Office of the Washington State Auditor
Pat McCarthy

Performance Audit

Opportunities to Improve Cowlitz County's Information Technology Security

July 11, 2019

Report Number: 1024178

Table of Contents

Introduction 3
Scope and methodology.....3
Audit Results 5
Recommendations.....5
Auditor's Remarks 5
Auditee Response 6
Appendix A: Initiative 900.....7

The mission of the State Auditor's Office

Provide citizens with independent and transparent examinations of how state and local governments use public funds, and develop strategies that make government more efficient and effective.

The results of our work are widely distributed through a variety of reports, which are available on our website and through our free, electronic **subscription service**.

We take our role as partners in accountability seriously. We provide training and technical assistance to governments and have an extensive quality assurance program.

For more information about the State Auditor's Office, visit **www.sao.wa.gov**.

Americans with Disabilities

In accordance with the Americans with Disabilities Act, this document will be made available in alternative formats. Please email **Communications@sao.wa.gov** for more information.

State Auditor's Office contacts

State Auditor Pat McCarthy
360-902-0360, **Pat.McCarthy@sao.wa.gov**

Scott Frank – Director of Performance & IT Audit
360-902-0376, **Scott.Frank@sao.wa.gov**

Kelly Collins, CPA – Director of Local Audit
360-902-0091, **Kelly.Collins@sao.wa.gov**

Peg Bodin, CISA – Assistant Director for IT Audit
360-464-0113, **Peggy.Bodin@sao.wa.gov**

Kathleen Cooper – Director of Communications
360-902-0470, **Kathleen.Cooper@sao.wa.gov**

To request public records

Public Records Officer
360-725-5617, **PublicRecords@sao.wa.gov**

Introduction

Government organizations have become increasingly dependent on computerized information systems to carry out their operations. These systems process, store and share sensitive and confidential information, including personal and financial data, to deliver services to residents.

Risks to a local government's information technology (IT) environment go beyond the activities of hackers stealing credit card information or Social Security numbers, or installing malware to disrupt communications. Errors or misuse of the system by employees or contractors can also jeopardize the operation of any entity that relies on computers and networks.

Furthermore, research by Verizon Wireless in their 2018 Data Breach Investigation Report shows that the public sector reported the most cybersecurity incidents. A 2018 study by the Ponemon Institute found that governments pay an average of $75 per record lost in a data breach

To help Washington's local governments protect their information technology (IT) systems, we are offering them the opportunity to participate in a performance audit designed to assess whether there are opportunities to improve those systems.

Cowlitz County chose to participate in this audit.

Scope and methodology

The performance audit we conducted was designed to answer the following questions:

- Are there opportunities to improve Cowlitz County's governance and oversight of cybersecurity?
- Are there opportunities to improve Cowlitz County's cybersecurity practices?

Identifying opportunities to improve cybersecurity governance and oversight

We reviewed the County's security policies and risk assessment processes, and its implementation of leading practices concerning cybersecurity governance and oversight. This review included interviews with two members of County leadership as well as the IT manager. For this review, we compared what we learned from our review to selected portions of the federal National Institute of Standards and Technology (NIST) Cybersecurity Framework Version 1.1. The framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. Both these activities require and facilitate increased governance and oversight by the organization's leadership.

Identifying opportunities to improve cybersecurity practices

We reviewed the County's IT security policies, procedures and standards to leading cybersecurity practices to identify any improvements the County could make to improve its cybersecurity practices. Our process also included interviews with various members of the County's IT department, as well as limited technical testing. For this review, we used selected leading practices from the Center for Internet Security's Top 20 Critical Security Controls, which were developed by a broad community of private and public sector stakeholders after examining the most common attack patterns. The Top 20 Critical Security Controls are a prioritized list of control areas designed to help organizations with limited resources optimize their security defense efforts to achieve the highest return on investments.

We provided detailed audit results to County management.

Next steps

Our performance audits of local government programs and services are reviewed by the local government's legislative body and/or by other committees of the local government whose members wish to consider findings and recommendations on specific topics. Representatives of the State Auditor's Office will review this audit with Cowlitz County's legislative body in Kelso, Washington. The public will have the opportunity to comment at this hearing. Please check Cowlitz County's website for the exact date, time and location. The State Auditor's Office conducts periodic follow-up evaluations to assess the status of recommendations, and may conduct follow-up audits at its discretion. See **Appendix A**, which addresses the I-900 areas covered in the audit.

Audit Results

We communicated the results of our audit work and recommendations to Cowlitz County management for its review, response and action. We found that while the County's IT policies and practices partially align with industry leading practices, there are areas where the County can make improvements in governance, oversight and cybersecurity practices.

Because publishing details about the tests performed and test results could increase the risk to the County, distribution of this information is considered confidential under RCW 42.56.420 (4), and under Generally Accepted Government Auditing Standards, Sections 7.40-43.

Recommendations

To help ensure Cowlitz County protects its IT systems and the information contained in those systems, we make the following recommendations:

- Continue efforts to improve and strengthen the County's governance and oversight of cybersecurity practices
- Consider further aligning cybersecurity, policies, and procedures with leading practices
- Consider further aligning cybersecurity controls with leading practices

Auditor's Remarks

The State Auditor's Office recognizes the willingness of Cowlitz County to volunteer to participate in this audit, demonstrating its dedication to making government work better. It is apparent the County's management and staff want to be accountable to the citizens and good stewards of public resources. Throughout the audit, they fostered a positive and professional working relationship with the Washington State Auditor's Office.

Auditee Response

Information Technology

207 N 4th Ave
Kelso, WA 98626
TEL (360) 577-3024
FAX (360) 423-9987
www.co.cowlitz.wa.us/IT

Board of County Commissioners
Arne Mortensen District 1
Dennis P. Weber District 2
Joe Gardner District 3

June 20th, 2019

Peg Bodin
Assistant Director of Information Audit
302 Sid Snyder Ave SW
Olympia, WA 98504

Dear Ms. Bodin,

On behalf of the Cowlitz County Information Technology Department, thank you for the opportunity to review and respond to the cybersecurity performance audit report, "Opportunities to Improve Cowlitz County's Information Technology Security."

It was a pleasure working with Peg Bodin, Michael Hjermstad and other State Auditor Staff as well as the subject matter experts who evaluated Cowlitz County Information Technology security controls. The engagement with your team was professional and collaborative.

Thank you for recognizing the measures we have taken to protect our technology environment from numerous threats. We appreciate the efforts of those involved to evaluate our information technology security program and the recommended opportunities for improvement. Several of the recommendations have already been put in to place. We remain committed to addressing the remaining recommendations in the report and to continuously improve our processes and capabilities.

Sincerely,

Randy Webster
IT Operations Manager
Cowlitz County

Appendix A: Initiative 900

Initiative 900, approved by Washington voters in 2005 and enacted into state law in 2006, authorized the State Auditor's Office to conduct independent, comprehensive performance audits of state and local governments.

Specifically, the law directs the Auditor's Office to "review and analyze the economy, efficiency, and effectiveness of the policies, management, fiscal affairs, and operations of state and local governments, agencies, programs, and accounts." Performance audits are to be conducted according to U.S. Government Accountability Office government auditing standards.

In addition, the law identifies nine elements that are to be considered within the scope of each performance audit. The State Auditor's Office evaluates the relevance of all nine elements to each audit. The table below indicates which elements are addressed in the audit. Specific issues are discussed in the Results and Recommendations sections of this report.

I-900 element		Addressed in the audit
1.	Identify cost savings	**No.** The audit did not identify measurable cost savings. However, strengthening IT security could help the County avoid or mitigate costs associated with a data breach.
2.	Identify services that can be reduced or eliminated	**No.** The audit objectives did not address services that could be reduced or eliminated.
3.	Identify programs or services that can be transferred to the private sector	**No.** The audit objectives were focused on improving the County's information system security program.
4.	Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**Yes.** The audit compares the County's IT security controls against leading practices and makes recommendations to align them.
5.	Assess feasibility of pooling information technology systems within the department	**No.** The audit did not assess the feasibility of pooling information systems; it focused on the County's IT security posture.
6.	Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**Yes.** The audit evaluates the roles and functions of IT security at the County and makes recommendations to better align them with leading practices.
7.	Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.** The audit did not identify a need for statutory or regulatory change.
8.	Analyze departmental performance, data performance measures, and self-assessment systems	**Yes.** Our audit examined and made recommendations to improve IT security control performance.
9.	Identify relevant best practices	**Yes.** Our audit identified and used leading practices published by the Center of Internet Security to assess the County's IT security controls, and by the National Institute of Standards and Technology to assess governance and oversight of cybersecurity activities.

Audit performed to standards

We conducted this performance audit under the authority of state law (RCW 43.09.470), approved as Initiative 900 by Washington voters in 2005, and in accordance with Generally Accepted Government Auditing standards (December 2011 revision) issued by the U.S. Government Accountability Office. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.