
Report highlights

What this report is about

NSW local councils provide a wide range of essential services and infrastructure to their communities and are increasingly reliant on digital technologies.

Councils need to manage cyber security risks to ensure their information, data and systems are appropriately safeguarded. Councils also need to be prepared to detect, respond and recover when a cyber security incident occurs.

The audit assessed how effectively three selected councils identified and managed cyber security risks.

The audit also included the Department of Planning, Housing and Infrastructure (Office of Local Government) and Department of Customer Service (Cyber Security NSW), due to their roles in providing guidance and support to local councils.

Audit findings

The audit found that the selected councils are not effectively identifying and

managing cyber security risks. Each of the councils undertook activities to improve their cyber security during the audit period, but this audit found significant gaps in their cyber security risk management and cyber security processes.

Such gaps result in unmitigated risks to the security of information and assets which, if compromised, could impact their local communities, service delivery and public infrastructure.

Cyber Security NSW and the Office of Local Government recommend that councils adopt requirements in the Cyber Security Guidelines for Local Government, but could do more to monitor whether the Guidelines are enabling better cyber security risk management in the sector.

Audit recommendations

In summary, the councils should:

- integrate assessment and monitoring of cyber security risks into corporate governance processes

- self-assess their performance against Cyber Security NSW's guidelines for local government
- develop and implement a risk-based cyber security improvement plan and program of activities
- develop, implement and test a cyber incident response plan.

Cyber Security NSW and the Office of Local Government should regularly consult on cyber security risks facing local government, and review the effectiveness of guidelines and related resources for the sector.

While this report focuses on the performance of the selected councils, the findings and recommendations should be considered by all councils to better understand their risks and challenges relevant to managing cyber security risks.

Fast facts

2 of 3

councils do not have a formal plan to improve their cyber security

3 of 3

councils do not have up to date plans and processes to support detection, response to and recovery from cyber incidents

3 of 3

councils are not effectively managing cyber security risks in relation to third parties