AUDIT REPORT
Citywide
Information Systems Maturity Assessment
March 2017

Office of the Auditor
Audit Services Division
City and County of Denver

Timothy M. O'Brien, CPA
Denver 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 for the purpose of ensuring the proper and efficient use of City resources and providing other audit services and information to City Council, the Mayor and the public to improve all aspects of Denver's government. He also chairs the City's Audit Committee.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities of the integrity of the City's finances and operations, including the integrity 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.

Audit Committee

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

Audit Management

Valerie Walling, CPA, CMC®, Deputy Auditor
Heidi O'Neil, CPA, CGMA, Director of Financial Audits

Audit Staff

Shannon Kuhn, CISA, Audit Supervisor
Jared Miller, CFE, Lead and/or Senior Auditors

Contractors

Hein and Associates
Bill Evert, Partner, Business Advisory Services
Donald McLaughlin, Business Advisory Services
Brian Cather, Business Advisory Services

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) 913-5247

Or download and view an electronic copy by visiting our website at: www.denvergov.org/auditor
Report number: **A2016-010**

Timothy M. O'Brien, CPA
Auditor

City and County of Denver

201 West Colfax Avenue, #705 • Denver, Colorado 80202

720-913-5000 • Fax 720-913-5253 • www.denvergov.org/auditor

March 16, 2017

AUDITOR'S REPORT

A third party has completed a Citywide Information Systems Maturity Assessment. The purpose of the assessment was to the determine the extent to which computer users within agencies and departments throughout the City have an understanding of how Technology Services handles and responds to cybersecurity risks.

The assessment found some areas of strength and some areas that need improvement, which have been communicated to the City's Technology Services department for further evaluation.

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

Denver Auditor's Office

Timothy M. O'Brien, CPA

Hein & Associates LLP
1999 Broadway, Suite 4000
Denver, Colorado 80202

www.heincpa.com
p 303.298.9600
f 303.298.8118

City and County of Denver

Information Systems Maturity Assessment

March 16, 2017

Information Systems Maturity Model Assessment
City and County of Denver

Background

Hein & Associates LLP (Hein) was tasked by the Office of the Auditor (Auditor) to evaluate the Information Systems Maturity Model of the City and County of Denver (City) for Technology Services and the Auditor. As part of deliverables, Hein will present a high level report to the Audit Committee and findings will be sent to Technology Services. The results of the report will be limited to discussing how to move towards an "optimized" risk reduction process and to reducing risk exposures to the City through continuous and rigorous assessments of their information systems.

A key to this improvement process is balancing the needs of various departments, while managing the implementation of both centralized and decentralized Information Technology strategies. Currently, the City has a combined decentralized and centralized approach to information systems requirements, which affects how risk is approached and managed by the City.

When applying and evaluating the Information Systems Maturity Model (see Figure 1) for the City, one must weigh how the results of this study 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 was to understand the current posture of the City's centralized Information Technology services (Technology Services). Hein began by sending surveys that addressed the different areas of the Information Systems Maturity Model (see Figure 1). The surveys were designed as a tool to assess areas of potential strengths and weaknesses during subsequent follow-up interviews with three separate departments overseen by Technology Services.

This engagement focused solely on providing a high level assessment on the information systems of the City, their posture in the maturity model, and how we could align that posture on the National Institute of Science and Technology (NIST) Cybersecurity Framework. The NIST standard is the generally accepted framework which was adopted after Executive Order 16636 was passed in 2013.

Hein used the Information Systems Maturity Model which helps organizations assess the strengths and weaknesses of various areas of their policies and procedures (see Figure 1).

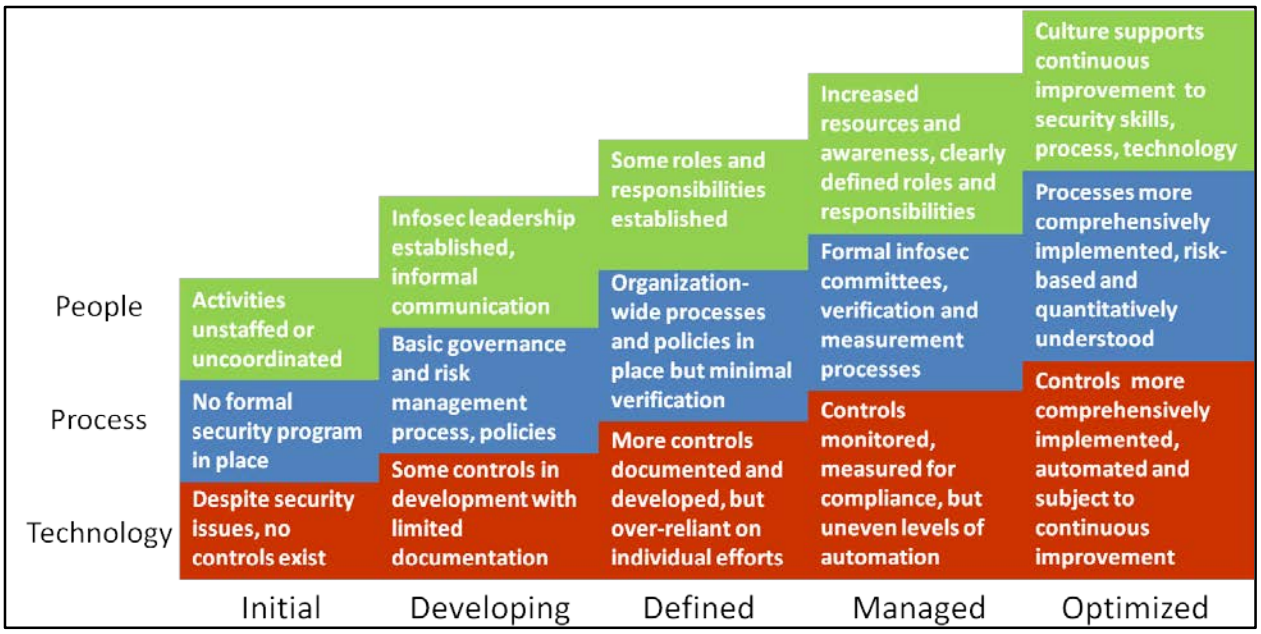

Figure 1

The Methodology

Hein collected survey results and conducted interviews in their high level assessment to evaluate the City and County of Denver's Technology Services' Cybersecurity maturity. Hein's methodology used five key functional process areas of Cybersecurity and include:

- *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.
- *Event Response:* Plans and actions taken in response to an identified Cybersecurity event.
- *Event Recovery:* Plans and actions taken for the resilience and restoration of capabilities or services impaired by a cyber security event.

The Results

The assessment incorporated surveys completed by employees of the City and two interviews with employees of predetermined departments. The survey encompassed an Information Technology survey and an end-user survey. The Information Technology survey targeted individuals that work in an Information Technology role or have job responsibilities in that capacity. The end-user survey targeted employees that do not have an Information Technology role. The

end-user survey and interviews provide critical information about how Technology Services operates with various departments as a centralized service and how end users perceive who is responsible for cybersecurity for their department.

Risk Identification

The risk identification function contains the basic ground work for understanding and managing Cybersecurity risk to assets, data, and systems capabilities. By having a high score in Risk Identification, organization's Cybersecurity efforts have a risk strategy in place with measurable goals tailored to the business and industry. Hein assessed that Technology Services has tools and strategies in place that track potential risk; however, we feel Technology Services is challenged with tracking the large amount of applications in various departments. Hein found the various departments are in the process of identifying risks. Additionally, the Information Governance Committee is working to create and update Information Technology policies and procedures. Based on the information provided, Hein assesses the maturity level of Risk Identification process area as Developing.

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. By having a high score in event protection and prevention, the organization may have multiple layers of Cybersecurity defense in the form of technologies, people and procedures in place. Hein assessed that Technology Services has tools and strategies in place that protect and prevent Cybersecurity events. Without a strong maturity level in the Risk Identification process area, these tools might not be effectively covering all areas of the City's IT infrastructure; therefore, we assess the maturity level of Event Protection and Prevention process area as Defined.

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. Hein assessed that Technology Services has tools in place to detect the presence of a Cybersecurity threat; however, without a strong maturity level in the Risk Identification process area, these tools might not be effectively covering all areas of the City's IT infrastructure. Based on previous engagements, interviews, and the survey, Hein assesses the maturity level of the Event Detection process area as Developing.

Event Response

The event response function is focused on ensuring a response plan is defined and the preparedness of the organization to take the appropriate actions in the event of a Cybersecurity threat. A high score in event response equates to the organization having a process and procedures in place that respond to a myriad of Cybersecurity incidents with varying levels of impact. Hein assessed that Technology Services has some procedures and policies in place that allow sufficient event response to Cybersecurity threats; however, there is an over-reliance on individual efforts within Technology Services. Hein assesses the maturity level of Event Response process area as Defined.

Event Recovery

The event recovery function is focused on what recovery actions should be taken during and after an event that would cause a loss of critical data. A high score in event recovery indicates a robust process for recovering from various types of service outages in a timely manner. Hein assessed that Technology Services has sufficient backup and recovery solutions implemented; however, as identified in Risk Identification, Technology Services could benefit further from having an updated list of critical applications in each department. Hein assesses the maturity level of Event Recovery process area as Defined.

Conclusion

The City and County of Denver, specifically the maturity level of Information Technology services, was assessed for the Auditor using Hein's Information Systems Maturity Model (see Figure 1). Hein identified strengths and weaknesses using the five aforementioned key functional process areas of Cybersecurity. Hein recognized that Technology Services faces many challenges with implementing a centralized Information Technology approach within various departments and their sub organizations. A combined assessment of strengths and weaknesses in these five process areas resulted in an overall maturity rating which was communicated to Technology Services and the Auditor. Additionally, Hein's assessment of the City, along with the associated findings, were reported to Technology Services.