Appendix five – About the audit

Audit objective

This audit assessed how effectively three selected councils (City of Parramatta Council, Singleton Council and Warrumbungle Shire Council) identified and managed cyber security risks.

Audit criteria

We addressed the audit objective by assessing whether:

1. The councils effectively identified and planned for cyber security risks.
    a) The council identified cyber security as a risk in its risk register.
    b) The council classified its information and systems by operational importance and identified relevant cyber risks.
    c) The council had the required cyber expertise, systems, policies, and processes in place to identify and manage cyber security risks.
    d) The council had a plan in place to ensure it meets an appropriate level of cyber security maturity based on its risk identification and assessment.
2. The councils had controls in place to effectively manage identified cyber security risks.
    a) The council had controls in place to address identified cyber security risks.
    b) The council's leadership and governance supported its approach to managing cyber security risks.
    c) The council effectively built cyber security awareness across the organisation through regular training and awareness raising activities.
    d) The council effectively managed cyber security risks relating to third party ICT providers.
3. The councils had processes in place to detect, respond to, and recover from cyber security incidents.
    a) The council undertook regular testing and monitoring of its ICT systems.
    b) The council had a plan in place to respond to, and recover from, cyber security incidents.
    c) The council reported cyber security incidents and actions taken in line with relevant legislation and policies.

Audit scope and focus

In assessing the criteria, we checked the following aspects:

1. risk management planning including workforce planning, the classification of information and systems by operational importance, and whether the council has a cyber security plan
2. effective identification and management of cyber security risks through risk assessments and control implementation processes, including in relation to managing third party cyber security risks
3. leadership and governance relevant to cyber security risk management and promoting a cyber security culture through training and awareness activities
4. processes to detect, respond to and recover from cyber security incidents, including monitoring and testing of systems, disaster recovery and business continuity planning, and cyber incident reporting and post-incident evaluation.

This audit focused on the selected councils' cyber security activities from 1 July 2021 to 31 October 2023.

This audit also included the Office of Local Government (part of the Department of Planning and Environment until 1 January 2024, now part of the Department of Planning, Housing and Infrastructure) and Cyber Security NSW (part of the Department of Customer Service) due to their roles in providing guidance and support to local government.

Audit exclusions

The audit did not:

- conduct simulated cyber security exercises on the selected councils, or undertake detailed assessment or testing of the effectiveness of specific cyber security controls
- conclude on whether the selected councils are compliant with the Cyber Security Guidelines – Local Government
- examine how the Department of Planning and Environment or the Department of Customer Service identify and manage cyber security risks, or the effectiveness of the controls these agencies have in place to manage their cyber security risks
- question the merits of Government policy objectives.

Audit approach

Our procedures included:

1. Interviewing:
    - Senior council staff with responsibility for cyber security
    - Other council staff with cyber security responsibilities
    - Council staff with enterprise risk management responsibilities
    - Cyber Security NSW staff
    - Office of Local Government staff.
2. Examining relevant documentation including:
    - Documentation relating to cyber security activities and incidents
    - Risk management frameworks and documentation
    - Minutes and papers from relevant executive and Audit, Risk and Improvement Committee meetings
    - Relevant internal and external audit reports and reviews
    - Staff training information and completion rates
    - A selection of contracts and contract management documentation.

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 Auditing 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 cooperation and assistance provided by City of Parramatta Council, Singleton Council, Warrumbungle Shire Council, the Department of Planning and Environment (Office of Local Government) and the Department of Customer Service (Cyber Security NSW).

Audit cost

The estimated cost of the audit is $744,000.