PERFORMANCE AUDIT 13 JULY 2021

Managing cyber risks

NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

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 *Government Sector Audit Act 1983* and the *Local Government Act 1993*.

We conduct financial or 'attest' audits of state public sector and local government entities' financial statements. We also audit the Consolidated State Financial Statements, a consolidation of all state public sector agencies' financial statements.

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 entities to ensure sound financial management.

Following a financial audit the Audit Office issues a variety of reports to entities and reports periodically to Parliament. In combination, these reports give opinions on the truth and fairness of financial statements, and comment on entity internal controls and governance, and 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 entity 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 entity's operations, or consider particular issues across a number of entities.

As well as financial and performance audits, the Auditor-General carries out special reviews, compliance engagements and audits requested under section 27B(3) of the *Government Sector Audit Act 1983*, and section 421E of the *Local Goverment Act 1993*.

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 *Government Sector Audit Act 1983,* I present a report titled **'Managing cyber risks'.**

Margaret Crawford
Auditor-General for New South Wales
13 July 2021

contents

Managing cyber risks

Auditor-General's foreword

Response to requests by audited agencies to remove information from this report

In preparing this audit report, I have considered how best to balance the need to support public accountability and transparency with the need to avoid revealing information that could pose additional risk to agencies' systems. This has involved an assessment of the appropriate level of detail to include in the report about the cyber security vulnerabilities identified in this audit.

In making this assessment, the audit team consulted with Transport for NSW (TfNSW), Sydney Trains, and Cyber Security NSW to identify content which could potentially pose a threat to the agencies' cyber security.

In December 2020, my office also provided TfNSW and Sydney Trains with a detailed report of many of the significant vulnerabilities identified in this audit, to enable the agencies to address the cyber security risks identified. The detailed report was produced as a result of a 'red team' exercise, which was conducted with both agencies' knowledge and consent. The scope of this exercise reflected the significant input provided by both agencies. More information on this exercise is at page 12 of this report.

TfNSW and Sydney Trains have advised that in the six months from December 2020 and at the time of tabling this audit report, they have not yet remediated all the vulnerabilities identified. As a result, they, along with Cyber Security NSW, have requested that we not disclose all information contained in this audit report to reduce the likelihood of an attack on their systems and resulting harm to the community. I have conceded to this request because the vulnerabilities identified have not yet been remediated and leave the agencies exposed to significant risk.

It should be stressed that the risks identified in the detailed report exist due to the continued presence of these previously identified vulnerabilities, rather than due to their potential publication. The audited agencies, alone, are accountable for remediating these vulnerabilities and addressing the risks they pose.

It is disappointing that transparency to the Parliament and the public on issues that potentially directly affect them needs to be limited in this way.

That said, the conclusions drawn in this report are significant in terms of risk and remain valid, and the recommendations should be acted upon with urgency.

Section one

Managing cyber risks

Executive summary

Cyber security risk is an increasing area of concern for governments in Australia and around the world. In recent years, there have been a number of high-profile cyber security attacks on government entities in Australia, including in New South Wales. Malicious cyber activity in Australia is increasing in frequency, scale, and sophistication. The Audit Office of New South Wales is responding to these risks with a program of audits in this area, which aim to identify the effectiveness of particular agencies in managing cyber risks, as well as their compliance with relevant policy.

Cyber Security NSW, part of the Department of Customer Service (DCS) releases and manages the NSW Cyber Security Policy (CSP). The CSP sets out 25 mandatory requirements for agencies, including making it mandatory for agencies to implement the Australian Cyber Security Centre Essential 8 Strategies to Mitigate Cyber Security Incidents (the Essential 8). The Essential 8 are key controls which serve as a baseline set of protections which agencies can put in place to make it more difficult for adversaries to compromise a system. Agencies are required to self-assess their maturity against the CSP and the Essential 8, and report that assessment to Cyber Security NSW annually.

The CSP makes agencies responsible for identifying and managing their cyber security risks. The CSP sets out responsibilities and governance regarding risk identification, including making agencies responsible for identifying their 'crown jewels', the agency's most valuable and operationally vital systems. Once these risks are identified, agencies are responsible for developing a cyber security plan to mitigate those risks.

This audit focussed on two agencies: Transport for NSW (TfNSW) and Sydney Trains. TfNSW is the lead agency for the Transport cluster and provides a number of IT services to the entire cluster, including Sydney Trains. This audit focussed on the activities of TfNSW's Transport IT function, which is responsible for providing cyber security across the cluster, as well as directly overseeing four of TfNSW's crown jewels. Sydney Trains is one of the agencies in the Transport cluster. While it receives some services from TfNSW, it is also responsible for implementing its own IT controls, as well as controls to protect its Operational Technology (OT) environment. This OT environment includes systems which are necessary for the operation and safety of the train network.

To test the mitigations in place and the effectiveness of controls, this audit involved a 'red team' simulated exercise. A red team involves authorised attackers seeking to achieve certain objectives within the target's environment. The red team simulated a determined external cyber threat actor seeking to gain access to TfNSW's systems. The red team also sought to test the physical security of some Sydney Trains' sites relevant to the agency's cyber security. The red team exercise was conducted with the knowledge of TfNSW and Sydney Trains.

This audit included the Department of Customer Service as an auditee, as they have ownership of the CSP through Cyber Security NSW. This audit did not examine the management of cyber risk in the Department of Customer Service.

This audit assessed how effectively selected agencies identify and manage their cyber security risks. The audit assessed this with the following criteria:

- Are agencies effectively identifying and planning for their cyber security risks?
- Are agencies effectively managing their cyber security risks?

Following this in-depth portfolio assessment, the Auditor-General for NSW will also table a report on NSW agencies' compliance with the CSP in the first quarter of 2021–22.

Conclusion

Transport for NSW and Sydney Trains are not effectively managing their cyber security risks. Significant weaknesses exist in their cyber security controls, and both agencies have assessed that their cyber risks are unacceptably high. Neither agency has reached its Essential 8 or Cyber Security Policy target levels. This low Essential 8 maturity exposes both agencies to significant risk. Both agencies are implementing cyber security plans to address identified cyber security risks.

This audit identified other weaknesses, such as low numbers of staff receiving basic cyber security awareness training. Cyber security training is important for building and supporting a cyber security culture. Not all of the weaknesses identified in this audit had previously been identified by the agencies, indicating that their cyber security risk identification is only partially effective.

Agency executives do not receive regular detailed information about cyber risks and how they are being managed, such as information on mitigations in place and the effectiveness of controls for cyber risk. As a result, neither agency is fostering a culture where cyber security risk management is an important and valued aspect of executive decision-making.

TfNSW and Sydney Trains are partially effective at identifying their cyber security risks and both agencies have cyber security plans in place

Both agencies regularly carry out risk assessments and have identified key cyber security risks, including risks that impact on the agencies' crown jewels. These risks have been incorporated into the overall enterprise risk process. However, neither agency regularly reports detailed cyber risk information to agency executives to adequately inform them about cyber risk. The Cyber Security Policy (CSP) requires agencies to foster a culture where cyber security risk management is an important and valued aspect of decision-making. By not informing agency executives in this way, TfNSW and Sydney Trains are not fulfilling this requirement.

Agencies' cyber security risk assessment processes are not sufficiently comprehensive to identify all potential risks. Not all of the weaknesses identified in this audit had previously been identified by the agencies.

To address identified cyber security risks, both agencies have received funding approval to implement cyber security plans. TfNSW first received approval for its cyber security plan in 2017. Sydney Trains received approval for its cyber security plan in February 2020. In 2020–21 TfNSW and Sydney Trains combined their plans into the Transport Cyber Defence Rolling Program business case valued at $42.0 million over three years. This is governed as part of a broader Cyber Defence Portfolio (CDP). The CDP largely takes a risk-based approach to annual funding. The Cyber Defence Portfolio Steering Committee and Board can re-allocate funds from an approved project to a different project. This re-allocation process could be improved by making it more risk-based.

TfNSW and Sydney Trains are not effectively managing their cyber security risks

Neither agency has fully mitigated its cyber security risks. These risks are significant. Neither TfNSW nor Sydney Trains have reduced their cyber risk to levels acceptable to the agencies. Both agencies have set a risk tolerance for cyber security risks, and the identified enterprise-level cyber security risks remain above this rating. Both agencies' self-attested maturity against the Essential 8 remains low in comparison to the agencies' target levels, and in relation to the significant risks and vulnerabilities that are exposed. Little progress was made against the Essential 8 in 2020.

Neither agency has reached its target levels of maturity for the CSP mandatory requirements. Not reaching the target rating of the CSP mandatory requirements risks information and systems being managed inconsistently or not in alignment with good governance principles. The Transport Cyber Defence Rolling Program has a KPI to achieve a target rating of three for all CSP requirements where business appropriate. TfNSW considers this target rating to be its target for all the CSP requirements. However TfNSW has not undertaken analysis to determine whether this target is appropriate to its business.

The CSP makes agencies accountable for the cyber risks of their ICT service providers. While both agencies usually included their cyber security expectations in contracts with third-party suppliers, neither agency was routinely conducting audits to ensure that these expectations were being met.

The CSP requires agencies to make staff aware of cyber security risks and deliver cyber security training. TfNSW is responsible for delivering cyber security training across the Transport cluster, including in Sydney Trains. TfNSW was not effectively delivering cyber security training across the cluster because training was not mandatory for all staff at the time of the audit and completion rates among those staff assigned the training was low. As such, only 7.2 per cent of staff across the Transport cluster had completed introductory cyber security training as at January 2021.

1. Key findings

Agencies had not identified all risks detected by this audit

TfNSW's and Sydney Trains' risk identification processes are not identifying all potential risks. Not all of the weaknesses identified in this audit – many of which are significant – had previously been identified by the agencies, indicating that cyber security risk identification is only partially effective.

Additional information on previously undetected vulnerabilities which were exposed in the course of this audit has been provided in detail to both agencies. Information about why it is not included here is provided in the Foreword to this report.

Agencies have assessed their enterprise-level cyber risks as being above acceptable levels

Risk tolerance is the amount of risk which an agency will accept or tolerate without developing further strategies to modify the level of risk. Transport IT reported five enterprise-level cyber security risks in TfNSW to the enterprise risk team in September 2020. At the time of the audit, all five risks were rated above the agency's risk tolerance. Four of these risks were rated as 'high' and the other risk was rated as 'very high'.

Sydney Trains has identified one main cyber security risk in its IT enterprise-level risk register and another risk with a potential cyber cause. Both of these IT risks are deemed to have a residual risk of 'unacceptable'.

Similarly, two cyber-related enterprise-level OT risks have been determined to be above the agency's risk tolerance. One risk is rated as 'unacceptable' and the other risk, while not entirely cyber related, is rated 'undesirable' and is deemed to have some causes which may stem from a cyber-attack.

Both agencies' CSP and Essential 8 maturity is low in comparison to their target levels, and in reference to the significant risk exposed

Both agencies have set target maturity ratings for the Essential 8 but none of the Essential 8 ratings across either agency are currently implemented to this level. Both agencies have a low level of Essential 8 maturity, both in terms of overall risk mitigation and in comparison with target levels. This low maturity exposes both agencies to significant risk and specific vulnerabilities.

Given that the Essential 8 include the controls which are most commonly needed to deter cyber-attacks, low maturity may leave open vulnerabilities without sufficient safeguards. The Cyber Defence Portfolio (CDP) work in 2019 and 2020 relevant to the Essential 8 largely focussed on determining the current state of the Essential 8 and creating a target state roadmap.

Cyber Security NSW allows each agency to determine their target level of maturity for the first 20 CSP mandatory requirements. All of Sydney Trains' target maturity levels are at least a three (defined), with a target of four (quantitatively managed) for many of the mandatory requirements. Sydney Trains has not met its target ratings against many of the mandatory requirements.

The Transport Cyber Defence Rolling Program has a program KPI to ensure that the entire cluster reaches a minimum maturity level of three against all the CSP requirements by 2023. This was the minimum requirement set by Cyber Security NSW during the 2019 CSP attestation reporting period. TfNSW has not met its target ratings against many of the mandatory requirements.

TfNSW has not reviewed its CSP targets to determine if a three is desirable for all requirements or if a higher target level may be more appropriate. It is important for senior management to set cyber security objectives as a demonstration of leadership and a commitment to cyber security.

TfNSW and Sydney Trains consider cyber security threats when performing risk assessments

CSP requirement 1.4 states that agencies must consider cyber security threats when performing risk assessments and include high and critical risks in the agency's overall risk management framework. Both agencies undertake detailed risk assessments for cyber security and have incorporated high and critical risks into their overall risk management framework.

TfNSW's Transport IT section compiles detailed cyber security risk information, including for high and critical risks. Transport IT also undertakes risk assessments for any IT system identified as one of the cluster's crown jewels, the most valuable and operationally vital systems in the cluster. Sydney Trains has undertaken its own risk assessments for its IT and OT crown jewels.

By not sharing detailed information about cyber risks with agency executives, neither agency is fostering a culture where cyber security risk management is an important and valued aspect of decision-making

CSP requirement 2.3 states that agencies must foster a culture where cyber security risk management is an important and valued aspect of decision-making. To ensure that this can be achieved, and to ensure adherence to good practice risk management, agencies should share risk information with agency executives so that it may be used to inform strategic decision-making.

The TfNSW enterprise risk team produces a 'risk profile' which aggregates common risk themes to present to TfNSW executives. This risk profile does not contain comprehensive information about cyber security risks and does not provide details which would be useful to inform strategic decision-making. The Deputy Secretary Corporate Services is responsible for reporting to the Executive Management Committee on cyber risks, but this only occurred irregularly throughout 2019 and 2020.

Sydney Trains' risk register includes high and critical cyber risks, along with detailed risk information such as potential causes, existing mitigations and planned mitigations. As with TfNSW, Sydney Trains executives only receive a risk profile without comprehensive information. Specifically, executives do not receive information on planned mitigations, meaning that it is difficult to use this information to inform strategic decision-making. Given that Sydney Trains has rated its cyber security risks at the highest risk category (unacceptable), it is vital that agency executives are fully informed about this. This audit found that they have not been provided this information in sufficient detail.

Both agencies have cyber security plans in place in line with the CSP

Part of CSP mandatory requirement 1.3 is that agencies must have an approved cyber security plan to manage the agency's cyber security risks. Both TfNSW and Sydney Trains are implementing plans to fulfil this CSP requirement.

In November 2017, TfNSW approved the Cyber Uplift Program (CUP) worth $36.9 million over three years starting in 2018–19. The CUP is designed to fund not just the cyber security of TfNSW as an agency in its own right, but also cyber security uplift across agencies in the Transport cluster. The CUP forms the majority of the broader Cyber Defence Portfolio (CDP). From 2020–21, TfNSW has moved to the Transport Cyber Defence Rolling Program for the entire Transport cluster. The total approved rolling business case value is $42.0 million over three years starting in 2020–21. This is in addition to $18.1 million in TfNSW and Sydney Trains operational expenditure over that period.

Sydney Trains received final approval for the preliminary business case for the agency's Cyber Uplift Program in February 2020. Early work pre-empting this business case commenced in November 2019 and was scheduled for completion in 2020. Following this, Sydney Trains proposed a full $30.0 million, three-year business case covering both IT and OT. After an executive decision in March 2020, Sydney Trains joined the Transport Cyber Defence Rolling Program.

The Transport cluster is not effectively implementing cyber security awareness training

Agencies are responsible for implementing regular cyber security education for all employees and contractors under mandatory requirement 2.1 in the CSP, as part of building a cyber security culture. TfNSW is responsible for delivering cyber security awareness training to the whole Transport cluster, including Sydney Trains. While TfNSW has training available to staff, at the time of the audit it was not delivering this effectively. TfNSW did not make training mandatory for most staff nor did it require staff to repeat training regularly. Even among those staff who had been assigned the training, completion rates are low, indicating that it was not effectively monitoring delivery of the training. Cyber security training is important for building and supporting a cyber security culture.

Only 7.2 per cent of staff across the Transport cluster had completed the Cyber Safety for New Starters training course as at January 2021. This course is mandatory for new starters, however, only 53 per cent of staff assigned the Cyber Safety for New Starters training module had completed the course by January 2021. In Sydney Trains, only 4.2 per cent of staff had completed this training as at January 2021.

TfNSW has advised that it will implement mandatory annual training from July 2021 for all staff.

2. Recommendations

As a matter of priority, Transport for NSW and Sydney Trains should:

1. develop and implement a plan to uplift the Essential 8 controls to the agency's target state
2. address the vulnerabilities detected as part of this audit, and previously described in a detailed Audit Office report provided to both agencies.

By June 2022, Transport for NSW and Sydney Trains should:

3. ensure cyber security risk reporting to executives and their Audit and Risk Committees by:
    - reporting detailed cyber risk information on a regular basis
    - aligning reporting more closely with Treasury Policy TPP 12-03 'Risk management toolkit'
    - presenting mitigations for cyber risks to inform executives on plans to reduce risk to within risk tolerance
4. collect supporting information for the Cyber Security Policy self-assessments and undertake assurance to ensure that supporting information meets attested levels
5. classify all information and systems according to importance in line with Cyber Security Policy mandatory requirement 3.3 and integrate this with the crown jewels identification process
6. require more rigorous analysis to re-prioritise Cyber Defence Portfolio funding to ensure that decisions are made on a risk basis
7. improve cyber security training by:
    - making cyber security awareness training mandatory for all staff across cluster
    - repeating cyber security training on an annual basis in line with DCS-2020-05, Cyber Security NSW Directive - Practice Requirements for NSW Government
    - ensuring that training is completed by assigned staff.

By June 2022, Transport for NSW should:

8. assess the appropriateness of its target rating for each of the Cyber Security Policy mandatory requirements.

By June 2022, Department of Customer Service should:

9. clarify the requirement for the Cyber Security Policy reporting to apply to all systems
10. require agencies to report the target level of maturity for each mandatory requirement they have determined appropriate for their agency.

1. Introduction

1.1 Cyber Security Policy in NSW

Cyber Security NSW and the NSW Cyber Security Policy

Cyber Security NSW in the Department of Customer Service (DCS) sets cyber security policy in New South Wales. Cyber Security NSW first released the NSW Cyber Security Policy (CSP) on 1 February 2019, replacing the NSW Digital Information Security Policy (DISP). The CSP outlines a list of 25 mandatory requirements which agencies must implement and report against by 31 August each year. Cyber Security NSW updates the CSP annually. Appendix two contains a complete list of the 25 mandatory requirements at the time of this audit.

The mandatory requirements are split into five broad areas:

- Lead - Agencies must implement cyber security planning and governance and report against the requirements outlined in the CSP and other cyber security measures.
- Prepare - Agencies must build and support a cyber security culture across their agency and NSW Government more broadly.
- Prevent - Agencies must manage cyber security risks to safeguard and secure their information and systems.
- Detect/Respond/Recover - Agencies must improve their resilience including their ability to rapidly detect cyber incidents and respond appropriately.
- Report - Agencies must report against the requirements outlined in the CSP and other cyber security measures.

This audit focussed on the first three of these categories, as well as reporting against the CSP. The Audit Office of NSW released a report in March 2018 entitled 'Detecting and responding to cyber security incidents', which audited agencies' detection and response capabilities.

Cyber Security NSW has developed a maturity model for these mandatory requirements and has released guidance to assist agencies in implementing them. Agencies must report to Cyber Security NSW on the implementation of the mandatory requirements by 31 August each year. Agencies must report to Cyber Security NSW on their self-assessed maturity against the CSP mandatory requirements with a result from one to five, which represents the level of agency maturity. The five levels of implementation are:

- One - Initial
- Two - Managed/Developing
- Three - Defined
- Four - Quantitatively managed
- Five - Optimised.

While Cyber Security NSW did not audit the accuracy of the self-assessments in 2019 or 2020, in December 2020 DCS released 'DCS-2020-05 Cyber Security NSW directive - Practice Requirement for NSW Government', which advised that from 2021 agencies would be subject to audits by Cyber Security NSW to test compliance with the CSP.

The Auditor-General for NSW will table a report on agencies' compliance with the CSP in the first quarter of 2021–22.

The Australian Cyber Security Centre Essential 8 Strategies to Mitigate Cyber Security Incidents

Mandatory requirement 3.2 of the CSP requires agencies to implement the Australian Cyber Security Centre (ACSC) Essential 8 Strategies to Mitigate Cyber Security Incidents (the Essential 8). The ACSC is an Australian Government organisation which has released advice on eight essential cyber security strategies (the Essential 8) which organisations should implement. While these strategies will not guarantee protection against all cyber threats, they serve as a baseline set of protections which agencies can put in place to make it more difficult for adversaries to compromise a system. A summary of the Essential 8 controls are displayed in Exhibit 1.

Exhibit 1 - Summary of Essential 8 controls

Requirement	Importance
Mitigation Strategies to Prevent Malware Delivery and Execution	
1. Application whitelisting allows only approved programs to run on systems.	Non-approved applications (including malicious code) are prevented from executing. It is more effective than traditional anti-virus or anti-malware programs and can stop attacks that are not blocked by these tools.
2. Patch applications with security fixes once they are available.	Security vulnerabilities in applications can be used to execute malicious code on systems.
3. Configure Microsoft Office macro settings to only allow trusted macros to run within Office applications.	Microsoft Office macros can be used to deliver and execute malicious code on systems.
4. User application hardening, by switching off unneeded parts of applications.	Flash, ads and Java are popular ways to deliver and execute malicious code on systems.
Mitigation Strategies to Limit the Extent of Cyber Security Incidents	
5. Restrict administrative privileges to minimise the use of the most powerful accounts and protect them from misuse.	Admin accounts are the ‘keys to the kingdom’. Adversaries use these accounts to gain full access to information and systems.
6. Patch operating systems with security fixes once they are available.	Security vulnerabilities in operating systems can be used to further the compromise of systems.
7. Multi-factor authentication to add extra layers of protection and ensure only approved users can access systems.	Stronger user authentication makes it harder for adversaries to access sensitive information and systems.
Mitigation strategies to recover data and maintain system availability	
8. Daily backups of important data, software and configuration settings so that it can be restored if systems are compromised.	To ensure information can be accessed following a cyber security incident (e.g. a ransomware incident) limiting the loss of data to no more than one day.

Source: Australian Cyber Security Centre, 'Essential Eight Explained', June 2020.

As with the CSP mandatory requirements, agencies are required to report to Cyber Security NSW on their maturity against each of the Essential 8. Cyber Security NSW has modified the ACSC maturity scale against the Essential 8 for NSW Government agencies by adding a maturity level 'zero'. Agencies can use level 'zero' if the maturity of their implementation does not meet the requirements for level one of the ACSC maturity model. This means that the Essential 8 maturity rating operates on a scale of zero to three.

Information Security Management Systems (ISMS)

CSP mandatory requirement 3.1 requires agencies to implement an Information Security Management System (ISMS) covering at least the agency's crown jewels. Crown jewels are the most valuable or operationally vital systems or information in an organisation.

Mandatory requirement 3.1 also requires an ISMS to be compliant with, or modelled on, one or more recognised Standards. The most common Standard used for IT security is ISO27001. The ISO27000 definition of an ISMS can be seen in Exhibit 2.

Exhibit 2 - ISO27000: 2018 definition of an ISMS

> An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives.

Source: ISO27000:2018.

Aligning an ISMS with ISO27001 allows organisations to maintain a structured and comprehensive framework for identifying and assessing information security risks, selecting and applying applicable controls, and measuring and improving their effectiveness. Operating an ISMS certified against, or in alignment with, ISO27001, allows agencies to have greater confidence that they are managing information security risks. Information and systems which are part of an ISMS are likely to receive a higher degree of structured protection than those systems which are not part of an ISMS as it can help to put in place appropriate information management structures and processes.

1.2 Audited agencies

Two agencies were subject to this audit: TfNSW and Sydney Trains. Both agencies are part of the broader Transport cluster. TfNSW provides some cyber security services to the rest of the cluster through its Transport IT function and through the Cyber Defence Portfolio. These are discussed throughout the report.

The audit of TfNSW focused on Transport IT. TfNSW has numerous Divisions and four ISMS. TfNSW submitted the following four self-assessments against the CSP to Cyber Security NSW in 2020:

- Group IT (the former name for Transport IT)
- Ex-Roads and Maritime Services
- Customer Strategy and Technology (IT)
- Customer Strategy and Technology (OT).

Each of these self-assessments aligned to a separate ISMS in TfNSW. The TfNSW component of this audit considered primarily the Group IT reporting, as this ISMS covers four of TfNSW's crown jewels. Further, Transport IT (formerly Group IT) plays a key role in setting policy for the rest of the cluster, providing governance arrangements and standards which other Divisions across the Transport cluster either may or must implement. As such, the focus on Transport IT allowed the audit to consider both TfNSW activities specifically and cluster-wide activities more broadly.

The audit of Sydney Trains considered both the IT and Operational Technology (OT) ISMS. OT is technology which is used in ensuring the operations of the train network, and requires a fundamentally different approach to information security than IT. For example, not all of the Essential 8 apply to OT, and instead there are other similar controls which Cyber Security NSW has advised relevant organisations to implement in their place. OT also uses different Standards to IT; for example, ISO27001 does not apply to OT.

This audit also included the Department of Customer Service as an auditee, as they have ownership of the CSP through Cyber Security NSW. This audit did not examine the management of cyber risk in the Department of Customer Service.

1.3 Testing systems using a simulated cyber security exercise

For this audit, we conducted a simulated cyber security exercise on TfNSW and Sydney Trains, known as a red team. A red team involves authorised attackers seeking to achieve certain objectives within the target's environment. The red team typically has minimal knowledge of the target's environment and seeks to simulate how a determined threat actor would go about achieving those objectives.

This red team exercise simulated a determined external cyber threat actor seeking to gain access to TfNSW's systems. Further, the red team also sought to test the physical security of some Sydney Trains' sites relevant to the agency's cyber security. The red team exercise was conducted with the knowledge of TfNSW and Sydney Trains.

A more detailed report has been provided to the agencies outlining the detailed findings of the red team exercise to allow the agencies to take actions to address identified vulnerabilities.

1.4 About the audit

This audit assessed how effectively Transport for NSW and Sydney Trains identify and manage their cyber security risks. The audit assessed this with the following criteria:

- Are agencies effectively identifying and planning for their cyber security risks?
- Are agencies effectively managing their cyber security risks?

This audit also included the Department of Customer Service as an auditee, as they have ownership of the CSP through Cyber Security NSW. This audit did not examine the management of cyber risk in the Department of Customer Service.

2. Identifying and planning for cyber risks

2.1 Identifying cyber risks

Agencies consider cyber security threats when performing risk assessments

The CSP outlines mandatory requirements which relate to how cyber security risks should be managed in NSW Government agencies. Exhibit 3 contains the relevant requirements.

Exhibit 3 - CSP risk management requirements

Agencies must:

- 1.2 - ensure there is a governance committee at the executive level (dedicated or shared) to be accountable for cyber security including risks, plans and meeting the requirements of this policy. Agencies need to consider governance of ICT systems and OT to ensure no gaps in cyber security related to items such as video surveillance, alarms, life safety and building management systems that use automated or remotely controlled or monitored assets including industrial Internet of Things (IoT) devices
- 1.3 - have an approved cyber security plan to manage the agency's cyber security risks, integrated with business continuity arrangements. This must include consideration of threats, risks and vulnerabilities that impact the protection of the agency's information, ICT assets and services
- 1.4 - consider cyber security threats when performing risk assessments and include high and critical risks in the agency's overall risk management framework
- 1.5 - be accountable for the cyber risks of their ICT service providers and ensure the providers comply with the applicable parts of this policy and any other relevant agency security policies. This must include providers notifying the agency quickly of any suspected or actual security incidents and following reasonable direction from the agency arising from incident investigations.

Source: Cyber Security NSW, NSW Cyber Security Policy, February 2020.

CSP requirement 1.4 states that agencies must consider cyber security threats when performing risk assessments and include high and critical risks in the agency's overall risk management framework. Both agencies undertake detailed risk assessments for cyber security and have incorporated high and critical risks into their overall risk management framework.

TfNSW's Transport IT section compiles detailed cyber security risk information into aggregated enterprise-level cyber risks, including for high and critical risks. These high and critical risks are reported through the agency's enterprise risk management system, indicating that they have been incorporated into the overall enterprise risk process. The risks reported through this system are aggregated from lower-level risks, rather than presenting specific vulnerabilities.

Transport IT also offers a service on request from business areas to conduct a cyber security risk assessment for any system identified as one of the Transport cluster's crown jewels. Sydney Trains undertakes its own detailed risk assessments for its IT and OT crown jewels. These risk assessments contain information about security maturity, current vulnerabilities and recommendations for how to address the vulnerabilities. In December 2019, Sydney Trains undertook a review of its entire OT network and sought to identify areas of risk and potential improvement. This process allows for a fuller risk identification of crown jewels.

Transport IT identified a change in TfNSW's cyber security risk profile as a result of the COVID-19 pandemic. This indicates that TfNSW can undertake additional risk identification procedures when there are major potential changes to the operating environment.

Transport IT can undertake risk assessments when new IT projects come online or when existing systems undergo significant change. TfNSW provided evidence that this occurs in practice and that cyber security is a regular part of TfNSW project management. This process is not mandatory for major new projects or revisions to systems, meaning that there may be systems carrying risk that have not had this detailed assessment.

Sydney Trains IT has a cyber security risk assessment process which aims to conduct risk assessments when new information assets are introduced to Sydney Trains or when there are changes to existing information assets.

Sydney Trains' risk register includes high and critical cyber risks, along with detailed risk information such as potential causes, existing mitigations and planned mitigations. These risks are aggregated when reported to executives, rather than presenting specific vulnerabilities. Sydney Trains monitors and updates its key risks on a quarterly basis, involving relevant IT and OT staff. Sydney Trains' high and critical cyber risks are reported to the enterprise risk function.

Agencies did not identify all risks detected by this audit

TfNSW's and Sydney Trains' risk identification processes are not identifying all potential risks. Not all of the weaknesses identified in this audit – some of which were significant – had previously been identified by the agencies, indicating that cyber security risk identification is only partially effective.

Additional information on previously undetected vulnerabilities which were exposed in the course of this audit has been provided in detail to both agencies. The Foreword of this report provides information about why this detail is not included here.

Neither agency is presenting detailed cyber risk information to executives, limiting its potential usage in decision-making

Effective risk management relies on the communication of risk information to ensure that decision makers can make fully-informed decisions. CSP requirement 2.3 states that agencies must foster a culture where cyber security risk management is an important and valued aspect of decision-making. The CSP maturity model makes some of the expected behaviours clear. The maturity model states that one of the requirements for a 'Quantitatively managed' ranking against CSP requirement 2.3 is that leadership is aware of good cyber security practices and factor these into relevant decision-making. For an 'Optimised' ranking against this CSP requirement, the Secretary must be briefed on cyber security risk management as part of cluster risk management reporting.

While risk information can be presented in a variety of ways, risk registers help to meet the information needs of senior leaders and Audit and Risk Committees. NSW Treasury has provided information on what is typically contained in a comprehensive risk register in TPP 12-03, 'Risk management toolkit'. While both agencies include much of this information in their divisional cyber security risk registers, this comprehensive information is not shared with agency executives. Not sharing detailed information with agency executives limits the information available to make strategic cyber security decisions, such as which risks need further mitigation and the level of investment required for that mitigation.

Each Division of TfNSW, including Transport IT, reports risks through an enterprise risk platform. The Enterprise Risk team then produces a 'risk profile' which aggregates common themes. Risk profiles are summaries used to present an overview of information contained in risk registers. The aim of a risk profile is to promote consistent organisational understanding of significant risks and their controls. NSW Treasury has provided advice on the sorts of information that may be contained in a typical risk profile in TPP 12-03.

The risk profile provided to TfNSW executives does not contain comprehensive information about cyber security and does not provide some key details which would be useful as summaries of the information in risk registers. For example, the risk profile does not contain the key risks attached to each risk area, information on the implementation and effectiveness of controls and the key controls in place for the risks. This means that while cyber security is presented as an area of risk, no details are communicated to agency executives. In addition, while this risk information is due to be reported to agency executives on a quarterly basis, risk information was only presented once in 2020. This means that cyber risk information was not presented to agency executives frequently, reducing senior leadership oversight.

Throughout most of 2020, Sydney Trains reported detailed cyber risk information to agency executives. However, from late 2020 onwards, Sydney Trains executives only receive a risk profile without comprehensive information. Specifically, executives do not receive information on planned mitigations, meaning that it is difficult to use this information to make decisions in the future and determine whether additional actions are needed to address this risk. Given that Sydney Trains has rated cyber security risks at the highest risk category (unacceptable), it is vital that agency executives are fully informed about this.

By not reporting to agency executives about cyber security on a detailed and consistent basis, TfNSW and Sydney Trains are not fostering a culture where cybers security risk management is an important and valued aspect of decision-making, as required by the CSP.

Gaps in TfNSW and Sydney Trains' cyber governance limits the cyber risk information reported to senior executives

It is the responsibility of TfNSW's Deputy Secretaries to manage risks in their area of responsibility and to report risks to the Executive Management Committee as appropriate. Throughout 2019 and 2020, the Deputy Secretary Corporate Services presented cyber risk information to the Executive Management Committee irregularly. Given the enterprise-wide nature of cyber risk and the scale of cyber risk identified in TfNSW, it is important for all Divisions to be aware of the extent of cyber risks and the strategies in place to mitigate them and that regular updates on these are provided. The Executive Management Committee provides an appropriate venue for this information sharing.

As shown in Exhibit 3, CSP mandatory requirement 1.2 states that agencies must have a governance committee at the executive level to be responsible for cyber security, including risk management and cyber security plans. TfNSW's Cyber Defence Portfolio Board (CDP Board) fulfils the role of CSP mandatory requirement 1.2 for TfNSW. Cyber risks and mitigations are regularly discussed in each monthly meeting. The CDP Board is chaired by the Transport Group CIO and includes representatives from across the Transport cluster, including the CIO Group Rail, Finance & Business Services, who represents Sydney Trains.

The Transport Group CIO is the risk owner for TfNSW's enterprise-level cyber risks, and thus it is appropriate for them to be involved in the CDP Board, however prior to August 2019, the Deputy Secretary Corporate Services chaired the CDP Board meeting. Given the Deputy Secretary's role in keeping the TfNSW Secretary informed about cyber risk and the agency's cyber security plan, this may be a more appropriate arrangement.

Another key committee for risk management is the TfNSW Audit and Risk Committee (ARC). The CSP advises that each agency's Chief Information Security Officer (CISO) should attend agency risk committee meetings as an advisor or member. The TfNSW CISO attended two of five ARC meetings in 2020 to present on cyber security and also occasionally attends other Transport cluster ARCs. The CISO was not present at the other three TfNSW ARC meetings. This means that specialist advice on the technical details of cyber security was not available to inform the ARC's advice. Given that TfNSW had assessed cyber risk at the highest available level, it is important to ensure that the CISO is available to discuss this at the ARC.

Sydney Trains re-formed the Information Security Governance Committee (ISGC) in 2020 to bring together IT and OT governance and create a single forum for the discussion of cyber risk. This is in fulfillment of CSP requirement 1.2. The ISGC does not have a formal Terms of Reference, limiting its ability to operate as part of the Sydney Trains governance structure. The owners of Sydney Trains' enterprise risks attend this meeting, but none of the Chief Executive's direct reports attend the meeting.

Sydney Trains presented on cyber security to the Sydney Trains quarterly ARC meetings in 2020 as part of enterprise risk reporting, and the responsible IT staff attended to speak to these points.

Both agencies complied with the reporting and attestation requirements of the CSP, but there were some deficiencies in the reporting process

The CSP makes it mandatory for agencies to report on their compliance with the CSP to Cyber Security NSW and in their annual report. These requirements are outlined in Exhibit 4. Both agencies largely complied with these requirements of the CSP, though some areas of non-compliance were noted.

Exhibit 4 - CSP reporting requirements

Agencies must:

- 5.1 - report annually to their cluster CISO, or Cyber Security NSW, their compliance with the mandatory requirements in this policy, in the format provided by Cyber Security NSW. Cluster CISOs must provide all reports to Cyber Security NSW by 31 August
- 5.2 - report annually to their cluster CISO, or Cyber Security NSW, their maturity against the ACSC Essential 8, in the format provided by Cyber Security NSW. Cluster CISOs must provide all reports to Cyber Security NSW by 31 August
- 5.3 - report annually to their cluster CISO, or Cyber Security NSW, the agency's cyber security risks with a residual rating of high or extreme, in the format provided by Cyber Security NSW by 31 August
- 5.4 - report annually to their cluster CISO, or Cyber Security NSW, the agency's 'crown jewels'. Cluster CISOs must provide all reports to Cyber Security NSW by 31 August
- 5.5 - provide a signed attestation to Cyber Security NSW by 31 August each year and include a copy of its attestation in its annual report, as outlined in Section 4 (of the CSP). If the agency does not complete an annual report, an attestation must still be completed and signed off by its agency head and submitted to the cluster CISO.

Source: Cyber Security NSW, NSW Cyber Security Policy, February 2020.

Both agencies reported to Cyber Security NSW only on the coverage of its ISMS. Sydney Trains submitted two reports to Cyber Security NSW in 2020, one report for its IT ISMS and one report for its OT ISMS. TfNSW submitted four compliance reports to Cyber Security NSW in 2020, as outlined in the introduction.

Cyber Security NSW advised the Audit Office that while there was no specific guidance released on whether agencies should report against the ISMS or their entire network, the expectation was that agency maturity ratings would be provided for the entirety of the agency's systems, processes and people. Cyber Security NSW advised that agencies were free to determine how they developed their maturity rating on a risk basis, but the expectation was that the reporting would reflect the totality of systems. TfNSW and Sydney Trains could improve their reporting process by reporting on an organisation-wide basis, rather than just on the ISMS.

Mandatory requirement 5.2 of the CSP requires agencies to report to Cyber Security NSW on their Essential 8 ratings in the approved format. While both agencies reported to Cyber Security NSW, they deviated from the approved format. The maturity ratings provided to agencies as part of the reporting template contain only ratings zero, one, two or three. Both agencies returned reports to Cyber Security NSW that contained half points between these ratings. The instructions are clear that if an agency has partially implemented the requirements, they should note this in the comments, but the instructions do not advise to include half points.

TfNSW does not provide assurance around the accuracy of its self-assessed reporting levels

As shown in Exhibit 4, agencies are required to provide maturity ratings to Cyber Security NSW as part of its annual attestation process. The CSP makes agency heads accountable for ensuring that their agency complies with the CSP. To perform this role, accurate information about the agency's current maturity ratings is needed. While it is not required by the CSP, having an assurance review or internal audit of the self-assessment would assist agency heads in ensuring that the information provided to them about an agency's maturity level is accurate.

TfNSW has not undertaken any assurance or internal audit to ensure that the four self-assessments provided to Cyber Security NSW are accurate. Transport IT engaged a consultant to review the attestation statement that was included in TfNSW's annual report, but this did not involve checking the accuracy of results reported to Cyber Security NSW. TfNSW Divisions were also not required to provide any documentation to support their maturity ratings. This means that TfNSW did not receive assurance that stated results were accurate, nor were they in a position to review these without the supporting documentation.

The Auditor-General for NSW will table a report on agencies' compliance with the CSP in the first quarter of 2021–22.

Sydney Trains conducted an internal audit to validate its maturity ratings in 2020

Sydney Trains conducted an internal audit to determine the accuracy of its self-assessed maturity ratings in 2020. This involved reviewing supporting documentation to assess the adequacy of Sydney Trains' attestation. The review provided a list of issues and suggested actions that Sydney Trains agreed to implement throughout 2021 and 2022. Sydney Trains advised that an internal audit was not planned for 2021.

Contrary to the requirements of the CSP, TfNSW has not classified its information and systems according to importance

The CSP requires agencies to identify their crown jewels and report these to Cyber Security NSW. These requirements can be found in Exhibit 5. Crown jewels are the most valuable or operationally vital systems or information in an organisation.

Exhibit 5 - CSP crown jewels requirements

Agencies must:

- 3.3 - classify information and systems according to their importance (i.e. the impact of loss of confidentiality, integrity or availability), adhere to the requirements of the NSW Government Information Classification Labelling and Handling Guidelines and:
  - assign ownership
  - implement controls according to their classification and relevant laws and regulations
  - identify the agency's 'crown jewels' and report them to Cyber Security NSW as per mandatory requirement 5.4
- 5.4 - report annually to their cluster CISO, or Cyber Security NSW, the agency's 'crown jewels'. Cluster CISOs must provide all reports to Cyber Security NSW by 31 August.

Source: Cyber Security NSW, NSW Cyber Security Policy, February 2020.

CSP requirement 3.3 requires agencies to classify their information and systems according to their importance. Importance is defined in the CSP as the impact of losing the system on confidentiality, integrity or availability.

TfNSW has not compiled a comprehensive list of its IT systems nor has it classified its systems according to importance. Compiling this list would assist with crown jewel identification, as it could be used to systematically identify high-value information and systems. These high-value and high-risk systems may be suitable for further analysis to determine whether they are crown jewels. TfNSW's process for identifying its crown jewels was to hold discussions with business owners across the Transport cluster and ask these stakeholders what their highest risk assets were. Crown jewels may also be identified through a detailed assessment as new assets come online or are heavily altered.

Sydney Trains has carried out a risk rating for all of its IT systems. This risk assessment includes a determination of whether a system is business critical or operationally critical. While this could form a useful input as part of the crown jewels identification process, Sydney Trains follows the TfNSW crown jewels identification process. As such, Sydney Trains does not currently use its risk rating of systems as part of its crown jewels identification process. All IT crown jewels are identified as 'business critical', the highest risk rating for IT systems.

2.2 Planning for cyber risks

Both agencies have cyber security plans and governance in place in line with the CSP, but implementation of Sydney Trains' plan was delayed and was not approved until February 2020

Having identified cyber risks, the CSP requires agencies to design plans to mitigate them. Part of CSP mandatory requirement 1.3 is that agencies must have an approved cyber security plan to manage the agency's cyber security risks. Both TfNSW and Sydney Trains have developed plans to fulfil this CSP requirement, though Sydney Trains did not receive approval for its business case from TfNSW's Finance and Investment Committee until February 2020.

In November 2017, TfNSW approved the Cyber Uplift Program (CUP) worth $36.9 million over three years starting in 2018–19. The Cyber Uplift Program formed the majority of the Cyber Defence Portfolio (CDP). The CDP is made up of a series of programs which aim to uplift the organisation's cyber security posture. The CUP is designed to fund not just the cyber security of TfNSW, but also cyber security uplift across the Transport cluster.

Sydney Trains obtained final approval of the preliminary business case for the agency's Cyber Uplift Program in February 2020. The agency was able to commence early work for this business case in November 2019. This early work included a total value of $2.0 million commencing in November 2019 and spread across the 2020 calendar year, of which approximately $1.2 million was to be spent on security remediation and the remainder was allocated for the development of a full business case. This preliminary work was scheduled for completion in 2020. At the same time, Sydney Trains endorsed the development of a $30.0 million, three-year business case covering both IT and OT.

Sydney Trains commenced preliminary work on its Cyber Uplift Program in November 2019. This was not in line with the agency's cyber security strategy. The Sydney Trains Cyber Security Strategy and Roadmap was approved in December 2018 and suggested an approach to remediation and risk reduction that would commence in early 2019. Sydney Trains' approval for its business case came a year later than this initial plan. This delay was not commensurate with the scale of risk identified. Sydney Trains identified cyber risk as being one of its highest category risks. By not having an approved plan until February 2020, this risk was left exposed without dedicated mitigation on the required scale. Further, this meant that Sydney Trains did not implement CSP mandatory requirement 1.3, requiring a business plan, until February 2020.

In March 2020, TfNSW mandated that separate cyber business cases for each part of the Transport Cluster would not be approved, and that the Transport Cyber Defence Rolling Program for the entire Transport cluster should be created. This rolling business case replaces the final year of the CUP business case, though the new business case is still governed as part of the CDP. As a result of this change, TfNSW and Sydney Trains have combined as part of the Transport Cyber Defence Rolling Program case. The total approved business case value is $42.0 million over three years starting in 2020–21. This is in addition to $18.1 million in TfNSW and Sydney Trains operational expenditure over that period. Additional rolling business cases will be submitted as required following this.

To represent the CDP's cross-cluster approach, all Transport cluster agencies are represented on the CDP Board and the CDP Steering Committee, the two core elements of the CDP governance. One of the roles of the CDP Steering Committee is to decide on the prioritisation of funding each financial year. The CDP Board then endorses these funding changes. There is a separate governance committee for the Sydney Trains portion of the CDP funding which reports to the CDP Board, meaning that the Sydney Trains funding is focused on Sydney Trains' concerns but remains integrated with the Transport cluster.

Agencies used a risk-based approach to target funding initially in their cyber uplift plans but the re-prioritisation of funding could be more risk-oriented

Both agencies target their funding at high-risk areas at the start of each financial year. This has occurred across the CUP, the preliminary Sydney Trains Cyber Uplift Program and the combined Transport Cyber Defence Rolling Program. While the initial targeting of this funding was risk-based, the approach to changes in funding during each year has been less risk-oriented. This process could be improved by undertaking a more rigorous analysis of risk reduction to determine whether the new use of resourcing is preferable to the already-approved use of that funding.

Throughout 2019 and 2020, the CDP Steering Committee's approach to the prioritisation of funding across the original CUP and the Transport Cyber Defence Rolling Program was to determine which expenditure will present the highest risk reduction for the money and to fund those programs. Funding is also allocated to those pieces of work on which later projects are dependent. Prioritisation also occurred on the basis of reducing the highest rated risks. The initial targeting of the preliminary work for the Sydney Trains Cyber Uplift Program was determined by those pieces of work which could lay the foundation for overall risk reduction. After the Sydney Trains Cyber Uplift Program was combined with the Transport Cyber Defence Rolling Program, funding prioritisation occurred on the same basis as the rest of the CDP and as such took a risk-based approach to targeting funding.

In addition to determining the initial allocation of funds at the start of each year, the CDP Steering Committee can determine if any changes are required during each year. This re-prioritisation of funding occurred through 2019 and 2020. While the CDP aims to take a risk-based approach to funding, the re-allocated funding was not always judged on a risk basis to the same extent as the initial funding determinations. For example, there was no reference to total risk reduction, nor any analysis of why expenditure should be targeted at the program in question rather than another potential area for re-prioritisation.

The ability to re-direct funding in this way may be important for addressing pressing issues, however not taking a comparative approach to funding may result in a more reactive approach to risk management. An example of this is provided in Exhibit 6, which relates to the re-allocation of funding to Project La Brea, a project which commenced as part of the CDP following a critical cyber outage in June 2020.

Exhibit 6 - Re-allocation of funds to Project La Brea

On 11 June 2020 the State Transit Authority suffered a critical outage due to a cyber-attack. Project La Brea commenced on 25 June 2020 to rectify four key control weaknesses identified as a result of the cyber-attack. This project was moved into the CDP at a cost to the CDP of approximately $800,000. While many of the outcomes of this project would make the Transport cluster more difficult to attack, the re-prioritisation caused delays in some workstreams of the CDP which were already approved as part of the annual funding rounds. This delay came as a result of the need to re-assign staff from other workstreams to work on the Project La Brea uplift.

The cyber incident and re-allocation of resources had wide-ranging impacts on the CDP, with a number of workstreams experiencing delays in their timeline as a result. One of the workstreams impacted by this was the Essential 8 workstream which resulted in a delay in commencement from February 2021 to May 2021.

While the CDP Steering Committee and CDP Board may have felt it was preferable to re-allocate resources to Project La Brea, no work was presented to either governance committee justifying why this was a superior way to allocate resources compared to the other workstreams which were de-prioritised. This is indicative of a reactive allocation of CDP resources which does not fully take into account other potential sources of risk reduction.

Source: Audit Office analysis of TfNSW documents.

TfNSW provided evidence that as at January 2021 there was consideration of risk reduction in the re-allocation of underspent funds.

3. Managing cyber risks

Agencies have assessed their cyber risks as being above acceptable levels

An agency's risk tolerance is the amount of risk which the agency will accept or tolerate without developing further strategies to modify the level of risk. Risks that are within an agency's risk tolerance may not require further mitigation and may be deemed acceptable, while risks which are above the agency's risk tolerance likely require further mitigation before they become acceptable to the agency.

Both agencies have defined their risk tolerance and have identified risks which are above this level, indicating that they are unacceptable to the agency. TfNSW has defined 'very high' risks as generally intolerable and 'high' risks as undesirable. Its risk tolerance is 'medium'. Sydney Trains has four classifications of risk: A, B, C and D. A and B risks are deemed 'unacceptable' and 'undesirable' respectively, while C risks are considered 'tolerable'. This aligns with the TfNSW definition of a medium risk tolerance.

Transport IT reported five enterprise-level cyber security risks through its enterprise risk reporting tool in September 2020, all of which relate to cyber security or have causes relating to cyber security. These risks are in aggregate form, rather than relating to specific vulnerabilities. At the time of the audit, one of these risks was rated as very high and the other four rated as high. At this time, Transport IT had identified a further seven divisional-level risks which were above the agency's risk tolerance.

Similarly, Sydney Trains has identified one main cyber security risk in its IT enterprise-level risk register and another with a potential cyber cause. Both of these IT risks are deemed to have a residual risk of 'unacceptable'.

Similarly, two cyber-related OT risks have been determined to be above the agency's risk tolerance. One risk is rated as 'unacceptable'. Another risk, while not entirely cyber rated, is rated 'undesirable' and is deemed to have some causes which may stem from a cyber-attack.

Agencies have assessed their current cyber risk mitigations as requiring improvement

In addition to the risk ratings stated above, at the time of the audit neither agency believed that its controls were operating effectively. Transport IT had rated the control environments for its cyber security enterprise risks as 'requires improvement'. Mitigations were listed in the risk register for these risks but, in some cases, they were unlikely to reduce the risk to the target state or by the target date. For example, one risk had actions listed as 'under review' and no further treatment actions listed, but a due date of July 2021, while another risk was being treated by the CDP with a due date of July 2021. The CDP identified in May 2020 that while the average risk identified as part of that program will be reduced to a medium level by this date, ten high risks will still remain. Given the delays in the program, this number may be higher. As such, it seems unlikely that the enterprise risk will be reduced to below a 'high' level by July 2021.

Sydney Trains' IT and OT risk registers cross-reference controls and mitigations against the causes and consequences. The IT cyber security risk identified in the register had causes with no mitigations designed for them. Further, some of these causes did not have future mitigations designed for them. This risk also had controls in place which are identified as partially effective. For the unacceptable OT risk noted above, while there was a control designed for each of the potential causes, Sydney Trains had identified all of the controls in place as either partially effective or ineffective. This indicates that Sydney Trains was not effectively mitigating the causes of its cyber risks and, even where it had designed controls or mitigations, these were not always implemented to fully mitigate the cause of the risk.

Additional information on gaps in cyber mitigations which were exposed in the course of this audit has been detailed to both agencies. The Foreword of this report provides information about why this detail is not included here.

Essential 8 maturity is low across TfNSW and Sydney Trains and little progress was made in 2020

CSP mandatory requirement 3.2 states that agencies must implement the ACSC Essential 8. Agencies must also rate themselves against each of the Essential 8 on a maturity scale from zero to three and report this to Cyber Security NSW. A full list of the Essential 8 can be found in Exhibit 1. Both agencies have a low level of maturity against the Essential 8 not just in comparison to the targets they have set, but also in relation to the risks and vulnerabilities exposed. Both agencies have set target maturity ratings for the Essential 8 but none of the Essential 8 ratings across either agency are currently implemented to this level. Having a low level of Essential 8 maturity exposes both agencies to significant risks and vulnerabilities. Little progress was made between the 2019 and 2020 attestation periods.

Transport IT has set a target rating of three across all of the Essential 8. Sydney Trains has set a target rating of three for its IT systems. Sydney Trains had an interim target of two for its OT systems in 2020 and advised that this has since increased to three. It should be noted that not all the Essential 8 are applicable to OT systems.

None of the Essential 8 ratings across either agency are currently implemented to the target levels. Given that the Essential 8 provide the controls which are most commonly able to deter cyber-attacks, having maturity at a low level potentially exposes agencies to a cyber security attack.

Some work is underway across both TfNSW and Sydney Trains to improve the Essential 8 control ratings. The CDP provided some resources to the Essential 8 over 2019–20, with uplift focusing on specific systems. The CDP work in 2019 and 2020 relevant to the Essential 8 largely focussed on determining the current state of the Essential 8 and creating a target state roadmap. As a result, there was little improvement between the 2019 and 2020 attestation periods. The CDP has a workstream for the Essential 8 in its FY 2020–21 funding allocation, however as noted above in Exhibit 6 this was delayed as resources were redeployed to Project La Brea. Regardless, work on some specific aspects of the Essential 8 remain part of the 2020–21 CDP allocation, with workstreams allocated to improving three of the Essential 8. In addition, some work from Project La Brea should lead to an improvement in the Essential 8.

Sydney Trains' Cyber Uplift Program included a workstream which had in scope the uplift in the Essential 8 in IT. There were also other workstreams which aimed to improve some of the Essential 8 for OT systems. Work is also ongoing as part of the CDP to uplift these scores in Sydney Trains.

TfNSW and Sydney Trains have not reached their target maturity across the CSP mandatory requirements and TfNSW has not evaluated its cluster-wide target to ensure it is appropriate

Cyber Security NSW allows each agency to determine its target level of maturity for the first 20 CSP mandatory requirements. Agencies can tailor their target levels to their risk profile. Not reaching the target rating of the CSP mandatory requirements risks information and systems being managed inconsistently or not in alignment with good governance principles.

Sydney Trains has set its target level of maturity for IT and OT. All of Sydney Trains' target maturity levels are at least a three (defined), with a target of four (quantitatively managed) for many of the mandatory requirements. While Cyber Security NSW does not currently mandate a minimum level of maturity, in 2019 there was a requirement for each agency to target a minimum level of three.

Sydney Trains has not met its target ratings across the mandatory requirements.

The Transport Cyber Defence Rolling Program has a program KPI to ensure that the entire cluster reaches a minimum maturity level of three against all the CSP requirements by 2023. TfNSW has not reviewed its CSP mandatory requirement targets to determine if a three is desirable for all requirements or if a higher target level may be more appropriate. It is important for senior management to set cyber security objectives as a demonstration of leadership and a commitment to cyber security.

TfNSW has not met its target ratings across the mandatory requirements for its Group IT ISMS, which was the focus of this audit.

Both agencies claimed progress in their implementation of the mandatory requirements between 2019 and 2020. The audit did not seek to verify the self-assessed results from either agency.

Both agencies operate ISMS in line with the CSP

CSP mandatory requirement 3.1 requires agencies to implement an Information Security Management System (ISMS) or Cyber Security Framework (CSF), with scope at least covering systems identified as the agency's 'crown jewels'. The ISMS or CSF should be compliant with, or modelled on, one or more recognised IT or OT standard. As noted in the introduction, an ISMS 'consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets.' Both agencies operate an ISMS compliant with the CSP requirement.

As noted in the introduction, TfNSW operates four ISMS. The Transport IT ISMS is certified against ISO27001, the most common standard for ISMS certification. Three of TfNSW's six crown jewels are managed within this ISMS. The other ISMS are not certified to relevant standards, though TfNSW claims that they align with relevant controls. This is sufficient for the purposes of the CSP.

Sydney Trains operates two ISMS, one for IT and another for OT. Neither of these are certified to relevant ISMS Standards, however there have been conformance reviews of both IT and OT with relevant standards. These ISMS cover all crown jewels in the agency.

There are currently 11 ISMS in operation across the Transport cluster. TfNSW has proposed moving towards a holistic approach to these ISMS, with the CDP Board responsible for governing the available security controls and directing agency IT and OT teams to implement these.

Agencies are not routinely conducting audits of third-party suppliers to ensure compliance with contractual obligations

CSP mandatory requirement 1.5 makes agencies accountable for the cyber risks of their ICT service providers and ensuring that providers comply with the CSP and any other relevant agency security policies. The ACSC has provided advice on what organisations should do when managing third party suppliers of ICT. The ACSC advises that organisations should use contracts to define cyber security expectations and seek assurance to ensure that these contract expectations are being met. While both agencies usually include specific cyber security expectations in contracts, neither is routinely seeking assurance that these expectations are being met.

The NSW Government has mandated the use of the 'Core& One' contract template for low-value IT procurements and the Procure IT contract template for high-value IT procurements. Both of these contracts contain space for the procuring agency to include cyber security controls for the contractor to implement. The Procure IT contract template also includes a right-to-audit clause which allows agencies to receive assurance around the implementation of these controls. TfNSW and Sydney Trains used the mandated contracts for relevant contracts examined as part of this audit.

TfNSW included security controls in all the contracts examined as part of this audit. Compliance with ISO27001 was the most commonly stated security expectation. Of the contracts examined as part of this audit, only one contract did not have a right-to-audit clause. This contract was signed in October 2016. While these clauses are in place, TfNSW rarely conducted these audits on its third-party providers. Of the eight TfNSW contracts examined in detail, only two of these had been audited to confirm compliance with the stated security controls.

Sydney Trains included security controls in all but one of the contracts examined as part of this audit. Sydney Trains did not require contractors to be compliant with ISO27001, but only required compliance with whole-of-government policies. Sydney Trains does not routinely conduct audits of its third-party suppliers, however it did conduct deep-dive risk analyses of its top ten highest risk IT suppliers. This involved a detailed review of both the suppliers' security posture and also the contract underpinning the relationship with the supplier.

The CDP funding for 2020–21 includes a workstream for strategic third-party contract remediation. This funding is to conduct some foundational work which will allow the CDP to make further improvements in future years. While this funding will not address gaps in contract requirements or management across all contracts, this workstream aims to reduce the risks posed by strategic suppliers covering critical assets. Similarly, work is currently underway as part of the CDP to conduct OT risk assessments for key suppliers to Sydney Trains in a similar way to the work undertaken for IT suppliers.

Sydney Trains has risk assessed its third-party suppliers but TfNSW has not done so

It is important to conduct a risk assessment of suppliers to identify high-risk contractors. This allows agencies to identify those contractors who may require additional controls stated in the contract, those who require additional oversight, and also where auditing resources are best targeted.

Sydney Trains has risk assessed all its IT suppliers and, as noted above, has conducted a deep-dive risk analysis of its top ten highest risk suppliers. TfNSW has not undertaken similar analysis of its key suppliers, however it has identified risks attached to each of its strategic suppliers and has documented these. As a result of not risk assessing its suppliers, TfNSW cannot take a targeted approach to its contract management.

TfNSW demonstrated poor records handling relating to the contracts examined as part of this audit

TfNSW was not able to locate one of the contracts requested as part of the audit's sample. Other documentation, such as contract management plans, could not be located for many of the other contracts requested as part of this audit. These poor document handling practices limits TfNSW's ability to effectively oversee service providers and ensure that they are implementing agreed controls. It also limits public transparency on the effectiveness of these controls.

The Transport cluster is not effectively implementing cyber security awareness training

Agencies are responsible for implementing regular cyber security education for all employees and contractors under mandatory requirement 2.1 in the CSP. TfNSW is responsible for delivering this training to the whole Transport cluster, including Sydney Trains. The Transport cluster has basic cyber awareness training available for all staff. TfNSW also offers additional training provided by Cyber Security NSW targeted at executives and executive assistants. While TfNSW has training available to staff, it is not delivering this effectively. TfNSW does not make training mandatory for most staff nor does it require staff to repeat training regularly. Even among those staff who have been assigned the training, completion rates are low, meaning that delivery is not effectively monitored. Cyber security training is important for building and supporting a cyber security culture.

TfNSW is responsible for creating and rolling out all forms of training to agencies within the Transport cluster. Both TfNSW and Sydney Trains have the same mandatory cyber awareness training that is automatically assigned to new starters. At the time of the audit, this training was not mandatory for ongoing staff. TfNSW does make additional cyber security training available to staff who can choose to undertake the training themselves, or can be assigned the training by their manager. All TfNSW cyber security training is delivered via online modules and it is the responsibility of managers to ensure that it is completed.

Cyber security training completion rates for both TfNSW and Sydney Trains are low. Only 13.5 per cent of staff across the Transport cluster had been assigned the Cyber Safety for New Starters training as of January 2021. Although this course is mandatory for new starters, only 53 per cent of staff assigned the Cyber Safety for New Starters training module had completed the course by January 2021. As a result, only 7.2 per cent of staff across the entire Transport cluster had completed this training at that time. In Sydney Trains, less than one per cent of staff had completed this training as at January 2021 and a further 7.6 per cent of staff have completed the 'Cyber Security: Beyond the Basics' training. These low completion rates indicate that TfNSW is not effectively rolling out cyber security training across the cluster.

In December 2020, the Department of Customer Service released 'DCS-2020-05 Cyber Security NSW Directive - Practice Requirement for NSW Government', which made annual cyber security training mandatory for all staff from 2021. In line with this requirement, TfNSW has advised that it will be gradually implementing mandatory annual training from July 2021 for all staff.

The Transport cluster undertakes activities to build a cyber-aware culture in accordance with the CSP, but awareness remains low

Increasing staff awareness of cyber security risks and maintaining a cyber secure culture are both mandatory requirements of the CSP. While TfNSW does undertake some activities to build a cyber aware culture, awareness of cyber security risks remains low. This can be demonstrated by the low training rates outlined above, and the 'Spot the Scammer' exercise, described in Exhibit 7. TfNSW is responsible for delivering these awareness raising activities across the cluster.

TfNSW frequently communicates with staff across the Transport cluster about various cyber security risks through multiple avenues. Both agencies use the intranet, emails and other awareness raising activities to highlight the importance for staff to be aware of the seriousness of cyber risks. Advice given on the intranet includes tips for spotting scammers on mobile phones, promoting the cluster-wide training courses, as well as various advice that staff could use when dealing with cyber risks in the workplace.

In addition to these awareness raising activities, TfNSW has also undertaken a cluster-wide phishing email exercise called 'Spot the Scammer'. This is outlined in Exhibit 7. This exercise was carried out in 2019 and 2020 and allowed the Transport cluster to measure the degree to which staff were able to identify phishing emails. As can be seen in Exhibit 7, the results of this exercise indicate that staff awareness of phishing emails remains low.

Exhibit 7 - Spot the Scammer exercise

In both 2019 and 2020, TfNSW performed a ‘Spot the Scammer’ exercise in which they sent out over 25,000 emails to staff based on a real phishing attack in order to measure awareness and response. The exercise tested staff 'click through rate', the percentage of staff who clicked on the fake phishing link. In 2019, these results were then compared to industry benchmarks, with over a 20 per cent click through rate being considered 'very high'. Both TfNSW and Sydney Trains were considered to have a ‘very high’ click through rate in comparison to these benchmarks in both 2019 and 2020. This indicates that staff awareness of phishing emails was low. The click through rate for TfNSW was 24 per cent in 2020, an increase from 22 per cent in 2019. For Sydney Trains, the click through rate in 2020 was 32 per cent, which was a decrease from 40 per cent in 2019.

Source: Audit Office analysis of TfNSW documents.

Section two

Appendices

Appendix one – Response from agencies

Response from Department of Customer Service

McKell Building – 2-24 Rawson Place, Sydney NSW 2000
Tel 02 9372 8877 | TTY 1300 301 181
www.nsw.gov.au

Office of the Secretary

Our reference: COR-03592-2021

Ms Margaret Crawford
Auditor-General
Audit Office of NSW
By email: mail@audit.nsw.gov.au

Dear Ms Crawford

Thank you for your letter dated 4 June 2021 and for the opportunity to respond to your audit report *Managing Cyber Risks*. The work of the Audit Office of New South Wales (NSW Audit Office) is an invaluable and key part of improving both the cyber security resilience and accountability of NSW Government entities.

Managing Cyber Risks is a thorough report that has raised important issues regarding the cyber security of NSW Government entities. The Department of Customer Service (the Department) notes the recommendation to "clarify the requirement for the Cyber Security Policy reporting to apply to all systems." The Cyber Security Policy covers the security of Information Technology (IT), Operational Technology (OT), the Internet of Things (IoT) and other connected systems and devices.

To keep pace with a rapidly evolving cyber threat environment, Cyber Security NSW is undertaking a review of the Cyber Security Policy for its 2022 iteration. With the intention to reduce ambiguity, this review will include clearer wording and instructions on the various sections of reporting maturity levels.

The Department also notes the recommendation to "require agencies to report the level of maturity for each mandatory requirement they have determined appropriate for their agency." The Cyber Security Policy is a risk-based Policy whereby agencies determine the appropriate level of maturity based on their risk appetite. Agencies are encouraged to strive for a level across the board collectively, rather than set a benchmark of level 3 for all Mandatory Requirements. However, as part of the current review of the Cyber Security Policy, the Department will explore the option of implementing formalised processes for agency-determined target maturity levels. Likewise, the Department will also consider implementation of the evolving advice from the Australian Cyber Security Centre (ACSC) on risk-based approaches to cyber resilience. This includes consideration of new guidance on the ACSC Essential Eight. Any such changes will be made in close consultation with the reporting entities.

Consistent with the position of the Australian National Audit Office (ANAO) and based on the advice of Australian Signals Directorate (ASD), the Department believes that the interests of accountability and transparency must be balanced with the need to manage risks. This includes risks identified by the ASD in disclosure of information which may be used by adversaries to target their malicious activities. Whilst the Department recognises that the NSW Audit Office is considering this level of balance, we trust that the Audit Office will continue to assess risks associated with the level of disclosure of confidential and sensitive information and seek advice from the ASD, to keep in line with the changing threat environment.

The Department continues to have some concerns regarding the commissioning of external providers to undertake penetration and red team testing. Effective collaboration between all parties on the scope and approach for red team testing would provide a vehicle to identify and address any vulnerabilities whilst safeguarding the very systems and services NSW Government entities, such as Transport for NSW in this instance, are working to protect. The cyber security of NSW Government entities is a collective responsibility and all entities must work together to make NSW Government systems and services more secure, trusted and resilient.

The Department seeks to continually improve the Cyber Security Policy and other processes used to assist these entities, including supporting documentation and the provision of advice. This report is a timely reminder that there is still much work to be done. With the assistance of agencies like the NSW Audit Office, the Department will continue to engage with Transport for NSW, Sydney Trains and all NSW Government entities to assist in uplifting their cyber security posture.

Yours sincerely

Emma Hogan
Secretary

Date: 02/07/21

Response from Transport for NSW

Transport for NSW

Your ref: D2110328
Our Ref: OTS20/07456

Ms Margaret Crawford
Auditor-General
Audit Office of NSW
GPO Box 12
SYDNEY NSW 2000

Dear Ms Crawford

Thank you for the opportunity to respond to the Performance Audit Report (the Report) on managing cyber risks. Transport for NSW (TfNSW) and Sydney Trains welcome the findings of the Report and are committed to further strengthening our organisational and operational cyber security to protect our customers, our staff and our critical infrastructure. Cyber security risk management remains, and has always been, an important part of TfNSW and Sydney Trains executive oversight and decision-making and we are committed to continuing to focus and invest in uplifting our cyber security capabilities.

In the current cyber security environment of constantly evolving threats and high-profile cyberattacks on all types of organisations in Australia and overseas, TfNSW and Sydney Trains recognise the need to continuously improve our cyber defence capabilities to protect our staff, the NSW Government, and the people of NSW.

We are pleased to advise that there has been measurable uplift in TfNSW and Sydney Trains' cyber maturity in line with our unprecedented investment in Transport's Cyber Defence Portfolio. This Report and its recommendations will serve as constructive input to underpin our ongoing efforts as we continue to focus on improving cyber security as a key priority in our journey towards Future Transport 2056.

TfNSW and Sydney Trains have come a long way over recent years and have invested diligently in planning and delivering measures to address cyber security using a prioritised, risk-based approach. Over the 2019/20 and 2020/21 financial years, our $26 million investment has delivered an uplift in cyber security maturity across the Transport cluster, evidenced by the increase in maturity of essential cyber controls in annual reporting to the Department of Customer Service (Cyber Security NSW) for the last two years.

As a clear demonstration of the continued importance and value placed on cyber security, from July 2020 through to June 2023, Transport will have invested an additional $60 million to support the ongoing uplift of our Cyber Defence Portfolio. In addition, $20 million will be allocated to the Cyber Defence Program from the Digital Restart Fund to further uplift Cyber security.

This journey of continuous improvement and maturity uplift across one of Australia's largest and most complex government entities demonstrates our focus on and commitment to cyber security resilience. Our current and future investments will continuously reduce our cyber security risks in the coming years.

TfNSW and Sydney Trains were among the first NSW Government agencies to recognise the need for robust cyber risk management. Accordingly:

Transport for NSW
231 Elizabeth Street, Sydney NSW 2000 | PO Box K659, Haymarket NSW 1240
T 02 8202 2200 | **F** 02 8202 2209 | **W** transport.nsw.gov.au | ABN 18 804 239 602

- In 2017, TfNSW initiated the Transport IT risk management program. This program has implemented tools and processes to cover, among other things, cyber security risk management as well as cross cluster critical IT assets.

- In 2018, TfNSW initiated the Cyber Uplift Program followed by Sydney Trains in 2019. The mandate was to develop tools and processes to uplift cyber risk management. This program continues to deliver on the mandate.

- Since 2019, TfNSW and Sydney Trains have invested diligently in planning and delivering measures to address cyber security risks using a prioritised, risk-based approach.

Both TfNSW and Sydney Trains have robust and detailed governance forums where reporting and discussions on cyber security are undertaken by executives with the appropriate specialised expertise.

TfNSW and Sydney Trains' evidenced multi-layered 'defence-in-depth' approach to protecting assets (data, systems and identities) supports a proactive approach to stopping cyberattacks before they occur, protecting our transportation services and safeguarding customer data.

While the Report identifies specific instances for further uplift, TfNSW and Sydney Trains' cyber security controls already effectively prevent a significant number of intrusion attempts and our teams continuously monitor our cyber security environment and respond quickly to cyber security threats.

From July 2021, cyber security training will become mandatory for all staff. In addition to formal training, we frequently communicate with staff across the Transport cluster about cyber security risks through the intranet, emails, communities of practice, and other awareness raising activities to highlight the importance for staff to be aware of the seriousness of cyber risks.

TfNSW and Sydney Trains will continue driving a culture of improved cyber security risk identification, management and reporting. Since 2019, regular reporting to all levels of management has been delivered through the Cyber Defence Portfolio. Transport's independent Audit and Risk Committees also receive detailed quarterly cyber security updates from Transport's Chief Information Security Officer. Further, cyber security risks are embedded in agency enterprise risk reporting to ensure the detailed management and remediation of cyber risks at an operational level and support strategic and investment decisions.

As a demonstration of our commitment to continuously improve cyber security culture and governance, enhanced and more detailed monthly cyber reporting has been introduced to the Transport Executive; based on Cybersecurity NSW reporting requirements, with further refinements being developed across the NSW Government. A new Technology Steering Committee, comprising members of the Transport Executive and key subject matter experts, has been designed to provide a greater consolidation of executive direction and oversight of Transport's customer technology, information technology and operational technology functions.

Cyber security management is a journey of continual improvement against threat actors whose tactics regularly change, and we will continue to respond to this challenge across our systems,

Transport for NSW
231 Elizabeth Street, Sydney NSW 2000 | PO Box K659, Haymarket NSW 1240
T 02 8202 2200 | **F** 02 8202 2209 | **W** transport.nsw.gov.au | ABN 18 804 239 602

our information and the critical operational and customer services we deliver across all modes of transport in NSW.

If you have any further questions, Fiona Trussell, Deputy Secretary Corporate Services would be pleased to take your call. I hope this has been of assistance.

Yours sincerely

Rob Sharp
Secretary

24/06/2021

Transport for NSW
231 Elizabeth Street, Sydney NSW 2000 | PO Box K659, Haymarket NSW 1240
T 02 8202 2200 | **F** 02 8202 2209 | **W** transport.nsw.gov.au | ABN 18 804 239 602

Appendix two – Cyber Security Policy mandatory requirements

Version three of the NSW Cyber Security Policy was in effect for the 2020 reporting period. The below is a list of the 25 mandatory requirements that were in effect at the time of this audit.

Requirement 1	**Agencies must implement cyber security planning and governance. Agencies must:**
1.1	Allocate roles and responsibilities as detailed in this policy.
1.2	Ensure there is a governance committee at the executive level (dedicated or shared) to be accountable for cyber security including risks, plans and meeting the requirements of this policy. Agencies need to consider governance of ICT systems and OT to ensure no gaps in cyber security related to items such as video surveillance, alarms, life safety and building management systems that use automated or remotely controlled or monitored assets including industrial Internet of Things (IoT) devices.
1.3	Have an approved cyber security plan to manage the agency's cyber security risks, integrated with business continuity arrangements. This must include consideration of threats, risks and vulnerabilities that impact the protection of the agency's information, ICT assets and services.
1.4	Consider cyber security threats when performing risk assessments and include high and critical risks in the agency's overall risk management framework.
1.5	Be accountable for the cyber risks of their ICT service providers and ensure the providers comply with the applicable parts of this policy and any other relevant agency security policies. This must include providers notifying the agency quickly of any suspected or actual security incidents and following reasonable direction from the agency arising from incident investigations.

Requirement 2	**Agencies must build and support a cyber security culture across their agency and NSW Government more broadly. Agencies must:**
2.1	Implement regular cyber security education for all employees and contractors, and ensure that outsourced ICT service providers understand and implement the cyber security requirements of the contract.
2.2	Increase awareness of cyber security risk across all staff including the need to report cyber security risk.
2.3	Foster a culture where cyber security risk management is an important and valued aspect of decision-making and where cyber security risk management processes are understood and applied.
2.4	Ensure that people who have access to sensitive or classified information or systems and those with privileged system access have appropriate security screening, and that access is removed when they no longer need to have access, or their employment is terminated.
2.5	Share information on security threats and intelligence with Cyber Security NSW and cooperate across NSW Government to enable management of government-wide cyber risk.

Requirement 3	Agencies must manage cyber security risks to safeguard and secure their information and systems. Agencies must:
3.1	Implement an Information Security Management System (ISMS) or Cyber Security Framework (CSF), with scope at least covering systems identified as an agency's 'crown jewels'. The ISMS or CSF should be compliant with, or modelled on, one or more recognised ICT/OT standard (see guideline for more information).
3.2	Implement the ACSC Essential 8.
3.3	Classify information and systems according to their importance (i.e. the impact of loss of confidentiality, integrity or availability), adhere to the requirements of the NSW Government Information Classification Labelling and Handling Guidelines and: • assign ownership • implement controls according to their classification and relevant laws and regulations • identify the agency's 'crown jewels' and report them to Cyber Security NSW as per mandatory requirement 5.4.
3.4	Ensure cyber security requirements are built into procurements and into the early stages of projects and the system development life cycle (SDLC), including agile projects.
3.5	Ensure new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data including processes for internal fraud detection.

Requirement 4	Agencies must improve their resilience including their ability to rapidly detect cyber incidents and respond appropriately. Agencies must:
4.1	Have a current cyber incident response plan that integrates with the agency incident management process, the NSW Government Cyber Incident Response Plan.
4.2	Test their cyber incident response plan at least every year, and involve their senior business and IT executives, functional area coordinators (if applicable), as well as media and communication teams.
4.3	Deploy monitoring processes and tools to allow for adequate incident identification and response.
4.4	Report cyber security incidents to Cyber Security NSW according to the NSW Cyber Security Response Plan.
4.5	Participate in whole-of-government cyber security exercises as required.

Requirement 5	Agencies must report against the requirements outlined in this policy and other cyber security measures. Agencies must:
5.1	Report annually to their cluster CISO, or Cyber Security NSW, their compliance with the mandatory requirements in this policy, in the format provided by Cyber Security NSW. Cluster CISOs must provide all reports to Cyber Security NSW by 31 August.
5.2	Report annually to their cluster CISO, or Cyber Security NSW, their maturity against the ACSC Essential 8, in the format provided by Cyber Security NSW. Cluster CISOs must provide all reports to Cyber Security NSW by 31 August.
5.3	Report annually to their cluster CISO, or Cyber Security NSW, the agency's cyber security risks with a residual rating of high or extreme, in the format provided by Cyber Security NSW by 31 August.
5.4	Report annually to their cluster CISO, or Cyber Security NSW, the agency's 'crown jewels'. Cluster CISOs must provide all reports to Cyber Security NSW by 31 August.
5.5	Provide a signed attestation to Cyber Security NSW by 31 August each year and include a copy of your attestation in your annual report, as outlined in section 4. If your agency does not complete an annual report, an attestation must still be completed and signed off by your agency head and submitted to your cluster CISO.

Appendix three – About the audit

Audit objective

This audit assessed how effectively selected agencies identify and manage their cyber security risks.

Audit criteria

We addressed the audit objective by examining the following criteria:

1. Agencies are effectively identifying and planning for their cyber security risks:
    - Agencies are identifying cyber security risks and have plans and governance arrangements in place to address these risks.
    - Agencies have complied with the reporting and attestation requirements of the NSW Cyber Security Policy.
    - Agencies have identified and classified their information and systems including identification of their 'crown jewels'.
2. Agencies are effectively managing their cyber security risks:
    - Agencies are implementing strategies to build and support a cyber security culture across their agency including training and awareness raising.
    - Agencies are implementing strategies to manage identified risks including implementing an Information Security Management System that is compliant with recognised standards and implementing the ACSC Essential 8.
    - Agencies are identifying and managing cyber security risks with third parties.

Audit scope and focus

In assessing the criteria, we checked the following aspects:

- identification of risks and risk management planning including the identification of the agency's crown jewels
- governance arrangements and organisational investment in cyber security
- activities to improve the cyber aware culture of the agency including staff training
- agency strategies to manage identified risks including implementation of the Essential 8
- management of cyber security risks arising from relationships with third parties.

This audit focused on Transport for NSW and Sydney Trains and their cyber security activities in the 2019 and 2020 calendar years, including the Cyber Security Policy reporting periods.

Audit exclusions

The audit did not:

- examine the whole-of-government implementation of the NSW Cyber Security Policy and the effectiveness of the Department of Customer Service's role in implementing the Policy
- examine the effectiveness of agencies to detect or respond to cyber security incidents
- question the merits of government policy objectives.

Audit approach

Our procedures included:

1. Interviewing:
    - senior staff with responsibility for cyber security
    - staff with enterprise risk management responsibilities
    - other staff with cyber security responsibilities
    - Cyber Security NSW staff.
2. Examining relevant documentation including
    a) cyber security risk assessments
    b) cyber security plans
    c) self-assessments against the Cyber Security Policy
    d) minutes and papers from relevant governance committees
    e) relevant internal audit reports
    f) staff training information and completion rates
    g) a selection of contracts and contract management documentation.
3. Conducting a 'red team' simulation targeted at Transport for NSW and Sydney Trains.

The audit approach was complemented by quality assurance processes within the Audit Office to ensure compliance with professional standards.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Audit Standard ASAE 3500 ‘Performance Engagements’ and other professional standards. The standards require the audit team to comply with relevant ethical requirements and plan and perform the audit to obtain reasonable assurance and draw a conclusion on the audit objective. Our processes have also been designed to comply with requirements specified in the *Government Sector Audit Act 1983* and the *Local Government Act 1993*.

Acknowledgements

We gratefully acknowledge the co-operation and assistance provided by Transport for NSW, Sydney Trains and Department of Customer Service.

Audit cost

The estimated cost of the audit is $620,000.

Appendix four – Performance auditing

What are performance audits?

Performance audits determine whether state or local government entities carry out their activities effectively, and do 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 an audited entity, or more than one entity. They can also consider particular issues which affect the whole public sector and/or the whole local government sector. They cannot question the merits of government policy objectives.

The Auditor-General's mandate to undertake performance audits is set out in section 38B of the *Government Sector Audit Act 1983* for state government entities, and in section 421B of the *Local Government Act 1993* for local government entities.

Why do we conduct performance audits?

Performance audits provide independent assurance to the NSW Parliament and the public.

Through their recommendations, performance audits seek to improve the value for money the community receives from government services.

Performance audits are selected at the discretion of the Auditor-General who seeks input from parliamentarians, state and local government entities, other interested stakeholders and Audit Office research.

How are performance audits selected?

When selecting and scoping topics, we aim to choose topics that reflect the interests of parliament in holding the government to account. Performance audits are selected at the discretion of the Auditor-General based on our own research, suggestions from the public, and consultation with parliamentarians, agency heads and key government stakeholders. Our three-year performance audit program is published on the website and is reviewed annually to ensure it continues to address significant issues of interest to parliament, aligns with government priorities, and reflects contemporary thinking on public sector management. Our program is sufficiently flexible to allow us to respond readily to any emerging issues.

What happens during the phases of a performance audit?

Performance audits have three key phases: planning, fieldwork and report writing.

During the planning phase, the audit team develops an understanding of the audit topic and responsible entities 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 audited entity, program or activities are assessed. Criteria may be based on relevant legislation, internal policies and procedures, industry standards, best practice, government targets, benchmarks or published guidelines.

At the completion of fieldwork, the audit team meets with management representatives 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 management representatives to check that facts presented in the draft report are accurate and to seek input in developing practical recommendations on areas of improvement.

A final report is then provided to the head of the audited entity who is invited to formally respond to the report. The report presented to the NSW Parliament includes any response from the head of the audited entity. The relevant minister and the Treasurer are also provided with a copy of the final report. In performance audits that involve multiple entities, there may be responses from more than one audited entity or from a nominated coordinating entity.

Who checks to see if recommendations have been implemented?

After the report is presented to the NSW Parliament, it is usual for the entity's audit committee to monitor progress with the implementation of recommendations.

In addition, it is the practice of Parliament's Public Accounts Committee 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 received by the NSW Parliament. These reports are available on the NSW Parliament website.

Who audits the auditors?

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

The Public Accounts Committee appoints an independent reviewer to report on compliance with auditing practices and standards every four years. The reviewer's report is presented to the NSW Parliament and available on its website.

Periodic peer reviews by other Audit Offices test our activities against relevant standards and better practice.

Each audit is subject to internal review prior to its release.

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.

Professional people with purpose

OUR VISION

Our insights inform and challenge government to improve outcomes for citizens.

OUR PURPOSE

To help Parliament hold government accountable for its use of public resources.

OUR VALUES

Pride in purpose

Curious and open-minded

Valuing people

Contagious integrity

Courage (even when it's uncomfortable)

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

Level 19, Darling Park Tower 2
201 Sussex Street
Sydney NSW 2000 Australia

PHONE +61 2 9275 7100
FAX +61 2 9275 7200

mail@audit.nsw.gov.au

Office hours: 8.30am-5.00pm
Monday to Friday.