Media contact: Vanessa Sprunt
Mobile: 0427 953 993
Email: vanessa.sprunt@audit.wa.gov.au

29 March 2023

Many local governments are not fixing computer control weaknesses to prevent cyber attacks, despite previous warnings about risks

The Auditor General's report *Information Systems Audit – Local Government 2021-22* tabled in Parliament today.

Auditor General Ms Caroline Spencer said 324 general computer control weaknesses were reported to 53 local government entities for the 2021-22 year.

'Disappointingly, 69% of these weaknesses were unresolved issues from the prior year, including 27 of the 31 significant findings.

'Entities need to prioritise addressing audit findings to safeguard their systems and information, and reduce the risk of compromise to their confidentiality, integrity and availability.

'Local government entities are increasingly adopting technologies and systems to deliver efficiencies in their operations and improve the delivery of services to the communities they serve. As local government entities' digital footprints increase, so too do their risks.

'Our information systems audits are designed to help local government entities to identify and mitigate these risks and protect citizens' information against inappropriate disclosure, loss or misuse,' Ms Spencer said.

This year entities were audited against an updated capability maturity model, with five of the 10 control categories now relating to information and cyber security controls.

The majority of entities failed to meet the benchmark in the information and cyber security categories.

In other categories, we saw improvements in IT risk management, change management, physical security, IT operations and business continuity.

The report includes a number of case studies that the local government sector and community can learn from:

- One entity did not have a cyber security awareness program despite experiencing three cyber attacks in three years. The entity attributes these attacks to phishing or poor password hygiene. We first raised this issue with the entity in 2020.
- In 2022, an entity's staff account was compromised and used to instigate a phishing attack on third parties. The entity did not have a cyber security incident response plan to coordinate a response and communicate with impacted third parties. We had recommended, in 2021, the entity develop a plan.
- At one entity we found poor physical control around IT infrastructure, along with the back door to the office and records room left unlocked during the day despite being publicly accessible. Cash takings were also left in an unlocked safe. These weaknesses increase the likelihood of unauthorised access to systems and theft of public property and information.

- One entity had not configured its finance application to stop the same individual from approving purchase orders and invoices for the purchase of goods and services. Although the entity had manual controls in place, these could be bypassed.

Ms Spencer said local government entities of all sizes can fine-tune their existing systems and practices to uplift their resilience to the ever present and evolving nature of cyber security threats. Notably, many weaknesses do not require expensive technology investments to fix.

The local government sector should use the case studies and recommendations in this report to inform enhancements to their general computer controls. This will build much needed digital trust and public confidence in the local government sector’s capacity to successfully operate in the digital economy.

Report resources

- PDF version