a large proportion of Sydney's water supply. SWC has provided a risk register which shows high current risks and SWC recommendations for improvements. However, SWC has not provided evidence to indicate that its recommendations have been adopted. Our audit mandate does not extend to directly examining controls in third party providers so we cannot be more conclusive on the adequacy of controls for the plant.

Exhibit 1: Limitations of the Audit Office of New South Wales mandate

In its September 2013 report to parliament on the Efficiency and Effectiveness of the Audit Office of New South Wales, the Public Accounts Committee recommended the Public Finance and Audit Act 1983 be amended to enable the Auditor-General to 'follow the dollar' by being able to directly audit functions performed by entities, including private contractors and other non-government organisations, on behalf of the State in the delivery of government programs.

Our inability to gauge the effectiveness of security at the Prospect WTP is an example of where this extension of powers would enable the Audit Office of New South Wales to directly gather evidence from third party providers to provide assurance to the NSW Parliament.

SWC has deployed dedicated intrusion detection technologies with monitoring by a service provider. The NSW Government Digital Information Security Policy (DISP) states that access to digital information and digital information systems must be monitored and controlled. As previously noted, the policy does not apply to State Owned Corporations; however, it is recommended for adoption. We found security logs are also collected for a range of other technologies but monitoring of these logs is ad-hoc and the logged data is incomplete.

The risks associated with such weaknesses are illustrated by a recent incident involving operational anomalies in a wastewater treatment facility in the United States. Note that this exhibit is an example only and is not intended to imply that Sydney Water's assets and operations are at the same level of risk or exposure.

Exhibit 2: Example of risks associated with unauthorised access to treatment plant equipment

The asset owner reported that a control system maintenance employee had improperly accessed the control system on at least four separate occasions. According to the report, one of these instances resulted in the overflow of the system's wastewater treatment process.

An incident response team performed extensive analysis of the control system and historical trending data around the four dates provided by the asset owner. The team was unable to conclusively determine if the suspected employee had unauthorised access on the date of the overflow or if that access resulted in the basin overflowing. The factors that significantly contributed to the inconclusive findings included:

- each host did not record logon events
- typically, only one username was used throughout the network
- a lack of network monitoring systems in place to verify the alleged activity
- logging was not enabled or was irrelevant for any of the remote access tools seen on the hosts (pcAnywhere, RealVNC, NetVanta VPN client, Windows Remote Desktop)
- operating system records were eliminated due to the age of reported access event.

Lessons learned: This incident highlights the importance of detailed logging capabilities and policies related to logging analysis. Also, network administrators should implement least privilege practices and ensure that each user has unique logon credentials that provide access to only those systems the employee needs to control.

Source: US Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Newsletter, May-August 2014.

Recommendations

Sydney Water Corporation, by July 2015, should:

Management controls

1. extend the corporate ISMS to oversee the security of the process control environment, including the management of operational level risks and controls.
2. develop a comprehensive security plan for the whole environment (building on SWC's SCADA security policy).
3. document and undertake additional risk mitigation to reduce risks to acceptable levels, and clearly document what levels of risk can be tolerated.
4. obtain current documentary evidence to indicate that the risks associated with the security of process control systems at Prospect Treatment Plant are mitigated to acceptable levels.

Security operations controls

5. introduce a formalised procedure and approach to the assessment of security alerts and the recording of risk management decisions in response to these alerts. This should include assessing the commodity application and control system vendor software vulnerability notices and recording the risk management decisions.

Technical security controls

6. improve the logging of security related events.

4.2 Network architecture

The IT network security is able to manage some threats to the system but not others. Security controls are defined in strategic level risk assessments although a comprehensive security plan/architecture has not yet been developed. A SCADA security policy has also been developed, and has been communicated to the control system provider, however, there is no obvious implementation plan in place.

SWC has established security zones within its network to mitigate risks. We found that SWC's separation of zones may not be sufficient to protect the system from targeted malicious attacks, although such attacks would require a level of physical access and knowledge of SWC. We note that the risk assessments did not specifically identify the risks associated with current zoning arrangements.

SWC advised that it has adopted the TISN security architecture guidelines in terms of gateways. It also advised that it is investigating a range of solutions to enhance the effectiveness of security zoning.

Recommendations

Sydney Water Corporation should:

7. investigate closer alignment to the TISN Critical Infrastructure Resilience Good Practice guidelines to more effectively manage threats to the system (by December 2015).
8. implement the Top 4 ASD mitigation guidelines (by December 2015).
9. consider implementing the ASD top 35 mitigations guidelines for the protection of process control engineering workstations and SCADA servers (by December 2016).

4.3 Operational, technical and physical controls

Controls have been implemented to limit a number of risks, however, the protection environment requires improvement to defend against targeted malicious attacks. SWC has advised that a business case to rectify this has been developed and is awaiting approval.

The SWC main office and the treatment plants visited had good levels of physical security. The main office has access barriers and additional security for the data centre. The plants visited have perimeter fences and access controlled gates. They also have locked doors to the operations room and main switchroom. Building security is integrated with the identity management solution so that a HR exit leads to removal of physical and logical (that is, IT) access.

Servers and process controllers have been physically secured, however, the IT security of process controllers should be improved. The IT security of the server's workstations is below the recommendations of Microsoft or the TISN Critical Infrastructure Security Guidelines. Some components use out-of-date software. The system's protection against targeted attacks or new computer viruses is low.

Recommendations

Implement control enhancements to effectively manage potential threats to the system by:

Management controls

10. determining the appropriate controls to limit unauthorised access to computer accounts including SCADA application software and computer operating systems (by July 2015).

Technical security controls

11. enhancing monitoring of SCADA security (by December 2015).

Additional details have been provided to SWC.

5. Managing the risk to business continuity, including an emergency response capability

Findings:

Sydney Water Corporation (SWC) is well equipped to deal with the impact of continuity and security incidents. It has developed and tested procedures for business continuity and disaster recovery and provided training to staff. It has established a back-up operations centre which is tested on a regular basis, and also established redundant systems such as additional control units and backup power supplies for key facilities.

5.1 Response capability for system-related incidents

The NSW Government Digital Information Security Policy (DISP) requires controls to be in place to counteract disruptions to business activities and to protect critical business processes from the effects of major failures of digital information systems or disasters. It goes on to state that the timely resumption of business processes in the event of a failure must be ensured.

SWC employees have been trained in how to respond to and manage security incidents. Three staff received specialist Commonwealth Government sanctioned TISN training in the USA. One security incident management test scenario has been conducted.

Technical redundancy is provided for key equipment including additional programmable logic controllers, dual electrical feeds and standby generators where feasible.

SWC has established a separate SCADA Operations Centre off site to enhance its disaster recovery capabilities. SWC advised that operations are moved to this centre one day a month for testing purposes. This control was operating effectively.

5.2 Plans for system-related incident response and business continuity

SWC has developed and maintains business continuity management tools such as a business impact analysis (BIA) and business continuity plans (BCP).

SWC's Hydraulic System Services has developed a security incident response plan and a broader incident response plan. A business continuity plan for the System Operation Centre is well defined and periodically tested. The plan is industry best practice and is based on ISO22301 – business continuity management system.

Appendices

Appendix 1: About the audit

This audit assessed whether the systems used to operate and manage critical infrastructure are secure and if systems go down, there are sound recovery arrangements.

Audit scope

Process control systems are widely used in utilities, transport and other infrastructure. We propose to focus on water and sewer supply and metropolitan traffic management.

We have focused on water and sewerage systems due to the potential:

- impact on supply and the health and safety consequences thereof
- physical damage to plant and equipment that can be caused by a hack on a water/sewage control system (for example broken valves, burnt-out pumps etc).

We have focused on metropolitan traffic management because of:

- the sensitivity of Sydney road systems to any disruptions, with the consequence of major congestion
- the safety risk associated with traffic management failures, including failed traffic lights
- a recent Queensland Audit Office audit on the security of traffic management systems found significant weaknesses.

The audit did not examine:

- efficiency and effectiveness of the selected process control systems in undertaking their functions of traffic control and water/wastewater management, except regarding the effectiveness of security and business continuity planning and management
- efficiency and effectiveness of other IT management systems implemented across the organisations, nor the IT security or business continuity arrangements in the organisations generally.

While the audit expressed an opinion on security and business continuity arrangements for the selected systems, it is not intended to identify all issues or potential issues in these systems or their wider environment. The audit was undertaken on a risk basis having regard to the resources and time available for the audit. The audit does not guarantee the security of the audited systems or that business continuity would be efficiently and effectively achieved in the event of an incident. It can only comment on the risks and mitigation of these risks.

Details of our approach to selecting topics and our forward program are available on our website.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Audit Standards ASAE 3500 on performance auditing, and to reflect current thinking on performance auditing practices. Our processes have also been designed to comply with the auditing requirements specified in the *Public Finance and Audit Act 1983*.

Acknowledgements

We gratefully acknowledge the co-operation and assistance provided by the RMS, SWC and TfNSW. In particular we wish to thank our liaison officers and staff who participated in interviews and provided material relevant to the audit.

Audit team

Gary Gaskell and Neil Avery conducted the performance audit. Sean Crumlin and Kathrina Lo provided direction and quality assurance.

Audit cost

Including staff costs, printing costs and overheads, the estimated cost of the audit is $247,969.

Appendix 2: Glossary of terms

An **Access Control List** (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are granted on written objects. For instance, an ACL might give Alice access to read and write a file and Bob access to only read it.

In computer security, a **DMZ** or demilitarised zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organisation's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has direct access to equipment in the DMZ, rather than any other part of the network.

A **Disaster Recovery Plan** (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Given organisations' increasing dependency on information technology to run their operations, a disaster recovery plan is increasingly associated with the recovery of information technology data, assets, and facilities.

An **Information Security Management System** (ISMS) is a management process with a set of policies concerned with information security management or IT related security and availability risks. The governing principle behind an ISMS is that an organisation should implement, design and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.

An **Intrusion Detection System** (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

A **Local Area Network** (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building, using network media. The defining characteristics of LANs, in contrast to wide area networks (WANS), include their smaller geographical area and non-inclusion of leased telecommunication lines.

Logical security consists of software safeguards for an organisation’s systems, including user identification and password access, authenticating, access rights and authority levels. These measures are to ensure that only authorised users are able to perform actions or access information in a network or workstation. It is a subset of computer security.

A **security zone** is an area within a network occupied by a group of systems and components with similar requirements for the protection of information and characteristics associated with those requirements. These shared requirements and characteristics will include a common data classification, including shared:

- data confidentiality and integrity requirements
- access controls
- audit, logging, and monitoring requirements.

A **Server** is a running instance of an application (Software) capable of accepting requests from the client and giving responses accordingly. Servers can run on any computer including dedicated computers, which individually are also often referred to as ‘the server’. In many cases, a computer can provide several services and have several servers running. The advantage of running servers on a dedicated computer is security.

Servers often provide essential services across a network, either to private users inside a large organisation or to public users via the Internet. Typical computing servers are database servers, file servers, mail servers, print servers, web servers, gaming servers, and application servers.

Standard Operating Environment (SOE) is a standard implementation of an operating system and its associated software. SOEs can include the base operating system, a custom configuration, standard applications used within an organisation, software updates and service packs. An SOE can apply to servers, desktops, laptops and mobile devices.

Virtual Private Network (VPN) extends a private network across a public network, such as the internet. It enables a computer to send and receive data across shared or public network as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

A **Workstation** is a special computer designed for technical or scientific applications. Intended primarily to be used by one person at a time, they are commonly connected to a local area network and run multi-user operating systems. The term workstation has also been used loosely to refer to everything from a mainframe computer terminal to a PC connected to a network.

A **business continuity plan** is a plan to continue operations if a place of business (for example, an office, worksite or data center) is affected by adverse physical conditions, such as a storm, fire or crime. Such a plan typically explains how the business would recover its operations or move operations to another location. For example, if a fire destroys an office building or data center, the people and business or data center operations would relocate to a recovery site.

Appendix 3: Key Recommendations from the TISN Critical Infrastructure Security Guidelines

Australian Government/Industry Trusted Information Sharing Network for Critical Infrastructure Resilience for Systems of National Significance developed by the IT Security Expert Advisory Group (ITSEAG) of the Critical Infrastructure Advisory Council (CIAC). Below are some extracts from the security guidelines that provide example of the TISN's recommendations for the securing of SCADA or operational technology.

Generic SCADA Risk Management Framework for Australian Critical Infrastructure

- The Critical Infrastructure Protection Risk Management Framework (RMF) is based on traditional standards based risk management frameworks, as described in ISO/IEC 31000 – Risk Management and ISO/IEC 27005 – Information Security Risk Management standards
- Where organisations have existing Corporate Risk Management and Security Frameworks in place it is important that this SCADA risk framework aligns with the corporate frameworks to ensure organisational consistency
- Risks associated with external interdependencies such as an incident impacting multiple organisations (for instance with supply chains and business partners) should be considered.
- The risk management scope should include:
  - centralised SCADA Management and Control
  - data communications
  - front-end processing
  - field monitoring and control.

SCADA Architecture Principles – Good Practice Guide

- Detailed security architecture and zone requirements are documented in SCADA design specifications.
- The SCADA zone is not accessible from untrusted or semi-trusted networks.
- Good practice: Connections in and out of the SCADA zone are kept to a minimum
- Best practice: Controls should be in place at the internal DMZ that limits any interaction originating from the IT environment to the internal DMZ (or operational technology/SCADA environment).
- Users in the IT environment cannot perform actions in the operational technology (SCADA) environment.
- Security testing occurs annually or whenever changes to the architecture occur.

Implementing Gateways – Good Practice Guide

- Gateway security zones are separated through the use of appropriately configured firewalls.
- Appropriate logging and monitoring procedures are performed at gateway devices.
- Potential vulnerabilities are monitored through review of security bulletins and subscription services where available.
- Signature based intrusion detection systems maintain an up to date list of attack signatures.
- Alerts are monitored 24 hours a day. Any alerts are reviewed as a security incident and tuned on an ongoing basis.
- Incident response procedures are in place.
- Best Practice:
  - A security information and event management (SIEM) solution is in place for centralised log management.
  - Network controls restrict access on physically dedicated communication links.

Hardening of SCADA ICT Systems Good Practice Guide

- Segregate the SCADA network from the corporate network utilising a DMZ and stateful firewall.
- Ensure critical components provide required redundancy.
- Ensure only authorised personnel can access or operate SCADA system.
- Configure systems to prompt users to change passwords prior to an expiry date being reached.
- Ensure unique user IDs are assigned to all users.
- Ensure that generic logins are not used to authenticate into administrative consoles.
- Enforce the construction of strong passwords within SCADA systems.
- Ensure that the latest service packs and critical (software) patches are applied to servers.
- Ensure that the latest vendor approved firmware, patches and critical updates are applied to field devices.
- Implement anti-virus gateways to monitor outgoing and incoming web and email traffic.
- Encrypt information transmitted over wireless networks.
- Develop and conduct a programme to perform vulnerability assessments and penetration tests.
- Develop and maintain a business continuity management process.
- Best practice:
    - Implement an account lock-out counter
    - Prohibit the use of external media where possible.

Monitoring of SCADA Networks – Good Practice Guide

- Implement network intrusion detection on the SCADA network.
- Unauthorised parties should not be able to alter log source processes, executable files, configuration files, or other components.
- Utilise anti-virus detection software on all servers and workstations within the SCADA network.
- Implement a centralised real-time monitoring platform.

SCADA Good Practice Guide – Knowing Your Network

- SCADA roles and responsibilities are clearly defined.
- Risk assessments are performed over SCADA networks.
- Training and security awareness procedures are in place for SCADA personnel.
- Vulnerability management policies and procedures are in place.

Performance auditing

What are performance audits?

Performance audits determine whether an agency is carrying out its activities effectively, and doing so economically and efficiently and in compliance with all relevant laws.

The activities examined by a performance audit may include a government program, all or part of a government agency or consider particular issues which affect the whole public sector. They cannot question the merits of government policy objectives.

The Auditor-General's mandate to undertake performance audits is set out in the *Public Finance and Audit Act 1983.*

Why do we conduct performance audits?

Performance audits provide independent assurance to parliament and the public.

Through their recommendations, performance audits seek to improve the efficiency and effectiveness of government agencies so that the community receives value for money from government services.

Performance audits also focus on assisting accountability processes by holding managers to account for agency performance.

Performance audits are selected at the discretion of the Auditor-General who seeks input from parliamentarians, the public, agencies and Audit Office research.

What happens during the phases of a performance audit?

Performance audits have three key phases: planning, fieldwork and report writing. They can take up to nine months to complete, depending on the audit's scope.

During the planning phase the audit team develops an understanding of agency activities and defines the objective and scope of the audit.

The planning phase also identifies the audit criteria. These are standards of performance against which the agency or program activities are assessed. Criteria may be based on best practice, government targets, benchmarks or published guidelines.

At the completion of fieldwork the audit team meets with agency management to discuss all significant matters arising out of the audit. Following this, a draft performance audit report is prepared.

The audit team then meets with agency management to check that facts presented in the draft report are accurate and that recommendations are practical and appropriate.

A final report is then provided to the CEO for comment. The relevant minister and the Treasurer are also provided with a copy of the final report. The report tabled in parliament includes a response from the CEO on the report's conclusion and recommendations. In multiple agency performance audits there may be responses from more than one agency or from a nominated coordinating agency.

Do we check to see if recommendations have been implemented?

Following the tabling of the report in parliament, agencies are requested to advise the Audit Office on action taken, or proposed, against each of the report's recommendations. It is usual for agency audit committees to monitor progress with the implementation of recommendations.

In addition, it is the practice of Parliament's Public Accounts Committee (PAC) to conduct reviews or hold inquiries into matters raised in performance audit reports. The reviews and inquiries are usually held 12 months after the report is tabled. These reports are available on the parliamentary website.

Who audits the auditors?

Our performance audits are subject to internal and external quality reviews against relevant Australian and international standards.

Internal quality control review of each audit ensures compliance with Australian assurance standards. Periodic review by other Audit Offices tests our activities against best practice.

The PAC is also responsible for overseeing the performance of the Audit Office and conducts a review of our operations every four years. The review's report is tabled in parliament and available on its website.

Who pays for performance audits?

No fee is charged for performance audits. Our performance audit services are funded by the NSW Parliament.

Further information and copies of reports

For further information, including copies of performance audit reports and a list of audits currently in-progress, please see our website www.audit.nsw.gov.au or contact us on 9275 7100

Performance audit reports

No	Agency or issues examined	Title of performance audit report or publication	Date tabled in parliament or published
248	Transport for NSW Roads and Maritime Services Sydney Water Corporation	*Security of critical IT infrastructure*	21 January 2015
247	Roads and Maritime Services WestConnex Delivery Authority Infrastructure NSW Transport for NSW NSW Treasury Department of Premier and Cabinet	*WestConnex: Assurance to the Government*	18 December 2014
246	Department of Education and Communities	*The Learning Management and Business Reform Program*	17 December 2014
245	Environment Protection Authority Department of Trade and Investment, Regional Infrastructure and Services	*Managing contaminated sites*	10 July 2014
244	Office of Finance and Services Department of Education and Communities Forestry Corporation of NSW Fire and Rescue NSW NSW Businesslink Pty Ltd Essential Energy Sydney Trains	*Making the most of Government purchasing power – Telecommunications*	26 June 2014
243	NSW Treasury	*Use of purchasing cards and electronic payment methods*	5 June 2014
242	NSW Police Force	*Effectiveness of the new Death and Disability Scheme*	22 May 2014
241	Road and Maritime Services	*Regional Road funding – Block Grant and REPAIR programs*	8 May 2014
240	NSW State Emergency Service	*Management of volunteers*	15 April 2014
239	Fire and Rescue NSW NSW Rural Fire Service	*Fitness of firefighters*	1 April 2014
238	Transport for NSW Department of Attorney General and Justice Department of Finance and Service Roads and Maritime Services NSW Police Force Department of Education and Communities	*Improving legal and safe driving among Aboriginal people*	19 December 2013
237	Department of Education and Communities	*Management of casual teachers*	3 October 2013
236	Department of Premier and Cabinet Ministry of Health – Cancer Institute NSW Transport for NSW – Rail Corporation NSW	*Government Advertising 2012-13*	23 September 2013
235	NSW Treasury NSW Police Force NSW Ministry of Health Department of Premier and Cabinet Department of Attorney General and Justice	*Cost of alcohol abuse to the NSW Government*	6 August 2013
234	Housing NSW NSW Land and Housing Corporation	*Making the best use of public housing*	30 July 2013
233	Ambulance Service of NSW NSW Ministry of Health	*Reducing ambulance turnaround time at hospitals*	24 July 2013

No	Agency or issues examined	Title of performance audit report or publication	Date tabled in parliament or published
232	NSW Health	*Managing operating theatre efficiency for elective surgery*	17 July 2013
231	Ministry of Health NSW Treasury NSW Office of Environment and Heritage	*Building energy use in NSW public hospitals*	4 June 2013
230	Office of Environment and Heritage - National Parks and Wildlife Service	*Management of historic heritage in national parks and reserves*	29 May 2013
229	Department of Trade and Investment, Regional Infrastructure and Services – Office of Liquor, Gaming and Racing Independent Liquor and Gaming Authority	*Management of the ClubGRANTS scheme*	2 May 2013
228	Department of Planning and Infrastructure Environment Protection Authority Transport for NSW WorkCover Authority	*Managing gifts and benefits*	27 March 2013
227	NSW Police Force	*Managing drug exhibits and other high profile goods*	28 February 2013
226	Department of Education and Communities	*Impact of the raised school leaving age*	1 November 2012
225	Department of Premier and Cabinet Division of Local Government	*Monitoring Local Government*	26 September 2012
224	Department of Education and Communities	*Improving the literacy of Aboriginal students in NSW public schools*	8 August 2012
223	Rail Corporation NSW Roads and Maritime Services	*Managing overtime*	20 June 2012
222	Department of Education and Communities	*Physical activity in government primary schools*	13 June 2012
221	Community Relations Commission For a multicultural NSW Department of Premier and Cabinet	*Settling humanitarian entrants in NSW: services to permanent residents who come to NSW through the humanitarian migration stream*	23 May 2012
220	Department of Finance and Services NSW Ministry of Health NSW Police Force	*Managing IT Services Contracts*	1 February 2012

Performance audits on our website

A list of performance audits tabled or published since March 1997, as well as those currently in progress, can be found on our website www.audit.nsw.gov.au.

audit office
OF NEW SOUTH WALES

Our vision

To make the people of New South Wales proud of the work we do.

Our mission

To perform high quality independent audits of government in New South Wales.

Our values

Purpose – we have an impact, are accountable, and work as a team.

People – we trust and respect others and have a balanced approach to work.

Professionalism – we are recognised for our independence and integrity and the value we deliver.

Professional people with purpose

audit.nsw.gov.au

Professional people with purpose
Making the people of New South Wales proud of the work we do.

Level 15, 1 Margaret Street
Sydney NSW 2000 Australia

t +61 2 9275 7100
f +61 2 9275 7200
e mail@audit.nsw.gov.au
office hours 8.30 am–5.00 pm

audit.nsw.gov.au

audit office
OF NEW SOUTH WALES