Audit Report

Recorder’s Office
Document Recordation Application

April 2019

Angela M. Darragh, CPA, CISA, CFE
Audit Director
# TABLE OF CONTENTS

REPORT DETAILS ....................................................................................................................................... - 2 -

BACKGROUND ....................................................................................................................................... - 2 -

OBJECTIVES, SCOPE, AND METHODOLOGY .......................................................................................... - 2 -

CONCLUSION ......................................................................................................................................... - 4 -

FINDINGS, RECOMMENDATIONS, AND RESPONSES ................................................................................. - 5 -

FINDING 1 – ONCORE PASSWORD STANDARDS NEED IMPROVEMENT (HIGH) ............................... - 5 -

FINDING 2 – USER ACCOUNT CONTROLS NEED IMPROVEMENT (HIGH) ........................................... - 6 -

FINDING 3 – NO FORMAL DISASTER RECOVERY PLAN IN PLACE (HIGH) ........................................... - 7 -

FINDING 4 – PROOF OF LABOR ON PATENTED MINE DOCUMENTS UNDERCHARGED– (MEDIUM) .... - 8 -

FINDING 5 – AUDIT LOGS ARE NOT BEING REVIEWED (MEDIUM) .................................................... - 9 -

FINDING 6 – NO PATCH MANAGEMENT FOR APPLICATION (MEDIUM) ............................................. - 10 -

FINDING 7 – USER PERMISSIONS NEEDS IMPROVEMENT (MEDIUM) ............................................... - 11 -

FINDING 8 – AUTO-INDEXING FUNCTION (LOW) ................................................................................ - 11 -
REPORT DETAILS

BACKGROUND

The office of Clark County Recorder was established July 1, 1909. County Recorders are elected every four years in accordance with Nevada Revised Statute (NRS) 247.010. Debbie Conway, the current Clark County Recorder, began her first term in January 2007 and was re-elected in 2010, 2014 and 2018. The County Recorder’s Office, which consists of approximately 60 employees, is located on the 2nd floor of the Government Center at 500 South Grand Central Parkway, Las Vegas, Nevada.

The County Recorder’s Office serves the cities of Las Vegas, North Las Vegas, Henderson, Boulder City, Laughlin, Mesquite, and other areas of Clark County. The Recorder’s Office records and preserves public records. The Office also provides for subsequent retrieval of records for public viewing and produces copies and certification of records. In addition, it collects Real Property Transfer Tax (RPTT) on transfers of real property. The Recorder’s Office records documents in digital images to be kept as a permanent record. All records are indexed by the name of the principal parties of the document and by the year of recording.

Examples of typical recorded documents include: land records, financing documents, unpatented mining claim records, military discharge papers, homestead declarations, mechanics' liens, federal tax liens, and real property transfer tax.

The Recorder’s current recordation application, OnCore, was implemented in August 2009. The licensing fee for OnCore was $1,875,000, with an annual maintenance fee of $375,000. The Recorder’s Office is upgrading the application to Acclaim in 2019.

According to reported County Recorder’s Office statistics, the office recorded 734,301 documents in 2017 and collected $137,512,008.90 in Real Property Transfer Tax. Previously, marriage licenses were recorded by the Recorder’s Office. However, since 2015, it is now handled by the Clerk’s Office. At present, the on-line index contains the official records from 1988, the Uniform Commercial Code documents from 1986, and also federal tax liens from 1984 to the present (Indices for years prior to the on-line index of these records are available on microfilm.)

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this audit was to determine whether controls are in place to ensure the confidentiality, integrity and availability of the data held within the OnCore System.
We obtained an understanding of the OnCore operating and control environment by meeting with staff and performing a walkthrough of the application process. In order to achieve our objective we performed the following procedures:

- We interviewed staff in the Recorder’s Office, and reviewed OnCore’s password configurations to compare current application password practices, with Clark County Information Technology Security directives.

- We interviewed staff from the Recorder’s Office Information Technology Division and Clark County Information Technology Department regarding policy and procedures for patch management, vendor management, and system operations, and compared to industry best practices.

- We interviewed Recorder’s Office staff regarding policy and procedures on disaster recovery, business contingency planning, and testing of the plan. We reviewed samples of the recovery testing that was completed in 2017 and obtained and reviewed backup guidelines and policy.

- We performed a walk-through of the OnCore server location and observed the physical security that is in place.

- We obtained a listing of all OnCore user accounts and compared with County personnel records to determine whether all active accounts belong to current employees and whether inactive employees retained access to the system. We also reviewed the listing for the usage of generic accounts.

- We reviewed user rights and roles to determine whether users were given the appropriate level of system access to complete their duties.

- We obtained a system listing of all OnCore user accounts created and deleted during the audit period and cross referenced to physical documentation to review for proper approval.

- We reviewed all of the OnCore database and the database query system’s user accounts to determine whether all active accounts belong to current employees that should have access.

- We obtained a report of all documents recorded during our audit period. We used professional judgment to select 15 samples from each quarter, for a total of 60 samples. We then tested each item to determine whether the recorded documents were indexed correctly, had the correct requirements for recording, and had the appropriate indexing information in accordance with the recording guide provided by the Recorder’s Office.
- We obtained the fee schedule effective October 1, 2017 and verified that the fees are allowed by Nevada Revised Statutes.

Our procedures considered the period of January 1, 2017 to December 31, 2017. The last day of fieldwork was November 15, 2018.

Our review included an assessment of internal controls in the audited areas. Any significant findings related to internal control are included in the detailed results.

While some samples selected were not statistically relevant, we believe they are sufficient to provide findings for the population as a whole.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

CONCLUSION

Based on our testing, we believe the Recorder’s Office has adequate controls for their document recordation application, OnCore. However, we believe some application controls could be improved to strengthen the OnCore application. Further, a disaster recovery plan should be formally created to improve preparedness. The Recorder’s Office should do a periodic review of fees within OnCore to ensure the fees match the published fee schedule and Nevada Revised Statutes.

Each finding includes a ranking of risk based on the risk assessment that takes into consideration the circumstances of the current condition including compensating controls and the potential impact on reputation and customer confidence, safety and health, finances, productivity, and the possibility of fines or legal penalties.

Auditee responses were not audited and the auditor expresses no opinion on those responses.
FINDINGS, RECOMMENDATIONS, AND RESPONSES

FINDING 1 – ONCORE PASSWORD STANDARDS NEED IMPROVEMENT (HIGH)

During our testing, we found that OnCore passwords are not encrypted and the application allows passwords to be reused after 3 change periods. OnCore also does not disable users after 3 failed logon attempts and password minimal length was not set. Following are County requirements for passwords according to Information Technology Directive 1:

Clark County Information Technology Security Policy (IV)(C)(2)(a)(1)&(2)
“User passwords must be at least eight characters in length and consist of two or more of the following: capital letters, lower case letters, numbers, and special characters (%*S@!). User passwords should not include common names or phrases, proper names or dictionary words. User passwords must be changed every ninety (90) days and may not be reused for at least ten (10) password change periods. Administrator passwords must be changed every 45 days and must never be reused.”

Clark County Information Technology Security Policy (IV)(C)(2)(a)(4)
“Passwords shall be encrypted during transmission and storage on all County Computing Systems and Networks”

Clark County Information Technology Security Policy (IV)(C)(2)(g)
“User Accounts will be disabled after 3 failed logon attempts. After lockout, the account may be automatically reactivated after a minimum of 30 minutes or after an authorized IT administrator manually resets the account.”

Having less than optimal password standards for application access increases the risk of unauthorized access, which may lead to application data being compromised and/or unauthorized transactions being performed. In addition, weak password practices decrease accountability should a password be compromised.

RECOMMENDATION

1. Modify the security settings so that passwords may not be reused for at least ten password changes and increase the minimal length to be at least eight characters. Administrative users should be prompted to change their password every 45 days and should never be allowed to repeat a password.
2. Request OnCore modify the system to ensure passwords are encrypted during transmission and while at rest.
3. Modify the security settings so that a user account is disabled after three incorrect logon attempts. After lockout, the account may be automatically reactivated after a minimum of 30 minutes or after an authorized IT administrator manually resets the account.

**MANAGEMENT RESPONSE**


With the implementation of Acclaim, all password security policies will continue to be met in the application.

**FINDING 2 – USER ACCOUNT CONTROLS NEED IMPROVEMENT (HIGH)**

Within OnCore, we found that there were three vendor accounts that were active, and two generic account that were being utilized, one of which had supervisor rights. Also, there was an employee that is no longer with the County that still had an active user account within the database.

Having vendor accounts that are not disabled after use could allow for misuse of accounts, such as unauthorized changes to the system. The use of generic accounts, with supervisor rights, that are accessed by multiple people allows for changes within the system without accountability. Database accounts of previous employees that remain active allows for possible account misuse and unauthorized changes to the database. Following are the Clark County Information Technology Directive 1 requirements:

*Clark County Information Technology Security Policy (IV)(C)(2)(e)*

Generic and Guest Accounts. The use of generic and guest accounts is not permitted. Individuals who require access to County Computing Systems and Networks must be assigned and must use a unique User ID with limited permissions. All default guest accounts must be deleted. The use of a generic email account is permitted when the account is assigned to a specific County employee(s).

*Clark County Information Technology Security Policy (IV)(C)(2)(d)*

Vendor/Contractor and Other Third Party Accounts. Accounts set up for use by vendors/contractors and other third parties for remote access, development, or maintenance must be restricted to the specific County computing system(s) and network segment that they have been approved to access. Accounts will be enabled for the periods of time that work is being performed and be disabled during those periods of time the account is not required for use.
**Clark County Information Technology Security Policy (IV)(C)(1)(b)**

Disabling User IDs. User IDs must be disabled immediately for any individual who is no longer affiliated with the County or for any individual who has otherwise lost authorization for access to County Computing Systems and Networks. User IDs for employees of the County on a leave of absence for prolonged personal or health reasons must be disabled on the first day of leave. The User ID will be reinstated upon official notification that the employee has returned from leave. User IDs that remain inactive for a period of time exceeding 60 days must be disabled. User IDs that remain inactive for a period of time exceeding 90 days must be deleted.

**RECOMMENDATION**

1. Obtain approval for the generic accounts.
2. Implement a process to monitor generic account use or have alerts set to notify management of any abnormal uses.
3. Deactivate vendor accounts after the work is performed and follow the same account creation and deletion process for granting and deactivating accounts.
4. Immediately disable the user that is no longer associated with Clark County and implement a periodic review of all users.

**MANAGEMENT RESPONSE**

Exception request for service/generic accounts will be approved by CCIT. All vendor accounts and users no longer associated with Clark County have been disabled.

Periodic review of all users will be implemented.

With the implementation of Acclaim, Clark County IT Security Policies/requirements, (IV)(C)(2)(e), (IV)(C)(2)(d) will provide better monitoring to better adhere to the policies and requirements.

**FINDING 3 – NO FORMAL DISASTER RECOVERY PLAN IN PLACE (HIGH)**

During our review, we found the Recorder’s Office is in the process of developing a disaster recovery plan. There is currently no formal disaster recovery plan in place.

The current business contingency plan allows for deputies to record the document if the network is down, however the plan is not very robust and does not accommodate any other scenarios.
Disaster recovery testing is being done informally on an annual basis when the Recorder’s Office refreshes the test environment with production data.

Clark County Information Technology Directive 1 requires departments to develop, test, and train on business continuity and disaster recovery plans. It states:

Clark County Information Technology Security Policy (IV)(O)
O. Business Continuity and Disaster Recovery. To mitigate the ranges of vulnerabilities to County Computing Systems and Networks and ensure their availability, continuity of operations and disaster recovery processes and procedures shall be developed for all County Computing Systems and Networks. This includes developing a contingency planning policy statement, conducting business impact analyses, identifying preventative controls, developing and maintaining recovery strategies, developing and maintaining contingency plans, testing the plan, conducting training and exercises, and maintaining the plan.

RECOMMENDATION

1. Complete the development of the disaster recovery plan, implement continuous maintenance of Business Contingency and Disaster Recovery plan, and document the results of testing of each plan.
2. Conduct training and exercises of the business contingency plan and document results.

MANAGEMENT RESPONSE

OnCore provides a Business Continuity (BC) module that has been used by the Recorder’s Office on a few occasions since its inception shortly after initial go live. The module provides recording transaction intake and queuing for paper based transactions received over the counter or via mail during system unavailability due to network or database failure.

When the system is once again available, the queued transactions are submitted to the database via an eRecording-like interface for recordation in the order in which they were received for processing.

Acclaim will have the same BC module once in place in August of 2019.

Disaster Recovery (DR) plan does exist and will be in place Spring 2019. Annual review of DR/BC will take place.

FINDING 4 – PROOF OF LABOR ON PATENTED MINE DOCUMENTS UNDERCHARGED—(MEDIUM)
During our testing, we found that the Recorder’s Office did not charge the same fee for “Proof of Labor on Patented Mine” and “Amended Proof of Labor, Patented Mines” as they did for the other Proof of Labor mining documents. Other Proof of Labor mining documents are charged a fee of $27, however “Proof of Labor on Patented Mines” and “Amended Proof of Labor, Patented Mines” are charged only $25. We believe the additional $2 fee, to bring the total to $27, should also be charged on the “Proof of Labor on Patented Mine” and “Amended Proof of Labor, Patented Mines” based on NRS 247.310. Following is the NRS related to this $2 fee that is the difference between the two charges:

NRS 247.310 Fees for recording certain documents concerning mining claims; payment of fees to county treasurer.

1. Except as otherwise provided by law, county recorders shall charge the following fees for recording affidavits of proof of labor on mining claims and for recording, pursuant to subsection 3 of NRS 517.230, affidavits of intent to hold mining claims:

   For recording any such affidavits that embrace therein one claim............... $2
   For each additional mining claim embraced in the affidavit...................... 2

RECOMMENDATION

1. Consult with District Attorney’s Office for clarification on if the fees should be charged.
2. Adjust fees based on District Attorney recommendations.

MANAGEMENT RESPONSE

Upon consultation with our District Attorney, the recording fee has been adjusted to reflect the recommendation provided as of 12/14/2018.

FINDING 5 – AUDIT LOGS ARE NOT BEING REVIEWED (MEDIUM)

During our review, we found the Recorder’s Office application records audit logs, however the logs are not being reviewed. Not reviewing audit logs could delay the identification of unauthorized access or granting of additional permission without prior authorization, resulting in lack of user permission controls.

Audit log production and review is essential to maintain system integrity and detect erroneous or fraudulent activity. In addition, in applications where users have elevated user rights in order to complete their duties due to application limitation, review of audit logs is essential to ensure user accountability. Audit logs also assist in monitoring for system intrusion.
RECOMMENDATION

1. Periodically review audit logs in areas such as login exceptions, user account creation, and user permission changes.
2. Periodically review audit logs for high risk transactions such as supervisor overwrites and document deletion.

MANAGEMENT RESPONSE

Report will be generated for OnCore/Acclaim.

Review schedule will be quarterly.

FINDING 6 – NO PATCH MANAGEMENT FOR APPLICATION (MEDIUM)

Currently the Recorder’s Office does not have a patch management process in place for OnCore. There is no tracking of patches that are or are not implemented. Not tracking patches that are not installed could leave the system open to known vulnerabilities. Patch management processes should be put in place to track patches that are installed and patches that were omitted, as well as the patch notes to identify the changes of each patch.

RECOMMENDATION

1. Create a patch management process to identify patches that were installed or omitted, with patch notes to identify the changes of the patch.

MANAGEMENT RESPONSE

There will be no future patches or release updates for OnCore. An annual release update will be provided for Acclaim with appropriate release notes provided in the electronic user guide. Intermittent patches to address issues will be provided along with related notes in the electronic user guide.
FINDING 7 – USER PERMISSIONS NEEDS IMPROVEMENT (MEDIUM)

We found that the Recorder’s Office has users that have more access than required to accomplish their job duties due to a limitation on permissions by the vendor. Users having additional permission granted allows for possible misuse and the ability to make unauthorized changes within OnCore.

The Recorder’s Office should ensure any future replacement software has the capability to separate permissions to only grant the minimum set of rights necessary to accomplish each user’s assigned departmental tasks. This is required by Clark County Information Technology Directive 1, as stated below:

Clark County Information Technology Security Policy (IV)(C)(2)(b)
User Accounts. Authorized user access to County Computing Systems and Networks must be controlled on the basis of rights and permissions that are assigned to each user or group. Each authorized user or group shall be granted the minimum set of rights and permissions necessary to accomplish their assigned departmental tasks. Users who are granted access to excluded/exempt data or

RECOMMENDATION

1. Include the availability of granular user permissions and roles in the requirements for replacement software.
2. Request a full list of permissions and the individual rights each permission allows from the vendor and complete a review of user permissions to ensure they are appropriate.

MANAGEMENT RESPONSE

With the implementation of Acclaim, permissions are role based at the user and group level. Each workspace, module, button, doctype, etc. can be controlled by roles at the user or user group level.

Each System Role within Acclaim has an associated description which explains what access/permission it allows.

Custom County Roles can be created within Acclaim to granulize each users experience within the Application.

FINDING 8 – AUTO-INDEXING FUNCTION (LOW)

During our testing, we found that the auto-indexing function does not always capture all the parties correctly, which could result in difficulty for constituents finding their appropriate documents. We
found 8 out of sixty sampled documents (13%) had errors with the auto indexing function. Quality assurance is done during downtime or after recording is done to ensure proper indexing. However, due to the Recorder’s Office workload, there is not sufficient time to verify all of the indexing. Without the review to ensure auto index is working correctly, constituents could have difficulty finding their appropriate documents.

RECOMMENDATION

1. Review auto indexing data more frequently and update auto indexing software as they notice patterns of inaccurate indexing from the quality assurance process.

MANAGEMENT RESPONSE

With Acclaim, like OnCore, Intellidact autoindexing will provide 6-12 month updates to the Automated Index Knowledgebase to ensure issue patterns are addressed as new document templates are recorded.

Additionally, the Recorder has a manual Quality Assurance process which follows the autoindexing process.

The more accurate LBX artificial intelligence indexing and redaction software will replace Intellidact Fall 2019.