Assessment Team
Jared Miller, CISA, CFE, CDPSE, Information Systems Audit Manager
Nick Jimroglou, CISA, CDPSE, Information Systems Audit Lead

Contractors
CP Cyber LLC
Bill Evert, Partner
Donald McLaughlin, Lead Consultant
Brian Cather, Lead Consultant

Audit Management
Timothy M. O’Brien, CPA, Auditor
Valerie Walling, CPA, Deputy Auditor
Dawn Wiseman, CRMA, Audit Director

Audit Committee
Timothy M. O’Brien, CPA, Chairman
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

You can obtain copies of this report by contacting us:

Office of the Auditor
201 West Colfax Avenue, #705
Denver CO, 80202
(720) 913-5000  |  Fax (720) 913-5253

Or download and view an electronic copy by visiting our website at:
www.denverauditor.org.

Cover photo by Denver Auditor’s Office staff.
AUDITOR'S LETTER

July 21, 2022

On behalf of the Denver Auditor's Office, CP Cyber LLC conducted a cybersecurity assessment of an agency in the City and County of Denver. This assessment found some areas of strength and some areas that need improvement. Because of the information security sensitivities involved with this assessment, we have communicated these issues separately to the relevant city agency for its remediation.

This assessment is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, “General Powers and Duties of Auditor.”

We extend our appreciation to the city personnel who assisted and cooperated with us and CP Cyber during the assessment. For any questions, please feel free to contact me at 720-913-5000.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor
**BACKGROUND**

**Application Security**

For each service the City and County of Denver provides its residents, the city usually has a supporting website or application it must develop, support, and host.

Many of these applications need to be publicly accessible so that individuals can log in, submit files, or fill out forms. The data the city collects through these means is potentially sensitive or personal information that must be protected to ensure both confidentiality and data integrity.

Each application the City and County of Denver uses increases the risk to the city, because each one can potentially provide a way for a digital attacker to probe the city’s systems, try to gain a foothold into the city’s network, or compromise a user’s or employee’s account.

Because of that risk, software applications must be configured with security controls to protect them against such malicious attacks. Applications are widely available, so even the tools that protect us — such as those that alert us to vulnerabilities — can be a source of significant risk.

Information security professionals understand that attempted attacks happen constantly. These attacks try to take advantage of common vulnerabilities, default configurations in systems, and weak passwords. This makes security assessments — which verify whether issues exist — increasingly important.

The city uses controls such as multifactor authentication to protect accounts from unauthorized access, but the city also needs to consider other scenarios to ensure the overall security of the applications it uses so it can best protect the data being stored.

**Web Application Assessments**

Application security assessments use both manual and automated tests to identify vulnerabilities, security flaws, and threats to web applications. An assessment may involve using any of the known kinds of malicious attacks — such as poor security configurations — to see whether a vulnerability can be exploited. In this way, information security professionals can more accurately determine the risks to an organization.

To ensure the testing is thorough and that all risks are addressed, information security experts will rely on a testing methodology framework — such as the one from the Open Web Application Security Project, a global...
nonprofit foundation that works to improve software security.¹

The foundation’s framework is “an open-source web application that explains secure coding principles in multiple programming languages” and was designed to help train teams to write secure computer code.²

This tool aims to help organizations address vulnerabilities that lead to the most common attacks. Organizations can do this by analyzing current trends and threats and updating the organization’s approach to align itself with known threats.

The Open Web Application Security Project updated its framework in 2017 and again in 2021. In that time, security threats have changed substantially — demonstrating the ever-evolving nature of cybersecurity.

Some of what were the most prevalent attacks have decreased since 2017, while other emerging threats have become more common. For example, in 2017, injection — an attack method that inputs malicious data into a web application — was by far the most common attack. As developers learned how to code to better protect against this attack, injection became less common.

By 2021, attackers focused more on uncovering broken access controls.

To do this, an attacker might sign up for a free, basic account that should only be able to read data. The attacker would then explore the various ways that a user might upload files. Then, by changing the request that goes between their computer and the application’s server, the attacker can, for example, request to delete a file. Such basic account access should not be able to do this, so if the request went through, the access control would be considered broken.

Other Relevant Frameworks

Aside from the Open Web Application Security Project’s framework, other frameworks also exist to help organizations address web application security risks.

The National Institute of Standards and Technology — a laboratory and nonregulatory federal agency within the U.S. Department of Commerce — has its own cybersecurity framework that also helps organizations build a security strategy to increase their “security maturity” while prioritizing improvements to specific controls for web applications.³

---

Other available web application frameworks include the Open Source Security Testing Methodology and the Information Systems Security Assessment Framework — but these are outdated compared to the Open Web Application Security Project's guidance.4

---

Office of the Auditor

The Auditor of the City and County of Denver is independently elected by the residents of Denver. He is responsible for examining and evaluating the operations of city agencies and contractors for the purpose of ensuring the proper and efficient use of city resources. He also provides other audit services and information to City Council, the mayor, and the public to improve all aspects of Denver’s government.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the city’s finances and operations, including the reliability of the city’s financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of city operations, thereby enhancing residents’ confidence and avoiding any appearance of a conflict of interest.

201 West Colfax Avenue #705
Denver CO, 80202
(720) 913-5000 | Fax (720) 913-5253
www.denverauditor.org

Our Mission

We deliver independent, transparent, and professional oversight in order to safeguard and improve the public’s investment in the City and County of Denver. Our work is performed on behalf of everyone who cares about the city, including its residents, workers, and decision-makers.