ASSESSMENT REPORT
An Agency of the City & County of Denver
Cybersecurity Assessment
OCTOBER 2018

Office of the Auditor
Audit Services Division
City and County of Denver
Timothy M. O’Brien, CPA
Denver Auditor
Consultants
Comerstone Partners
Bill Evert, Partner
Donald McLaughlin, Lead Consultant
Brian Cather, Lead Consultant

Audit Team
Nicholas Jimroglou, CISA, Lead IT Auditor

Audit Management
Timothy M. O’Brien, CPA, Auditor
Valerie Walling, CPA, CMC®, Deputy Auditor
Kevin Sear, CPA, CIA, CISA, CFE, CGMA, Audit Manager

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 access an electronic copy by visiting our website at: www.denverauditor.org
October 18, 2018

AUDITOR'S REPORT

Cornerstone Partners has completed a cybersecurity assessment of an agency within the City and County of Denver. The purpose of the assessment was to evaluate deficiencies and make recommendations to further improve the agency's cybersecurity.

The assessment resulted in recommendations for improvements, which have been communicated to the City's agency and Technology Services for further remediation.

We extend appreciation to Technology Services and the agencies' personnel who assisted and cooperated with us and Cornerstone Partners during the assessment.

Denver Auditor’s Office

[Signature]

Timothy M. O’Brien, CPA
Auditor
An Agency of City and County of Denver
- Information Systems Cybersecurity Assessment

October 18, 2018
An Agency of City and County of Denver
Information Systems Cybersecurity Assessment

Background

Cornerstone Partners LLC (“Cornerstone”) was tasked by the Auditor to evaluate the Information Systems cybersecurity of an agency of the City and County of Denver (“City”) for Technology Services and the Auditor’s Office. As part of deliverables, Cornerstone will present to the Audit Committee and findings will be sent to Technology Services. The results of the report will be limited to discussing any findings, vulnerabilities and risks found on an agency of the City and County of Denver.

A key to this improvement process is balancing the need for public access and transparency, while managing the implementation of both centralized and decentralized cybersecurity strategies. Currently, the City has a decentralized approach to information systems requirements, which affects how risk is approached and managed by the City.

When applying and evaluating the information systems cybersecurity for the agency of the City, one must weigh how the results of this assessment would influence the understanding of their overall risk levels and vulnerabilities. This understanding will help drive the allocation of valuable resources that are required for maintaining and actively improving its information system requirements and capabilities. The differing approaches to risk tolerance, levels of maturity between offices and departments, and the public facing requirement of the City affects the way they implement control measures and risk control processes.
Scope of Work

The scope of this engagement began with understanding the current posture of the agency of the City. The City’s operating requirements of openness, transparency, and accessibility was crucial in understanding the scope of work. Cornerstone understands how the City must balance the public facing data requirements with the need to protect and ensure the confidentiality, integrity, and availability of data on its information systems.

This engagement focused on assessing the information systems cybersecurity of an agency of the City utilizing the National Institute of Science and Technology (NIST) Cybersecurity Framework (figure 1).

![Figure 1](image)

The Methodology

Cornerstone collected evidence and performed testing to enable an effective cybersecurity assessment of the agency of the City and County of Denver. The NIST methodology uses five key functional process areas of cybersecurity; however, the fourth and fifth key functional process areas, event response and event recovery, were not in scope during this engagement. The areas in scope included:

- **Risk Identification**: Tools, strategies, and techniques for the identification and tracking of potential risks, and the organization’s willingness to accept cybersecurity risk.

- **Event Protection and Prevention**: Tools, strategies, and techniques used to safeguard and ensure delivery of critical information technology infrastructures and systems.

- **Event Detection**: Tools, strategies, and techniques used to detect potential and actual occurrences of a cybersecurity event taking place, or an event that has taken place.
Passwords

Many websites and online applications require new users to create accounts and passwords to proceed, so it’s no surprise that many system users in an organization struggle to keep up with best practices for password security. Adding to organizations’ frustration with user-developed weak passwords is the fact that the computing power available to nefarious agents for password cracking just gets bigger and bigger.

Recognizing the needed evolution for password policies, In June, the United States National Institute for Standards and Technology (NIST) released new password security guidelines. Some of the new guidelines include:

**Password Length** - NIST’s new guidelines suggest a minimum of 8 characters; however, it is in our belief that passwords should be a minimum of 14 characters. Users should increase the minimum password length for more sensitive accounts. NIST also recommends entities should allow a maximum length of at least 64 characters, so no more “Sorry, your password can’t be longer than 16 characters.”

**User Pass Phrases** - NIST also recommends encouraging users to create unique passphrases they can remember, using whatever characters they want.

**Don’t Use Common Passwords** – Agency’s should check new passwords against a dictionary of known-bad choices. You don’t want to let people use “Password123” and so on. If this is not possible to implement, we recommend enforcing passphrases longer than 14 characters.

**Password Expiration** - No more expiration without reason. If users decide to have a long, hard-to-guess password, we shouldn’t make them change it unnecessarily. A unique passphrase longer than 14 characters would require a less frequent password change and is often easier to remember than a “complex” password. The 22-character passphrase “thebluecatappearsgreen” is more secure and easier to remember than this 8-character passphrase “U$9O378^”.

If the agency decides to implement and/or change any of their current password policies, we recommend that they force each user to change their password in order to fully implement the policy change.
The Results

The assessment incorporated four parts: wireless, application, network, and social engineering. Wireless security would include any WiFi Access Points or the configuration of wireless networks at the agency’s locations. The application security would include any configurations and source code of applications that are critical to the agency’s mission. The network security would include any device, connection, or asset the agency’s employees could access. The social engineering included our attempt to gain unauthorized network access using phishing campaigns.

Risk Identification

The risk identification function contains the basic ground work for understanding and managing cybersecurity risk to assets, data, and systems capabilities.

Event Protection and Prevention

The event protection and prevention function is focused on helping the organization develop and implement safeguards to reduce the impact of a potential cybersecurity event.

Event Detection

The event detection function is focused on assisting the organization on developing and implementing safeguards to detect the presence of a cybersecurity threat. By detecting cybersecurity events in a timely manner, the organization can reduce the potential impact the threat can have on the organization.

Conclusion

Cornerstone assessed the cybersecurity of an agency of the City and County of Denver for the Auditor and Technology Services. Cornerstone utilized the NIST Cybersecurity Framework and identified strengths and weaknesses using the three-aforementioned key functional process areas of cybersecurity. A combined assessment of strengths and weaknesses in these three process areas was communicated to Technology Services and the Auditor. Additionally, Cornerstone’s assessment of the agency of the City, along with the associated findings, were reported to Technology Services.
Office of the Auditor

The Auditor of the City and County of Denver is independently elected by the citizens 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 citizen confidence and avoiding any appearance of a conflict of interest.

Our Mission

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