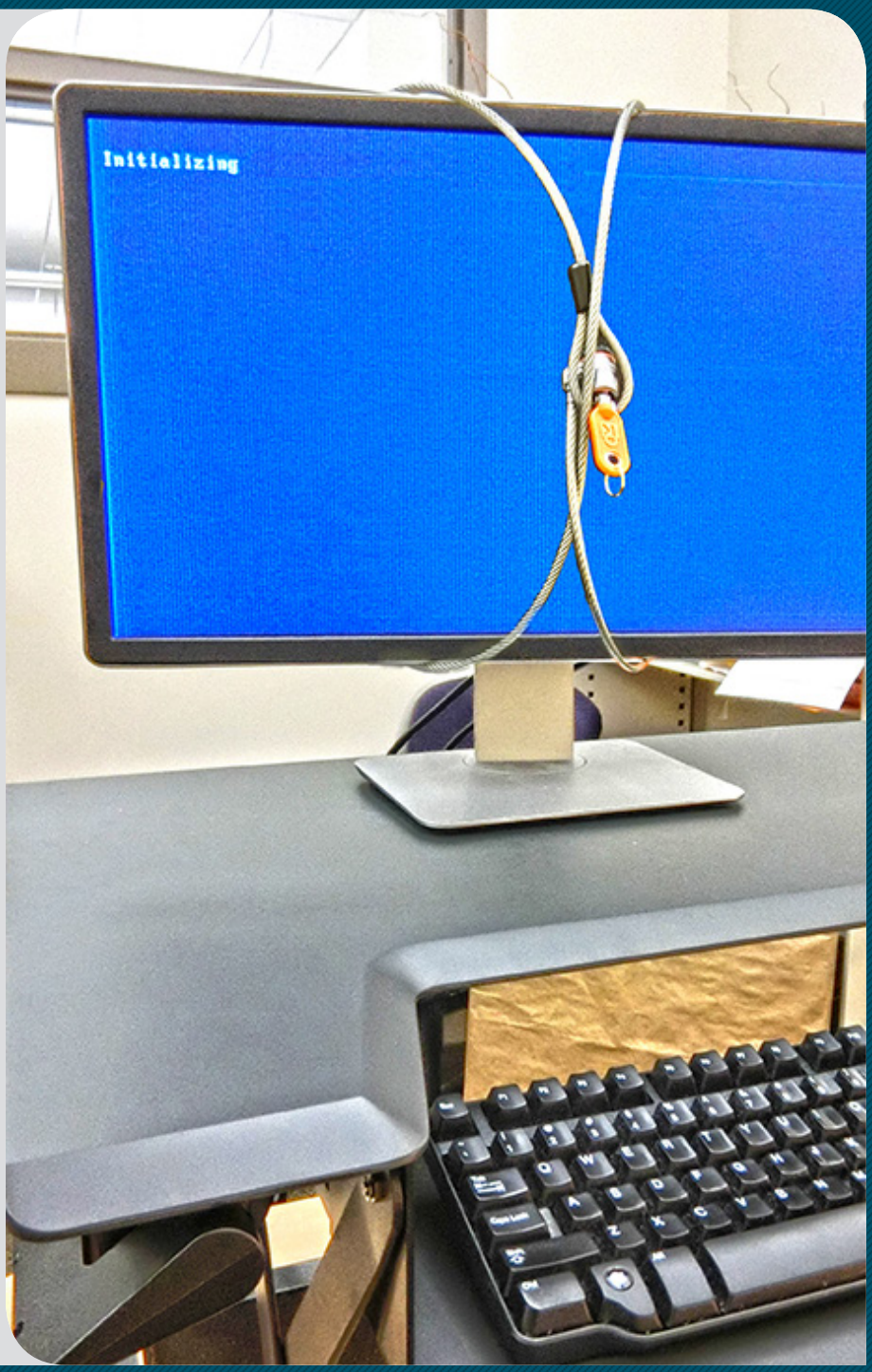
AUDIT REPORT

Information Systems Maturity Assessment

October 2016

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
Jeffrey Garcia, Esq, Executive Council
Heidi, O'Neil, CPA, CGMA, Director of Financial Audits

Audit Services Division

Shannon Kuhn, CISA, IT Audit Supervisor
Jared Miller, Lead Auditor

Consultants

Hein and Associates LLP
Bill Evert, Partner, Business Advisory Services
James Taylor, Manager, Business Advisory Services
Donald McLaughlin,Associate, Business Advisory Services
Brian Cather, Associate, 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: **A2016-005**

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

October 20, 2016

AUDITOR'S REPORT

A third party has completed a cybersecurity assessment of a selected Agency with the City and County of Denver (City). The purpose of the audit was to determine if controls were in place to effectively prevent unauthorized access to data and systems within the Agency.

Our audit 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.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, *General Powers and Duties of Auditor*, and was conducted in accordance with generally accepted government auditing standards. 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.

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

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

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

www.heincpa.com
p 303.298.9600
f 303.298.8118

An Agency of City and County of Denver

Information Systems Maturity Assessment

October 20, 2016

Information Systems Maturity Model Assessment
An Agency of City and County of Denver

Background

Hein & Associates LLP ("Hein") was tasked by the Auditor to evaluate the Information Systems Maturity Model of an agency of the City and County of Denver ("City") for Technology Services and the Auditor's Office. As part of deliverables, Hein will present a 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 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 Maturity Model (see Figure 1) for the agency of 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 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. Hein 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 solely on assessing the information systems of an agency 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) 800-53 Rev. A. 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 infrastructure (see Figure 1).

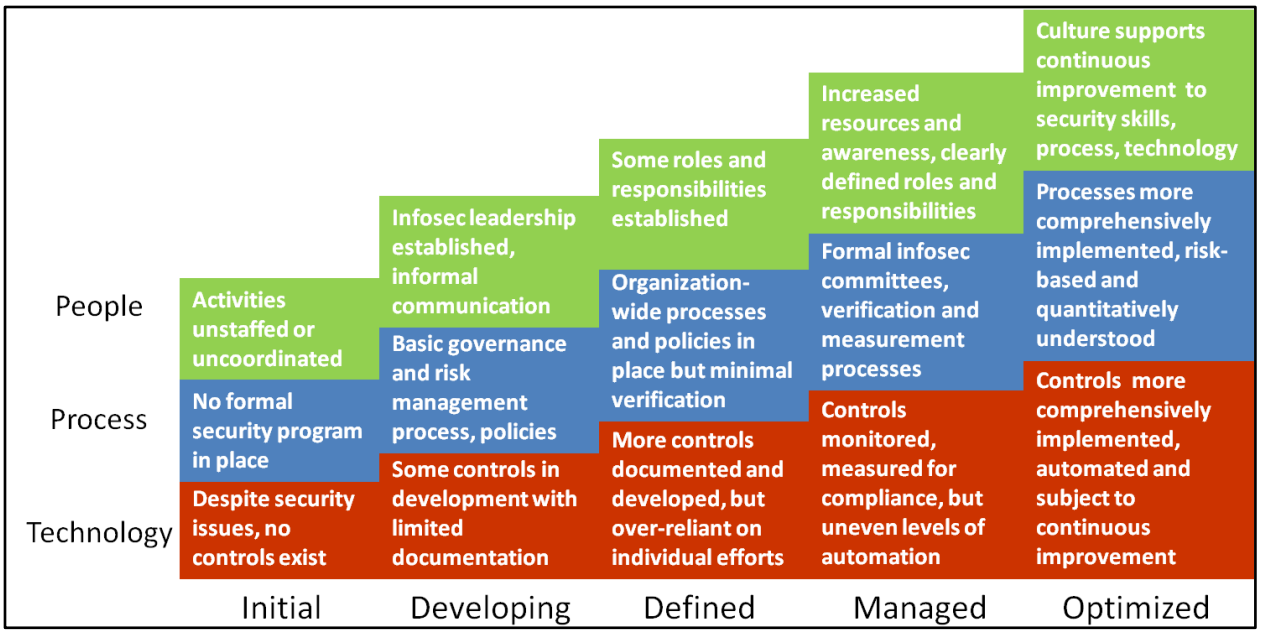


Figure 1

The Methodology

Hein collected evidence and performed testing to enable an effective Cybersecurity maturity assessment of the agency of the City and County of Denver. Hein's methodology uses five key functional process areas of Cybersecurity; however, the fifth key functional process area, event recovery, was 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.
- *Event Response:* Plans and actions taken in response to an identified Cybersecurity event.

The Results

The assessment incorporated three parts: external network, internal network, and physical access. The external network encompasses the assets and protections in place by the City that must be traversed to access internal assets. The internal network would include any device, connection, or asset a City employee could access. Physical access would encompass the process of entering the building, badging, personnel questioning a potential network attacker, and deactivating or locking unused assets.

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.

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.

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.

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.

Conclusion

An agency of the City and County of Denver was assessed for the Auditor and Technology Services using Hein's Information Systems Maturity Model (see Figure 1). Hein identified strengths and weaknesses using the four aforementioned key functional process areas of Cybersecurity. A combined assessment of strengths and weaknesses in these four process areas resulted in an overall maturity rating which was communicated to Technology Services and the Auditor. Additionally, Hein's assessment of the agency of the City, along with the associated findings, were reported to Technology Services.