

**CARSON CITY CONSOLIDATED MUNICIPALITY
NOTICE OF MEETING OF THE
AUDIT COMMITTEE**

Day: Tuesday
Date: September 13, 2022
Time: Beginning at 1:30 pm
Location: Community Center, Robert 'Bob' Crowell Board Room
851 East William Street
Carson City, Nevada

AGENDA

NOTICE TO THE PUBLIC:

• **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. Livestream of the meeting is provided solely as a courtesy and convenience to the public. Carson City does not give any assurance or guarantee that the livestream or cable channel access will be reliable. Although all reasonable efforts will be made to provide livestream, unanticipated technical difficulties beyond the control of City staff may delay, interrupt, or render unavailable continuous livestream capability.**

• **The public may provide public comment in advance of a meeting by written submission to the following email address: publiccomment@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. Public comment during a meeting is limited to three minutes for each speaker.**

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 - July 12, 2022

5. For Possible Action: Adoption of Agenda

6. Meeting Items

6.A For Possible Action: Discussion and possible action regarding the retest of the Internal Vulnerability Assessment and External Penetration initially performed on October 30, 2020, and any additional recommendations noted. (Sheri Russell, srussell@carson.org)

Staff Summary: Eide Bailly, LLP completed the Retest of the Internal Vulnerability Assessment and External Penetration. These assessments were conducted from September 14 to October 1, 2020. After completing these assessments and delivering the Final Reports, Carson City had the opportunity to remediate the identified vulnerabilities. Eide Bailly performed the retest of the vulnerabilities from April 25 to April 28, 2022 and aimed to examine the effectiveness of Carson City's remediation activities. Briefing will address all remaining internal audit findings, recommendations, and staff response(s).

6.B For Possible Action: Discussion and possible action regarding the Endpoint Security Assessment and Wireless Assessment Internal Audits and recommendations. (Sheri Russell, srussell@carson.org)

Staff Summary: Carson City's Internal Auditor Eide Bailly, LLP completed the Endpoint Security Assessment and Wireless Assessment Internal Audits. These assessments were conducted in April 2022. After completing these assessments and delivering the Final Reports, Carson City had the opportunity to remediate the one identified vulnerability in the Wireless Assessment. Staff has already begun to address all remaining internal audit findings and recommendations and is available for questions.

6.C For Possible Action: Discussion and possible action regarding the Preliminary Risk Assessment of Body Worn Camera Program and recommendations. (Sheri Russell, srussell@carson.org)

Staff Summary: The Preliminary Risk Assessment of Body Worn Camera Program project was approved to be performed by the Carson City Internal Auditor, Eide Bailly, LLP, for the Fiscal Year 2023 Audit Work Program. The project was completed, and internal auditors are now seeking direction on the continuation of more detailed testing or not. Internal auditors will provide a briefing and will address the high-level findings, recommendations, and staff response(s).

6.D 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 providing 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.

6.E For Possible Action: Discussion and possible action to identify, discuss, and provide recommendations to the Board of Supervisors on projects to be performed by the Internal Auditor for the period ending June 30, 2023. (Sheri Russell, SRussell@Carson.org)

Staff Summary: Carson City Staff, Eide Bailly and the Audit Committee, had a discussion regarding the FY 2023 Internal Audit projects at the March 8, 2022, and July 12, 2022 Audit Committee Meeting. Staff has not taken the FY 23 audit projects as recommended to the Board

of Supervisors yet pending the outcome of the high-level review of the Sheriff's Body Worn Camera Project. After hearing the outcome of that report, internal auditors are seeking direction as to continuation of this project, or to reallocate the budget to a different internal audit project.

6.F For Presentation Only: Discussion regarding Fiscal Year ("FY") 2023 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 2023 audit work program as well as any items received through the Fraud, Waste & Abuse Hotline.

6.G For Discussion Only: Discussion regarding dates for the next meeting of the Audit Committee.

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 Finance Department. You are encouraged to attend this meeting and participate by commenting on any agenda 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 Finance Department in writing at 201 North Carson Street Ste 3, Carson City, NV, 89701, or by calling (775) 887-2133 at least 24 hours in advance.

To request a copy of the supporting materials for this meeting contact Amanda Fencl at afencl@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.

This notice has been posted at the following locations:

www.carson.org

<http://notice.nv.gov>

CARSON CITY AUDIT COMMITTEE (AC)
Draft Minutes of the July 12, 2022 Meeting
Page 1

A regular meeting of the Carson City Audit Committee was scheduled for 1:30 p.m. on Tuesday, July 12, 2022 in the Community Center Robert “Bob” Crowell Board Room, 851 East William Street, Carson City, Nevada.

PRESENT: Chairperson Stephen Ferguson
Member Bonnie Duke
Member Lisa Schuette
Member James Wells

STAFF: Sheri Russell, Chief Financial Officer
Hope Sullivan, Community Development Director
Mihaela Neagos, Deputy District Attorney
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

(1:31:21) – Chairperson Ferguson called the meeting to order at 1:31 p.m. Roll was called, and a quorum was present.

3. PUBLIC COMMENT:

(1:31:39) – Chairperson Ferguson entertained public comments; however, none were forthcoming.

4. FOR POSSIBLE ACTION: APPROVAL OF MINUTES – MARCH 8, 2022

(1:33:28) – Chairperson Ferguson introduced the item and entertained comments, questions, and a motion.

(1:33:51) – MOTION: Member Wells moved to approve the March 8, 2022 meeting minutes as modified. Member Schuette seconded the motion. The motion carried 4-0-0.

5. FOR POSSIBLE ACTION: ADOPTION OF AGENDA

(1:34:39) – Chairperson Ferguson entertained comments or changes to the agenda; however, none were forthcoming.

(1:34:50) – MOTION: Member Schuette moved to adopt the agenda as presented. Member Wells seconded the motion. The motion carried 4-0-0.

6. MEETING ITEMS

6.A FOR POSSIBLE ACTION: DISCUSSION AND POSSIBLE ACTION REGARDING A RECOMMENDATION TO THE BOARD OF SUPERVISORS ON THE APPROVAL OF THE REVIEW

CARSON CITY AUDIT COMMITTEE (AC)
Draft Minutes of the July 12, 2022 Meeting
Page 2

AND SELECTION COMMITTEE’S RECOMMENDATION FOR CONTRACT AWARD TO EIDE BAILLY, LLP FOR CARSON CITY INTERNAL AUDIT SERVICES FOR A NOT TO EXCEED AMOUNT OF \$110,000 ANNUALLY RETROACTIVELY FROM JULY 1, 2022 THROUGH JUNE 30, 2025 WITH TWO (2) ONE-YEAR OPTIONS TO RENEW.

(1:35:06) – Chairperson Ferguson introduced the item. Ms. Russell referenced the Staff Report and the accompanying attachments, all of which are incorporated into the record. Chairperson entertained clarifying questions, none of which were forthcoming, and a motion.

(1:38:02) – MOTION: Member Wells moved to recommend that the Board of Supervisors approve the contract with Eide Bailly, LLP for Internal Audit Services through June 30, 2025 with two one-year options to renew. Member Duke seconded the motion. The motion carried 4-0-0.

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 PROVIDING A RECOMMENDATION TO THE BOARD OF SUPERVISORS TO CLOSE COMPLETED FINDINGS AND/OR RECOMMENDATIONS.

(1:38:25) – Chairperson Ferguson introduced the item. Ms. Russell referenced the Staff Report and the Audit Findings Tracking Report, both of which are incorporated into the record. She also responded to clarifying questions.

(1:41:43) – MOTION: Member Wells moved for the Board of Supervisors to close Social Media Study Item #13 and IT Vulnerability Audit Items #1 through #10. Member Schuette seconded the motion. The motion carried 4-0-0.

6.C FOR POSSIBLE ACTION: DISCUSSION AND POSSIBLE ACTION REGARDING THE RETEST OF THE INTERNAL VULNERABILITY ASSESSMENT AND EXTERNAL PENETRATION INITIALLY PERFORMED ON OCTOBER 30, 2020, AND ANY ADDITIONAL RECOMMENDATIONS NOTED.

(1:42:21) – Chairperson Ferguson introduced the item. Eide Bailly Manager of Cybersecurity Business Development Alex Brown referenced the Retest of the Internal Vulnerability Assessment and External Penetration Summary Report, which is incorporated into the record. He and Ms. Russell also responded to clarifying questions. Based on Member Wells’ input regarding the Report, Ms. Russell proposed that Eide Bailly revise the Report to add generic findings so Staff have items identified for closure, and she could write those items on the Findings Tracking Report for approval during the next AC meeting.

(1:51:52) – Eide Bailly Lead Partner Kim Higgins suggested an executive session for the AC to review the details that were not outlined in the report. Ms. Neagos stated that there are sometimes closed meetings for discussing items within a confidential capacity; however, she would also need to research how to announce a

CARSON CITY AUDIT COMMITTEE (AC)
Draft Minutes of the July 12, 2022 Meeting
Page 3

closed session so that the meeting is open to the public while some information remains confidential. Chairperson Ferguson and Member Wells were in favor of a closed session. No formal action was taken on this item.

6.D FOR POSSIBLE ACTION: DISCUSSION AND POSSIBLE ACTION REGARDING THE COMMUNITY DEVELOPMENT DEPARTMENT INTERNAL AUDIT AND RECOMMENDATIONS.

(1:56:36) – Chairperson Ferguson introduced the item. Eide Bailly Senior Manager Audrey Donovan referenced the Staff Report and the Community Development Department internal audit report, both of which are incorporated into the record. She and Ms. Sullivan also responded to clarifying questions.

(2:04:00) – Ms. Sullivan clarified that the Carson City Building Division began using EnerGov in November 2019, and she provided Ms. Donovan and her team with the issues pertaining to the EnerGov system over a year ago. She stated that she and Ms. Donovan’s team had discovered that the city of Henderson used EnerGov for business licenses and had experienced much of what Building Division was experiencing in terms of “the labor intensiveness” of the system. Additionally, the city of Henderson instructed a third party to prepare a report to analyze the EnerGov system for its business license system, and based on that report, Ms. Sullivan contacted approximately five other communities in Nevada and elsewhere that were using EnerGov for business licenses, all of which were experiencing the same issues that the Building Division was experiencing with EnerGov. Ms. Sullivan indicated that the report for the city of Henderson validated that the Building Division was not dealing with a user error issue, and Building Division Staff’s experience was that they were not able to get the support they needed from the EnerGov company. She was working with the IT Department to identify consultants who are familiar with the EnerGov system, and she stated that “what we found with some of the computer systems is somebody becomes a[n] expert on it, and they leave the company and hang out their own shingles so the people who are at the company who are new are not as experienced with the software.” She indicated that Building Division Staff were also trying to identify vendors, one of which is a vendor that the city of Henderson was using for EnerGov, and she asked for every division or department that was using EnerGov to articulate the challenges with the system and the objective changes needed to make the system work. Ms. Sullivan was also able to identify some funds for the consultant. She also believed that a lot of what “drove decision making on these systems” was the compatibility with the Tyler Munis system, and because that compatibility is important, the Building Division wished to give the EnerGov system a chance to be successful. Member Wells was concerned about hiring a consultant as opposed to finding another alternative due to other jurisdictions having the same problem with EnerGov, and he inquired about whether the problem was fixable.

(5:53:09) – Chairperson Ferguson entertained a motion.

(2:53:15) – MOTION: Member Schuette moved to approve the Community Development Department internal audit report and direct Staff to work on the recommendations as discussed. Member Duke seconded the motion. The motion carried 4-0-0.

6.E FOR POSSIBLE ACTION: DISCUSSION AND POSSIBLE ACTION TO IDENTIFY, DISCUSS, AND PROVIDE RECOMMENDATIONS TO THE BOARD OF SUPERVISORS ON

CARSON CITY AUDIT COMMITTEE (AC)
Draft Minutes of the July 12, 2022 Meeting
Page 4

PROJECTS TO BE PERFORMED BY THE INTERNAL AUDITOR FOR THE PERIOD ENDING JUNE 30, 2023.

(2:54:34) – Chairperson Ferguson introduced the item. Ms. Russell referenced the Staff Report and the Citywide Risk Assessment and Annual Audit Plan for fiscal year (FY) 2023, both of which are incorporated into the record. She and Ms. Donovan also responded to clarifying questions. Based on discussion regarding body worn video recording equipment, Chairperson Ferguson believed it would be worthwhile to complete a risk assessment, and Ms. Donovan suggested including an understanding of how body camera footage is processed and the type of data that is being stored as well as whether there is a policy and a process to dictate what is stored “and for how long and where.” Member Wells added that Nevada Revised Statute (NRS) 289.830 requires all jurisdictions to devise policies and a list of items that must be included in a policy for body worn video recording equipment, and the footage must be kept for at least 15 days. He believed that the risk assessment needed to start by evaluating the policies and if there were wide discrepancies in the policies between the different units of the City that were using the body worn video recording equipment.

(3:19:59) – In response to Ms. Russell’s question, the Members agreed with tabling the rest of the Budget until the risk assessment had been completed.

(3:21:15) – MOTION: Member Wells moved to recommend to the Board of Supervisors approval of the 2022/2023 Audit Program with the revision of the body worn video recording equipment to be an initial 40-hour risk assessment, with any of the remaining hours to be allocated on conclusion of the risk assessment. Member Schuette seconded the motion. The motion carried 4-0-0.

6.F FOR POSSIBLE ACTION: DISCUSSION AND POSSIBLE ACTION REGARDING THE REVIEW OF AGREED UPON PROCEDURES SUGGESTED BY EIDE BAILLY REGARDING UTILITY BILLING, IF SELECTED FOR THE FISCAL YEAR 2023 AUDIT WORK PROGRAM.

(3:21:17) – Chairperson Ferguson introduced the item and entertain Member comments on the Utility Billing, which is incorporated into the record. Member Wells commented that the website for utility billing was “very vague,” and it was difficult to tell how much it costed to pay the utility bill online. He stated that he called in regards to the website and discovered that there was a 2.45 percent fee when using debit card or credit card to pay the utility bill online, and he wished to review the cost of accepting debit card and credit card transactions versus the cost of processing checks and cash, as he believed there were more costs that are associated with processing checks and cash. Ms. Donovan pointed out that the rationale for using credit card and assuming the additional fees helped mitigate the risk of cash being misappropriated or checks not clearing, and credit cards “come with a degree of assurance that, even if it’s fraud, the City will receive the full amount ... charged to that credit card.”

(3:30:47) – Chairperson Ferguson entertained a motion.

(3:30:58) – MOTION: Member Wells moved to direct Eide Bailly and Staff to proceed with the Utility Billing agreed upon procedures as discussed on the record, including the addition of the costs related to the acceptance of cash, checks, and credit cards as well as the review of FISH involvement in the URAP.

CARSON CITY AUDIT COMMITTEE (AC)
Draft Minutes of the July 12, 2022 Meeting
Page 5

Member Schuette seconded the motion. The motion carried 4-0-0.

6.G FOR PRESENTATION ONLY: DISCUSSION REGARDING FISCAL YEAR 2022 AUDIT WORK PROGRAM UPDATE AND HOTLINE ACTIVITY.

(3:31:33) – Chairperson Ferguson introduced the item. Ms. Donovan indicated that there was nothing to report for the Fraud, Waste, and Abuse Hotline, as the three items reported to the Hotline did not have anything to do with the City.

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

(3:33:42) – Chairperson Ferguson introduced the item, and the Members agreed with the meeting date of September 13, 2022 at 1:30 p.m.

7. PUBLIC COMMENT

(3:36:45) – Chairperson Ferguson entertained public comments; however, none were forthcoming.

8. FOR POSSIBLE ACTION: TO ADJOURN

(3:37:02) – Chairperson Ferguson adjourned the meeting at 3:37 p.m.

The Minutes of the July 12, 2022 Carson City Audit Committee meeting are so approved this day 13th of September 2022.

Audit Committee Agenda Item Report

Meeting Date: September 13, 2022

Submitted by: Sheri Russell

Submitting Department: Finance

Item Type: Formal Action / Motion

Agenda Section:

Subject:

For Possible Action: Discussion and possible action regarding the retest of the Internal Vulnerability Assessment and External Penetration initially performed on October 30, 2020, and any additional recommendations noted. (Sheri Russell, srussell@carson.org)

Staff Summary: Eide Bailly, LLP completed the Retest of the Internal Vulnerability Assessment and External Penetration. These assessments were conducted from September 14 to October 1, 2020. After completing these assessments and delivering the Final Reports, Carson City had the opportunity to remediate the identified vulnerabilities. Eide Bailly performed the retest of the vulnerabilities from April 25 to April 28, 2022 and aimed to examine the effectiveness of Carson City's remediation activities. Briefing will address all remaining internal audit findings, recommendations, and staff response(s).

Suggested Action:

I move to approve the report and direct staff to work on the recommendations as discussed.

Attachments:

[SR - IT Volatility Update Internal Audit Report.docx](#)

[Carson City Retest 2022 - Obfuscated Report.docx](#)



STAFF REPORT

Report To: Audit Committee

Meeting Date: September 13, 2022

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

Agenda Title: For Possible Action: Discussion and possible action regarding the retest of the Internal Vulnerability Assessment and External Penetration initially performed on October 30, 2020, and any additional recommendations noted. (Sheri Russell, srussell@carson.org)

Staff Summary: Eide Bailly, LLP completed the Retest of the Internal Vulnerability Assessment and External Penetration. These assessments were conducted from September 14 to October 1, 2020. After completing these assessments and delivering the Final Reports, Carson City had the opportunity to remediate the identified vulnerabilities. Eide Bailly performed the retest of the vulnerabilities from April 25 to April 28, 2022 and aimed to examine the effectiveness of Carson City's remediation activities. Briefing will address all remaining internal audit findings, recommendations, and staff response(s).

Agenda Action: Formal Action/Motion

Time Requested: 20 minutes

Proposed Motion

I move to approve the report and direct staff to work on the recommendations as discussed.

Board's Strategic Goal

Efficient Government

Previous Action

June 22, 2021 – The Audit Committee approved the Fiscal Year 2022 internal audit program.

July 12, 2022 – Item was brought before the Audit Committee with discussion on correction of the audit report presented.

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.

Applicable Statute, Code, Policy, Rule or Regulation

Carson City Charter Article 3 Section 3.075, CCMC 2.14.040

Financial Information

Is there a fiscal impact? Yes No

Is it currently budgeted? Yes No

Alternatives

Do not approve or provide alternative direction to internal auditors or staff.

Board Action Taken:

Motion: _____

1) _____

2) _____

Aye/Nay

(Vote Recorded By)

Consulting Services

Cybersecurity



**INSPIRED TO HELP YOU
BE MORE SECURE**

Carson City

Retest – Summary Report

April 2022

Submitted By:

Nathan Kramer – CEH
Senior Threat Management Consultant

Michael Nougier – CISSP, PMP
Director, Cybersecurity Services



Overview

Carson City contracted Eide Bailly to conduct an Internal Vulnerability Assessment and External Penetration Test. These assessments were conducted from September 14 to October 1, 2020. After completing these assessments and delivering the Final Reports, Carson City had the opportunity to remediate the identified vulnerabilities. Eide Bailly then performed a retest of the vulnerabilities from April 25 to April 28, 2022, and aimed to examine the effectiveness of Carson City's remediation activities.

Eide Bailly highly recommends performing a retest after an initial assessment is complete and the organization has been able to remediate any identified issues. Retesting attempts to reproduce each vulnerability to validate remediation activities were successful. Penetration Test and Vulnerability Assessment Retests can provide many benefits to your organization, including:

- Demonstration of your organization's commitment to security
- Decreased mean time to remediation (MTTR) due to defined windows of retest
- Improved security of your data and network, which reduces the likelihood of a breach
- Independent validation of vulnerability remediation
- Ability to provide peace of mind for your organization and its stakeholders

The table below summarizes the original findings and the results of the retest.

External Penetration Test

Risk Rating	Total	Remediated	Partially Remediated	Not Remediated
High	5	5	0	0
Medium	5	5	0	0
Low	2	2	0	0
Total	12	12	0	0

Internal Vulnerability Assessment

Risk Rating	Total	Remediated	Partially Remediated	Not Remediated	Not Tested
Critical	21	12	8	1	1*
High	16	8	7	1	0
Medium	65	7	58	0	0
Total	103	27	73	2	1

*Finding #2 from the original assessment delivered in October 2020 was not retested due to Carson City restrictions.

The technical details of the retest results, including a full list of the original findings and remediated/not remediated hosts, have been obfuscated from this report for security purposes. A version of this report that includes those details was provided to Carson City's Technology team in April of 2022.

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. These recommendations repeated from the October 2020 report as the associated findings have not been fully remediated.

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.

Risk Rating Information

The findings are summarized within the body of the report and include the assignment of risk and CVSS score. The risk was determined based on our expertise of the defined risk with subjective consideration of the impact to the organization and is not based solely on CVSS.

Critical Risk - A vulnerability identified as "critical risk" should be viewed as an immediate priority for mitigation and remediation. These findings identify conditions in which exploits readily exist and/or are currently being exploited. If exploited will most likely result in the compromise and/or unauthorized access of a networked system, application, or information system. Significant security breaches and/or costly downtime may result if the vulnerability is not mitigated promptly.

High Risk - A vulnerability identified as "high risk" should be viewed as a top priority for mitigation and immediate attention. These findings identify conditions that could directly result in the compromise or unauthorized access of a network, system, application, or information. Significant security breaches or costly downtime may result if the vulnerability is not addressed within an appropriate time frame.

Medium Risk - A vulnerability identified as "medium risk" should be viewed as an essential priority for mitigation which should be addressed as soon as possible. These findings may identify conditions that, while they do not immediately or directly result in a compromise, do provide a capability or information that could result in a compromise or network disruption in combination with other vulnerabilities.

Low Risk - A vulnerability categorized as "low risk" identifies a condition that does not immediately or directly results in a compromise. However, it may provide information that could be used to gain insight into how to compromise or gain unauthorized access to a network, system, application, or information. While they can be prioritized for mitigation at a lower level, they are still of concern and may lead to more severe security threats.

About Eide Bailly

Eide Bailly advocates penetration testing for impact instead of penetration testing for coverage. Penetration testing for coverage has risen in popularity in recent years as a simplified assessment method used in situations where the goal is to meet regulatory needs. As a form of vulnerability scanning, penetration testing for coverage includes selective verification of discovered issues through exploitation, allowing service providers to conduct the work mainly through automated toolsets and maintain product consistency across multiple engagements.

Penetration testing for impact is a form of attack simulation under controlled conditions, closely mimics the real-world, targeted attacks that organizations face daily. In addition, penetration testing for impact is a goal-based assessment, which creates more than a simple vulnerability inventory instead of providing the true business impact. Instead, an impact-based penetration test identifies areas for improvement that will result in the highest rate of return for the business.

Penetration testing for impact poses the challenge of requiring a high skill set to complete. However, as demonstrated in this report, Eide Bailly believes that it is uniquely qualified to deliver world-class results when conducting penetration tests for impact due to the level of expertise found within our team of security professionals.

Eide Bailly offers a product that cannot be matched in the market. However, we may not be the right fit for every job. Eide Bailly typically conducts consulting services with a low volume, high skill ratio to allow Eide Bailly staff to mimic real-world situations closely, enabling customers to have increased access to industry-recognized expertise while keeping costs reasonable. High volume/fast turn-around engagements are often not a good fit for our services. Eide Bailly is focused on conducting high-quality, high-impact assessments and actively seeks out customers in need of services that other vendors cannot deliver.

If you would like to discuss your penetration testing needs, please contact us at khendrickson@eidebailly.com.

Audit Committee Agenda Item Report

Meeting Date: September 13, 2022

Submitted by: Sheri Russell

Submitting Department: Finance

Item Type: Formal Action / Motion

Agenda Section:

Subject:

For Possible Action: Discussion and possible action regarding the Endpoint Security Assessment and Wireless Assessment Internal Audits and recommendations. (Sheri Russell, srussell@carson.org)

Staff Summary: Carson City's Internal Auditor Eide Bailly, LLP completed the Endpoint Security Assessment and Wireless Assessment Internal Audits. These assessments were conducted in April 2022. After completing these assessments and delivering the Final Reports, Carson City had the opportunity to remediate the one identified vulnerability in the Wireless Assessment. Staff has already begun to address all remaining internal audit findings and recommendations and is available for questions.

Suggested Action:

I move to approve the report and direct staff to work on the recommendations as discussed.

Attachments:

[SR - Endpoint and Wireless Internal Audit Reports.docx](#)

[Carson City Endpoint Security Assessment 2022 - Obfuscated Report.docx](#)

[Carson City Wireless Assessment 2022 - Obfuscated Report.docx](#)



STAFF REPORT

Report To: Audit Committee

Meeting Date: September 13, 2022

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

Agenda Title: For Possible Action: Discussion and possible action regarding the Endpoint Security Assessment and Wireless Assessment Internal Audits and recommendations. (Sheri Russell, srussell@carson.org)

Staff Summary: Carson City's Internal Auditor Eide Bailly, LLP completed the Endpoint Security Assessment and Wireless Assessment Internal Audits. These assessments were conducted in April 2022. After completing these assessments and delivering the Final Reports, Carson City had the opportunity to remediate the one identified vulnerability in the Wireless Assessment. Staff has already begun to address all remaining internal audit findings and recommendations and is available for questions.

Agenda Action: Formal Action/Motion

Time Requested: 20 minutes

Proposed Motion

I move to approve the report and direct staff to work on the recommendations as discussed.

Board's Strategic Goal

Efficient Government

Previous Action

N/A

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.

Applicable Statute, Code, Policy, Rule or Regulation

Carson City Charter Article 3 Section 3.075, CCMC 2.14.040

Financial Information

Is there a fiscal impact? Yes No

Is it currently budgeted? Yes No

Alternatives

Do not approve or provide alternative direction to internal auditors or staff.

Board Action Taken:

Motion: _____

1) _____

2) _____

Aye/Nay

(Vote Recorded By)

Consulting Services

Cybersecurity



**INSPIRED TO HELP YOU
BE MORE SECURE**

Carson City

Endpoint Security Assessment – Summary Report

April 2022

Submitted By:

Nathan Kramer – CEH
Senior Threat Management Consultant

Michael Nougier – CISSP, PMP
Director, Cybersecurity Services



Overview

Carson City contracted Eide Bailly to conduct an Endpoint Security Assessment to determine their 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. The goal of the Endpoint Security Assessment is to identify how an attacker could circumvent Carson City's endpoint defenses, workstation security configurations, and group policy settings in order to determine the impact of a cybersecurity incident.

Efforts were placed on identifying and exploiting security weaknesses that could allow an onsite attacker to gain unauthorized access to organizational data or escalate privileges. The assessment was conducted with the level of access that a standard employee would have. The assessment was conducted following industry best practices and standards, with all tests and actions being conducted under controlled conditions.

This report documents the Endpoint Security Assessment performed on a standard employee workstation issued by Carson City, conducted from April 25 to April 28, 2022.

Scope

The scope of this Endpoint Security Assessment was limited to the workstation and user account provided by Carson City.

Summary of Results

Based on the results of the Endpoint Security Assessment, Eide Bailly identified five (5) high, five (5) medium, and one (1) low-risk finding. The technical details of this assessment's results, including a full list of the findings and recommendations, have been obfuscated from this report for security purposes. A version of this report that includes those details was provided to Carson City's Technology team in April of 2022.

Recommendations:

1. Remediate the vulnerabilities identified in the city workstation and user account during the Endpoint Security Assessment to address the following high-risk findings: Undetected virus; security changes by users; disabled networks security controls; unquoted service paths; and unsecure ciphers.
2. Remediate the following medium and low risk findings noted on the Endpoint Security Assessment: enforce BitLocker; implement newer version of TLS; require signing on remote service; upgrade the remote Windows host; apply vendor recommended setting for remote host; implement best practice web browsing solution (noted in report).

Risk Rating Information

The findings are summarized within the body of the report and include the assignment of risk and CVSS score. The risk was determined based on our expertise of the defined risk with subjective consideration of the impact to the organization and is not based solely on CVSS.

Critical Risk - A vulnerability identified as "critical risk" should be viewed as an immediate priority for mitigation and remediation. These findings identify conditions in which exploits readily exist and/or are currently being exploited. If exploited will most likely result in the compromise and/or unauthorized access of a networked system, application, or information system. Significant security breaches and/or costly downtime may result if the vulnerability is not mitigated promptly.

High Risk - A vulnerability identified as "high risk" should be viewed as a top priority for mitigation and immediate attention. These findings identify conditions that could directly result in the compromise or unauthorized access of a network, system, application, or information. Significant security breaches or costly downtime may result if the vulnerability is not addressed within an appropriate time frame.

Medium Risk - A vulnerability identified as "medium risk" should be viewed as an essential priority for mitigation which should be addressed as soon as possible. These findings may identify conditions that, while they do not immediately or directly result in a compromise, do provide a capability or information that could result in a compromise or network disruption in combination with other vulnerabilities.

Low Risk - A vulnerability categorized as "low risk" identifies a condition that does not immediately or directly results in a compromise. However, it may provide information that could be used to gain insight into how to compromise or gain unauthorized access to a network, system, application, or information. While they can be prioritized for mitigation at a lower level, they are still of concern and may lead to more severe security threats.

About Eide Bailly

Eide Bailly advocates penetration testing for impact instead of penetration testing for coverage. Penetration testing for coverage has risen in popularity in recent years as a simplified assessment method used in situations where the goal is to meet regulatory needs. As a form of vulnerability scanning, penetration testing for coverage includes selective verification of discovered issues through exploitation, allowing service providers to conduct the work mainly through automated toolsets and maintain product consistency across multiple engagements.

Penetration testing for impact is a form of attack simulation under controlled conditions, which closely mimics the real-world, targeted attacks that organizations face on a day-to-day basis. Penetration testing for impact is a goal-based assessment, which creates more than a simple vulnerability inventory instead of providing the true business impact of a breach. An impact-based penetration test identifies areas for improvement that will result in the highest rate of return for the business.

Penetration testing for impact poses the challenge of requiring a high skill set to complete. As demonstrated in this report, Eide Bailly believes that it is uniquely qualified to deliver world-class results when conducting penetration tests for impact due to the level of expertise found within our team of security professionals.

Eide Bailly offers a product that cannot be matched in the market. However, we may not be the right fit for every job. Eide Bailly typically conducts consulting services with a low volume, high skill ratio to allow Eide Bailly staff to more closely mimic real-world situations, enabling customers to have increased access to industry-recognized expertise, all while keeping costs reasonable. High volume/fast turn-around engagements are often not a good fit for our services. Eide Bailly is focused on conducting high-quality, high-impact assessments and actively seeks out customers in need of services that other vendors cannot deliver.

If you would like to discuss your penetration testing needs, please contact us at khendrickson@eidebailly.com.

Consulting Services

Cybersecurity



**INSPIRED TO HELP YOU
BE MORE SECURE**

Carson City

Wireless Assessment – Summary Report

April 2022

Submitted By:

Nathan Kramer – CEH
Senior Threat Management Consultant

Michael Nougier – CISSP, PMP
Director, Cybersecurity Services



Overview

Carson City contracted Eide Bailly to conduct a Wireless Assessment. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against the organization. The goal of the Wireless Assessment was to identify what vulnerabilities are present throughout Carson City's wireless networks.

Efforts were placed on identifying and exploiting security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The assessment was conducted with the level of access that a guest user would have. The assessment was conducted following industry best practices and standards, with all tests and actions being conducted under controlled conditions.

This report documents the Wireless Assessment performed on Carson City's wireless networks, conducted from April 25 to April 28, 2022.

Scope

The scope of this assessment was limited to Carson City's wireless networks and infrastructure as well as publicly available information. Eide Bailly tested the wireless networks in both the Carson City City Hall and Carson City Courthouse.

Summary of Results

Based on the testing performed, Eide Bailly determined that Carson City properly segments its wireless networks by using an open guest network that is separate from its secured corporate networks. None of the networks identified within scope had WPS or other vulnerable extensions enabled. Eide Bailly found that all of Carson City's secured networks are using WPA2. This protocol is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. Eide Bailly also noted that Carson City's wireless networks use the MGT-CCMP encryption mechanism, which is the security standard used with WPA2 wireless networks.

Additionally, Carson City's wireless networks require both a username and password in order to successfully authenticate and obtain network access. By requiring a username and password combination, rather than simply requesting only a password, Carson City implements an extra layer of wireless network security.

Overall, Eide Bailly identified one (1) low-risk finding throughout the Wireless Assessment. This issue was brought to the Carson City IT team immediately and the issue was remediated.

The technical details of this assessment's results, including a full technical writeup of the testing performed, have been obfuscated from this report for security purposes. A version of this report that includes those details was provided to Carson City's Technology team in April of 2022.

About Eide Bailly

Eide Bailly advocates penetration testing for impact instead of penetration testing for coverage. Penetration testing for coverage has risen in popularity in recent years as a simplified assessment method used in situations where the goal is to meet regulatory needs. As a form of vulnerability scanning, penetration testing for coverage includes selective verification of discovered issues through exploitation, allowing service providers to conduct the work mainly through automated toolsets and maintain product consistency across multiple engagements.

Penetration testing for impact is a form of attack simulation under controlled conditions, which closely mimics the real-world, targeted attacks that organizations face on a day-to-day basis. Penetration testing for impact is a goal-based assessment, which creates more than a simple vulnerability inventory instead of providing the true business impact of a breach. An impact-based penetration test identifies areas for improvement that will result in the highest rate of return for the business.

Penetration testing for impact poses the challenge of requiring a high skill set to complete. As demonstrated in this report, Eide Bailly believes that it is uniquely qualified to deliver world-class results when conducting penetration tests for impact due to the level of expertise found within our team of security professionals.

Eide Bailly offers a product that cannot be matched in the market. However, we may not be the right fit for every job. Eide Bailly typically conducts consulting services with a low volume, high skill ratio to allow Eide Bailly staff to more closely mimic real-world situations, enabling customers to have increased access to industry-recognized expertise, all while keeping costs reasonable. High volume/fast turn-around engagements are often not a good fit for our services. Eide Bailly is focused on conducting high-quality, high-impact assessments and actively seeks out customers in need of services that other vendors cannot deliver.

If you would like to discuss your penetration testing needs, please contact us at khendrickson@eidebailly.com.

Audit Committee Agenda Item Report

Meeting Date: September 13, 2022

Submitted by: Sheri Russell

Submitting Department: Finance

Item Type: Formal Action / Motion

Agenda Section:

Subject:

For Possible Action: Discussion and possible action regarding the Preliminary Risk Assessment of Body Worn Camera Program and recommendations. (Sheri Russell, srussell@carson.org)

Staff Summary: The Preliminary Risk Assessment of Body Worn Camera Program project was approved to be performed by the Carson City Internal Auditor, Eide Bailly, LLP, for the Fiscal Year 2023 Audit Work Program. The project was completed, and internal auditors are now seeking direction on the continuation of more detailed testing or not. Internal auditors will provide a briefing and will address the high-level findings, recommendations, and staff response(s).

Suggested Action:

I move to approve the report and direct staff to work on the recommendations as discussed. (and to continue with detailed audit procedures.)

Attachments:

[SR - Sheriff's Body Cam Internal Audit Report.docx](#)

[CC Sheriff_Preliminary Risk Assessment of BWC Program.docx](#)



STAFF REPORT

Report To: Audit Committee

Meeting Date: September 13, 2022

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

Agenda Title: For Possible Action: Discussion and possible action regarding the Preliminary Risk Assessment of Body Worn Camera Program and recommendations. (Sheri Russell, srussell@carson.org)

Staff Summary: The Preliminary Risk Assessment of Body Worn Camera Program project was approved to be performed by the Carson City Internal Auditor, Eide Bailly, LLP, for the Fiscal Year 2023 Audit Work Program. The project was completed, and internal auditors are now seeking direction on the continuation of more detailed testing or not. Internal auditors will provide a briefing and will address the high-level findings, recommendations, and staff response(s).

Agenda Action: Formal Action/Motion

Time Requested: 20 minutes

Proposed Motion

I move to approve the report and direct staff to work on the recommendations as discussed. (and to continue with detailed audit procedures.)

Board's Strategic Goal

Efficient Government

Previous Action

N/A

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.

Applicable Statute, Code, Policy, Rule or Regulation

Carson City Charter Article 3 Section 3.075, CCMC 2.14.040

Financial Information

Is there a fiscal impact? Yes No

Is it currently budgeted? Yes No

Alternatives

Do not approve or provide alternative direction to internal auditors or staff.

Board Action Taken:

Motion: _____

1) _____

2) _____

Aye/Nay

(Vote Recorded By)



Preliminary Risk Assessment of Body Worn Camera Program

September 2022

CARSON CITY SHERIFF DEPARTMENT

Submitted By:

Eide Bailly LLP

Audrey Donovan, CIA, CGAP, CRMA
Senior Manager, Risk Advisory Services

TABLE OF CONTENTS

Objective & Scope.....	3
Methodology.....	3
Background and Results.....	3
OBSERVATION #1: Body Worn Camera Activation.....	4
RECOMMENDATION for Observation #1.....	4
OBSERVATION #2: Video Uploads & Categorization.....	6
RECOMMENDATION for Observation #2.....	6
OBSERVATION #3: Monitoring BWC Program.....	7
RECOMMENDATION for Observation #3.....	7
OBSERVATION #4: BWC Policy.....	8
RECOMMENDATION for Observation #4.....	8
Appendix A.....	9
Appendix B.....	10



Objective & Scope

The objective was to perform a preliminary risk assessment (RA) of the Body Worn Camera (BWC) program within the Sheriff's Office to assess risk of the program and provide the Audit Committee with information to make an informed decision on whether the program should have an internal audit performed.

The Scope of the engagement is the Sheriff's Office BWC program including the City Jail as of the assessment period, July through August 2022.

We conducted this engagement in accordance with the International Standards for the Professional Practice of Internal Auditing. Those standards require that we plan and perform the engagement to obtain sufficient and 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 objectives. Our work was limited to those areas specified in the "Objective, Scope, and Methodology" sections of this report.

Methodology

Based on the above objective, we performed the following procedures:

- Obtained and reviewed the Nevada Revised Statute (NRS) 289.830 specific to body worn camera.
- Obtained and reviewed the Sheriff's Office policies and procedures (P&Ps).
- Compared P&Ps to NRS 289.830.
- Discussed the BWC program, related processes, and system vendor with the City's Undersheriff, Jerome Tushbant.
- Performed best practice research on BWC programs.

Background and Results

The Sheriff's Office implemented the requirements of NRS. 289.830 with the passing of Senate Bill 176 that stated law enforcement agencies must require their uniformed peace officers who routinely interact with the public to wear portable event recording devices by July 1, 2018.¹ The law requires the adoption of P&Ps that include specific requirements for the use of body camera device and video retention of no less than 15 days (see Appendix A for NRS 289.830).

A body-worn camera (BWC) is a small, battery-powered camera worn by uniformed officers to record interactions with the public. The cameras are used to promote transparency and accountability through objective evidence. The policy includes procedures for: when to activate and deactivate the camera, when and where recording is prohibited, data retention, oversight, and the disclosure or release of videos.

Through our discussions with the Undersheriff, every deputy, sergeant, and investigator are equipped with a body worn camera. Deputies are required to go on duty with all equipment in good working order to include a charged and working BWC. A failure to report a non-working device, without good cause, could result in disciplinary action. Supervisors are required to conduct periodic inspections of equipment to include a visual check that the deputy has the BWC device in their possession.

Marked and unmarked emergency vehicles, with the exception of motorcycles, are installed with Axon cameras equipped with high-tech features such as the Axon "signal" technology. This technology will activate another

¹ Carson City body cameras were rolled out in mid-June, 2018, 2 weeks ahead of schedule.

Axon camera if it is within approximately 11 yards of an equipped vehicle with their emergency lights turned on. This allows Carson City and others' with the technology, such as Nevada Highway Patrol to benefit from the others' camera footage.

The audio and video data from the cameras is stored in the cloud through a third-party vendor Axon, that provides storage and data management for both body and vehicle cameras for all City uniformed officers including the 4 jailors within the City Jail.² Depending on how the video is classified (misdemeanor, use of force, arrest, liability, pedestrian, etc.) determines the amount of time the data is stored. Theoretically, the data could be stored in the cloud indefinitely.

All personnel that have a body-worn camera assigned and/or personnel with responsibilities directly related to the BWC Program need to have active access to Axon's cloud storage system, Evidence.com. It is this active access that labels the uploaded video with the owner name. To preserve audit trails for departing employees, users are deactivated rather than being deleted altogether.

Evidence.com is a web-based portal which provides users roles, responsibilities, video reviews, and other settings for BWC as well as in-car cameras. A review of the user list is typically performed when an employee is hired, terminated, or moves assignment. This review was performed during our assessment as a result of the Sheriff's Office adding in-car cameras to Evidence.com. Overall, review tends to occur a few times a month.

Our preliminary risk assessment identified opportunities for the Sheriff's Office to improve the City's BWC Program. Like any evolving program, there are opportunities for the Sheriff's Office to improve the administration of the BWC program. We would like to thank the Sheriff and Under Sheriff for their cooperation and responsiveness to our requests and questions during our assessment.

OBSERVATION #1: Body Worn Camera Activation

The BWC Policy³ lists multiple instances when an officer is required to activate his or her BWC when responding to a call for service. One specific instance relates to dispatched 911 calls and self-initiated activities in which a deputy would normally notify dispatch, such as when an officer pulls someone over. In these instances, the 911 dispatch CAD (computer-aided dispatch) number should be included with the associated video footage that is uploaded.

Currently, the Sheriff's Office does not perform video matching or monitoring of dispatch calls to ensure events that should have a BWC video, do in fact have a video. This level of review would provide information about the effectiveness of the BWCs activation rate.

RECOMMENDATION for Observation #1

The Sheriff's Office should establish a process that ensures all officers responding to 911 dispatch calls and all self-initiated activities requiring dispatch notification have a BWC video. Additionally, performance metrics and goals should be established for BWC activation.⁴

Management Response:

² Camera footage within the jail, except BWC, is maintained by the City's IT Department. The data storage is a current on-going project and at the time of our assessment this project was at 90% complete. Currently, the City has been storing this and other data forever due to lack of data retention policy, which the District Attorney's office is currently working on finalizing.

³ The Portable Audit/Video Recorders Policy.

⁴ Best Practice performance metric compares the number of videos taken to the Computer-Aided Dispatched calls the officer has responded to. Best Practice BWC goal is >80% activation rate.

With the recent installation of the Axon “Signal” product, body cameras automatically activate when emergency lights are turned on by nearly any Carson City Sheriff’s enforcement vehicles. This will dramatically reduce the number of non-activations.

Additionally, as of September 1, 2022, the Carson City Sheriff’s Office will be testing the Axon “Performance” product which further addresses this concern. The product collects data on BWC users and compares dispatch records with video records to determine the rate of compliance. Performance is a proprietary system within the Axon environment, as such no other vendor can provide the same service.

The Sheriff’s Administration has high hopes that the Performance product will efficiently provide insight into the use of BWC’s and allow for immediate feedback. Since this product would have a budgetary impact, the office and Axon would need to negotiate terms. Axon representatives have indicated if there is a good faith intent to acquire this product a long-term trial period would be supported, pending a budgetary decision.

At this time, setting metrics and goals are problematic as the complete system; BWC, in-car cameras, along with the Signal system, has only recently been combined and is now online. It will take time to create a baseline and configure Performance to work with data from our existing systems. It is our intention to create an internal working group to divide labor and determine achievable goals.

Please note, Performance will be labor intensive to include setup and maintenance. Maintenance would include making multiple changes with the “command hierarchy” for all personnel moves as well as creating reports, monitoring the data, and investigating deficiencies/anomalies. This is beyond the requirement of line level supervisors who is tasked with randomly reviewing officers BWC video (required in the Early Alert System). With the unfunded legislative requirements, administration of the BWC program may need to fall to a dedicated specialized employee.

We believe, if Performance is funded, we will be able to provide meaningful information and address Recommendation #1 by July 1, 2023.

OBSERVATION #2: Video Uploads & Categorization

Currently, the BWC policy does not specify when a BWC device should be uploaded or categorized. Regular and timely video uploads enhance accountability and transparency as well as ensuring the availability of videos of evidentiary significance. Best practice identification and preservation of video requires BWCs to be docked at the conclusion of each shift to allow automatic uploads of any data collected to Axon's cloud storage system, Evidence.com. Prompt docking ensures BWC files are backed up and secured within Evidence.com.

To assist with identifying and preserving data recordings, video is to be properly categorized by the officers. The retention time of each video is based on these categories. Per policy, officers should categorize their BWC recordings. This can be completed after docking the BWC device or during the officer's shift via the Axon View app. The officer is responsible for ensuring the information is accurate and complete.

RECOMMENDATION for Observation #2

The Sheriff's Office should update their BWC policy to address when the video upload and categorization is to occur. Additionally, the Sheriff's Office should perform routine monitoring of the uploads and the categorization of videos for completeness and accuracy. Lastly, performance metrics and goals should be established for BWC uploads and categorization of videos. This may be accomplished through the use of Axon Performance dashboard.

Axon Performance dashboard provides key performance metrics on;

- 1) activation rate - Compares the number of videos taken to the CAD calls the officer has responded to (see Observation #1).
- 2) power cycle - Calculates the total time the BWC is powered on while disconnected from a docking station and is used to identify officers that fall below the agency set percentage.
- 3) categorization rate - Compares the number of videos the officer has categorized to the total number of videos taken.
- 4) identification rate - Compares the number of videos with an officer added or confirmed ID to the total number of officer videos.

Management Response:

The Carson City Sheriff's Office will incorporate into policy instructions when to upload and categorize video from a BWC. This task will be complete in the next 30 days.

Monitoring of the uploads and categorization of videos can be done through the Axon "Performance" product. See Response #1 for details.

In terms of the four-performance metrics, see Response #1 for details.

OBSERVATION #3: Monitoring BWC Program

The Sheriff's Office is finalizing the BWCs Early Warning Policy to comply with NRS 289.823 that requires law enforcement agency to establish a system to identify peace officers who display bias indicators or other problematic behavior (see Appendix B). Management oversight is a key component for a strong internal control structure. However, management oversight of BWC policy is not performed to track for trends or patterns, which would also provide additional opportunities to improve training and identify departmental weaknesses. Monitoring for compliance with the BWC program helps managers to achieve desired results through effective oversight.

Monitoring for compliance with the BWC program is currently not performed due to the limitations of the Axon services, which would require another trial period, set for December 2022, to assess cost and functionality for true random video sampling for review. This will allow supervisors and shift supervisors the ability to review based on set criteria, such as traffic stops, randomly identify the video to review, notate the video reviewed and outcomes, and maintain an audit trail of who reviewed and when.

RECOMMENDATION for Observation #3

The Sheriff's Office should continue to roll out the BWC program's Early Warning Policy to comply with NRS 289.823. Furthermore, the policy should implement a system and methodology to monitor the BWC video for compliance with the BWC program and policy, and identification of opportunities for improvement to include all uniformed personnel with BWC devices, including the Jailors. This should include an evaluation of the total reviews that need to be completed in order to be statistically significant in comparison to the total of BWC footage of each uniformed personnel with a BWC device or other means of how supervisors chose videos for review, such as utilizing the feature within the Axon software that aids in the random selection of the videos for review. Lastly, the supervisor's monitoring of the videos should also be reviewed for compliance with set methodology and intent of the program and related policies.

Management Response:

The Sheriff's Office has established policy to address the Early Warning Policy, as per NRS 289.823. The implementation of Performance will take up the recommendations above.

In terms of jailors, they are not required to have BWC; however, they have been issued provide additional audio/visual documentation and record of events. The internal workgroup mentioned above will address and publish policy for camera use within the jail.

These recommendations can be addressed specific to the patrol/investigations divisions through data supplied by the Performance product. See Response #1.

OBSERVATION #4: BWC Policy

As part of our assessment we reviewed the procedures outlined in the BWC policy and compared them to the requirements in the NRS 289.830 and noted for section 1.f., that disciplinary rules for peace officers have not been established in policy. The state statute, section 1.f., requires that disciplinary rules for peace officers be established for failure to operate a BWC device in accordance with policy, intentional manipulation of a video recorded to a BWC device, or prematurely erasing a video recorded by a BWC device. Having a policy for disciplining these actions creates an understanding and expectation for officers if this were to happen.

RECOMMENDATION for Observation #4

Review and update the current BWC policy to reflect current operating practices and alignment with NRS 289.830. Specifically, the policy should be updated to include disciplinary actions.

Management Response:

BWC policy is currently in review as a natural course of implementing the in-car camera as well as the early warning polices.

Although not specifically mentioned in the BWC policy, it is a violation of Standards of Conduct for an employee's, "Failure to operate a portable recording device as required by the Office and/or editing or erasing any portion of a recording". See policy 339.5.8.(J). Discipline for the violation can range from a warning up to and including termination.

Appendix A

NRS 289.830

Certain law enforcement agencies shall require certain peace officers to wear portable event recording device while on duty; adoption of policies and procedures governing use; request for and inspection of record made by device.

1. A law enforcement agency shall require uniformed peace officers that it employs and who routinely interact with the public to wear a portable event recording device while on duty. Each law enforcement agency shall adopt policies and procedures governing the use of portable event recording devices, which must include, without limitation:
 - (a) Except as otherwise provided in paragraph (d), requiring activation of a portable event recording device whenever a peace officer is responding to a call for service or at the initiation of any other law enforcement or investigative encounter between a uniformed peace officer and a member of the public;
 - (b) Except as otherwise provided in paragraph (d), prohibiting deactivation of a portable event recording device until the conclusion of a law enforcement or investigative encounter;
 - (c) Prohibiting the recording of general activity;
 - (d) Protecting the privacy of persons:
 - (1) In a private residence;
 - (2) Seeking to report a crime or provide information regarding a crime or ongoing investigation anonymously; or
 - (3) Claiming to be a victim of a crime;
 - (e) Requiring that any video recorded by a portable event recording device must be retained by the law enforcement agency for not less than 15 days; and
 - (f) Establishing disciplinary rules for peace officers who:
 - (1) Fail to operate a portable event recording device in accordance with any departmental policies;
 - (2) Intentionally manipulate a video recorded by a portable event recording device; or
 - (3) Prematurely erase a video recorded by a portable event recording device.
2. Any record made by a portable event recording device pursuant to this section is a public record which may be:
 - (a) Requested only on a per incident basis; and
 - (b) Available for inspection only at the location where the record is held if the record contains confidential information that may not otherwise be redacted.
3. As used in this section:
 - (a) "Law enforcement agency" means:
 - (1) The sheriff's office of a county;
 - (2) A metropolitan police department;
 - (3) A police department of an incorporated city;
 - (4) A department, division or municipal court of a city or town that employs marshals;
 - (5) The Nevada Highway Patrol; or
 - (6) A board of trustees of any county school district that employs or appoints school police officers.
 - (b) "Portable event recording device" means a device issued to a peace officer by a law enforcement agency to be worn on his or her body and which records both audio and visual events occurring during an encounter with a member of the public while performing his or her duties as a peace officer.

Appendix B

NRS 289.823 (“Early Warning Policy”)

Requirement for law enforcement agency to establish early warning system to identify peace officers who display bias indicators or other problematic behavior; duties of law enforcement agency upon such identification.

1. Each law enforcement agency shall establish an early warning system for the purpose of identifying peace officers employed by the law enforcement agency who:
 - (a) Display bias indicators by, for example:
 - (1) Having a large number of citizen complaints;
 - (2) Being part of a large number of incidents involving the use of force;
 - (3) Making a large number of arrests for resisting an officer;
 - (4) Having a large number of the arrests that he or she has made result in no charges being filed because of issues such as improper searches or detentions; or
 - (5) Having a negative attitude regarding programs that enhance relations between law enforcement and the community.
 - (b) Display other problematic behavior by, for example:
 - (1) Having a large number of motor vehicle crashes;
 - (2) Abusing sick leave; or
 - (3) Showing any other behavioral signs that are indicative of a decline in performance.
2. If a peace officer is identified by the early warning system as displaying bias indicators or other problematic behavior, the law enforcement agency that employs the peace officer shall:
 - (a) Increase its supervision of the peace officer; and
 - (b) Provide additional training and, if appropriate, counseling to the peace officer.
3. If a peace officer is repeatedly identified by the early warning system as displaying bias indicators or other problematic behavior, the law enforcement agency that employs the peace officer shall consider the consequences that should be imposed, including, without limitation, whether the peace officer should be transferred from any high-profile assignments or subject to any discipline.



Caring for our external and internal clients with a passion to go the extra mile.

Respecting our peers and their individual contributions.

Conducting ourselves with the highest level of integrity at all times.

Trusting and supporting one another.

Being accountable for the overall success of the Firm,
not just individual or office success.

Stretching ourselves to be innovative and creative, while managing the related risks.

Recognizing the importance of maintaining a balance between work and home life.

Promoting positive working relationships.

And, most of all, enjoying our jobs ... and having fun!



What inspires you, inspires us.

eidebailly.com

Audit Committee Agenda Item Report

Meeting Date: September 13, 2022

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 providing 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.

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 9-7-2022.pdf](#)



STAFF REPORT

Report To: Audit Committee

Meeting Date: September 13, 2022

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 providing 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: 15 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

N/A

Background/Issues & Analysis

Staff is recommending the following items to the Audit Committee for closure:

- IT Vulnerability Audit – All items recommended for closure – an updated report will be presented.
- Community Development – Finding 8 related to Charles Abbott workflow processes.
- Wireless Assessment – 1 finding immediately remediated.

Validation of all IT Volatility procedures has been completed by Eide Bailly and a new report will be presented at the September 13, 2022 Audit Committee meeting. Staff is recommending closure of the old IT Vulnerability report and will work on completing the findings in the new report.

Staff will take the items that the Audit Committee recommends for closure to the Board of Supervisors for final closure.

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) _____

2) _____

Aye/Nay

(Vote Recorded By)

Carson City
Internal Audit Summary
Updated - 6/22/21

Carson City - Audit Findings Tracking Summary Report (revised 3-8-22)

Report Name	Report Submittal	AC/BOS Report Approval	Reporting Entity	Report Findings	Completed Findings	AC Approval	BOS Approval	Notes
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	
Grants Audit	6/30/2018	9/30/2018	Internal Auditor	1	1	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	5	6/22/2021	10/3/2019	
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	20	6/22/2021	8/20/2020	
Social Media Study	11/25/2019	1/6/2020	Internal Auditor	13	13	6/22/2021		#13 recommended for closure
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	3/4/2021	Internal Auditor	4	4	8/4/2020	3/4/2021	
IT Volatility Audit	10/30/2020	12/8/2020	Internal Auditor	10	10	3/8/2022		All items recommended for closure
Fleet Audit	3/30/2021	3/30/2021	Internal Auditor	6	6	3/8/2022	7/7/2022	
Revenue and Receivables Audit	5/25/2021	6/22/2021	Internal Auditor	3	3	12/7/2021	7/1/2020	
Payroll Internal Controls Testing	11/22/2021	12/7/2021	Internal Auditor	3	3	3/8/2022	7/7/2022	
Community Development Department	6/29/2022		Internal Auditor	8	1	7/12/2022		One item recommended for closure
IT Volatility Retest Report	7/12/2022		Internal Auditor	6	4			Three items recommended for closure
Wireless Assessment	4/30/2022		Internal Auditor	1	1			One item immediately remediated
Endpoint Security Assessment	4/30/2022		Internal Auditor	2	2			Two items remediated
Prelim Risk Assess. Body Worn Camera Prog.	9/1/2022		Internal Auditor	4	0			
Total (including archived reports)				166	153			

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 - Audit Committee closed
P	Partially Addressed items
N	Not yet addressed
Y	For Discussion today

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
13		The City does not have an Information Security Response Plan	Create an Information Security Response Plan to include procedures for responding to security incidents, communication protocol and determine system impact.	Y	6/30/2022	6/30/2022	N	CIO will create an Information Security response Plan. UPDATE: Plan is complete.

Carson City
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 decommissioned if our customer agency's business needs support this outcome. This will increase security, availability, and integrity of Carson City's infrastructure and data.	Y	3/31/2022	6/13/2022	Y	Staff is making progress on resolving issues. IT has been updating systems on a continuous basis. Some systems will require funding to stay current, extended support has been purchased for endpoint security to protect legacy systems. Maintenance will be performed with approval from the affected department(s). UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT TO BE PRESENTED TO AUDIT COMMITTEE 7-12-2022.
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 occurring 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.	Y	3/31/2022	6/13/2022	Y	Staff has continued to make progress on system hardening, changing default accounts and passwords and change management including the use of automated deployment tools and templates. Work is being conducted to update patch deployment systems. UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT TO BE PRESENTED TO AUDIT COMMITTEE 7-12-2022.
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.	Y	3/31/2022	6/13/2022	Y	Staff does not have the recommendation yet, but has begun to approach new vendors with this requirement. Update: Staff will work with external vendors to ensure that these standards are being followed for the Carson City websites they host. UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT TO BE PRESENTED TO AUDIT COMMITTEE 7-12-2022.
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.	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.	Y	3/31/2022	6/13/2022	Y	In the December 2020 Audit Committee meeting, it was decided to re-test in August 2021. This was pushed to the last quarter of FY22, as we have a new CIO. UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT TO BE PRESENTED TO AUDIT COMMITTEE 7-12-2022.
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 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.	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 decommissioned if our customer agency's business needs support this outcome. This will increase security, availability, and integrity of Carson City's infrastructure and data.	Y	3/31/2022	6/13/2022	Y	Staff is making progress on resolving issues; Current Status 11.24.2021: IT has been updating systems on a continuous basis. Some systems will require funding to stay current, extended support has been purchased for endpoint security to protect legacy systems. Maintenance downtime will be performed with the approval from the affected department(s). UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT TO BE PRESENTED TO AUDIT COMMITTEE 7-12-2022.

Carson City
IT Vulnerability Audit
October 30, 2020

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 occurring 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.	Y	3/31/2022	6/13/2022	Y	Staff is continuing to make progress on system hardening and change management including the use of automated deployment tools and templates. Update: A new application is being setup to track all changes and approvals within the environment. UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT TO BE PRESENTED TO AUDIT COMMITTEE 7-12-2022.
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.	Y	3/31/2022	6/13/2022	Y	A new application is being setup to track all managed systems within the environment. These managed systems will have regular patching cycles based on the manufacturer's recommendations. Staff expects to be able to demonstrate significant progress at the time of the audit follow-up. UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT TO BE PRESENTED TO AUDIT COMMITTEE 7-12-2022.
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.	Y	3/31/2022	6/13/2022	Y	An existing application is being utilized to ensure default credentials are changed on all managed systems. Staff expects to be able to demonstrate significant progress at the time of the audit follow-up. UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT TO BE PRESENTED TO AUDIT COMMITTEE 7-12-2022.
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 increased 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.	Y	3/31/2022	6/13/2022	Y	A new application is being utilized to conduct vulnerability assessments on an established cadence. Staff expects to be able to demonstrate significant progress at the time of the audit follow-up. UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT TO BE PRESENTED TO AUDIT COMMITTEE 7-12-2022.
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.	Some issues identified in this report require a small effort to remediate and staff will remediate them in a timely fashion. Others are systemic issues that have already been identified 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.	Y	3/31/2022	6/13/2022	Y	Staff expects to be able to demonstrate progress at the time of the re-test. Update: Using the results from the new vulnerability scanning application, critical and high vulnerabilities will be able to be addressed. Legacy systems are still planned for a migration to more modern operating systems with the permission of each department. UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT TO BE PRESENTED TO AUDIT COMMITTEE 7-12-2022.

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.

Carson City
Community Development Internal Audit
June 2022

Item No.	BOS Closure	Finding	Recommendation	City - Remediation Plan (Course of Action & Expected Benefits)	Finding corrected? (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Validation (Y,N)	Status Comments
1		Entergov has tripled the amount of data entry involved in processing a business license when compared to the legacy system. A poorly executed customer interface on the portal coupled with the inability to require payment prior to permit issuance caused the shutting down of the customer portal. Business licenses issued can be issued without payment and credits to potentially fictitious customers can go undetected, creating an opportunity for fraud and potential lost revenue for the City.	The City should continue to work with Energov to determine if the necessary updates can be made to improve efficiency, incorporate preventative controls, and features that will help effectively service customers. Alternatively, if there is no resolution with Energov, then the City should look into alternative software solutions.	Community Development has met with IT and are currently working with Energov to determine if resolution of the issues is feasible. If not, the staff will investigate alternative systems. Staff has underfilled a position to hire a consultant in anticipation of not being able to resolve issues. Community Development has set a date of January 1, 2023 and the Director will be the lead in working with the consultant.	N	1/1/2023			
2		Business license fees list on the website is not complete per CCMC 4.04.020, it is missing Fictitious Filing Fees \$20 and Technology Fees of \$5.	The Director should work to provide an updated list of business fees to the customers for transparency on the website.	The fees can be added to the portion of the website that addresses business license fees as well as included on other materials associated with business license fees. Planning Manager will be responsible.	N	1/1/2023			
3		Lot of great information in the full report. This finding has to do with whether or not we should continue to outsource with Charles Abbott (CAA). There isn't enough data regarding time CAA spends on their services to fully understand all the costs of each Building Permit.	Recommendation is that the City should use the benchmarking data as well as obtain further data on the number of hours each permit takes to process from intake, plan review, permit issuance, inspections, re-inspections, etc., in order to determine if we should continue outsourcing, move to a hybrid approach, or insource all together.	The current contract will expire in August 2024. By July 2023 the Director should provide an analysis to the City Manager/ Board of Supervisors relative to the recommendation to insource, continue outsourcing, or utilizing a hybrid approach. This will provide the City with a year to determine the preferred structure.	N	7/1/2023			
4		It was noted that there was a lack of monitoring of performance metrics as required by the City's contract with CAA. For example: permit transaction reports are attached to monthly invoices, however, the City does not monitor for timeliness of permit related activities or accuracy of the Permit fee calculations. There is also no formal customer feedback process or means of sharing unsolicited feedback with the Director.	Director should enforce the contract requirement for CAA to provide monitoring information to the City. The City and CAA should establish a customer feedback loop. Additional the City should consider an independent audit of the consultants performance. Lastly, a quarterly or annual trend analysis of reported issues should be created and shared with the Director.	CAA typically does not have sole responsibility for a building permits review. The delay could come from a City department. Director will work with City Managers off on customer survey's both internal and external to the City. Reporting and Surveys will be Directors responsibility.	N	1/1/2023			
5		Reinspection fee was not charged for FY 2021 and 2022 Resulting in losses to the City of \$33,000 and \$17,000 respectively. There were many instances where the Final Inspection was performed, but the permit was canceled, and auditor was unable to determine the cause for such a late cancellation.	Director should require that re-inspection fees are charged to ensure the City receives payment for work performed. Director should also determine why there were 199 permits in 2021 and 84 permits in 2022 that a final inspection was noted, but no permit was issued.	Director will work with CAA to ensure they start charging the reinspection fee. Director also agrees to look into the canceled permits where inspections occurred by September 30, 2022 and report out to the City Manager, and Audit Committee.	N	9/30/2022			
6		Building Division has not evaluated the cost of its services in 15 years to determine if the fee fully covers the costs. There is currently no reliable data on how much in employee and CAA time it takes to issue a Permit. National Association of Home Builders has stated that construction permit fees are typically 1.7% of total project cost, but City per Permit cost only came to .48% of total project costs.	As an enterprise fund building permit fees should be designed to cover all direct costs. City should use the information contained in the report to help with a cost of service study. A review of expenses should also be done to determine that appropriate and legitimate expenses are properly reported.	Community Development staff does not have the skill set to pursue this recommendation, and we would need to outsource a consultant to pursue this task. Director is watching the fund closely to make sure that non-building related activities are not paid out of this fund.	N	1/1/2023			

Carson City
Community Development Internal Audit
June 2022

Item No.	BOS Closure	Finding	Recommendation	City - Remediation Plan (Course of Action & Expected Benefits)	Finding corrected? (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Validation (Y,N)	Status Comments
7		CAA contract states that the Building Official with CAA is to provide building code enforcement. Based on interviews and discussions with Director and Building Official, CAA is not providing building code enforcement.	Director and possibly DA should enforce the contract language related to code enforcement and work to come to a resolution with CAA.	Director, DA's office and Building Official are schedule to meet in August 2022 to further discuss.	N	11/1/2022			
8		Final Plan Review doesn't include all Department Final Sign-off, which causes plan delays when inspectors note that final reviews were not signed off.	Process workflow should be implemented to address version controls, for resubmittals of the plans to all plan reviewers to ensure a newer version of the plan is rerouted to all relevant parties for final review.	Director will request that CAA implement a workflow process that addresses the version controls and final reviews sign-off.	Y	9/1/2022	8/6/2022		Community Development has reviewed the workflow in energov to verify no one is dropped off the review and the permits techs are implementing

Carson City
IT Vulnerability Update Internal Audit
April 2022

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: 103 - Original Report - RETEST - 27 Remediated, 73 partially remediated, only 2 not remediated.								
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 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.	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 decommissioned 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	6/30/2025			Decision need to be made by the System / Software owner for a replacement. Funding will be needed to replace systems and the infrastructure to support any new system. Some system do not have upgrade path leading to a full replacement. Some systems have be scheduled for replacement in 2025. Example: Tiburon
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 occurring 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.	Y	12/31/2022	1/31/2022		Change Control Policy and Processes implemented January of 2022. Current records state process begin in January 2022 within Manage Engine.
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	6/30/2025			Current process is Patch, Reboot, and Scan on the with end units the last Thursday of each month and servers last Wednesday of each month. There are exclusions for high risk and Public Safety units and servers. Reference cell L3 for High Risk Legacy systems.
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.	Y	6/30/2022	7/26/2022		SOP Created - System Hardening Process has been established which contains Peer Review. Policy is in Policy Tech.
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 increased 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	11/1/2021	11/1/2021		SOP Created - System Hardening Process has been established which contains Peer Review. Policy is in Policy Tech.

Carson City
IT Vulnerability Update Internal Audit
April 2022

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
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.	Some issues identified in this report require a small effort to remediate and staff will remediate them in a timely fashion. Others are systemic issues that have already been identified 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.	Y	4/30/2022	4/30/2022		Comment - This is the retest - 1 year after initial report. Direction on closure, or change retest, to 1 year?

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.

Carson City
 End Point User Internal Audit
 April 2022

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: 11 Findings - 5 High Risk, 5 medium risk, 1 low risk.								
1		Remediate the vulnerabilities identified in the City workstation and user account during the Endpoint Security Assessment to address the following high risk findings: undetected virus; security changes by users; disabled networks security controls; unquoted service paths; and unsecure ciphers.	Staff is actively working on noted recommendations, starting with High Risk areas.	Y	6/30/2022	8/1/2022		Hardening processes are in place. Current AV has been notified on virus gaps and have updated their virus signatures / definitions. Google has been locked down to meet the Security Changes within the Audit. Unsecure Ciphers removed.
2		Remediate the following medium and low risk findings noted on the Endpoint Security Assessment: enforce BitLocker; implement new versions of TLS; require signing on remote services; upgrade the remote host; apply vendor recommended settings for remote host; implement best practice web browsing solution (noted in report).	Staff is actively working on noted recommendations, starting with High Risk areas.	Y	6/30/2022	8/1/2022		Items have been remediated

Carson City
Preliminary Risk Assessment of Body Worn Camera Program
September 2022

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 Sheriff's Office should establish a process that ensures all officers responding to 911 dispatch calls and all self-initiated activities requiring dispatch notification have a BWC video. Additionally, performance metrics and goals should be established for Body Worn Camera ("BWC") activation.	Sheriff is reviewing Axon and other performance products, and will need to build performance metrics and goals.	N	7/1/2023			
2		The Sheriff's Office should update their BWC policy to address when the video upload and categorization is to occur. Additionally, the Sheriff's Office should perform routine monitoring of the uploads and the categorization of videos for completeness and accuracy. Lastly, performance metrics and goals should be established for BWC uploads and categorization of videos.	Sheriff's office agrees and will incorporate into policy instruction when to upload and categorize video from a BWC.	N	10/30/2022			
3		The Sheriff's Office should continue to roll out the BWC program's Early Warning Policy to comply with NRS 289.823. Furthermore, the policy should implement a system and methodology to monitor the BWC video for compliance with the BWC program and policy, and identification of opportunities for improvement to include all uniformed personnel with BWC devices, including the Jailors. This should include an evaluation of the total reviews that need to be completed in order to be statistically significant in comparison to the total of BWC footage of each uniformed personnel with a BWC device or other means of how supervisors chose videos for review, such as utilizing the feature within the Axon software that aids in the random selection of the videos for review. Lastly, the supervisor's monitoring of the videos should also be reviewed for compliance with set methodology and intent of the program and related policies.	The Sheriff's Office has established policy to address the Early Warning Policy, as per NRS 289.823. The implementation of Performance will take up the recommendations above. In terms of jailors, they are not required to have BWC; however, they have been issued provide additional audio/visual documentation and record of events. The internal workgroup mentioned above will address and publish policy for camera use within the jail.	N	7/1/2023			
4		Review and update the current BWC policy to reflect current operating practices and alignment with NRS 289.830. Specifically, the policy should be updated to include disciplinary actions.	BWC policy is currently in review as a natural course of implementing the in-car camera as well as the early warning policies. Although not specifically mentioned in the BWC policy, it is a violation of Standards of Conduct for an employee's, "Failure to operate a portable recording device as required by the Office and/or editing or erasing any portion of a recording". See policy 339.5.8.(J). Discipline for the violation can range from a warning up to and including termination.	N	10/30/2022			

Audit Committee Agenda Item Report

Meeting Date: September 13, 2022

Submitted by: Sheri Russell

Submitting Department: Finance

Item Type: Formal Action / Motion

Agenda Section:

Subject:

For Possible Action: Discussion and possible action to identify, discuss, and provide recommendations to the Board of Supervisors on projects to be performed by the Internal Auditor for the period ending June 30, 2023. (Sheri Russell, SRussell@Carson.org)

Staff Summary: Carson City Staff, Eide Bailly and the Audit Committee, had a discussion regarding the FY 2023 Internal Audit projects at the March 8, 2022, and July 12, 2022 Audit Committee Meeting. Staff has not taken the FY 23 audit projects as recommended to the Board of Supervisors yet pending the outcome of the high-level review of the Sheriff's Body Worn Camera Project. After hearing the outcome of that report, internal auditors are seeking direction as to continuation of this project, or to reallocate the budget to a different internal audit project.

Suggested Action:

I move to approve allocating the remaining \$_____ funding to the _____ internal audit project and recommending the FY 2023 Audit Work Program as presented to the Board of Supervisors.

Attachments:

[SR - FY 23 Internal Audit Program.docx](#)



STAFF REPORT

Report To: Audit Committee

Meeting Date: September 13, 2022

Staff Contact: Sheri Russell, Chief Financial Officer & Steve Ferguson, Audit Committee Chairman

Agenda Title: For Possible Action: Discussion and possible action to identify, discuss, and provide recommendations to the Board of Supervisors on projects to be performed by the Internal Auditor for the period ending June 30, 2023. (Sheri Russell, SRussell@Carson.org)

Staff Summary: Carson City Staff, Eide Bailly and the Audit Committee, had a discussion regarding the FY 2023 Internal Audit projects at the March 8, 2022, and July 12, 2022 Audit Committee Meeting. Staff has not taken the FY 23 audit projects as recommended to the Board of Supervisors yet pending the outcome of the high-level review of the Sheriff's Body Worn Camera Project. After hearing the outcome of that report, internal auditors are seeking direction as to continuation of this project, or to reallocate the budget to a different internal audit project.

Agenda Action: Formal Action/Motion

Time Requested: 20 minutes

Proposed Motion

I move to approve allocating the remaining \$_____ funding to the _____ internal audit project and recommending the FY 2023 Audit Work Program as presented to the Board of Supervisors.

Board's Strategic Goal

Efficient Government

Previous Action

N/A

Background/Issues & Analysis

Based on discussions at the March 8, 2022 meeting and July 12, 2022 meeting, staff is moving forward with the following audits:

Risk Assessment 2024	\$ 12,000
Utility Billing	50,000
Sheriff Body Worn Cameras	45,000
Follow-up	2,400
Fraud, Waste & Abuse Hotline	500
Special Projects/Validation	<u>100</u>
2023 Budget	\$110,000

After a high-level review of the Sheriff's Body worn camera and the report presented today, please let staff know if they would prefer that Eide Bailly continue with the larger project, or if they would like to allocate the remaining funding to a different internal audit project.

Applicable Statute, Code, Policy, Rule or Regulation

CCMC 2.14.040

Financial Information

Is there a fiscal impact? Yes No

If yes, account name/number: General Fund Internal Auditor / Professional Services

1010800-500309

Is it currently budgeted? Yes No

Explanation of Fiscal Impact: \$110,000 has been budgeted for FY 23.

Alternatives

N/A

Board Action Taken:

Motion: _____

1) _____

2) _____

Aye/Nay

(Vote Recorded By)

Audit Committee Agenda Item Report

Meeting Date: September 13, 2022

Submitted by: Sheri Russell

Submitting Department: Finance

Item Type: Other / Presentation

Agenda Section:

Subject:

For Presentation Only: Discussion regarding Fiscal Year ("FY") 2023 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 2023 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: September 13, 2022

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

Agenda Title: For Presentation Only: Discussion regarding Fiscal Year (“FY”) 2023 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 2023 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 Chapter 3.075, 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)

Audit Committee Agenda Item Report

Meeting Date: September 13, 2022

Submitted by: Sheri Russell

Submitting Department: Finance

Item Type: Other / Presentation

Agenda Section:

Subject:

For Discussion Only: Discussion regarding dates for the next meeting of the Audit Committee.

Suggested Action:

Discussion only.

Attachments: