PERFORMANCE AUDIT

Work in progress: Audit description

Improving Ransomware Resiliency at Local Governments

Ransomware is a type of software designed to deny access to a computer system or the data it stores until the victim pays the demanded ransom. Typically, the hacker gains access to a network and encrypts or steals a copy of the data present, then contacts the victim to extort money in exchange for a decryption key or a promise to delete stolen data without publishing it. Ransomware attacks are of particular concern because they can deny government employees access to systems and data essential to delivering critical government services. Such attacks can expose school, health, or banking data and compromise systems used by police, courts and utilities. They can also cost governments thousands – if not millions – of dollars, whether in ransom payments, increased insurance premiums, or in replacing affected systems. As attackers continue to hone their tactics, local governments expected to keep systems secure and available struggle to keep pace.

To help local governments prevent and respond to this increasing risk, the State Auditor's Office offers performance audits that specifically examine a government's resiliency to ransomware. We offer these audits with funding through Initiative 900, at no cost to participating governments. Audit results are confidential under state law (RCW 42.56.240); as an added precaution, we also keep the identity of these organizations confidential.

Preliminary scope, objectives and methodology

These audits typically include the following procedures at local governments that volunteer for the assessment:

- **Technical testing to identify opportunities to make systems more secure.** Real-time security assessments of systems and networks, including identifying and assessing vulnerabilities and whether they could be exploited by internal or external attackers.
- **Comparing current IT security controls to leading practices.** Interviews with key IT staff plus other activities to determine how closely existing practices align with selected ransomware resiliency leading practices.

These performance audits will seek to answer the following questions:

- Does the government have vulnerabilities in its IT environment that could lead to increased risk from external or internal threats?
- Do the government's IT security practices align with leading practices that contribute to ransomware attack resiliency?

Timing: Audit work will continue through June 2026, with results provided to each government as we complete the audit. We will issue a public report covering audits completed at the end of each fiscal year.

Office of the Washington State Auditor
Pat McCarthy

Director of Performance and IT Audit:
Scott Frank
(564) 999-0809
Scott.Frank@sao.wa.gov

Assistant Director of IT Audit:
Peg Bodin
(564) 999-0965
Peggy.Bodin@sao.wa.gov

IT Security Audit Manager:
Erin Laska
(360) 594-0615
Erin.Laska@sao.wa.gov

Office of the Washington State Auditor
P.O. Box 40021
Olympia, WA 98504-0021
www.sao.wa.gov

uploaded October 2025