



AUDIT DEPARTMENT

Audit Report

Clark County Water Reclamation District Imaged Document Access

November 2011

Angela Darragh, CPA, CISA, CFE
Audit Director

AUDIT COMMITTEE:

Commissioner Steve Sisolak

Commissioner Chris Giunchigliani

Commissioner Lawrence Weekly



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 Darragh, CPA, CFE, CISA, Director



November 10, 2011

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

Dear Mr. Burnette:

At the request of the Water Reclamation District, we have conducted an audit of Imaged Document Access. Our procedures were performed as of August 17, 2011. We performed a preliminary survey to obtain an understanding of access controls. We then performed observations and analysis.

The objective of our audit was to determine whether controls are adequate to reasonably safeguard imaged documents from unauthorized access.

We concluded that imaged document access controls are not adequate to reasonably safeguard imaged documents from unauthorized access. Significant weaknesses exist in controls over security of shared files and shared drives, authorized users, assignment of user groups to document types, user group rights, and safeguarding of sensitive paper documents. We also noted that imaged documents are retained indefinitely and some paper documents are not retained for the length of time in accordance with record retention schedules. Written operational policies and procedures do not exist for accounts payable, payroll, or system back-ups and testing that would include the imaging process. Written policies and procedures also do not exist for imaging processes and handling of sensitive documents.

A draft report was provided to the District for comment and their response is included. We appreciate the cooperation and assistance provided by the Water Reclamation District.

Sincerely,

/s/ Angela Darragh

Angela Darragh, CPA
Audit Director

TABLE OF CONTENTS

BACKGROUND	1
OBJECTIVES, SCOPE, AND METHODOLOGY	2
RESULTS IN BRIEF	2
DETAILED RESULTS	2
User Access Not Sufficiently Restricted	2
Kofax Batch Access is Not Restricted	2
User Group Rights Not Adequately Limited	3
Sensitive Imaged Documents Historically Accessible to All Users	4
Users with Inappropriate Access.....	4
Shared Files and Drives Leave Imaged Documents Vulnerable 5	
Unsecured Database in Shared Files	5
Test Server Imaged Documents Vulnerable.....	6
Security Not Tested after Upgrade Install	6
Sensitive Paper Documents Not Reasonably Safeguarded	6
Non-Compliance with Record Retention Schedules	7
Lack of Written Policies and Procedures	7
APPENDICES	9
Appendix A: Management Response Letter	9

BACKGROUND Clark County Water Reclamation District (District) utilizes two computer applications for records management. Kofax initially captures documents through a scan process transforming them into manageable imaged information. Kofax features include form recognition that allow for automatic indexing of documents based on form types. A profile is automatically created for each document assigning a sequential document number, document type based on form recognition configuration, user (author), date scanned, security, and retention schedule for archiving. During the scanning process, Kofax will reject documents that are not recognized or read error. All document profiles and imaged documents are manually verified when scanned. Rejects, errors, and miscellaneous document profiles are manually corrected. Kofax is a batch processing application. After validation, indexing, and manual corrections of profiles, batches are manually closed. Imaged documents temporarily reside in a database maintained in a shared file until the batch is closed.

Kofax is integrated with the Cyberdocs application. Cyberdocs is the application utilized for records management which has capabilities that promote safeguarding and security of documents that contain sensitive information. The imaged documents and profile information flow from Kofax to the Cyberdocs database that is maintained in a separate shared file. During the integration process, document types are automatically assigned to user groups based on program configuration. Users are assigned to user groups in Cyberdocs. Rights to user groups are also assigned in Cyberdocs. These rights may include, view, edit, copy, delete, and control access. All users may print documents.

Sensitive information is regulated by the state. It is the responsibility of the District as a data collector to maintain reasonable security measures to protect records from unauthorized access, acquisition, destruction, use, modification, or disclosure. Reasonable belief that sensitive information has been accessed by unauthorized persons constitutes a data breach and sets off notification requirements and the potential for the District to pursue an action for damages against the person who unlawfully caused the data breach.

Cyberdocs has advanced capabilities to manage document workflow with document sharing in the office and remotely. These advanced capabilities are currently not utilized within the District.

Kofax and Cyberdocs applications have been in place for approximately 15 years. Cyberdocs was recently upgraded in May of 2011.

**OBJECTIVES, SCOPE, AND
METHODOLOGY**

The objective of our review is to determine whether controls are adequate to reasonably safeguard imaged documents from unauthorized access.

Our services consisted of conducting a preliminary survey to obtain an understanding of records management processes and access to imaged documents. Preliminary survey procedures included interviews with management and staff, observations, walkthroughs, gathering of information, and review of relevant laws, rules, and regulations. Analyses and detailed testing were then performed sufficient to conclude on objectives. The last day of fieldwork was August 17, 2011.

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.

RESULTS IN BRIEF

Imaged document access controls are not adequate to reasonably safeguard imaged documents from unauthorized access. Significant weaknesses exist in controls over security of shared files and shared drives, authorized users, assignment of user groups to document types, user group rights, and safeguarding of sensitive paper documents. We also noted that imaged documents are retained indefinitely and some paper documents are not retained for the length of time in accordance with record retention schedules. Written operational policies and procedures do not exist for accounts payable, payroll, or system back-ups and testing that would include the imaging process. Written policies and procedures also do not exist for imaging processes and handling of sensitive documents.

DETAILED RESULTS

**User Access Not Sufficiently
Restricted**

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. A factor that partially, but not sufficiently mitigates risk of unauthorized access, is that batches are not available for any length of time as these are generally, but may not always be, immediately processed and closed. The concern is that some of these batches contain sensitive documents that could be potentially viewed by users that are not authorized.

As of August 17, 2011 there are 79 potential users without restricted access that could view sensitive documents through batch processing.

Recommendation We recommend that controls over batch security by user be established 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. We further recommend that any unusual transactions such as batches disappearing or with an inappropriate status change be immediately reported to Information Technology Division (IT) and appropriate management in order that IT may determine who accessed the scanned documents while in process.

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.

- **Edit and Copy Function** – All users may edit profiles, edit contents, and copy. Edit profiles is a feature that allows the user to change any information in the profile including document type. Edit content allows a user to edit word documents that are imaged. The program will then save the edited copy under a separate file name. A document may be copied. This creates another document in the records management application with the same profile.
- **Delete Function** - There are currently five users that may delete that include three IT personnel, one manager, and the accounting supervisor. According to the database administrator, the IT help desk is called and a ticket must be completed requesting a document to be deleted. Anyone with access may request a document delete. IT will then delete the document. Deleted documents are not retrievable. Kofax assigns a document number when information is scanned. If the document is deleted then the related document number will no longer be available.
- **Control Access Function** – The same five users that may delete may also activate or deactivate a user.
- **Printing** – Anyone with access to Cyberdocs may print a document.

Recommendation We recommend that the edit and copy rights not be given to any user as these functions were primarily intended for use in document workflow, annotation, and sharing. 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 as this leaves documents susceptible to deletion by error or unauthorized destruction. Some paper documents are destroyed after imaging, leaving the imaged record as the sole source, which is vulnerable with current weaknesses in access controls. Add-on programs are available for virtual deletes that remove the document from viewing access but retain the document in the database for more controlled destruction processes. This may provide safeguards over important and sensitive imaged documents that are the sole source of information.

We further recommend implementing 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.

We also recommend that printing be restricted to those with a business need for such access to further safeguard sensitive information and assist in record retention compliance.

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.

Recommendation The District determined, based on recommendations provided during the course of our procedures, to perform a mass change of document type and user group to limit access to sensitive imaged documents. We believe this process will provide reasonable safeguards for unauthorized access to sensitive imaged documents.

Users with Inappropriate Access

We analyzed users for active employment status. Several exceptions were noted for both active and inactive users. We found the following:

- Seven generic user names were established.
- One employee had two separate user identifications.
- Five names could not be verified through Human Resources

and, after discussion with District Human Resources, appeared to be temporary employees.

- Three individuals with active user logins were no longer employees.
- Access was not deactivated for two former employees until after a substantial time period.
- Three names were identified as consultants by the database administrator but did not have associated company name for verification.

These are indications that adequate procedures are not in place to maintain appropriate login status on current users.

Recommendation We recommend that generic user names not be allowed for user access for accountability purposes. For efficiency purposes, we recommend that only one user identification be used per employee. We further recommend that policies and procedures be established for activating and deactivating users to minimize potential unauthorized access. Finally, monitoring and signed approval of user lists by assigned user groups, document type access, and employment status should occur periodically on a consistent basis by management other than IT personnel.

Shared Files and Drives Leave Imaged Documents Vulnerable

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.

Kofax files are temporarily retained in the shared drive while in batch processing and move to the Cyberdocs database when the batch is closed. Kofax files will ordinarily not be available on the shared drive for long periods if batches are closed promptly.

Databases should be secured in the shared drives to minimize risk of unauthorized access and misuse of information.

Recommendation We recommend that shared files be secured to allow only database administrators access. This vulnerability was immediately corrected by the District.

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.

Recommendation We recommend that all imaged documents be secured and vulnerabilities addressed. The District will be immediately implementing the removal of all scanned documents from the test server.

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.

Recommendation We recommend that procedures be implemented 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.

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 has immediately implemented procedures for sensitive documents as part of "Direct Pays". Procedures will include handling of documents by a confidential employee, 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.

Recommendation We believe these procedures will provide reasonable safeguards for sensitive paper documents.

**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.

When records are maintained for timeframes that differ from required record retention schedules, as approved by the State and in accordance with State Statutes, the risk is increased that the entity will be exposed to inappropriate record destruction, data breaches, and litigation. In addition, the costs of providing additional space on servers to store the information continues to increase. The District is also not in compliance with state approved record retention schedules.

Legal record retention schedules have been recently updated and some record retention policies are currently being redefined.

Recommendation We recommend that the District arrange to meet with the County Records Manager to implement improved control procedures to correct weaknesses identified. Specifically, we recommend:

- a) Develop a plan for removal and/or adjustment of sensitive information from Accounts Payables records.
- 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.
- c) Identify improvement areas, with additional focus placed on management oversight and compliance with established Administrative Guideline 14.

**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.

Written policies and procedures allow higher-level management to set controls over processes to ensure that operations are effective and efficient and procedures safeguard assets and information. Policies and procedures also serve as a training tool for staff and provide consistency. Properly implemented, policies and procedures assist to ensure that processes are occurring as management intends.

Recommendation We recommend that written policies and procedures be developed and implemented 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.

APPENDICES

Appendix A: Management Response Letter



MEMORANDUM

Richard Mendes
General Manager

TO: Angela Darragh, Acting Audit Director, Clark County Audit Department

FROM: Richard Mendes, General Manager *RM*

SUBJECT: Clark County Water Reclamation District Imaged Document Access Audit – Management Response

DATE: October 27, 2011

Clark County Water Reclamation District (CCWRD) sincerely appreciates the level of effort required by your department to complete this audit and have finalized our review of the draft report. This was a very thorough audit and as such, identified some areas of weakness in our security and housekeeping model that we plan to address as outlined in the following responses to identified issues. We would like to thank you and all of your staff that participated in completing this audit and look forward to working with you in the future.

Please let me know if you need any further information.

AUDIT RECOMMENDATION:

Controls over batch security by user should be established for sensitive documents or implement some other form of mitigating controls.

DISTRICT RESPONSE:

The District agrees with the finding and has changed the batch process to incorporate the recommended changes of uninterrupted and immediate batch processing. This issue was corrected August 25, 2011. In addition District staff is developing new procedures and work instructions to prevent and identify these weaknesses in the future. The departmental procedures and work instructions will be completed by November 30, 2011.

AUDIT RECOMMENDATION:

We recommend that the Edit and Copy rights not be given to any user as these functions were primarily intended for use in document workflow, annotation, and sharing. 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 as this leaves documents susceptible to deletion by error or unauthorized destruction. Some paper documents are destroyed after imaging, leaving the imaged record as the sole sources, which is vulnerable with current weaknesses in access controls. Add-on programs

are available for virtual deletes that remove the documents from viewing access but retain the document in the database for more controlled destruction processes. This may provide safeguards over important and sensitive imaged documents that are the sole source of information.

We further recommend implementing 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.

We also recommend that printing be restricted to those with a business need for such access to further safeguard sensitive information and assist in record retention compliance.

DISTRICT RESPONSE:

The District agrees with the audit finding and has modified user access rights in the Kofax/CyberDocs application to reflect the recommended changes. This was completed on August 25, 2011.

District staff is working with the vendor to investigate/identify compatible software and methods of removing documents from viewing access in accordance with defined retention schedules. This will require further investigation. However, this issue has been currently addressed by restricting the Delete functionality. This was completed on August 25, 2011.

The document/system Control Access Function is restricted to system administrator staff in the IT Department. Modification to Control Access requires a departmental manager approval and must be submitted in writing to the IT Service Center. Once the request is received, a work order is created for the system administrator staff and is then implemented. The process and format for requesting changes to document/system access will be incorporated in departmental procedures and work instructions. The process has been in place for quite some time. The departmental procedures and work instructions will be completed by November 30, 2011.

District staff contacted the support vendor, "5280 Solutions", On September 21, 2011 to discuss the audit recommendation of limiting the Print functionality to specific users. The support vendor stated that there is no way to selectively limit printing within the application and does not know of a third party product for this functionality.

AUDIT RECOMMENDATION:

Some personnel should not be authorized to handle sensitive information.

DISTRICT RESPONSE:

The District agrees with the finding. All document types and user groups were changed to comply with the audit recommendation in order to protect sensitive imaged documents from unauthorized viewing or printing. This action was completed on September 1, 2011.

AUDIT RECOMMENDATION:

Adequate procedures are not in place to maintain appropriate login status on current users. We recommend that generic user names not be allowed for user access for accountability purposes. For efficiency purposes, we recommend that only one user identification be used per employee. We further recommend that policies and procedures be established for activating and deactivating users to minimize unauthorized access potential. Finally, monitoring and signed approval of user lists by assigned user groups, document type access, and employment status should occur periodically on a consistent basis by management other than IT personnel.

DISTRICT RESPONSE:

The District agrees with the recommendation regarding generic user names and has corrected the issue. This was completed on August 31, 2011.

In reference to the issue of multiple login ID's for individuals, although there are 2 user ID's for one individual, this discrepancy is by design and will remain. The issue evolved due to a problem with the specific individual's active directory account. As a result of the issue, a new account was created and the first account was disabled. Since the original ID is associated as the owner of numerous documents in the system, removing this account will cause "orphan" documents and cause system issues in the database.

Monitoring and signed approval of user access lists by assigned user groups, document type access, and employment status will occur on a quarterly basis beginning December 1, 2011.

AUDIT RECOMMENDATIONS:

We recommend that shared files be secured to allow only database administrators access.

DISTRICT RESPONSE:

This vulnerability was immediately corrected by the District once it was brought to our attention as a result of the audit. This was completed on August 16, 2011.

AUDIT RECOMMENDATION:

Imaged documents also reside in the test server. All security vulnerabilities found with production server imaged documents are replicated on the test server. We recommend that all imaged documents be secured and vulnerabilities addressed.

DISTRICT RESPONSE:

This vulnerability was immediately corrected on August 16, 2011 by removing all production scanned documents from the test server. In addition, policy, procedures and work instructions have been written which prohibit the use of production documents for testing and verification purposes on a test system. This was completed August 31, 2011.

AUDIT RECOMMENDATION:

We recommend that procedures be implemented 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.

DISTRICT RESPONSE:

The District agrees with the finding. Procedures and work instructions are currently being developed and will be completed by November 30, 2011.

AUDIT RECOMMENDATION:

The District has immediately implemented procedures for sensitive documents as part of "Direct Pays". Procedures will include handling of documents by a confidential employee, forwarding cover sheets only with the approval signatures to Accounts Payable. Paper documents will be destroyed and access will be restricted for imaged documents. The auditors believe these procedures will provide reasonable safeguards for sensitive paper documents. Sensitive paper documents currently filed in the Accounts Payable files will be removed to restricted access.

DISTRICT RESPONSE:

The processes described by the Auditor above have been implemented. In addition, all sensitive documents in the Accounts Payable files have been pulled out of the Accounting file room, are being securely held, and will be destroyed as soon as the imaged sensitive documents have been moved to the secure imaging location. The District will complete the destruction of these documents by November 30, 2011.

AUDIT RECOMMENDATION:

When records are maintained for timeframes that differ from required record retention schedules, as approved by the State and in accordance with State statutes, the risk is increased that the entity will be exposed to inappropriate record destruction, data breaches, and litigation. In addition, the costs of providing additional space on servers to store the information continues to increase. The District is also not in compliance with state approved record retention schedules.

Legal record retention schedules have been recently updated and some record retention policies are currently being redefined. The auditor recommends that the District arrange to meet with the County Records Manager to implement improved control procedures to correct weaknesses identified. Specifically the auditor recommends:

- a. Develop a plan for removal and/or adjustment of sensitive information from Accounts Payable records.
- 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.
- c. Identify improvement areas, with additional focus placed on management oversight and compliance with established Clark County Administrative Guideline 14.

DISTRICT RESPONSE:

The District agrees with the auditor's recommendation to meet with Clark County Records Manager to discuss the areas of concern listed above and to secure all sensitive documents.

- a. District management has removed all sensitive documents from the Accounting Department's file room; are being securely held, and will be destroyed as soon as the imaged sensitive documents have been moved to the secure imaging and placed in a secure imaging file; three years of documents are held in the file room. Older documents are held in the District's secure Records Archive Room where only the District's Security Department and the General Manager's executive assistant have a key.
- b. The District is addressing this issue by requiring document owner's to review and identify expired documents and requesting appropriate IT system administrators remove the documents from the imaging system. In addition, the District is formalizing a Records Management program to include policy/procedure/work instructions to manage the on-going process of records management.

AUDIT RECOMMENDATION:

Written policies and procedures allow higher-level management to set controls over processes to ensure that operations are effective and efficient and procedures safeguard assets and information. 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. Policies and procedures also serve as a training tool for staff and provide consistency. Properly implemented, policies and procedures assist to ensure that processes are occurring as management intends.

These policies and procedures should include safeguarding of sensitive information and record retention for imaged, paper documents, and working copies. We recommend that written policies and procedures be developed and implemented with the assistance of District staff.

DISTRICT RESPONSE:

Management will follow Auditor's recommendation by developing the recommended policies and procedures in all described areas of concern listed above. District Management anticipates that all written policies and procedures pertaining to this audit will be completed by December 1, 2011. |