Appendix four – About the audit

Audit objective

This audit assessed agencies' compliance with the NSW Department of Customer Service's Policy 'DCS-2020-02 NSW Cyber Security Policy'.

Audit criteria

We addressed the audit objective by:

1. verifying that the CSP's mandatory requirements for reporting and attestation have been performed
2. verifying the accuracy of agency self-assessments against the CSP's mandatory requirements, including their implementation of the Australian Cyber Security Centre's (ACSC) Essential 8
3. assessing the extent to which maturity levels meet or exceed the 'level three - Defined' threshold (i.e. are documented and practiced on a regular and consistent basis)
4. assessing progress towards target maturity levels across government since the CSP was introduced.

Audit procedures

Our audit procedures included:

1. interviewing:
    a) information security and risk management staff at each case study agency
    b) cluster Information Security staff where they are involved in self-assessments for the case study agencies
    c) agency staff responsible for managing IT Service Providers
    d) agency staff responsible for management of cyber security training to staff
    e) agency staff responsible for security screening of people who have access to sensitive or classified information or systems and those with privileged system access
    f) agency staff responsible for the operation of ACSC Essential 8 controls (patching, whitelisting, hardening, backups, Multifactor authentication, etc.)
    g) Cyber Security NSW staff.

3. examining:
    a) self-assessments and attestations produced by agencies
    b) materials produced by agencies to complete and support their self-assessments
    c) policies and procedures addressing the mandatory requirements of the CSP
    d) technical configurations and settings relevant to the CSP's requirements or the ACSC Essential 8
    e) agency risk registers, risk assessments, risk tolerance or appetite statements, and supporting documents
    f) agency information and asset registers relevant to classification of information and systems
    g) agency uplift plans and proposals for measures to increase cyber security
    h) budgets and expenditure details for such measures or projects.
4. analysing data:
    a) data collected by Cyber Security NSW on agency self-assessments since the launch of the CSP.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Audit Standard ASAE 3100 Compliance Engagements and 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 *Public Finance and Audit Act 1983*.

Acknowledgements

We gratefully acknowledge the co-operation and assistance provided by the participating agencies and by Cyber Security NSW, as well as those stakeholders who participated in the discussions held during the audit.

Audit cost

Including staff costs and overheads, the estimated cost of the audit is $237,000.