CARSON CITY CONSOLIDATED MUNICIPALITY
NOTICE OF MEETING OF THE
AUDIT COMMITTEE

Day: Tuesday
Date: December 8, 2020
Time: Beginning at 1:00 pm
Location: Community Center, Bob Boldrick Theater
851 East William Street
Carson City, Nevada

AGENDA

NOTICE TO THE PUBLIC:

The State of Nevada and Carson City are currently in a declared State of Emergency in response to the global pandemic caused by the coronavirus (COVID-19) infectious disease outbreak. In accordance with the Governor's Declaration of Emergency Directive 006, which has suspended the provisions of NRS 241.020 requiring the designation of a physical location for meetings of public bodies where members of the public are permitted to attend and participate, public meetings of Carson City will NOT have a physical location open to the public until such time this Directive is removed.

• Members of the public who wish only to view the meeting but do NOT plan to make public comment may watch the livestream of the Audit Committee meeting at www.carson.org/granicus and by clicking on "In progress" next to the meeting date, or by tuning in to cable channel 191.

• The public may provide public comment in advance of a meeting by written submission to the following email address: oluedtke@carson.org. For inclusion or reference in the minutes of the meeting, your public comment must include your full name and be submitted via email by not later than 3:00 p.m. the day before the meeting.

• Members of the public who wish to provide live public comment may do so during the designated public comment periods, indicated on the agenda, via telephonic appearance by dialing the numbers listed below. Please do NOT join by phone if you do not wish to make public comment.

Join by phone:
Phone Number: +1-408-418-9388
Meeting Number: 146 374 6041

1. Call to Order

2. Roll Call

3. Public Comments and Discussion:
The public is invited at this time to comment on and discuss any topic that is relevant to, or within the authority of, the Carson City Audit Committee. In order for members of the public to participate in the Committee's consideration of an agenda item, the Committee strongly encourages members of the public

to comment on an agenda item during the item itself. No action may be taken on a matter raised under public comment unless the item has been specifically included on the agenda as an item upon which action may be taken.

4. For Possible Action: Approval of Minutes - August 4th, 2020

5. For Possible Action: Adoption of Agenda

6. Meeting Items

6.A For Possible Action: Discussion and possible action regarding the approval of Internal Audit and recommendations to the City Departments. (Sheri Russell, srussell@carson.org)

Staff Summary: Eide Bailly, LLP completed the Internal and External Network Vulnerability internal audit from the FY21 Audit Work Program. Briefing will address internal audit findings, recommendations and agency response(s).

6.B For Possible Action: Discussion and possible action regarding the monitoring, review and closure of internal audit findings and/or recommendations included in the Audit Findings Tracking Report and provide a recommendation to the Board of Supervisors to close completed findings and/or recommendations. (Sheri Russell, SRussell@carson.org)

Staff Summary: City staff will discuss the monitoring, review and closure of the previous internal auditor findings and/or recommendations included in the Audit Findings Tracking Report.

6.C For Presentation Only: Discussion regarding FY 20 audit work program update and Hotline activity. (SRussell@Carson.org)

Staff Summary: Representatives from Eide Bailey, LLP will be discussing the progress of the FY 21 audit work program as well as any items received through the Fraud, Waste & Abuse Hotline.

7. Public Comment:

The public is invited at this time to comment on any matter that is not specifically included on the agenda as an action item. No action may be taken on a matter raised under this item of the agenda.

8. For Possible Action: To Adjourn

Agenda Management Notice - Items on the agenda may be taken out of order; the public body may combine two or more agenda items for consideration; and the public body may remove an item from the agenda or delay discussion relating to an item on the agenda at any time.

Titles of agenda items are intended to identify specific matters. If you desire detailed information concerning any subject matter itemized within this agenda, you are encouraged to call the responsible agency or the City Manager's Office. You are encouraged to attend this meeting and participate by commenting on any agendized item.

Notice to persons with disabilities: Members of the public who are disabled and require special assistance or accommodations at the meeting are requested to notify the City Manager's Office in writing at 201 North Carson Street, Carson City, NV, 89701, or by calling (775) 887-2100 at least 24 hours in advance.

To request a copy of the supporting materials for this meeting contact Maria Diaz at MDiaz@carson.org or call (775) 887-2133.

This agenda and backup information are available on the City's website at www.carson.org, and at the Finance Office - City Hall, 201 N. Carson Street, Ste 3, Carson City, Nevada (775) 887-2133

NOTICE TO PUBLIC: In accordance with the Governor's Emergency Declaration Directive 006 suspending state law provisions requiring the posting of public meeting agendas at physical locations, this agenda was posted electronically at the following Internet websites:
www.carson.org/agendas
http://notice.nv.gov

CARSON CITY AUDIT COMMITTEE (AC)
Draft Minutes of the August 4, 2020 Meeting
Page 1

A regular meeting of the Carson City Audit Committee was scheduled for 1:30 p.m. on Tuesday, August 4, 2020 in the Community Center Sierra Room, 851 East William Street, Carson City, Nevada.

PRESENT: Chairperson Stephen Ferguson
Member Lori Bagwell
Member Ernie Mayhorn
Member Margie Molina

STAFF: Sheri Russell, Chief Financial Officer
Todd Reese, Deputy District Attorney via WebEx
Danielle Howard, Public Meetings Clerk

NOTE: A recording of these proceedings, the committee's agenda materials, and any written comments or documentation provided to the Clerk, during the meeting, are part of the public record. These materials are available for review, in the Clerk's Office, during regular business hours.

1 - 2. CALL TO ORDER AND ROLL CALL

(1:44:26) – Chairperson Ferguson called the meeting to order at 1:44 p.m. Roll was called, and a quorum was present.

3. PUBLIC COMMENTS

(1:44:43) – Chairperson Ferguson entertained public comments; however, none were forthcoming.

4. POSSIBLE ACTION ON APPROVAL OF MINUTES – JUNE 15, 2020

(1:45:22) – Chairperson Ferguson introduced the item and entertained comments and/or a motion.

(1:45:40) – Member Mayhorn moved to approve the meeting minutes of June 15, 2020. Member Molina seconded the motion. Motion carried 4-0-0.

5. POSSIBLE ACTION ON ADOPTION OF AGENDA

(1:45:51) – Chairperson Ferguson noted that there were no modifications to the agenda.

6. PUBLIC MEETING ITEMS:

6.A FOR POSSIBLE ACTION: DISCUSSION AND POSSBLE ACTION REGARDING THE REVIEW OF AGREED UPON PROCEDURES ESTABLISHED BY EIDE BAILLY AND STAFF FOR THE AUDITS OF THE VEHICLE FLEET, IT VULNERABILITY, AND REVENUE AND ACCOUNTS RECEIVABLE FOR THE FISCAL YEAR (FY) 2021 AUDIT WORK PROGRAM.

(1:46:15) – Chairperson Ferguson introduced the item, and Eide Bailly Senior Manager Audrey Donovan presented the agenda materials remotely via WebEx. She and Ms. Russell also responded to clarifying questions.

(2:01:26) – Chairperson Ferguson entertained a motion.

(2:01:39) – MOTION: Member Bagwell moved to direct Eide Bailly and Staff to proceed with the agreed upon procedures as discussed on the record. Member Mayhorn seconded the motion. Motion carried 4-0-0.

6.B FOR PRESENTATION ONLY: DISCUSSION AND POSSIBLE ACTION REGARDING FISCAL YEAR (FY) 2020 AUDIT WORK PROGRAM UPDATE AND HOTLINE ACTIVITY.

(2:01:58) – Chairperson Ferguson introduced the item. Ms. Donovan noted that she did not have any new hotline activity to report. She indicated that the individual that had made four reports against the same individual through the hotline and was discussed in the previous meeting had moved forward with the Airport auditors, and City Manager Nancy Paulson had moved the reports forward to the board to discuss the issue with the auditors.

6.C FOR DISCUSSION ONLY: DISCUSSION REGARDING DATES FOR THE NEXT MEETING OF THE AUDIT COMMITTEE.

(2:03:51) – Chairperson Ferguson introduced the item. Ms. Russell recommended late November or early December for the next Committee meeting. There was consensus among the Committee to meet on December 8, 2020 at 1:30 p.m.

7. PUBLIC COMMENT

(2:05:15) – Chairperson Ferguson entertained public comments; however, none were forthcoming.

8. FOR POSSIBLE ACTION: TO ADJOURN

(2:05:32) – Chairperson Ferguson adjourned the meeting at 2:05 p.m.

The Minutes of the August 4, 2020 Carson City Audit Committee meeting are so approved this 8th day of December, 2020.

Audit Committee Agenda Item Report

Meeting Date: December 8, 2020
Submitted by: Sheri Russell
Submitting Department: Finance
Item Type: Formal Action / Motion
Agenda Section:

Subject:
For Possible Action: Discussion and possible action regarding the approval of Internal Audit and recommendations to the City Departments. (Sheri Russell, srussell@carson.org)

Staff Summary: Eide Bailly, LLP completed the Internal and External Network Vulnerability internal audit from the FY21 Audit Work Program. Briefing will address internal audit findings, recommendations and agency response(s).

Suggested Action:
I move to accept the Internal and External Network Vulnerability internal audit report and direct staff to work on the recommendations provided.

Attachments:
SR - FY 21 Release Internal Audits_IT Vulnerability.docx

Carson City Network Summary Document Oct 2020.pdf

STAFF REPORT

Report To: Audit Committee Meeting Date: December 8, 2020

Staff Contact: Audrey Donovan, Senior Manager, Eide Bailly, LLP

Agenda Title: For Possible Action: Discussion and possible action regarding the approval of Internal Audits and recommendations to the City Departments. (Sheri Russell, srussell@carson.org)

Staff Summary: Eide Bailly, LLP completed the Internal and External Network Vulnerability internal audits from the FY21 Audit Work Program. Briefing will address internal audit findings, recommendations and agency response(s).

Agenda Action: Formal Action/Motion Time Requested: 20 minutes

---

Proposed Motion

I move to accept the Internal and External Network Vulnerability internal audit reports and direct staff to work on the recommendations provided.

Board's Strategic Goal

Efficient Government

Previous Action

Fiscal Year 2021 internal audit program was approved by the Audit Committee on August 4th, 2020.

Background/Issues & Analysis

According to Carson City Municipal Code 2.14.040 the Audit Committee will review and make recommendations to the Board of Supervisors regarding the annual financial audit, performance, compliance and efficiency audits, including specific issues of concern providing a higher level of accountability over the use of public funds and the adequacy of any city department or office performance measure for internal audit purposes.

Certain specific items in the IT Vulnerability internal audit report have been obfuscated for Employee and Asset safety. Management has a full detailed copy of the specific findings and will ensure recommendations are addressed.

Applicable Statute, Code, Policy, Rule or Regulation

Carson City Charter Chapter 3.075, Carson City Municipal Code 2.14.040

Financial Information

Is there a fiscal impact? ☐ Yes ☒ No

Is it currently budgeted? ☐ Yes ☒ No

Alternatives

N/A

Board Action Taken:

Motion: _____ 1) _____ Aye/Nay

2) _____ _____

_____

_____

_____

_____

_____

(Vote Recorded By)

Risk Advisory Services
Network Testing Executive Summary

October 2020

CARSON CITY

Submitted By:

Eide Bailly LLP
Nathan Kramer, CEH
Associate, Risk Advisory Services

Joe Sousa, CISA, CEH
Manager, Cybersecurity and information Assurance

Eric Pulse, CISA, CISM, CRISC, GSEC, CFSA
Principal-in-Charge of Risk Advisory

October 19, 2020

James Underwood
Chief Information Officer
Carson City Information Technology
Carson City, Nevada

Dear James:

This report contains our findings and recommendations relating to the network testing Eide Bailly performed for Carson City in 2020.

No assessment of controls or security can ever provide total assurance or 100 percent protection against possible control failures or security intrusions on your systems. The potential effectiveness of specific controls and security measures is subject to inherent limitations and accordingly, errors or fraud may occur and not be detected. Furthermore, information networks, application and control environments are extremely dynamic in nature and our assessment of your controls, security methods, and procedures are conducted and documented as of the following specific period in time.

Assessment Service	Start Date	End Date
External Network Penetration Assessment	09/14/2020	09/23/2020
Internal Network Vulnerability Assessment	09/21/2020	10/01/2020

As a result, the projection of any conclusions, based on our assessment, to future periods is subject to the risk that (1) changes are made to the systems or controls; (2) changes are made in processing requirements; (3) changes are required because of the passage of time; or (4) new security exploits are discovered that may alter the validity of such conclusions. Therefore, Eide Bailly takes no responsibility for any lack of specific control failures, breach of security, or other errors of fraud related to any part of your operational environment other than those controls and security measures specifically tested and for any period of time other than the period specifically covered by our assessment conducted. Any subsequent control or security issues that may arise within those areas assessed or any control or security issues that are present at the time of this assessment, but that are outside the scope of this assessment, are solely the responsibility of Carson City.

We appreciate the courtesies and cooperation extended to us during this project, and appreciate the opportunity to be of service to Carson City. If you have any questions or need anything additional, please contact me at 605.367.6713 or jsousa@eidebailly.com.

Sincerely,

Joe Sousa, CISA, CEH
Manager, Cybersecurity and information Assurance

Executive Summary

Summary of Results

The table below contains a summary of the results for the area assessed during our assessment of Carson City.

Area Assessed	Rating	Results
External Network Penetration Assessment	**Elevated**	Eide Bailly identified five (5) high, five (5) medium and two (2) low risk findings.
Internal Network Vulnerability Assessment	**Elevated**	Eide Bailly identified twenty-two critical (22), sixteen (16) highs, and sixty-five (65) medium risk findings.

External Network Penetration Assessment

Eide Bailly was contracted by Carson City to conduct an External Penetration Test in order to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against the organization with the goals of: Identifying if a remote attacker could penetrate the organizations defenses and determining the impact of a security breach of confidentiality of the organization's private data, internal infrastructure and availability of the organization's information systems.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in PTES (Penetration Testing Execution Standard) with all tests and actions being conducted under controlled conditions.

Methodology

Eide Bailly utilized the PTES which defines the process related to a penetration testing. From the initial communication and information gathering, it also covers threat modeling phases where testers are working behind the scenes to get a better understanding of the tested organization through vulnerability research, exploitation and post exploitation.

The PTES consists of seven phases:

1. **Pre-engagement Interactions** - In this phase, we prepare and gather the required tools, operating systems, and software to start the penetration testing. Selecting the tools required during a penetration test depends on several factors such as the type and the depth of the engagement. Some of the tools include:

    - WHOIS
    - DNSEnum
    - Nessus
    - Nmap

2. **Intelligence Gathering** - In this phase, the information or data or intelligence is gathered to assist in guiding the assessment actions. The information gathering process is conducted to gather information about the employee in an organization that can help us to get access, potentially secret or private "intelligence" of a competitor, or information that is otherwise relevant to the target.

3. **Threat Modeling** - Threat modeling is a process for optimizing network security by identifying vulnerabilities and then defining countermeasures to prevent or mitigate the effects of threats to the system. Threat modeling is used to determine where the most effort should be applied to keep a system secure. This is a factor that changes as applications are added, removed, or upgraded or user requirements are evolved.

4. **Vulnerability Analysis** - Vulnerability Analysis is used to identify and evaluate the security risks posed by identified vulnerabilities. The Process of vulnerability is divided into two steps, Identification and Validation.

   Identification: Discovering the vulnerability is the main task in this step.
   Validation: In this step, we reduce the number of identified vulnerabilities to only those that are actually valid.

5. **Exploitation** - After finding the vulnerabilities, we try to exploit those vulnerabilities to breach the system and its security. For the Exploitation, we use different framework and software that are recommended for exploitative purpose and are freely available. Some of the most recommended tools include:

   - Kali Linux
   - Metasploit
   - Burp Suite

6. **Post Exploitation** - In the Post-exploitation phase, we determine the value of the machine compromised and to maintain control of the machine for later use. The value of the machine is determined by the sensitivity of the data stored on it and the machine's usefulness in further compromising the network.

7. **Reporting** - In this phase, we report the findings in a way that is understandable and acceptable by the organization that owns that system or hardware. It includes the defects that allow an attacker to violate an explicit (or implicit) security policy to achieve some impact (or consequence). In particular, defects that allow intruders to gain increased levels of access or interfere with the normal operation of systems are vulnerabilities.

Our external network penetration assessment was designed to answer the following questions for Carson City:

- **Was Eide Bailly able to compromise Carson City's external network security?**

  No. During the conduct of our testing, we were not able to compromise Carson City's external network security. We were also unable to obtain any sensitive information or gain sufficient access to any of Carson City's servers to gain control of those servers.

- **Did Eide Bailly identify any issues that Carson City should be aware?**

  Yes. Our testing did identify some security issues related to Carson City's external network. These issues are documented in "Carson City External Pen Test Report 2020.pdf" report provided to IT management.

- **What is Eide Bailly's assessment of Carson City's external network security?**

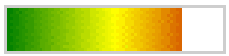
  Based on the expertise and experience of Eide Bailly, the recommendations and best practice guidelines identified in this report will provide a foundation to improve the security of the external network environment. Eide Bailly experts understand the implications of the challenges facing governments daily, and that security is a process, not a destination. As such, an external penetration assessment is the first step in securing internal, external, and DMZ resources. Eide Bailly understands organizational and operational needs and is committed to providing world class, quality service. Due to the constantly changing threat environment, we recommend an external penetration analysis be performed at least annually. Additionally, Eide Bailly security experts are also available on a

consultation basis to assist in remediation of any findings.

Eide Bailly assigns a risk level to each identified issue discovered during the assessment. We base this risk level on an expert analysis of the issue, its environment, and the severity of the identified issue. We derive the suggested remediation timeline from the potential for system compromise, overall damage to the environment/system, and criticality of information theft.

Twelve (12) findings were identified during the internal vulnerability assessment of the addresses provided. These findings are summarized below by risk (the risk ratings are defined in the Scope section of the report). We were able to assess the organization's performance through the vulnerability scanning and testing activities.

Based on our testing, we determined that we would rank the organization's external network risk as Elevated in the areas assessed.

Risk Level	Description
Critical 	Risk of immediate exploitation or critical level of exposure that can lead to system or application compromise or information theft. Remediation should be conducted immediately or as soon as possible.
High 	Significant risk of severe impact to system or application security. Remediation should be prioritized or within (1) month.
Elevated 	Risk of an elevated nature that may expose sensitive information or may be used in conjunction with other issues aiding in exploitation. Remediation should be prioritized based on the criticality of the system and information exposed or within (3) months.
Moderate 	Risk of a less critical nature that may potentially lead to information theft or misuse. Remediation should be included in the next security update or within six (6) months.
Minimal 	Risk of a non-critical nature that may lead to misuse or stability loss or enhancement features, which will improve security. This issue should be noted for reference; however, remediation is not strictly necessary.

Recommendations

Due to the impact to the overall organization as uncovered by our testing, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner. While a comprehensive list of items that should be implemented is beyond the scope of this engagement, some high-level items are important to mention.

1. **Update all systems that are currently running outdated software**: Lack of support implies that no new security patches for the product will be released by the vendor. As a result, the unsupported operating systems are likely to contain security vulnerabilities. These systems should either be updated to run a supported operating system or shut down in order to protect the security, availability, and integrity of Carson City's perimeter network.

2. **System hardening processes should be in place across all systems**: Misconfiguration and insecure deployment issues were discovered across various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all systems.

3. **Web development processes:** Ensure coding of website and web applications follow OWASP standards. The OWASP Top 10 is a standard awareness document for developers and web application security. Carson City should adopt this document and start the process of ensuring that their web applications minimize these risks.

4. **Recommend remediation scanning be performed.** Based on the number of issues identified we would recommend Carson City IT staff work toward remediating issues working on the most critical items first. Retesting should be performed within 6 months of this report.

Internal Network Vulnerability Assessment

Eide Bailly LLP conducted an internal vulnerability assessment to establish a comprehensive view of the Carson City's network as it appears from the inside. This allowed us to identify potential security weaknesses within the network configuration which could allow an intruder to gain unauthorized access or cause network disruptions. The assessment consisted of a semi-blind internal assessment where Eide Bailly was provided the internal network IP addresses. The scanning system utilized by the Eide Bailly consultant for testing was placed in a server VLAN which allowed access to each subnet and host without restrictions. Without this, Eide Bailly would have been placed on the user network and would have had limited access to scan hosts based on the level of segmentation in place.

Methodology

Efforts were placed on the identification and exploitation of security weaknesses that could allow an attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in PTES (Penetration Testing Execution Standard) with all tests and actions being conducted under controlled conditions.

For this security assessment, Eide Bailly followed a custom methodology patterned after actual attacks organizations are facing from hackers.

- Internal Infrastructure Foot printing
- Port Scanning and System Fingerprinting
- Vulnerability and Exploit Research
- Manual Verification of Identified Vulnerabilities

Our internal network vulnerability assessment was designed to answer the following questions for Carson City:

- **Could Eide Bailly compromise Carson City's internal network security?**

  Yes. During the conduct of our testing, we were able to compromise Carson City's internal network security. Systems were accessible with either default or no credentials. Systems were missing critical patches that could enable attackers to perform remote code execution on internal systems. Out-of-date systems and operating systems are running within the network. We were not able to obtain any sensitive information but did gain access to internal systems via multiple attack vectors.

- **Did Eide Bailly identify any issues that Carson City should be aware?**

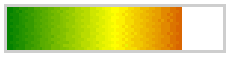
  Yes. Our testing did identify some security issues related to Carson City's internal network. These issues are documented in "Carson City Internal Vulnerability Report 2020.pdf" report provided to IT management.

- **What is Eide Bailly's assessment of Carson City's internal network security?**

  Eide Bailly LLP conducted an internal vulnerability assessment to establish a comprehensive view of the Carson City's network as it appears from the inside. This allowed us to identify potential security weaknesses within the network configuration which could allow an intruder to gain unauthorized access or cause network disruptions. The assessment consisted of a semi-blind internal assessment where Eide Bailly was provided the internal network IP addresses.

103 findings were identified during the internal vulnerability assessment of the addresses provided. These findings are summarized below by risk (the risk ratings are defined in the Scope section of the report). We were able to assess the organization's performance through the vulnerability scanning and testing activities.

Based on our testing, we determined that we would rank the organization's internal network risk as **Elevated** in the areas assessed.

Risk Level	Description
Critical 	Risk of immediate exploitation or critical level of exposure that can lead to system or application compromise or information theft. Remediation should be conducted immediately or as soon as possible.
High 	Significant risk of severe impact to system or application security. Remediation should be prioritized or within (1) month.
Elevated 	Risk of an elevated nature that may expose sensitive information or may be used in conjunction with other issues aiding in exploitation. Remediation should be prioritized based on the criticality of the system and information exposed or within (3) months.
Moderate 	Risk of a less critical nature that may potentially lead to information theft or misuse. Remediation should be included in the next security update or within six (6) months.
Minimal 	Risk of a non-critical nature that may lead to misuse or stability loss or enhancement features, which will improve security. This issue should be noted for reference; however, remediation is not strictly necessary.

Recommendations

Due to the impact to the overall organization as uncovered by our testing, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner. While a comprehensive list of items that should be implemented is beyond the scope of this engagement, some high-level items are important to mention.

1. **Update all systems that are currently running unsupported operating systems**: Lack of support implies that no new security patches for the product will be released by the vendor. As a result, the unsupported operating systems are likely to contain security vulnerabilities. These systems should either be updated to run a supported operating system or shut down in order to protect the security, availability, and integrity of Carson City's infrastructure and data.

2. **Implement and enforce implementation of change control across all systems**: Misconfiguration and insecure deployment issues were discovered across various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all systems.

3. **Implement a patch management program:** Operating a consistent patch management program per the guidelines outlined in NIST SP 800-40 is an important component in maintaining good security posture. This will help to limit the attack surface that results from running unpatched internal services.

4. **Change default credentials upon installation.** To reduce the risk of security breaches through default credentials which have been left configured on network devices, it's best to implement a process to change the passwords, and if possible, account names, when new equipment is installed.

5. **Conduct regular vulnerability assessments.** As part of an effective organizational risk management strategy, vulnerability assessments should be conducted on a regular basis. Doing so will allow the organization to determine if the installed security controls are installed properly, operating as intended, and producing the desired outcome. Consult NIST 800-30 for guidelines on operating an effective risk management program.

6. **Recommend remediation scanning be performed.** Based on the number of issues identified we would recommend Carson City IT staff work toward remediating issues working on the most critical items first. Retesting should be performed within 6 months of this report.

Audit Committee Agenda Item Report

Meeting Date: December 8, 2020
Submitted by: Sheri Russell
Submitting Department: Finance
Item Type: Formal Action / Motion
Agenda Section:

Subject:
For Possible Action: Discussion and possible action regarding the monitoring, review and closure of internal audit findings and/or recommendations included in the Audit Findings Tracking Report and provide a recommendation to the Board of Supervisors to close completed findings and/or recommendations. (Sheri Russell, SRussell@carson.org)

Staff Summary: City staff will discuss the monitoring, review and closure of the previous internal auditor findings and/or recommendations included in the Audit Findings Tracking Report.

Suggested Action:
Action will depend on the discussion. I move to [continue the monitoring and review of the items as discussed or] recommend to the Board of Supervisors closing the items discussed based on the correction of findings and recommendations included in the Audit Findings Tracking Report.

Attachments:
SR - Internal Audit Findings Tracking Report.docx

Audit Findings Summary 12-1-2020.pdf

STAFF REPORT

Report To: Audit Committee Meeting Date: December 8, 2020

Staff Contact: Sheri Russell, Chief Financial Officer

Agenda Title: For Possible Action: Discussion and possible action regarding the monitoring, review and closure of internal audit findings and/or recommendations included in the Audit Findings Tracking Report and provide a recommendation to the Board of Supervisors to close completed findings and/or recommendations. (Sheri Russell, SRussell@carson.org)

Staff Summary: Staff will discuss the monitoring, review and closure of the previous internal auditor findings and/or recommendations included in the Audit Findings Tracking Report.

Agenda Action: Formal Action/Motion Time Requested: 20 minutes

---

Proposed Motion

Action will depend on the discussion. I move to [continue the monitoring and review of the items as discussed or] recommend to the Board of Supervisors closing the items discussed based on the correction of findings and recommendations included in the Audit Findings Tracking Report.

Board's Strategic Goal

Efficient Government

Previous Action

On August 20, 2020 the Board of Supervisors closed all items recommended at the August 4, 2020 Audit Committee Meeting which included:

1) 2018 Audit – All addressed, no repeat finding in Fiscal Year (FY) 2019
2) 2019 Audit – Item addressed, was in fact a FY 2018 Finding that affected the FY 2019 audit, no such findings were noted in FY 2019
3) Capital Projects – All items have been addressed
4) Cash Handling – Items 1 thru 9, 12 thru 15, and 19.
5) Social Media – Items 1, 2 and 9
6) HR – All items have been addressed

Background/Issues & Analysis

Staff has experienced some roadblocks with the COVID-19 pandemic, but have still managed to bring a few items before the Audit Committee to recommend closure or validation:

1) Temporary Staffing – Item 2
2) Cash Handling – Items 11, 12 & 18
3) Social Media – Items 7 & 11
4) AP & P-Cards – All Items

Applicable Statute, Code, Policy, Rule or Regulation
N/A

Financial Information
Is there a fiscal impact? ☐ Yes ☒ No

If yes, account name/number:

Is it currently budgeted? ☐ Yes ☐ No

Explanation of Fiscal Impact:

Alternatives
N/A

Board Action Taken:

Motion: _____ 1) _____ Aye/Nay
2) _____ _____
_____
_____
_____
_____

_____
(Vote Recorded By)

Carson City
Internal Audit Summary
Updated - 8/7/20

Carson City - Audit Findings Tracking Summary Report (revised 8-7-20)

Report Name	Report Submittal	AC/BOS Report Approval	Reporting Entity	Report Findings	Completed Findings	AC Approval	BOS Approval	Notes
Community Facility Cost Recovery Study	11/28/2012	1/17/2013	Internal Auditor	15	15			
Community Facility Cost Recovery Eagle Valley Gol	10/3/2012	5/16/2013	Internal Auditor	4	4			
Fleet Management Efficiency Study	6/22/2013	7/18/2013	Internal Auditor	24	24			
Fleet Utilization Study	1/30/2014	4/3/2014	Internal Auditor	12	12			
Employee Efficiency Study	11/25/2014	12/4/2014	Internal Auditor	27	27			
Internal Controls Review	3/31/2015	6/4/2015	Internal Auditor	42	42	4/21/2015	11/15/2018	
Policy and Procedures Review	3/22/2016		Internal Auditor	5	5		12/21/2017	
Payroll Internal Controls Testing	7/27/2016	12/21/2017	Internal Auditor	2	2	8/8/2016	11/15/2018	
P-card Internal Controls Testing	7/27/2016	12/21/2017	Internal Auditor	2	2	8/8/2016	11/15/2018	
Small Works Projects Review	2/17/2017	12/21/2017	Internal Auditor	4	4	2/14/2017	12/21/2017	
Public Guardian Review	5/1/2017	12/21/2017	Internal Auditor	13	13	5/9/2017	11/15/2018	
Purchasing and AP Internal Controls Testing	7/6/2017	12/21/2017	Internal Auditor	12	12	7/12/2017	11/15/2018	
HTE Access Controls Testing	9/26/2017	12/21/2017	Internal Auditor	7	7	10/3/2017	12/21/2017	
FY 2014 CAFR	12/18/2014	12/18/2014	External Auditor	5	5	3/22/2016	12/18/2014	
FY 2015 CAFR	12/17/2015	12/17/2015	External Auditor	5	5	3/22/2016	12/17/2015	
Capital Projects Process Review	5/3/2018	8/20/2020	Internal Auditor	8	8	6/15/2020	8/20/2020	
Public Guardian Follow Up Review	5/3/2018	3/7/2019	Internal Auditor	8	8	5/10/2018	3/7/2019	
FY 2017 CAFR and Single Audit	11/30/2017	12/21/2017	External Auditor	4	4	5/10/2018	8/20/2020	
FY 2018 CAFR and Single Audit	12/6/2018	12/6/2019	External Auditor	3	3	6/15/2020	8/20/2020	
Temporary Staffing Audit	5/9/2019	5/6/2019	Internal Auditor	5	3	5/9/2019	10/3/2019	Only items 3-5
Fire Department Overtime Audit	5/9/2019	10/3/2019	Internal Auditor	2	2	5/9/2019	10/3/2019	
FY2019 CAFR and Single Audit	12/5/2019	12/5/2019	External Auditor	1	1	6/15/2020	8/20/2020	
Cash Handling 2019	12/3/2019	1/6/2020	Internal Auditor	20	15	6/15/2020	8/20/2020	Only items 1-9, 12-15, 19 & 20
Social Media Study	11/25/2019	1/6/2020	Internal Auditor	13	3	6/15/2020	8/20/2020	Only items 1, 2 & 9
HR Administration - Eligible EE Group Ins.	12/3/2019	1/6/2020	Internal Auditor	4	4	6/15/2020	8/20/2020	
AP and P-Card Audit Program	4/1/2020	6/15/2020	Internal Auditor	4	0			
IT Volatility Audit	10/30/2020		Internal Auditor	10				
Total (including archived reports)				262	230			

Legend:
- Report Submittal = date report submitted to City
- BOS Report Approval = date report adopted by BOS
- Reporting Entity = organization that prepared the report
- Report Findings = number of findings in the report
- Completed Findings = number of findings completed by management
- AC Approval = Audit Committee approval of completed findings
- BOS Approval = Board of Supervisors approval of completed findings
- Notes = notes about findings

Finding Corrected?

Y	Findings Addressed - project closed
P	Partially Addressed items
N	Not yet addressed
Y	For Discussion today

Carson City
Temporary Staffing Audit
May 9, 2019

Item No.	BOS Acceptance /Approval	BOS Closure	Recommendation	Dept.	Owner	Remediation Plan (Course of Action & Expected Benefits)	Est. Cost	Est. Savings	Finding corrected? (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Validation (Y,N)	Status Comments
1			We recommend the City conduct further evaluation by legal professional on the legal risks identified from this internal audit. "We noted Department of Labor considerations which may indicate an "employment relationship" between Carson and temporary employees.			Carson City District Attorney's Office is researching the any possible legal issues with hiring temporary employees through Marathon.	$ -	0	P	6/30/2021			DA has performed some research; however, the DA is still looking into the legal distinction between Temporary and Permanent employees. The DOL Fact Sheet on an "Employee Relationship" under the FLSA refers to distinguishing independent contractors and employees, which is not the same distinction here. UDPATE: Research needs to be conducted at the Nevada Supreme Court Library, which is currently closed due to COVID-19
2			Recommend a single timesheet format be used by temporary workers and for management to implement the requirement to accurately record break periods.			Management will speak with departments on how time is reported, there may be two approved methods, one being a spreadsheet if there are multiple employees and one being the Marathon Timesheet - which is their internal form.	$ -	0	*Y*	11/30/2020	11/30/2020		Finance is working with Departments on one City prepared timesheet when several Marathon employees are on the same timesheet. We have obtained the different lists used, and are now trying to find common ground. We are also still planning on allowing the use of the Marathon provided timesheet for smaller departments who only have one person on their staff for a very short period of time. Update: We have narrowed this down to two timesheets. Marathon standard timesheet, and one list that is used Citywide. The list contains employee signature as well as supervisor, and disclaimer.

Carson City
Cash Handling Audit 2019
December 3, 2019

Item No.	BOS Closure	Finding/Recommendation	Remediation Plan (Course of Action & Expected Benefits)	Est. Cost	Est. Savings	Finding corrected? (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Validation (Y,N)	Status Comments
10		COMMUNITY DEVELOPMENT: Controls are not in place to prevent or detect misappropriation of assets.	Analyze the security needs of each cash collection point and strengthen security controls whenever necessary.	$ -	0	N	6/30/2021			Community Development has current fiscal year budget available and is working with IT to get camera's installed.
11		Security controls are weak and are not in compliance with the City's Cash Handling Policy.	We recommend implementing tighter security controls in compliance with the City's Policy.	$ -	0	*Y*	1/31/2020	8/30/2020		Department puchased a locking cabinet and are very strict about keeping the cash drawer locked in the cabinet. As a side note, with Energove, they are finding that most customers are paying on-line, instead of coming to the counter.
16		Controls are not in place to prevent or detect misappropriation of assets	The department should analyze security needs of each cash collection point and strengthen security controls whenever necessary.	$ -	0	*Y*	6/30/2020	11/17/2020		The City's IT department is working on getting cameras for City Hall which will capture out front counter and safe. The cost of the project was included in the FY20 Budget and should be completed by November 30, 2020.
17		Cash handlers are subject to unannounced audits by the Treasurer's Office on an annual basis in those departments/areas where they maintain petty cash and/or change funds. However, this has not occurred since 2017, which is out of compliance with the City's Cash Handling Policy.	In accordance with the City's Cash Handling Policy, the Treasurer's Office should resume the annual surprise cash audits to ensure cash handling procedures are being followed throughout the departments.	$ -	0	N	6/30/2021			Treasurer's will resume the surprise cash audits in the Spring of 2020. The City has several software conversions taking place across City departments so we will resume the surprise cash audits after each Department has started using their new software and any resulting new procedures are in place. **UPDATE:** Well, COVID-19 became a factor this spring, and Treasurer's thought it prudent, not to visit other departments.
18		Daily cash reconciliation and end-of-shift process are not in compliance with both the City's Cash Handling Policy and the City' Cash Handling training video.	We recommend cash handlers follow the City's Cash Handling Policy. Alternatively, we recommend updating the policy to address the department's current process which is effective and sufficient.	$ -	0	*Y*	4/30/2020	11/30/2020		Morning count works better for the Treasurer's. By Spring of 2020 the Treasurer will prepare a document for approval which will outline the exceptions to the Cash Handling Policy for the Treasurer's Office. This will allow incorporation of any new procedures through the implementation of the upcoming software conversions. **UPDATE:** Policy has been updated.

Carson City
Social Media Study
November 25, 2019

Item No.	BOS Closure	Recommendation	Remediation Plan (Course of Action & Expected Benefits)	Finding corrected? (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Validation (Y,N)	Status Comments
3		We reviewed the citywide Social Media policy on PolicyTech which states, "Departments wishing to create and manage department specific social media assets,…should fill out a Social Media Asset Form (available on CCNET) and submit if for approval by the City Manager." However, this policy was not enforcement, which increases the risk to the City, as the social media site may not be administered or monitored in accordance with the citywide policy.	Evaluate enforcement practices related to non-compliance with the City's Social media policy and document the approach.	N	2/28/2021			CIO and Digital Media Coordinator will evaluate enforcement practices. **UPDATE:** The process for enforcement is depicted in the policy, which is being reviewed by the DA's office.
4		Social media site created without a formal request or approval obtained. We compared the current social media policy on PolicyTech to the draft version of the policy being updated and noted one area that should be included in the updated policy. The updated policy needs the method or methods for which the departments would obtain approval from the City Manager prior to creating a social media site.	Formalize the social media request and approval process prior to creating a new site.	N	2/28/2021			CIO, Digital Media Coordinator, and District Attorney's Office will update Social Media Policy and provide to CM for review. **UPDATE:** DA's office is still reviewing the Policy
5		Risks of employee's access to social media sites while on the City's network and personal mobile devices has not been addressed in the Unacceptable Behavior policy.	Update the unacceptable behavior policy	N	2/28/2021			HR Director will update policy as proposed and CM will review and approve. NOTE: Regarding 1st Amendment rights by accepting public employment the U.S. Supreme Court has found that citizens do not surrender their rights. However, an employer can impose certain restraints so long as the restrictions are based upon the government's interest in "promoting efficiency and integrity in the discharge of official duties and maintaining proper discipline in the public service." **UPDATE:** DA's office is still reviewing the Policy
6		Risks of employee's access to social media sites while on the City's network and personal mobile devices has not been addressed in the Computer Resources Usage policy.	Update the Computer Resources Usage Policy to include Employee personal use of social media using City devices and for business purposes using personally owned devices.	N	2/28/2021			HR Director will update policy as proposed and CM will review and approve. **UPDATE:** DA's office is still reviewing the Policy
7		Individual city departments have their own social media policy that does not align with the city's Social Media policy.	Review current social media accounts for compliance with set rules add modifications if necessary.	*Y*	12/31/2020	9/30/2020		CIO and Digital Media Coordinator shall review each departments social media polies and forward recommendations to the department director. **UPDATE:** All departments except Health and Human Services will fall under the proposed social media policy, the Digital Media Coordinator reviewed CCHHS policy and no changes are needed.
8		CCHHS department Marketing and Communications Procedures have several best practices including, content approval hierarchy, a style guide, and templates. However, the policy does not include controls over social media communications such as monitoring, archiving, and site removal.	Departments should update their social media policies to ensure they align with and refer to the Citywide Policy.	N	2/28/2021			CIO and Digital Media Coordinator shall review each departments social media polies and forward recommendations to the department director. **UPDATE:** Health and Human Services is currently being archived and monitored by the Digital Media Coordinator, CCHHS media now falls under the citywide monitoring and archiving guidelines, DA's office is still reviewing the Policy.

10		Social media archiving is likely not in compliance for those departments not actively monitored by the Digital Media Coordinator and the City's software - ArchiveSocial.	All deleted comments should be properly archived with comments.	N	2/28/2021			CIO, Digital Media Coordinator, and District Attorney's Office will update Social Media Policy and provide for CM for review. **UPDATE:** DA's office is still reviewing the Policy
11		The Digital Media Coordinator is responsible for the creation of the majority of the social media content and monitoring. As the number of the City's social media accounts continue to grow so do the comments and followers. As such, the need for more moderation and department interaction also continues to rise.	Recommend the City acquire the risk management and analytics suite of the current ArchiveSocial software to assist in the use of automated monitoring, analysis and alerts to violation of City policy.	N	9/30/2020	8/30/2020		CIO will provide cost estimate for risk management and analytics suite of the current ArchiveSocial Software for FY 21 budge cycle. - NOTE that recent court cases have found government social media accounts to be "designated pubic forums", meaning that individuals have a 1st amendment right to comment on government social media pages. However restrictions are permitted where they are viewpoint neutral and reasonable. To implement these restrictions, there must be an explicit policy indicating the government intent to restrict the forum to certain topics. Where the social media policy allows for departments to delete certain comments, clear guidelines will be needed. Additionally I would recommend disclaiming on the individual social media page what the purpose of the page is to limit the scope of the forum and disclaiming which types of comments will not be permitted. - **UPDATE:** Software for Archiving Social Media was purchased on August 30th.
12		Currently, the communications function is handled primarily by the Digital Media Coordinator, which has one staff member who splits their time doing other IT activities. An effective public information program relies in part upon timely information from City staff about upcoming projects, programs and services. For greater effectiveness and efficiency in informing the public, more employees should be solely dedicated to communications and its practices.	Determine duties regarding who is responsible for content and monitoring of such content.	N	12/30/2020			CM will meet with Department Directors to discuss the possibility of partially shifting content creation down to the department level which could allow for more timely content, responses, and relevant information. Additionally, Dept. Directors' responsibility for the detailed oversight and monitoring of the department's social media accounts will be incorporated into the Social Media Policy within the timeframes Stated above
13		The City does not have an Information Security Response Plan	Create a Information Security Response Plan to include procedures for responding to security incidents, communication protocol and determine system impact.	N	6/30/2021			CIO will create an Information Security response Plan.

Carson City
AP and P-Card Audit
April 1, 2020

Item No.	BOS Closure	Recommendation	Remediation Plan (Course of Action & Expected Benefits)	Finding corrected? (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Verified? (Y, N)	Status Comments
1		The transactional and monthly limits remain the same in the current manual, with additional verbiage which states that departments may implement more stringent limitations based on their requirements (Section 6. Cardholder Responsibilities – page 8) and another which states that Carson City will adjust limits as determined by demonstrated need (Section 15. Completing a P-Card Transaction – page 15). During P-Card transactional testing, it was noted that several transactions exceeded the $5,000 for single transactions and $10,000 per month, which is not reflective of a more stringent limitation.	The City should update the verbiage in the P-Card Program Manual (Section 6. Cardholder Responsibilities – Page 8) to state that the City will adjust limits as determined by demonstrated need which more accurately reflects their current allowable limits on a single transaction and on a monthly basis.	*Y*	12/31/2020	11/30/2020	Y - External Auditor asked to review	The City will update the P-Card Program Manual to reflect current cardholder responsibilities relating to adjusting current allowable limits. The Accounting Manager (Procurement Card Program Coordinator) will be responsible for updating the P-Card Program Manual, by the end of December 2020.
2		Exceeding approval limits is done through an exception-based process which needs to be documented in the City's P-Card policy and flagged/noted as an exception. Another transaction had the department-level approval approved by the cardholder (Executive Director of the Carson Tourism Authority – Component Unit).	The City should document the approval for increasing approval limits for those P-Card transactions that exceed the approval limits set in the system to ensure that transactions are processed within policy guidelines. Additionally, Board approvals or City Manager approval should be attached to cardholders' purchases, where applicable going forward.	*Y*	12/31/2020	11/30/2020	Y - External Auditor asked to review	The City will update the P-Card Program Manual to reflect the process for credit limit increases. Currently the Accounting Manager increases single transaction limits and/or monthly limits as requested by the CFO or Department Directors. Going forward, the Accounting Manager will document within the P-Card module in Munis the reason for the increase and the approving authority. The Accounting Manager will update the policy by the end of calendar year 2020. The Carson City Tourism Authority (CCTA) Executive Director's p-card transactions are currently approved by their Board. In addition to attaching the CCTA Board approval signature to the p-card backup, the City Manager will approve the Executive Director's p-card in Munis as of April 2020.
3		The City's current purchasing policy does not specify whether the City utilizes vendor services owned by city employees.	The City should update their existing policy to specify the City's use of employees as vendors and document how employee-vendor relationship is addressed to avoid potential issues such as conflict of interest, preferential treatment, double dipping, etc.	*Y*	12/31/2020	11/30/2020	Y - External Auditor asked to review	The City will update the Purchasing and Contracts policy to address potential risks when using vendors who are related to City employees. We are a small City and it is difficult to avoid employee-vendor relationships. However, it would require collusion from the Purchasing and Contracts Administrator, CFO, Accounting Managers and District Attorney's office as they are all responsible for reviewing and approving City Contracts and Purchase Orders. The policy will be updated by the end of December 2020.
4		The City's vendor master file has several duplicate vendors with the same name and/or the same address. Most are inactive accounts however there were a number of duplicate vendors left that either need to be inactivated or re-assessed. Additionally, there does not appear to be a process in place for periodic reviews of the vendor master file.	Process should be established to manage vendor master file. This process should include the review and clean-up of duplicate vendors, validation of vendor addresses, ensuring vendor data is complete, archiving inactive vendors and employee accounts, properly documenting miscellaneous vendor accounts that are used by the City for various purposes, and all other assessments that the City deems necessary.	*Y*	6/30/2021	10/31/2020	Y - External Auditor asked to review	The Finance Department performed a yearlong vendor cleanup process, prior to going live with Munis. During the import a lot of vendors were duplicated, and Finance has been working on flagging duplicate vendors as inactive. There will be cases where duplicate vendors cannot be avoided, such as a vendor with different remittance addresses and vendors who share office space. The Accounting Clerk will verify and deactivate duplicate vendors by the end of June 2021. **UPDATE: We had a new gal in the office and her first task was to go through the list and identify and clean-up duplicates. So this has been done, and we will go through the list on an annual basis to ensure this does not happen again. We have included this procedure in our Policies and procedures manual.**

Carson City
External Internal IT Vulnerability Audit
October 30, 2020

Item No.	BOS Closure	Recommendation	Remediation Plan (Course of Action & Expected Benefits)	Finding corrected ? (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Verified? (Y, N)	Status Comments
		NOTE: 12 Findings - External						
1		Update all systems that are currently running on outdated software: Lack of support implies that no new security patches for the product will be released by the vendor. As a result, the unsupported operating systems are likely to contain vulnerabilities. These systems should either be updated to run a supported operating system or shut down in order to protect the security, availability, and integrity of Carson City's perimeter network.	Staff is actively working on updating outdated systems and adjusting operations to be in line with industry best practices, such as automatic updates based on how critical a system is. Some legacy systems that cannot be updated will be isolated using a combination of identity based access rules and network security zones to mitigate the risk of their ongoing operation. Some of these systems may be decomissioned if our customer agency's business needs support this outcome. This will increase security, availability, and integrity of Carson City's infrastructure and data.	P	2/1/2021			
2		System hardening processes should be in place across all systems: Misconfiguration and insecure deployment issues were discovered across various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all systems.	Most issues identified in the external test were expected. Some sites do not use encryption as they don't warrant it with their purpose, others host apps that there are very few options for replacing/updating. Staff has implemented system hardening processes on many systems and will continue to expand on those efforts. Staff is working towards robust change management procedures that could prevent a misconfiguration from ocurring as a standard risk management step. Staff's current approach requires a scope of work and review by at least two employees when performing work on critical infrastructure.	P	6/1/2021			
3		Web development processes: Ensure coding of website and web applications follow OWASP standards. The OWASP Top 10 is a standard awareness document for developers and web application security. Carson City should adopt this document and start the process of ensuring that their web applications minimize these risks.	External findings that would fall under OWASP guidelines are Commercial Off The Shelf (COTS) applications under which the City has little control over development. The City can add OWASP as a procurement requirement for COTS applications, however this may limit the scope and range of options for the City as a whole when considering vendors of specialized software, such as the software from which this item stems. Staff will review this recommendation and consider how to implement it.	N	3/1/2021			
4		Recommend remediation scanning be performed: Based on the number os issues identified we would recommend Carson City IT staff work toward remediating issues working on the most critical items first. Retesting should be performed within 6 months of this report.	Carson City systems are regularly scanned and most by MS-ISAC / CIS as part of a federal program intended to harden local government systems. Most issues identified by the external audit were also identified by the MS-ISAC / CISC scanning effort and were known/expected. Staff will either remediate or document exceptions to all findings.	P	1/1/2021			
		NOTE: 103 - Internal						
1		Update all systems that are currently running on unsupported operating systems: Lack of support implies that no new security patches for the product will be released by the vendor. As a result, the unsupported operating systems are likely to contiain security vulnerabilities. These systems should either be updated to run a supported operating system or shut down in order to protect the security, availability, and integrity of Carson City's infrastructure and data.	Staff is actively working on updating outdated systems and adjusting operations to be in line with industry best practices, such as automatic updates based on how critical a system is. Some legacy systems that cannot be updated will be isolated using a combination of identity based access rules and network security zones to mitigate the risk of their ongoing operation. Some of these systems may be decomissioned if our customer agency's business needs support this outcome. This will increase security, availability, and integrity of Carson City's infrastructure and data.	P	2/1/2021			

2		Implement and enforce implementation of change control across all systems: Misconfiguration and insecure deployment issues were discovered across various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all systems.	Most issues identified in the external test were expected. Some sites do not use encryption as they don't warrant it with their purpose, others host apps that there are very few options for replacing/updating. Staff has implemented system hardening processes on many systems and will continue to expand on those efforts. Staff is working towards robust change management procedures that could prevent a misconfiguration from ocurring as a standard risk management step. Staff's current approach requires a scope of work and review by at least two employees when performing work on critical infrastructure.	P	6/1/2021			
3		Implement a patch management program: Operating a consistent patch management program per the guidelines outlined in NIST SP 800-40 is an important component in maintaining good security posture. This will help to limit the attack surface that results from running unpatched internal services.	Staff has deployed tools such as inventory, deployment, and recently endpoint management software (EMS) to assist with this effort. Inventory and deployment systems allow staff to track and update software. EMS allows staff to scan endpoints for known security issues that require a patch and force the patch to be installed as part of network policy. Staff is continually working towards further automating and integrating these tools into our workflow. At last count our inventory of applications has more than 6251 software packages and components, which makes this an evergreen maintenance item for staff, requiring much in the way of time and resources.	P	4/1/2021			
4		Change default credentials upon installation: To reduce the risk of security breaches through default credentials which have been left configured on network devices, it's best to implement a process to change the passwords, and if possible, account names, when new equipment is installed.	Staff will change the identified systems with default credentials where possible. Some examples identified by the audit do not support credentials for their regular operation. For these devices, staff is working towards isolating in a similar fashion to devices that cannot be reasonably patched as a compensating control.	P	7/1/2021			
5		Conduct regular vulnerability assessments: As part of an effective organizational risk management strategy, vulnerability assessments should be conducted on a regular basis. Doing so will allow the organization to determine if the installed security controls are installed properly, operating as intended, and producing the desired outcome. Consult NIST 800-30 for guidelines on operating an effective risk management program	Staff believes that regular third party auditing of IT systems is valuable and will contribute to an increase the security of Carson City systems and data. Performing audits such as this one regularly would likely require additional resources to obtain the audit and then act upon the results of the audit in a timely fashion.	N	7/1/2021			
6		Recommend remediation scanning be performed: Based on the number of issues identified we would recomment Carson City IT staff work toward remediating issues working on the most critical items first. Retesting should be performed within 6 months of this report.	Some issues identified in this report a small effort to remediate and staff will remediate them in a timely fashion. Others are systemic issues that have already been identifed by staff and require large-scale efforts to address in the long term. Additional resources would contribute towards addressing all of the identified issues in a more timely fashion.	P	1/1/2022			

Note: In this audit staff gave maximum access to the auditors to simulate an attacker gaining access to a sensitive area of the network. Many of the identified issues were discovered because we bypassed our usual security controls to allow the penetration tester greater access. The findings are valuable, but do not necessarily represent vulnerabilities that could be exploited from any part of the City network.

Audit Committee Agenda Item Report

Meeting Date: December 8, 2020
Submitted by: Sheri Russell
Submitting Department: Finance
Item Type: Other / Presentation
Agenda Section:

Subject:
For Presentation Only: Discussion regarding FY 20 audit work program update and Hotline activity. (SRussell@Carson.org)

Staff Summary: Representatives from Eide Bailey, LLP will be discussing the progress of the FY 21 audit work program as well as any items received through the Fraud, Waste & Abuse Hotline.

Suggested Action:
N/A

Attachments:
SR - Internal Auditor work program update.docx

STAFF REPORT

Report To: Audit Committee Meeting Date: December 8, 2020

Staff Contact: Audrey Donovan, Senior Manager, Eide Bailly, LLP

Agenda Title: For Presentation Only: Discussion regarding fiscal year (FY) 2020 audit work program update and hotline activity. (SRussell@Carson.org)

Staff Summary: Representatives from Eide Bailey, LLP will be discussing the progress of the FY 2021 audit work program as well as any items received through the Fraud, Waste & Abuse Hotline.

Agenda Action: Formal Action/Motion Time Requested: 10 minutes

---

Proposed Motion
N/A

Board's Strategic Goal
Efficient Government

Previous Action
N/A

Background/Issues & Analysis
Standing item for discussion and update.

Applicable Statute, Code, Policy, Rule or Regulation
Carson City Charter 3 Section 3.075, Carson City Municipal Code (CCMC) 2.14.040

Financial Information
Is there a fiscal impact? ☐ Yes ☒ No

If yes, account name/number:

Is it currently budgeted? ☐ Yes ☐ No

Explanation of Fiscal Impact: N/A

Alternatives
N/A

Board Action Taken:
Motion: _____ 1) _____ Aye/Nay

2) _____ _____

_____

_____

_____

_____

_____

_____

(Vote Recorded By)