



Audit Department

500 S Grand Central Pkwy Ste 5006 • PO Box 551120 • Las Vegas NV 89155-1120
(702) 455-3269 • Fax (702) 455-3893

Angela M. Darragh, CPA, CFE, CISA, Director

December 17, 2013

Mr. Don Burnette
Clark County Manager
500 South Grand Central Parkway, 6th Floor
Las Vegas, Nevada 89106

Dear Mr. Burnette:

We recently performed a follow-up audit of the Clark County Water Reclamation District Imaged Document Access audit dated November 10, 2011. The audit objective was to determine whether adequate corrective action was taken on the findings included in the audit report. Our audit procedures were performed as of November 1, 2013.

To conclude on the objectives of our audit, we interviewed management to determine the status of corrective action taken. We then performed observations and walkthroughs of Accounts Payable processes, Accounts Payable file room, and area where confidential documents are stored. We also performed interviews with Information Technology to understand changes made to Kofax scanning application and Cyberdocs records management application controls. We obtained documentation and performed detail tests of confidential document processes for hard copy and electronic forms, active users, user segregation of duties within Kofax and Cyberdocs, and access control configuration. Finally, we obtained and reviewed policies and procedures related to the areas being reviewed.

Clark County Water Reclamation District has taken adequate corrective action on 9 of the 10 findings reported in the original audit. Imaged documents managed through Cyberdocs continue to be retained indefinitely. Efforts should be made to adhere to the approved record retention schedule, which is audit clearance for accounting records, such as accounts payable and accounts receivable. We believe retaining records indefinitely presents a medium to high risk as a data breach and subsequent lawsuits could occur that could be financially significant and cause a loss of reputation.

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.

It is the department/division management's responsibility to decide if any appropriate action should be taken in response to reported audit findings. It is also their responsibility to assume the risk by not correcting a reported condition because of cost or other consideration.

We appreciate the cooperation and assistance provided Clark County Water Reclamation District during the course of this audit.

Sincerely,

A handwritten signature in blue ink that reads "Angela M. Darragh". The signature is written in a cursive style.

Angela M. Darragh, CPA
Audit Director



**Clark County
Water Reclamation
DISTRICT**

December 6, 2013

Ms. Angela M. Darragh
Clark County Audit Director
500 South Grand Central Parkway, 6th Floor
Las Vegas, Nevada 89106

SUBJECT: CCWRD IMAGED DOCUMENT ACCESS FOLLOW-UP AUDIT

Dear Ms. Darragh,

I acknowledge receipt of your follow-up audit Corrective Actions Status Report, along with the revised Corrective Actions Status statements for Item 9, and concur with your status findings. As noted and recommended, CCWRD is in the process of developing a plan to resolve the one (1) outstanding finding, Non-Compliance with Record Retention Schedules in our Cyberdocs environment.

Staff is currently gathering each CCWRD Business Center's document types, catalog structures, and naming conventions in order to develop a Cyberdocs document management plan. Upon completion of this information gathering process, staff will then associate these documents types with the appropriate records retention schedules in accordance with NAC 239 and begin the appropriate preservation or destruction of these documents.

We appreciate the level of effort required by your department to complete the original audit and the follow-up audit and appreciate your thoroughness in identifying these areas of weakness in our Cyberdocs records management.

Please do not hesitate to call me if you need any further information.

Sincerely,

Thomas A. Minwegen
General Manager

BOARD OF TRUSTEES

Lawrence L. Brown III, *Chair*. Steve Sisolak, *Vice Chair*.
Susan Brager. Tom Collins. Chris Giunchigliani. Mary Beth Scow. Lawrence Weekly.
Thomas A. Minwegen, *General Manager*

5857 East Flamingo Road, Las Vegas, Nevada 89122 (702) 668-8888, (800) 782-4324
cleanwaterteam.com

CLARK COUNTY WATER RECLAMATION DISTRICT
Imaged Document Access
Findings, Recommendations, and Corrective Actions Status
As of November 1, 2013



AUDIT DEPARTMENT
 Angela M. Darragh, CPA, CFE, CISA
 Audit Director

Original Report Issuance Date: November 10, 2011

Summary Audit Findings & Recommendations			Summary Management Disposition		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Actions Status	Implemented	Not Implemented	Other
1	Kofax Batch Access is Not Restricted						
	Kofax allows access to all batches in process by any user on the front end. There are no security features activated for front end processing. The concern is that some of these batches contain sensitive documents that could be potentially viewed by users that are not authorized.	<p>Establish controls over batch security by user for sensitive documents or some other form of mitigating controls. Mitigating controls may include that batch processing for sensitive document be performed without interruption or delays, with batches closed immediately upon completion of processing to minimize access availability.</p> <p>Immediately report any unusual transactions such as batches disappearing or batches that have an inappropriate status change to the Information Technology Division (IT) and appropriate management in order that IT may determine who accessed the scanned documents while in process.</p>	Y	Batch types and user groups in Kofax have been configured in order that sensitive document batch processing once scanned is segregated from regular scanning. In addition, one confidential employee is responsible for the scanning sensitive documents. There are three other confidential employees who have access.	✓		

Summary Audit Findings & Recommendations			Summary Management Disposition		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Actions Status	Implemented	Not Implemented	Other
2	User Group Rights Not Adequately Limited						
	There are five user groups. User group rights include view, edit, copy, delete, control access, and printing. All groups may perform all aforementioned functions except for the primary user group that may not delete or control access.	<p>Restrict edit and copy rights from any user. Edit profiles should be limited to batch processing with any necessary changes thereafter managed through a segregation of duties process (i.e. management authorization with IT changing profile). Delete rights after batches are closed should not be available to operational staff including supervisors and managers.</p> <p>Implement segregation of duties over the Control Access function. Rights to the Control Access function should not be given to operational staff. Operational staff should be authorizing access rights with IT personnel providing control access.</p>	Y	User groups in Kofax and Cyberdocs have been configured so that access may be limited to those authorized to process and view sensitive documents. Users are assigned to groups that segregates access.	✓		

Summary Audit Findings & Recommendations			Summary Management Disposition		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Actions Status	Implemented	Not Implemented	Other
3	Sensitive Imaged Documents Historically Accessible to All Users						
	Sensitive imaged documents such as workmen's compensation claims and unemployment claims were assigned to a category that allowed all users to access these documents. Some personnel should not be authorized to handle sensitive information, such as accounts payable, customer service, or temporary personnel.	The District determined, based on recommendations provided during the course of our procedures, to perform a mass change of document type and user groups to limit access to sensitive imaged documents. We believe this process will provide reasonable safeguards for unauthorized access to sensitive imaged documents.	Y	Sensitive documents may only be viewed by users within authorized groups in Kofax and Cyberdocs.	✓		

Summary Audit Findings & Recommendations			Summary Management Disposition		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Actions Status	Implemented	Not Implemented	Other
4	Users with Inappropriate Access						
	We analyzed users for active employment status. Several exceptions were noted for both active and inactive users. Exceptions include 7 generic users, 1 duplicate user, 5 names not verifiable through Human Resources, 3 active logins were no longer employed, 2 access deactivations did not occur within a reasonable period, and 3 consultants did not have a company name for verification.	<p>Do not allow generic user names for user access for accountability purposes.</p> <p>Assign only one user account per employee.</p> <p>Establish policies and procedures for activating and deactivating users to minimize potential unauthorized access.</p> <p>Perform a periodic comparison between user lists by assigned user groups, document type access, and employment status to verify all personnel have appropriate access.</p>	Y	The District has verified all users of Kofax and Cyberdocs. The District also implemented policies and procedures to consistently verify user information on an ongoing basis.	✓		

Summary Audit Findings & Recommendations			Summary Management Disposition		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Actions Status	Implemented	Not Implemented	Other
5	Unsecured Database in Shared Files						
	Kofax and Cyberdocs databases are maintained in shared files accessible to anyone with access to the shared drive. A user of either Kofax or Cyberdocs does not need to be logged in to access the files through the shared drive. Cyberdocs folder and files names are encrypted. However, the document image is a “.tif” file, is not encrypted, and may be easily viewed, as this is a common file type. Cyberdocs documents will remain indefinitely accessible to all with access to the shared drive.	Secure all shared files to allow only database administrator access.	Y	This vulnerability was immediately corrected by the District. Cyberdocs documents are now located in a secured area and are not accessible to all users.	✓		
6	Test Server Imaged Documents Vulnerable						
	Imaged documents also reside in the test server. All security vulnerabilities found with production server imaged documents are replicated on the test server.	Secure all imaged documents and address vulnerabilities. Remove all scanned documents from the test server.	Y	The District has written a script and policies and procedures to wipe test data once testing is completed.	✓		
7	Security Not Tested After Upgrade Install						
	Cyberdocs was upgraded in May of 2011 without testing to determine that security was set appropriately for users. When the system was upgraded, it appears that the authority to view all scanned documents was provided to the primary group that includes all users of Cyberdocs. Sensitive documents could then be viewed by all users. The lack of security for sensitive documents allowed for a potential data breach to occur.	Implement procedures to test security and functionality whenever an upgrade is installed prior to allowing live operational use. Testing should include access to sensitive documents and records after upgrade installs and on a consistent basis as scheduled periodically during the year.	Y	Policies and procedures are now in place to require testing of Kofax and Cyberdocs applications after upgrades.	✓		

Summary Audit Findings & Recommendations			Summary Management Disposition		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Actions Status	Implemented	Not Implemented	Other
8	Sensitive Paper Documents Not Reasonably Safeguarded						
	Documents containing sensitive information such as workmen's compensation and unemployment claims were historically imaged and hard copies forwarded to Accounts Payable for payment. Paper documents were then stored in the Accounts Payable files in a file room. While the file room is in a secure area not accessible by the general public and access is badge controlled, many personnel have access. The door to the file room may also remain open if personnel are in the room. Access to the file room by numerous personnel, who should not have access to sensitive documents, increases the risk of unauthorized access and misuse of sensitive information.	The District immediately implemented procedures for sensitive documents as part of "Direct Pays". Procedures will include handling of documents by a confidential employee, and forwarding cover sheets only with approval signatures to Accounts Payable. Paper documents will be destroyed and access will be restricted for imaged documents. Sensitive paper documents currently filed in the Accounts Payable files will be removed to restricted access. We believe these procedures will provide reasonable safeguards for sensitive paper documents.	Y	The District implemented policies and procedures to segregate the processing and handling of sensitive documents. Sensitive documents are now processed by one confidential employee who also scans the documents into Kofax. The hard copy sensitive documents are filed by the confidential employee into a separate locked file cabinet within a separate room of the Accounting Department. Hard copy sensitive documents are no longer retained in the Accounts Payable file room. Imaged sensitive documents may only be viewed by user groups with authorized access.	✓		

Summary Audit Findings & Recommendations			Summary Management Disposition		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Actions Status	Implemented	Not Implemented	Other
9	Non-Compliance with Record Retention Schedules						
	Imaged documents in Cyberdocs are retained indefinitely. Cyberdocs has been in use approximately 15 years. Records in Cyberdocs include various documents such as payroll records, employee recruitment records, agenda items, workmen’s compensation claims, unemployment claims, accounting documents, other accounts payable documents, inspections, lien documents, purchasing documents, and miscellaneous documents. Accounts Payable paper documents are retained five to six years. Accounts payable documents contain records such as workmen’s compensation claims and unemployment claims that should be destroyed within a different period than Accounts Payable documents.	<p>Arrange to meet with the County Records Manager to implement improved control procedures to correct weaknesses identified. Specifically, we recommend:</p> <p>a) Develop a plan for removal and/or adjustment of sensitive information from Accounts Payables records.</p> <p>b) Review the imaged documents that have exceeded the recommended disposition timeline pursuant to the records retention schedule and prepare for the deletion and/or destruction of records.</p> <p>c) Identify improvement areas, with additional focus placed on management oversight and compliance with established Administrative Guideline 14.</p>	Y	<p>a) Immediately following the original audit all sensitive documents were removed from the Accounts Payable records in Cyberdocs (and also hard copies). The sensitive documents were moved into a confidential file within Cyberdocs (locked cabinet for hard copies) and the only staff who have access are confidential employees (HR and Payroll).</p> <p>b) District has not implemented a process for electronic destruction of records within Cyberdocs. District is currently gathering each Business Center's document types, catalog structures, and naming conventions in order to develop a Cyberdocs document management plan. Upon completion of this information gathering process, staff will then associate these documents types with the appropriate records retention schedules in accordance with NAC 239 and begin the appropriate preservation or destruction of these documents.</p> <p>c) District has not identified improvement areas; however, the process outlined in item 9(b) will allow for identification of improvement areas, which will include management oversight.</p>		✓	

Summary Audit Findings & Recommendations			Summary Management Disposition		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Actions Status	Implemented	Not Implemented	Other
10	Lack of Written Policies and Procedures						
	Written operational policies and procedures do not exist for accounts payable, payroll, or system back-ups and upgrade installations testing that would include the imaging process and record retention. Written policies and procedures also do not exist for handling of sensitive documents.	Develop written policies and procedures with the assistance of District staff. Management should approve all policies and procedures, as these are the members of the organization that are ultimately responsible and have the expertise and experience in managing operations. These policies and procedures should include safeguarding of sensitive information and record retention for imaged, paper documents, and working copies.		Written policies and procedures exists for accounts payable, payroll, system back-ups and upgrade installations testing. Policies and procedures also exist for handling of sensitive documents.	✓		