Office of Audit & Compliance

THE UNIVERSITY OF TEXAS AT DALLAS
800 West Campbell Rd., ROC 32, RICHARDSON, TX 75080 (972) 883-2233

September 12, 2014

Dr. David Daniel, President,
Ms. Lisa Choate, External Chair of the Audit and Compliance Committee:

We have completed an audit of the OnBase application as part of our fiscal year 2014 Audit Plan, and the report is attached for your review. The audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The objectives of the audit were to ensure that the controls over the OnBase System are adequate to ensure that access to data is properly safeguarded and operational processes are efficient and effective.

Overall, we found that controls within the application should be strengthened by improving information technology processes. The attached report details recommendations that will enhance compliance and internal controls.

Management has reviewed the recommendations and has provided responses and anticipated implementation dates. Though management is responsible for implementing the course of action outlined in the response, we will follow up on the status of implementation subsequent to the anticipated implementation dates. We appreciate the courtesies and considerations extended to us during our engagement. Please let me know if you have any questions or comments regarding this audit.

Toni Stephens
Executive Director of Audit and Compliance

UT Dallas Responsible Parties:
Dr. Sue Taylor, Associate Vice President, Director Enterprise Application Services

Members of the UT Dallas Audit and Compliance Committee:
External Members:
Mr. Bill Keffler
Mr. Ed Montgomery
Ms. Cynthia Trochu
Dr. Hobson Wildenthal, Executive Vice President and Provost
Dr. Calvin Jamison, Vice President for Administration
Mr. Terry Pankratz, Vice President for Budget and Finance
Dr. Andrew Blanchard, Vice President for Information Resources and Chief Information Officer, Dean of Undergraduate Studies
Dr. Bruce Gnade, Vice President for Research
Dr. Darrelene Rachavong, Vice President for Student Affairs
Mr. Timothy Shaw, University Attorney

The University of Texas System:
Dr. Pedro Reyes, Executive Vice Chancellor for Academic Affairs
Alan Marks, Attorney
Mr. J. Michael Peppers, CIA, CRMA, CPA, FACHE, Chief Audit Executive
Ms. Moshmee Kalamkar, CPA, CIA, Audit Manager

State of Texas Agencies:
Legislative Budget Board
Governor's Office
State Auditor's Office
Sunset Advisory Commission

Executive Summary

OnBase, Report No. 1501

Audit Objective and Scope: To ensure that the controls over the OnBase System are adequate to ensure that access to data is properly safeguarded and operational processes are efficient and effective.

Audit Results:
The audit resulted in no recommendations considered as priority, or significant, to University operations. However, we offer the following recommendations to enhance the security and efficiency over the OnBase system processes:

Recommendations	*Estimated Implementation Date*
(1) Secure Confidential Information	Implemented by Enrollment Management prior to report issuance
(2) Implement Encrypted Disk Groups	January 1, 2015
(3) Enhance Operational Efficiency	January 1, 2015
(4) Limit Access to the OnBase Environment	December 31, 2014
(5) Strengthen Controls Around Service Accounts	October 1, 2014
(6) Improve Data Management	December 31, 2015
(7) Improve Governance Activities	December 31, 2015

Conclusion: Controls within the OnBase application can be strengthened. Implementation of the recommendations outlined in this report will help the enhance access and the efficiency of existing processes.

Responsible Vice President:	**Responsible Party:**
Dr. Andrew Blanchard, Vice President for Information Resources, Chief Information Officer, and Dean of Undergraduate Studies	Dr. Sue Taylor, Associate Vice President, Director Enterprise Application Services (EAS)

Staff Assigned to Audit:
Ali Subhani, CIA, CISA,GSNA, IT Audit Manager; Colby Taylor IT Staff Auditor

Table of Contents

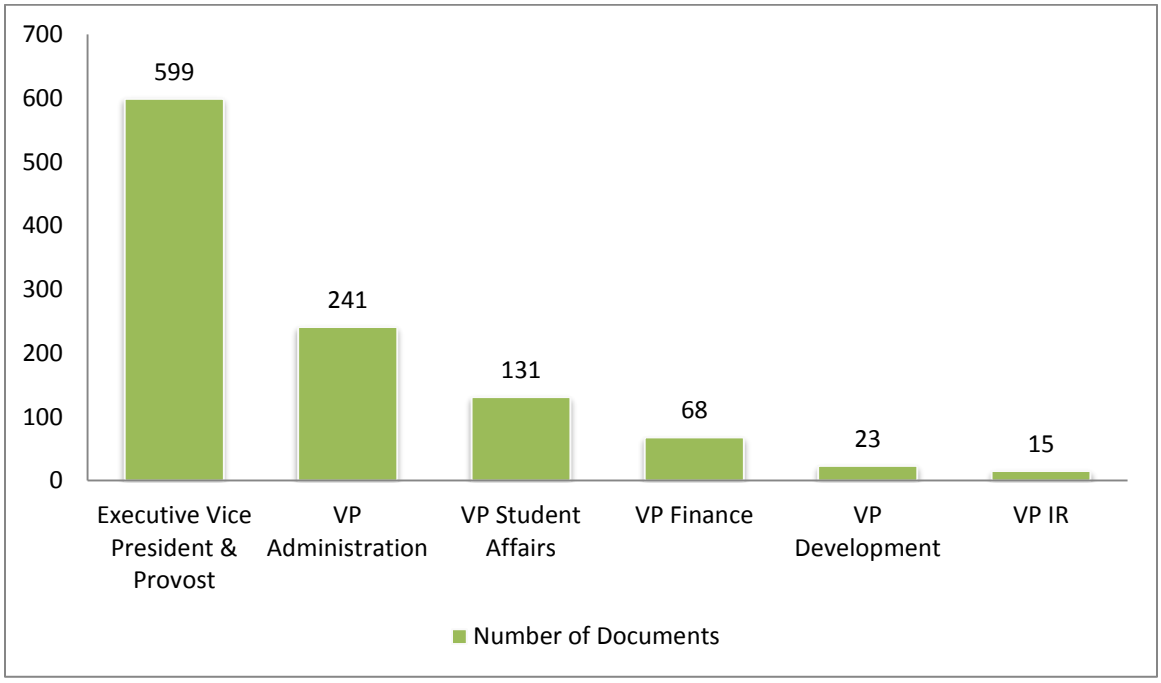
Background

Enterprise Application Services (EAS), within the Office of the Information Resources (IR), is responsible for administering the OnBase application (OBA) on campus. There are also functional users outside of the EAS team throughout the University that also perform certain technical tasks. The functional users are responsible for designing the business processes that will be implemented within OnBase. OnBase is an enterprise content management (ECM) solution that is used to store digitized academic and administrative business documents. OBA offers functionality to store, track, and process electronic documents, as well as to enhance workflow processes. Implementation of an ECM allows organizations to:

- **Reduce operating costs –** As the need for printing, transporting, and storing paper are eliminated. Additionally, productivity is gained as documentation can be transferred instantly.
- **Improve customer service** – As documents are not stored in multiple places, and real-time visibility into status of requests and transactions is gained.
- **Minimizes risk** – As the application allows for enforcement of security policies, and tracks all access and activities.

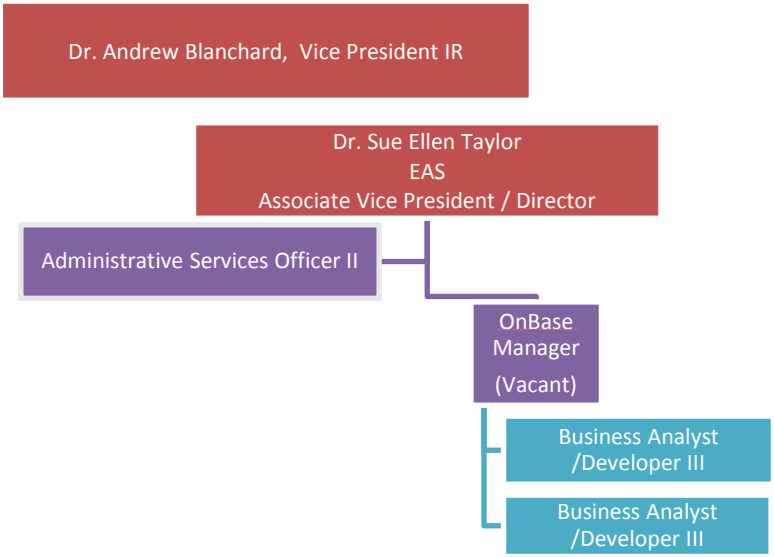
At UTD, approximately 1,099 document types are being scanned into the application. Currently, 765 individuals utilize OnBase.

ONBASE DOCUMENT TYPES



The OnBase Manager, who will report to the Associate Vice President/Director for EAS, will be responsible for leading the OnBase Team once hired. In the absence of the Manager, the Campus Solutions Manager has overseen management of the OnBase application. OnBase was implemented at UTD in calendar year 2006. At the beginning of the audit, the hardware that supported the OnBase application was upgraded, and new environments for testing and development were also created during the upgrade process.

OnBase Organizational Chart



Audit Objective

To ensure that the controls over the OnBase System are adequate to ensure that access to data is properly safeguarded and operational processes are efficient and effective.

Scope and Methodology

The scope of this audit was Fiscal Year 2014 to date, and our fieldwork concluded on July 31, 2014. To satisfy our objectives, we performed the following:

- Interviewed personnel to gain an understanding of the OnBase application.
- Reviewed the licensing agreement with the vendor.

- Gained an understanding of the process through which faculty and staff are provided access to the OnBase application.
- Evaluated authentication controls within the application and the database.
- Reviewed data security controls.
- Analyzed current processes to identify opportunities to improve efficiency.

Where applicable, we conducted our examination in accordance with the guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing*. The *Standards* set criteria for internal audit departments in the areas of independence, professional proficiency, scope and performance or audit work, and management of the internal auditing department.

Audit Results and Management's Responses

Overall, we found that controls over the OnBase system can be strengthened. Our audit work indicated that the following controls currently exist:

- Access logs exist to identify users that are logging into the application.
- An authentication process for user accounts is functioning as intended.
- Separate environments have been recently implemented to segregate the production environment from test and development.
- The server supporting the application was current on operating system updates.

A priority recommendation is defined as one that may be material to operations, financial reporting, or legal compliance. This would include an internal control weakness that does not reduce the risk of irregularities, illegal acts, errors, inefficiencies, waste, ineffectiveness, or conflicts of interest to a reasonable low level. We have **no priority recommendations** resulting from this audit; however, the following recommendations will help strengthen information technology processes.

Audit Recommendations

(1) ***Secure Confidential Information***

According to TAC 202.75 2(A)1, " *Confidential information shall be accessible only to authorized users. An information file or record containing any confidential information shall be identified, documented, and protected in its entirety in accordance with §202.70(1) of this chapter.*" During the audit one public folder managed by Enrollment Management was identified that included confidential personally identifiable information such as social security numbers, names, UTD ID's, birth dates, addresses, and test scores. Public folders are accessible to any individual that has access to the internal network. Based on the analysis that performed the number of students or applicants whose data was at risk were:

- 116,523 Social Security Numbers.
- 356,652 Individual Taxpayer Identification Numbers (ITIN).

The data was not stored within the OnBase application, but was rather housed on a server controlled by Enrollment Management. An attempt was made to determine whether the information had been compromised. However, the logs that would be required to validate that information had not been breached, were not available for the entire period inappropriate security privileges had been applied to the folder. Based on the analysis of the logs that were available, and after input from the Chief Information Security Office (CISO), a decision was made that the incident was not a breach of security as no documentation that indicated unauthorized acquisition of computerized data was identified.

Recommendation: Security privileges for the folder should be adjusted by Enrollment Management so that only individuals with a valid business have access to the personally identifiable data.

Estimated Date of Implementation: *Implemented prior to report issuance as a result management response was not requested.*

Person Responsible for Implementation: *Wray Weldon, Enrollment Management*

(2) ***Implement Encrypted Disk Groups***

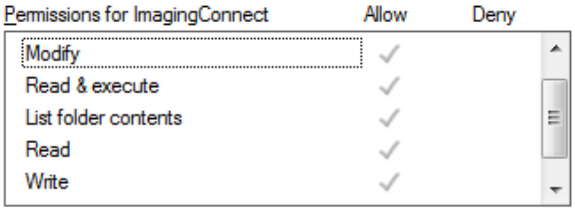
Encrypted Disk Groups offer an additional layer of security for data that is stored in the OnBase application. They allow for automatic encryption of documents as they are imported into OnBase and stored on a file server. This makes the data indecipherable if it is accessed from outside the OnBase application. It was noted that encrypted disk group functionality was not being utilized as the institution did not have licenses for the technology. The following data was noted as being stored in unencrypted disk group(s):

- Social Security Numbers.
- Bank Account Information.
- Employee and Student Addresses.
- Personal Banking Data such as account numbers and routing data.
- FERPA protected data such as test scores, grades, and transcripts.
- Vendor payment documentation that identifies patient names that medical equipment is being purchased for.

The dataset must be protected in line with FERPA, TAC 202, and HIPAA requirements.

Due to the manner in which security privileges were applied on the file server where OnBase data is being stored, currently all 765 current OnBase users have the ability to directly view or delete the underlying data without logging into the application. A user

would require prior knowledge of the network path where the data is saved in order to directly access data from the file server. The following security privileges were noted on the shares where OnBase data was being stored:



Additionally, a user could also copy or delete large data sets off of the file server and save on external media. Currently there is no logging that is in place to detect abuse of security privileges on the file server. Without adequate logging, individual accountability cannot be established. According to TAC 202.75[1] *"(A) Information resources systems shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or effect the release of confidential information. (B) Appropriate audit trails shall be maintained to provide accountability for updates to mission critical information, hardware and software and for all changes to automated security or access rules*."

Recommendation: Management should

- Implement encrypted disk group functionality in order to achieve compliance with requirements that require adequate protection of sensitive data that is housed on the file server that supports OnBase.
- Revise folder security privileges to better restrict sensitive data.
- Additionally, logging of high risk activities within the OnBase environment should be performed. A formal review process for the logs should also be implemented.

Management's Response: The access vulnerability identified by the audit pertains to an Onbase client that has reached end-of-life. Multiple departments have been migrated to the new Unity Client with enhanced security capabilities. Additional security is being considered at the database and server levels as well as the option to set up logging of access by any user, system files or system administrators.

Estimated Date of Implementation: *January 1, 2015*

Person Responsible for Implementation: *Dr. Sue Ellen Taylor*

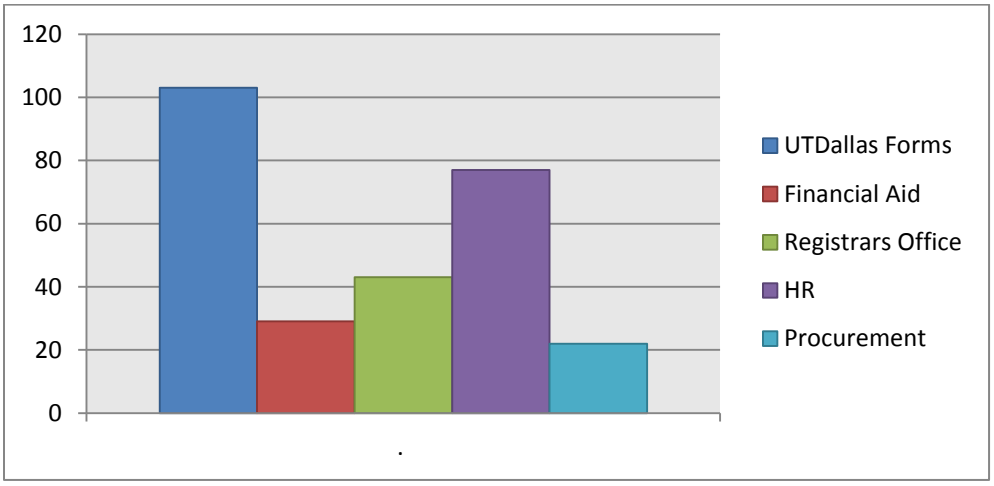
[1] http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=75

(3) ***Enhance Operational Efficiency***

The OnBase application is being used for academic and non-academic populations throughout the campus. However, many business processes are still paper based. Based on a review of forms that are utilized across the institution, it was noted that there is potential for transitioning current paper based business processes into the OnBase application. Such a transition would help streamline business processes across the institution and result in significant cost saving. Best practices would suggest utilizing technologies that improve operational efficiencies so that limited resources can be adequately utilized.

To demonstrate the potential efficiencies that can be gained, we counted the number of paper forms that are currently being utilized by a sample number of departments, the following was noted:

NUMBER OF PAPER FORMS UTILIZED OUTSIDE OF ONBASE



Additionally, it was noted that currently the documentation that is being retained in OnBase appears to be scanned copies of paper documentation that is received. The relevant data must be manually extracted from the paper documentation by employees as they manually enter the data into application after reviewing the documentation. The OnBase application offers the following functionality:

- **Electronic Forms / Unity Forms** – can be directly configured in the application reducing the need for printing paper documentation, and later scanning into the application. Implementation of electronic forms offer key benefits such as completeness at the point of entry, processes are triggered upon form submission and automatically routed to the right place reducing the frustration that is caused by loss of paper forms as they are routed.

- **Optical Character Recognition (OCR)** – allows relevant data that is present in an image to be automatically translated into a format that can be searched. The institution is currently licensed for the free version of the OCR package which does not allow accurate conversion of data consistently, unless the forms that are being scanned in are in a very specific format. There are additional licensing costs in order to make use of the package that offers more accurate OCR functionality.
- **Workflow** – allows for the data within the application to be electronically routed to the appropriate department for approval.

During the audit process it was observed that the application functionality noted above was not being utilized. As a result, the full benefit of implementing an ECM has not being realized. Additionally, a manual scanning process requires staff to be dedicated to complete the scanning jobs which does not appear to be the most efficient use of resources as the application offers functionality to automatically import data if electronic forms are correctly designed and set up.

Additionally, the manual scanning of forms by the user department into OnBase negatively impacts the speed with which data is available within the application. For example, voucher documentation is currently being housed in OnBase; however, there is a delay of 7.5 months between when a transaction is processed in PeopleSoft and when the corresponding documentation is available for review within OnBase.

Lastly, OnBase Integration for Oracle PeopleSoft Enterprise (OIOPE) allows users to view and search OnBase data directly from the PeopleSoft application. The OIOPE also automatically syncs data between the two applications. Currently, OIOPE is not implemented. However, according to the Associate Vice President, Director of EAS it is on the project list to be deployed in the future when development and consulting resources are available to do the work.

Recommendation: Management should:

- Develop a committee that has adequate representation from across campus that will oversee transition of the current paper forms that are utilized and convert them into electronic forms. The process owners of the paper forms should be required to convert the forms into OnBase with appropriate support from EAS.
- Adjust current business processes so that the full potential benefit of implementation of an ECM can be gained.
- Implement application functionality that will enhance the efficiency of operations.
- Consider implementation of OIOPE.

Management's Response: *1. Future plans have included the establishment of a campus-wide committee to review electronic signatures, evaluate business processes, and explore ECM solutions. The oversight committee can recommend electronic signatures, review and evaluation of business processes, and evaluate ECM solutions.*

2. Not all forms are conducive to electronic processing. Significant change in policy regarding the use of electronic signatures must be addressed before all forms can be converted to electronic format. 3. Evaluation for a campus-wide assessment related to the capabilities of eforms will be addressed with the onboarding of new management. 4. Due to limited resources, the implementation of OIOPE has not been identified as a priority by PeopleSoft governance at this time.

Estimated Date of Implementation: *January 1, 2015, as it will require both developer time and consulting resources from Hyland*

Person Responsible for Implementation: *Sue Ellen Taylor*

(4) ***Limit Access to the OnBase Environment***

According to TAC 202.75 3 (B)[2], *"A user's access authorization shall be appropriately be modified or removed when the user's employment or job responsibilities within the institution of higher education change."* During the audit the following opportunities to limit access to the application were noted:

- 104 individuals currently have access to the OnBase application even though they had not logged into the application for more than 365 days.
- Four accounts had access to the OnBase database even though they had not logged into the database for more than 30 days.
- Three individuals were noted as having maintained access to documentation within the OnBase application even though they were not current employees.
- Instances were noted where the employees privileges within OnBase were not updated once the employee had transferred to a new department.
- The Manager user group within the application is a privileged access group that allows access to a significant number of documents within the OnBase application. Four individuals were identified that did not have a business need for the privileges that were being provided by membership in the user group.
- The ImagingADMINS user group within the application is a privileged user group that allows access to every document and the ability to modify configurations within the OnBase application. 5 individuals were identified with membership in the ImagingADMINS user group even though there was no business need for them having such privileges.

Without tighter control around user management within the application the institution risks non-compliance with state law.

[2] http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=75

Recommendation: A process to periodically review individuals that currently have access to the OnBase application should be put in place. Additionally, privileges for users should be limited to what is required to perform their job responsibilities.

Management's Response: *Management is in agreement with the recommendation. Quarterly reviews are being implemented.*

Estimated Date of Implementation: *December 31, 2014*

Person Responsible for Implementation: *Sue Ellen Taylor*

(5) ***Strengthen Controls Around Service Accounts***

Service accounts can be described as accounts that do not correspond to an actual person. They are often configured at the time applications are originally set up so that certain automated processes and tasks can take place without minimal user intervention. Hackers will often target service accounts because they normally provide a higher level of access in comparison to a normal user account. During a review of the controls around service accounts, it was noted that:

- Passwords for service accounts are not being changed in line with university policies.
- The OnBase team was not aware of 18 service accounts that we identified that had privileged access.
- Documentation that detailed the processes that were run under each service account, and the individual with ownership of the account, did not exist at the time of the audit.

Service account membership within privileged user groups should be restricted. According to TAC 202.75 d),[3] "*Information resources systems which use passwords shall be based on industry best practices on password usage and documented institution of higher education risk management decisions*." Additionally, according to UTD Information Security Manual,[4] "*Passwords for accounts associated with Category I, II & III data types (see Data Classification Standards): Must:*

- *Be at least eight characters in length.*
- *Contain at least three of the following within the first 8 characters: upper case letters, lower case letters, numbers, and special characters (e.g. ! @ # $ % & * ( ) - + = < >)*
- *Be changed semi-annually."*

[3] http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&ti=1&ch=202&rl=75
[4] http://www.utdallas.edu/infosecurity/documents/SecurityOperationsManual.pdf

Recommendation: Management should ensure that controls around service accounts be enhanced by:

- Ensuring passwords are being changed in line with university policies.
- Better tracking the accounts that are currently active.
- Maintaining documentation of the processes that are being run within service account and assigning formal ownership of the account to one individual.
- Limiting service account membership within privileged user group as much as possible

Management's Response: *Timelines for changing service account passwords will be adhered to and active accounts will be reviewed. Ownership of the service account will follow EAS standard policy of having a primary account owner as well as a secondary backup.*

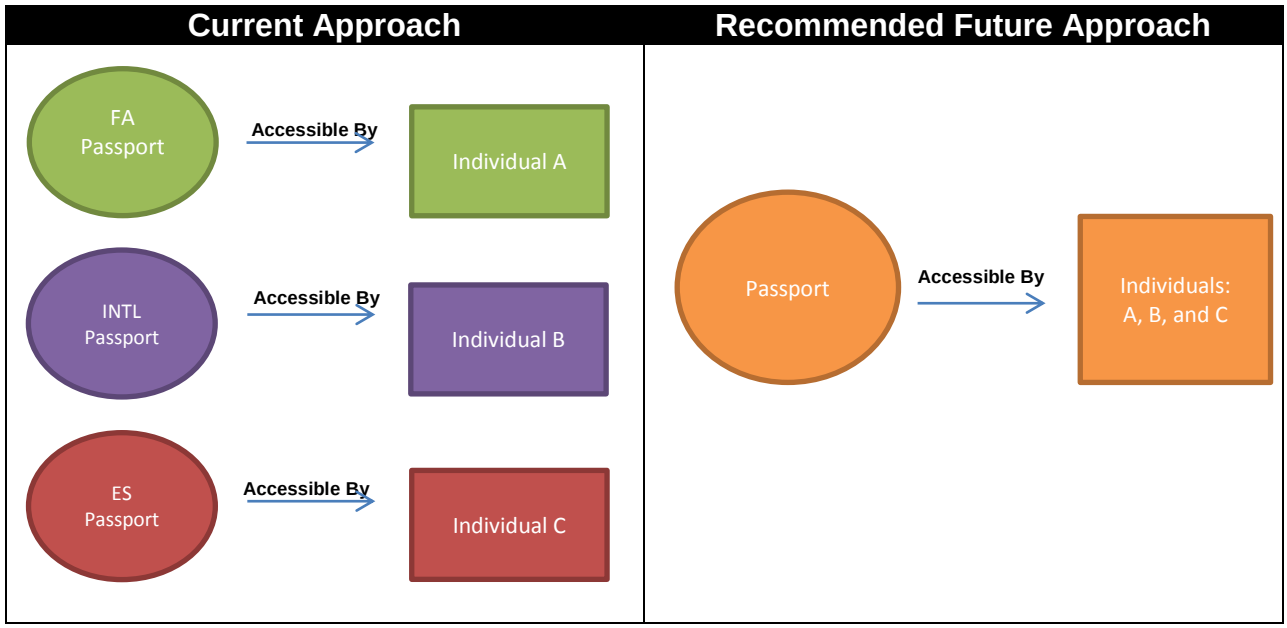
Estimated Date of Implementation: *October 1, 2014*

Person Responsible for Implementation: *Sue Ellen Taylor*

(6) ***Improve Data Management***

During the audit the following opportunities to improve data management were noted:

- Data that must be accessed by multiple departments is being scanned into the application under different document types creating duplication. For example, the Registrar's Office, Enrollment Services, Financial Aid, and the International Student Services Office all have a business need to retain copies of an individual's passport. However, rather than creating one document type and giving individuals from different department access to that document; multiple document types have been created with the same underlying data.



Under certain instances this approach may be due to the fact that certain documents have differing record retention requirements across departments.

- According to UTS 165 14.1 b2, "*the institution shall use and collect social security numbers only as reasonably necessary for the proper administration or accomplishment of the institution's business, governmental, education and medical purposes.*" The application is currently maintaining social security information on forms from the period when social security numbers (SSN) were the primary key for individuals. For example, Computer Account Request (CAR) forms with the SSN are currently in the application from the period beginning in 2006.
- Data is being maintained for longer than the record retention requirements of the university. This results in the institution having to make investments in additional storage infrastructure. Additionally, it was noted that current disk group utilization for select disk groups was very close to the maximum amount of space that could be utilized by the disk groups. Once space on the disk groups is exhausted, the application performance may be negatively impacted. Currently, functional users are not required to specify the anticipated space needs for the upcoming fiscal year. As a result, IR must support all anticipated space needs of the users without too much advance notice.
- Keywords must be set up when a particular document type is being configured for use within OnBase. Currently, keywords that indicate that confidential data is present in a document are being configured even though the document does not include the particular data set.

Recommendation: Management should:

- Implement a process where an analysis is performed prior to creating new document types. This will ensure that potential duplication of data is minimized.
- Consolidate data types that contain the same underlying data into one document type.
- Only maintain SSN data for individuals if there is a business need for this data. SSN data should be sanitized when it is no longer required.
- Implement a record retention process that is in line with the university's record retention policies.
- Implement a yearly budgeting process where functional owners are required to specify the anticipated space needs for the upcoming year for their document groups. IR should monitor and ensure that departments are staying below the space requirements that they had planned for on a regular basis.
- Ensure that keywords that indicate that confidential data is present are only set up when underlying data supports such a configuration.

Management's Response: *We are in partial agreement with the recommendations. Analysis is completed prior to the identification of new document types to reduce duplication when possible. Unfortunately, a like or similar document type may be used across multiple departments that appears to be the same but may address different retention dates and uses within the departments. Thus it is not always practical to consolidate like documents. OnBase technicians are working with functional departments to deploy automated retention rules based on department, UT Dallas, UT System, State and Federal retention policies which will result in a limited amount of space reallocation. Space allocation is not currently required of OnBase users as the application architecture is designed to dynamically adjust department folders to increase and/or decrease as documents are added and/or removed. Algorithms for determining space requirements and allocations have not been implemented and management of space is expected to improve with the implementation of a standard retention approach. Data owners in academic and administrative departments will need to come to agreement regarding limitations on document storage allocations and define procedures to appropriately address the issue fairly across the campus. All keywords are identified by the data owners in collaboration with the OnBase technicians. Currently business processes do not support a methodology for designating/identifying the use of confidential data as keywords. Instead the business need generally dictate the definition of all keywords.*

Estimated Date of Implementation: *December 31, 2015*

Person Responsible for Implementation: *Sue Ellen Taylor*

(7) ***Improve Governance Activities***

The OnBase application was initially configured in 2006. Due to implementation of higher priority systems such as PeopleSoft, governance of the OnBase application has generally been inadequate. During the audit, the following opportunities to enhance governance around the application were noted:

- Prior to the start of the audit, there were no separate environments that were in place for testing and development. As a result, all changes or new development were directly created and tested within production environment. Currently a formal change management process does not exist.
- There is no published schedule of the development projects that are currently planned for the OnBase application.
- Documentation of business processes that are utilized and the overall architecture that supports the application is generally lacking.
- A documented disaster recovery plan for the application did not exist. IR has an overarching business continuity plan which did not adequately address OnBase according to the OnBase System Administrator.

According to TAC 202.70 [5], "*Information resources shall be available when needed. Continuity of information resources supporting critical governmental services shall be ensured in the event of a disaster or business disruption."*

Recommendation: Management should improve governance activities by:

- Formalizing a change management process.
- Developing a published schedule of planned development projects with the anticipated date of completion and sharing it with the functional leads on a regular basis.
- Improving documentation so that an understanding of the application can be easily gained by an individual in the event of transition.
- Documenting a disaster recovery plan.

Management's Response: *We are in the process of formalizing a change management procedure and establishing an ECM Users Group that will provide oversight and prioritization of projects for the Imaging team. Roles and responsibilities are being reviewed and updated as needed. Disaster Recovery for the application and data has been provided at an off-site location and included in the EAS Business Continuity Plan since 2008 and updated on a regular basis.*

Estimated Date of Implementation: *December 31, 2014*

[5] http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70

Person Responsible for Implementation: *Sue Ellen Taylor*

Auditor's Follow-up Comment: *The EAS Business Continuity Plan was reviewed. While the plan was developed in line with university requirements, it did not include detailed procedures, technical requirements, and logistics for execution of all recovery strategies. The adequacy of the business continuity plans that are being developed will be evaluated during the Business Continuity audit during fiscal year 2015.*

Conclusion

Based on the audit work performed, we conclude that controls within the OnBase application can be strengthened. Implementation of the recommendations outlined in this report will help the enhance access controls and the efficiency of existing processes.

We appreciate the courtesy and cooperation received from the management and staff of within EAS during this audit.