Agenda Item No: 17.A

STAFF REPORT

Report To: Board of Supervisors **Meeting Date:** July 7, 2022

Staff Contact: Sheri Russell, Chief Financial Officer

Agenda Title: For Possible Action: Discussion and possible action regarding recommendations of the Carson City Audit Committee to approve the completed remediation plans and remove findings from the Audit Findings Tracking Summary Report. (Sheri Russell, srussell@carson.org)

Staff Summary: The completed remediation plans for various recommendations and findings have been presented and approved by the Audit Committee. Upon approval by the Board of Supervisors, the completed recommendations and findings will be considered closed and removed from the Audit Findings Tracking Summary Report maintained by the internal auditor and City staff.

Agenda Action: Formal Action / Motion **Time Requested:** 10 Minutes

---

Proposed Motion
I move to approve the Audit Committee's recommendation as presented.

Board's Strategic Goal
Efficient Government

Previous Action
N/A

Background/Issues & Analysis
Eide Bailly has been contracted by Carson City to provide internal auditor services starting July 1, 2018 through June 30, 2022. A new contract will be reviewed by the Audit Committee on July 12 for presentation to the Board of Supervisors on August 4 for approval consideration, proposed to be retroactive to July 1, 2022 if approved.

Staff has addressed the recommendations and/or findings contained in the Audit Findings Tracking Summary Report with remediation plans and recommends closure on the items described below. The internal auditor has validated remediation as requested, and the Audit Committee is recommending closure of the following findings:

- IT Vulnerability Audit - All items. An updated findings report will be presented at the July 12, 2022 Audit Committee meeting.
- Fleet Management Audit - Item #1 (final item) is validated and recommended for Closure.
- Payroll Audit - Item #1 & #3 (final items) are recommended for Closure.

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

Financial Information
Is there a fiscal impact? No

If yes, account name/number: N/A

Is it currently budgeted? No

Explanation of Fiscal Impact: N/A

Alternatives
Do not accept the recommendation and/or provide alternative direction to staff.

Attachments:
Audit Findings Summary 3-8-2022.pdf

Board Action Taken:

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

_____
(Vote Recorded By)

Carson City
Internal Audit Summary
Updated - 3/8/22

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	
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	12	6/22/2021		
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		3/8/2022		All items recommended for closure
Fleet Audit	3/30/2021	3/30/2021	Internal Auditor	6	5	3/8/2022	7/1/2020	#1 recommended for closure
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	1	3/8/2022	12/16/2021	#1 and #3 recommended for closure
Total (including archived reports)				273	259			

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.	P	6/30/2022			CIO will create an Information Security response Plan. **UPDATE:** Plan is in review process.

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; **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.**

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
Fleet Management Audit
March 10, 2021

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		FINDING 1 - Inventory Security and Tracking: RECOMMENDATION: Short-term solution - restrict access to Inventory to Fleet Services personnel by installing facility locks if feasible. Long-term solution - incorporate a tracking mechanism by implementing parts tracking sheet where Fleet personnel can sign, date, and identify the parts used and removed from inventory. Consider bar code technology or one designated Fleet Technician responsible for tracking fleet.	This was a recommendation in the last Internal Audit as well. The Fleet Facility is secured within the Public Works Corporate Yard and restricted to badge-only access. To date, there is no known instance of inventory loss; however, management agrees that there are opportunities to reduce risk and improve security over inventory. Management will submit a supplemental budget request for the position with the FY22 budget requests for consideration by the Board of Supervisors.	P	1/31/2022	7/1/2021	Y	Tracking sheet has been implemented. Facilities Division is installing additional restrictions on inventory access concurrent with hiring of Fleet Warehouse Coordinator (new FY22 position). Anticipated to be completed August 2021. **STATUS:** Requested Internal Audit Validation once position is up and running (5-6 Months). **STATUS UPDATE:** Auditor has validated process in place, procedures working as intended. Recommend Closure

Carson City
Payroll
November 22, 2021

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		FINDING 1 - No formalized tracking mechanism or process for a periodic review and assessment of payroll related statutory changes. - Internal Auditor recommends that the City implement a tracking mechanism with appropriate documentation or payroll related regulatory changes. Including sign-off from HR Director and Chief Financial Officer.	Staff agree with the finding and plan to create an internal memo with necessary support, annually, likely in December/January when Regulatory Changes primarily occur. This memo will be routed to HR Director and CFO for signature, and retained by Finance.	Y	2/28/2022	2/28/2022	N	This is working as intended; HR Director and CFO signed off on the memo that Finance circulated regarding IRS and contract changes. Recommend Closure
3		FINDING 3 - It was noted that HR employees in User Key Roles have full access to payroll related functions in Munis including the role permissions in "Pay Type Maintenance" and "projection run number Maintenance Access" functions. - Internal Auditor recommends that the City's IT department perform further review and modifications, where needed of Munis system functionality pertaining to user role and permissions granted to HR and Finance employees to ensure proper segregation of duties.	Management agrees, IT Application Team will work with HR and Finance to test permissions for existing HR Roles in the Munis Test Environment. Role will be tested against operational and department responsibilities and updated to comply with the principle of least privilege.	Y	12/31/2021	12/31/2021	N	IT has corrected this issue and removed access that was not necessary. Recommend Closure