



**Washington
County Auditor's
Office**

**Auditor Review
of
Information Security**

Final Report
November 29, 2002



John Hutzler, CIA, CGAP,
CCSA County Auditor

Auditor's Review of Information Security

We conducted this review to determine whether the County had an appropriate information security management program and the extent to which Information Technology Services (ITS) had implemented the six Basic Controls identified by the Center for Internet Security Controls in CIS Controls, Version 7.1.¹ The CIS Controls are best practices developed by a community of IT experts to mitigate the most common attacks against systems and networks.

We initiated this audit on October 1, 2020 and completed our fieldwork on July 12, 2021. On the same day that we started this audit, ITS began a multi-year project to investigate, select and implement an information security framework.

At the time of our fieldwork, we found concerning deficiencies in County information security management and serious deficiencies in the implementation of the CIS Basic Controls. However, ITS reports that its project to implement an information security framework is well underway. ITS may have already addressed the control deficiencies we found a year and a half ago.

We recommend the following actions to improve the security of the County's information technology:

1. The County Administrator should formally establish and authorize ITS' role and responsibilities as the centralized technology service provider, serving all Washington County agencies.
2. The County Administrator should submit for adoption by the Board of County Commissioners (BCC) an Administrative Policy establishing an information security governance framework for the County. The governance framework should include an information security steering committee of appropriate stakeholders to provide oversight of the information security program.
3. The County Administrator should implement the information security governance framework adopted by the BCC through administrative procedures that assign responsibility for development and implementation of an entity-wide information security program to a qualified Information Security Officer (ISO) with sufficient staff, budget, authority, and independence to effectively implement information security entitywide.
4. The ISO and the steering committee should propose entitywide information security policies and procedures for adoptions by the BCC or the County Administrator.
5. The ISO should implement an information security program that uses industry accepted methods and processes to continuously assess and address technology risks, including the deficiencies identified in this review.

We considered the risks posed by publicly releasing any information related to security findings. We balanced the need for stakeholders, such as the BCC, to be informed on critical or systemic IT security issues affecting the County against the need to protect the County from cybersecurity threats. In accordance with ORS 192.345 (23) and generally accepted government auditing standards, we excluded some details of the information security weaknesses from this public report. A more detailed confidential report to the County Administrator and Chief Information Officer was provided through the Office of County Counsel.

¹ Toward the end of our fieldwork, CIS implemented CIS Controls Version 8, which changed the priority of some controls. We completed our review using CIS Controls v.7.1.



WASHINGTON COUNTY

Memorandum

To: John Hutzler, Washington County Auditor

From: Tanya Ange, County Administrator

cc: David Martinez, Assistant County Administrator
Sam Kim, Interim Chief Information Officer

Date: 11/28/2022

Subject: Auditor's Review of Information Security

I wish to thank the Washington County Auditor's Office for the Auditor's Review of Information Security for the period of October 1, 2020 and July 12, 2021 for Washington County. I also welcome this opportunity to provide some background as well as respond to the report.

Background

IT Services continues to keep the County safe and secure using best practices, reasonable industry standard measures, and realistic security goals based on our actual current state to counter the ever-increasing threats.

At the time the Auditor's review began, IT Services began discussions on information security framework to further explore. In October 1, 2021, IT Services started working in earnest on the multi-year project to investigate, select, and implement a security framework.

The information security audit was initiated by the Auditor's Office on October 1, 2020. Their field work was completed on July 12, 2021 with a preliminary report provided on March 22, 2022. IT Services had originally planned on selecting and implementing a formal security framework in FY 2019-2020. Onset of the pandemic required a One Washington County approach and pivot towards response and recovery efforts. This required IT Services to shift work on researching, designing and implementing the security framework to start during FY 2021-22. The IT staff resources were also required to respond to the audit further impacted staff capacity.

IT Services selected the latest CIS Controls 8.0 framework, which has a different set of basic controls than the older version 7.1. The audit was based on the 7.1 framework. The framework implementation is well underway and IT Services has made tremendous progress which continues today.

Response to the Auditor's Review of Information Security

It should be noted that the audit was conducted prior to IT Services formally selecting and implementing the CIS framework and that the audit is not a risk assessment. It only reviews how well the county is performing against a framework that had not yet been put in place during the audit period. It does not accurately reflect the current state of the County's security posture.



WASHINGTON COUNTY

As such, I acknowledge that there were deficiencies in County information security management and in the implementation of the CIS Basic Controls.

I agree with the overall audit finding that Washington County needs to continue to work towards implementing an industry-standard information security framework and have made great progress to that end. Specific to the recommendations, a board policy is being drafted that addresses all five recommendations with the target dates indicated:

Recommendations	Target Date/Notes
1. The County Administrator should formally establish and authorize ITS' role and responsibilities as the centralized technology service provider, serving all Washington County agencies.	March 2023
2. The County Administrator should submit for adoption by the Board of County Commissioners (BCC) an Administrative Policy establishing an information security governance framework for the County. The governance framework should include an information security steering committee of appropriate stakeholders to provide oversight of the information security program.	March 2023
3. The County Administrator should implement the information security governance framework adopted by the BCC through administrative procedures that assign responsibility for development and implementation of an entity-wide information security program to a qualified Information Security Officer (ISO) with sufficient staff, budget, authority, and independence to effectively implement information security entitywide.	June 2023 IT Services is currently in the process of recruiting for an ISO to implement a County-wide security program and the accompanying governance framework.
4. The ISO and the steering committee should propose entitywide information security policies and procedures for adoptions by the BCC or the County Administrator.	August 2023
5. The ISO should implement an information security program that uses industry accepted methods and processes to continuously assess and address technology risks, including the deficiencies identified in this review.	November 2023

As previously stated in this memorandum, IT Services will continue to keep the County safe and secure as well as continue the implementation of CIS controls framework. I welcome follow-up audits once the implementation is complete.

I am truly grateful to the Washington County Auditor's Office for their partnership and dedication to keeping the County safe from cyber threats.