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.