Office of Internal Audit
800 W. Campbell Rd. SPN 32, Richardson, TX 75080
Phone 972-883-4876 Fax 972-883-6846

January 5, 2016

Dr. Hobson Wildenthal, President *ad interim*
Ms. Lisa Choate, Chair of the Institutional Audit Committee:

We have completed an audit of Physical Access Controls Management as part of our fiscal year 2015 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 objective of our audit was to assess applications that are involved in protecting the physical infrastructure of the institution, and evaluate the highest risk applications for compliance with applicable regulations, policies and procedures.

Physical access controls can be strengthened. The attached report details recommendations that will enhance the security and effectiveness of applications that are involved in protecting the physical infrastructure of the institution.

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
Institutional Chief Audit Executive

UT Dallas Responsible Parties:
Chief Larry Zacharias, Chief of Police
Mr. Richard Dempsey, P.E., Associate Vice President for Facilities Management
Ms. Paulina Schleppenbach, Director of Comet Card Office

Members of the UT Dallas Institutional Audit Committee:
External Members:
Mr. Bill Keffler
Ms. Julie Knecht
Mr. Ed Montgomery
Mr. David Crain, Vice President and Chief Information Officer
Dr. George Fair, Vice President for Diversity and Community Engagement
Dr. Gene Fitch, Vice President for Student Affairs
Dr. Bruce Gnade, Vice President for Research
Dr. Calvin Jamison, Vice President for Administration
Dr. Inga Musselman, Acting Provost
Mr. Terry Pankratz, Vice President for Budget and Finance
Mr. Tim Shaw, University Attorney, ex-officio

The University of Texas System:
System Audit Office

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

Executive Summary

Physical Access Controls Management, Report No. 1609

Audit Objective and Scope: The objective of our audit was to assess applications that are involved in protecting the physical infrastructure of the institution, and evaluate the highest risk applications for compliance with applicable regulations, policies and procedures.

The following is a summary of the audit recommendations by risk level. See the Appendix for additional details.

Recommendation	Risk Level	Estimated Implementation Date
(1) Strengthen Controls around the C-Cure Application	**High**	May 31, 2016
(2) Restrict Clearances for Door Readers	**Medium**	May 31, 2016
(3) Enhance Emergency Lockdown Procedures	**Medium**	September 30, 2016
(4) Restrict User Access Privileges within the Application	**Medium**	Implemented November 2015
(5) Enhance Controls around the Key Database	**Medium**	September 1, 2016
(6) Consolidate Applications	**Low**	*Will not be implemented*
(7) Develop Standard for Minimum Physical Access Controls in New Construction	**Low**	September 1, 2016

Responsible Vice President:

- Dr. Calvin Jamison, Vice President for Administration (1) – (5); (7)
- Dr. Gene Fitch, Vice President for Student Affairs (6)

Responsible Parties:

- Chief Larry Zacharias, Chief of Police (1) – (4)
- Mr. Rick Dempsey, Associate Vice President for Facilities Management (5) (7)
- Ms. Paulina Schleppenbach, Director of Comet Card Office (6)

Staff Assigned to Audit:

Ali Subhani, CISA, CIA, GSNA, IT Audit Manager; Colby Taylor, IT Staff Auditor; student interns from the Internal Auditing Education Partnership Program: Janaki Bhupatiraju and Sheron Chakalakal

Table of Contents

Background

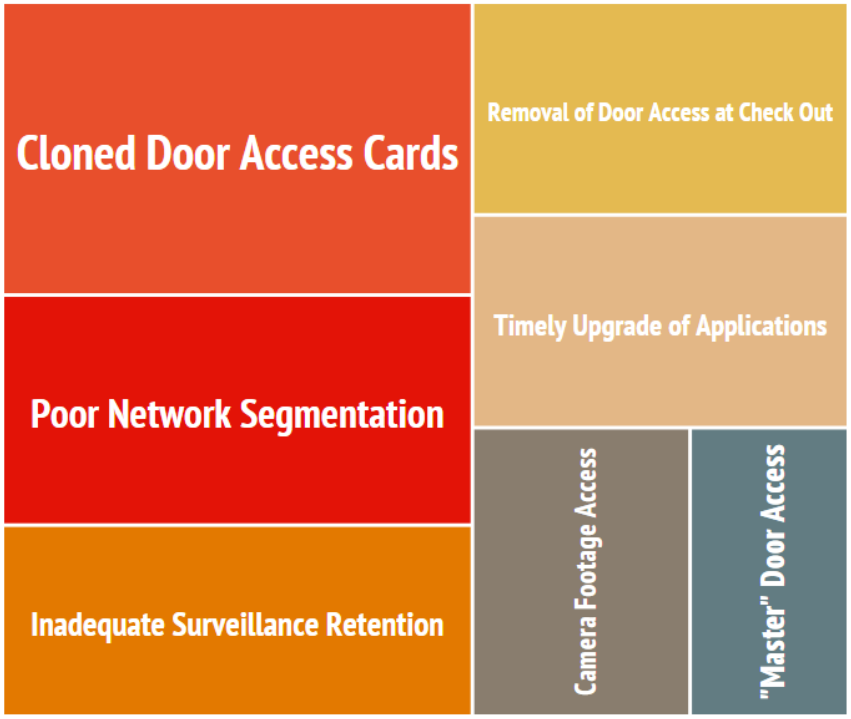
Historically, a building could be secured with a few locks and a dependable security guard. But today's threats are sophisticated, and the security to fight them must be even more so. High tech access control systems—featuring card readers, intelligent video surveillance, electronic locking devices, and the computers that control them—are becoming standard for building security. At UT Dallas, the following three applications help maintain physical security on campus:

- C-Cure – is utilized to manage electronic door access privileges. Comet Card holders are provided physical access to portions of campus through electronic door access readers.

- Salient – is utilized for retention of video surveillance footage from security cameras across campus.

- Physical Key Database – is utilized to manage the keys that are assigned and cut for door access across the campus.

The Police Department (PD), reporting to the Vice President for Administration, administers both applications. Following is a depiction of some of the risks that must be appropriately managed as these applications are operated.



Audit Objective

The objective of our audit was to assess applications that are involved in protecting the physical infrastructure of the institution, and evaluate the highest risk applications for compliance with applicable regulations, policies and procedures.

Scope and Methodology

The scope of this audit was FY 2015 operations, and our fieldwork concluded on October 5, 2015. To satisfy our objectives, we performed the following:

- Investigated the state of the user management within the various applications as well as how user security is being maintained and enforced.
- Determined if controls related to access to the data of the application are executing effectively and efficiently.
- Established if controls related to knowledge management and data monitoring within the applications were in place.
- Investigated the reports that were available to review door access.
- Determined if adequate policies and procedures were in place for effective system management.
- Investigated if adequate controls are present to prevent access to personally identifying information within the applications.

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

Controls
Our audit work indicated that the following controls currently exist:

- Configuration within the door access application that allows for automated locking of doors to occur on a predetermined schedule is in place. This reduces the likelihood that doors will remain unlocked outside of regular business hours.
- Records to support access requests are being maintained consistently. This helps validate that requests were appropriately authorized.
- An informal hardware replacement strategy exists that replaces aged hardware with equipment that is up to date. Such a strategy is in line with prudent financial management as it minimizes the need for big capital outlays at one time.

- Surveillance footage is generally being maintained for a minimum of fourteen days. This appears to be an adequate minimum retention period for retention of surveillance. Based on other institutions this time frame is appropriate and in line with the resources available to the surveillance system.
- Logging that tracks the identity of the individuals that make updates to cards or clearances is enabled.
- Roles with different levels of access privileges within the C-Cure exist and are being utilized.
- A formal process to document and authorize electronic door access requests through campus exists and is being followed. Subsequently, the PD has developed trusted approvers that can authorize access requests for portions of campus.
- In discussions with stakeholders that were involved in the door access application, general consensus was that their needs were being met within the application.

Audit Recommendations

Priority Findings – UT System - A UT System priority finding is defined by the UT System Audit Office as: "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*"[1] We have **no UT System Priority Findings** resulting from this audit.

However, although the above controls are in place, opportunities exist to enhance physical access controls as outlined below.

(1) Strengthen Controls Around the C-Cure Application

Risk Level: **High**★

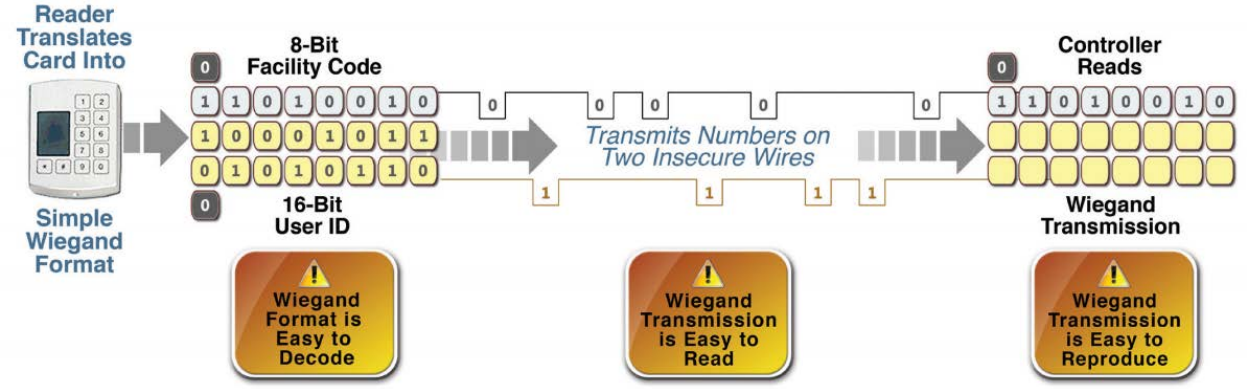
The following observations were made during the audit related to the C-Cure application:

- The institution currently uses contactless HID proximity cards to allow physical access to different areas on campus. HID proximity cards are widely utilized in different industries as security badges. However, HID cards are vulnerable to being easily read, modified and cloned by individuals without having physical possession of the card. This leaves the institution vulnerable as the proximity cards permit access to critical facilities such as data centers and research labs.

HID CARD EXAMPLE

[1] Appendix A defines the risks for all internal audit recommendations.

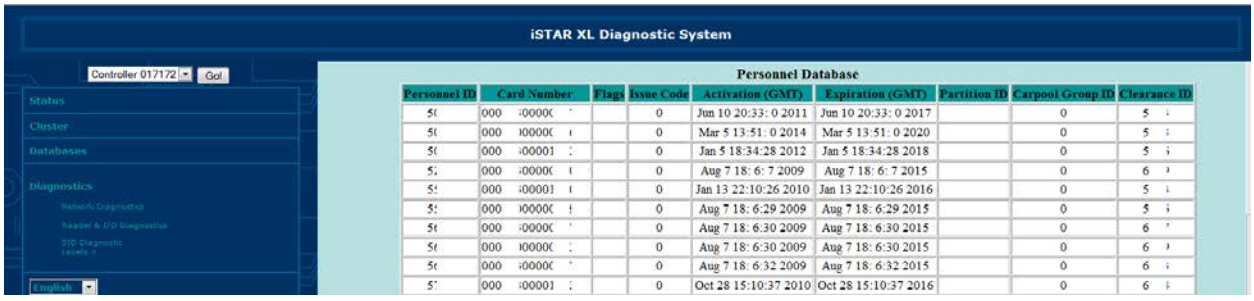
- The current door access hardware that is in place makes use of the Weigand protocol. Weigand can be used to describe a number of different items used within access control systems such as the format in which data is stored on a card, or the protocol which is used to transmit the data. The Weigand protocol is known to have weaknesses such as transmitting the data in an easy to reproduce manner which could allow an unauthorized individual to gain access to facilities.



2

- Network segmentation is a best practice that helps ensures that critical network resources are protected from the general user community. C-Cure related hardware such as door panels and controllers are not adequately segregated from the university-wide network to minimize the risk of abuse to those devices. Access to door controllers would allow an individual to gather personnel clearances, personnel ids and card numbers; data set which would be helpful to a hacker in identifying privileged access that should be duplicated to create a new card.

SAMPLE DATA THAT IS ACCESIBLE DUE TO LACK OF SEGMENTATION



Recommendation: Use of the HID proximity cards and Weigand protocol should be re-evaluated to determine if it aligns with the risk appetite of the institution.

[2] http://multimedia.3m.com/mws/media/833804O/beyond-wiegand-access-control-in-the-21st-century.pdf

Network controls to segregate the C-Cure application and associated hardware from the university wide network should be implemented.

Management's Response: *The decision to transition to a more secure card entry system would have to involve several departments within the University Community that utilized the current card for one purpose or another. As such, all users would need to determine the issues and impact on their area if a transition were to occur or a compromise in existing processes. PD believes it is necessary to assemble a campus work group, consisting of the PD, Internal Audits, Comet Center, Auxiliary Services, University Library, and others to discuss the security risks of the current card technology, how and if that risk can be affectively managed, and the challenges to implementing a new, more secure technology. The work group will determine the scope of the security risk and determine if a new technology should be adopted.*

UTD PD will either ask IR to segregate the CCURE data gathering panels to limited access networks or disable the publicly accessible web page.

Estimated Date of Implementation: *The work group will make its recommendation before the end of May 2016.*

Person Responsible for Implementation: *Daniel Calhoun, PD Applications/Systems Manager*

(2) ***Restrict Clearances for Door Readers***
Risk Rating: **Medium**☆

In order for cardholders to access facilities, the correct clearance(s) must be assigned. During the audit the following opportunities to better manage clearances were noted:

- 1,098 active cards with clearances were noted for individuals that were not currently affiliated with the university.
- Twenty-four individuals were assigned the "All Door Access" clearance without a strong business need; the clearance provides the capability to make use of electronic door access readers in a large portion of campus.
- 38,403 cards were noted as being active for users that were not affiliated with the university. The cards did not have clearances assigned to allow access to any part of campus.

Recommendation: Processes should be put in place to remove clearances and disable access cards when users are no longer affiliated with the university. An annual review should be performed of clearances that grant all door access.

Management's Response: *PD has requested from IR an improved process to disable cards in CCURE when they are disabled in Premisys.*

PD is in discussions with Information Security about improving the employee checkout process and possibly utilizing their eCAT system to grant/revoke door access clearances. PD believes the burden for removing door access must fall on the department requesting door access. PD has also been in contact with UT Dallas Human Resources and has learned that a new exit/separation procedure is being prepared. This procedure in all likelihood would include such things as collection of issued keys, collection of Comet Cards, and could also include CCURE access removal.

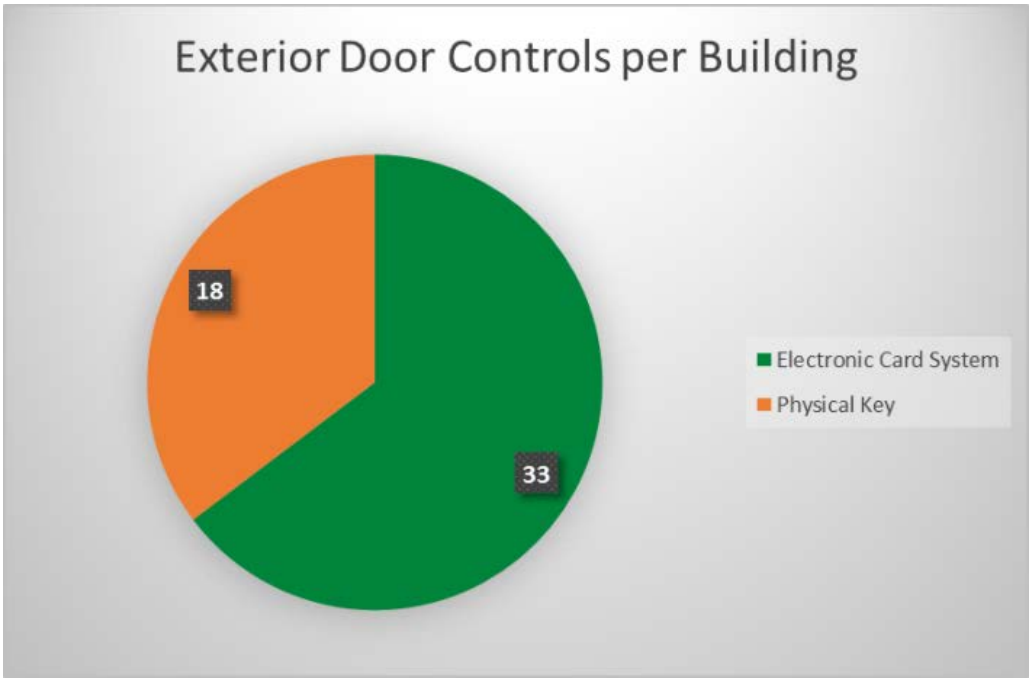
PD performs annual audits on all its clearances; however, the "All Doors" clearance was not included. The "All Doors" clearance will be added to the list of audited clearances.

Estimated Date of Implementation: *May 2016*

Person Responsible for Implementation: *Daniel Calhoun, PD Applications/Systems Manager*

(3) ***Enhance Emergency Lockdown Process***
Risk Rating: **Medium**☆

There are currently differing technologies that are utilized to secure external doors within buildings throughout campus. As a result, physical access to the exterior door of older buildings is generally provided via keys whereas buildings that are newer are being controlled via electronic card access. This lack of uniformity has a negative impact on the timeliness with which PD staff are able to lock down sections of the campus in the event of an emergency.



Additionally, opportunities were noted to better restrict access to classrooms in the event of an emergency as currently classrooms are unable to be locked from the interior of a room consistently. As a result it would be difficult to restrict entry to classrooms in the event of an emergency which may jeopardize the safety of students and faculty members.

Recommendation: A minimum level of electronic card access should be implemented across all campus external doors in order to improve campus safety. Additionally, devices that would restrict access to classrooms in the event of an emergency should be implanted.

Management's Response: *The PD was requested by Dr. David Daniel to obtain quotes for accomplishing this task. Our vendor has provided a quote for $430,000 to complete the project of installing electronic keycard locks on the remaining doors. Funding needs to be identified and it would be anticipated this would be at least a six-month completion project.*

Estimated Date of Implementation: *September 2016*

Person Responsible for Implementation: *Daniel Calhoun, PD Applications/Systems Manager*

(4) ***Restrict User Access Privileges within the Application***
Risk Rating: **Medium**☆

Adequate application controls are vital for safeguarding and maintaining the integrity and availability of the institution's key information technology infrastructure. During a review of the C-Cure application the following opportunities to further restrict privileges within the applications were noted:

C-Cure application

- Out of 12 administrator accounts, administrative privileges on seven different accounts that are utilized by outside contractors is excessive; as contractor access is currently not limited to a temporary period when work is actually being performed.
- Eighteen users who were not currently affiliated with the University had privileges to create personnel and modify user door clearances within the Residence Hall.
- One hundred and twelve student workers were noted as having privileges to issue temporary door access cards to individuals that may have misplaced their original card within the Residence Hall. This privilege is of high risk as it provides the capability to issue access to any student room within the Residence Hall.
- Seventeen individuals were noted as maintaining privileges that would have been required to carry out their prior job responsibilities. The privileges for these individuals were not updated when their job responsibilities changed.
- One shared account with administrative privileges was noted within C-Cure.

Recommendation: A process should be put in place to perform a periodic review of accounts with create and modify privileges. Contractor accounts should be disabled when not in use. Lastly, the privileges for student workers within the Residence Hall should be further limited so that they do maintain the privileges to issue temporary door access cards.

Management's Response: *PD disagrees with limiting contractor accounts. The door system encompasses over 1700 doors and 1900 inputs. Our security vendor has separate technicians assigned to new installs versus service calls. To properly and efficiently maintain and support the system, these technicians need access to CCURE. In fact, the new install technicians are working on our CCURE system almost every day.*

After consultation with Student Housing administrators, the privilege for student workers to issue new cards has been removed. With more staff on call at all times, they believe this privilege is no longer required.

The shared account access is intentional. To ensure the system's function in the event of administrative turnover, the system utilizes the shared account. The password for this account is only shared with the two PD CCURE administrators.

Estimated Date of Implementation: *Already completed as of November 2015.*

Person Responsible for Implementation: *Daniel Calhoun, PD Applications/Systems Manager*

(5) Enhance Controls around the Key Database

Risk Rating: **Medium**☆; Risk Factor: **Information Security**

During the audit, the following opportunities to enhance controls around the key database were noted:

- Social Security Numbers (SSN) for approximately 10,000 individuals are stored within the key database without any business need for retaining the data. While the data is restricted to a select group of 12 employees, we noted that there were five users who had access to the database who would not require access to the key database to perform their job duties.
- The key database requires individuals with access to it to login through a security page created and maintained within the Microsoft Access database. This mechanism to protect access is inherently week as users can easily circumvent the login page by employing a key combination that allows users to login without any password. The key combination is widely documented in online help forums.
- Data integrity issues were noted within the key database. As a result, it was difficult to fully validate the keys that had been issued to individuals.

During a review of key assignments, the following observations were noted:

- 137 master keys were issued to 38 employees who were no longer affiliated with the university. In addition, there is currently no formalized notification to senior management whenever master keys are lost or not returned after an individual's affiliation with the university has ended.
- 1,069 potentially missing keys were identified based on the key status that was documented within the key database. Additionally, 10,439 keys were noted as having been returned; however the return process was not consistently followed as there were no comments within the key database to validate whether the keys were lost, retired or reissued which made it difficult to confirm the key status.
- 81 master keys were issued to one individual; the only identifying piece of information for the individual within the key database was a Texas driver's license. As a result we were unable to fully substantiate the individual's affiliation with the university and subsequently their need for master keys.
- When employees terminate employment or transfer to another area on campus, the department should initiate the checkout process. This electronic system notifies the Key Shop that an employee should turn their keys in before leaving the University. Internal Audit recommended that the process be improved in May 2014, and the President formed a committee, led by the Office of Administration, to review the existing process and recommend improvements.

Recommendation: Confidential data that is not required for any business purpose should be removed from the application and database. Access to confidential data that must be maintained due to a legitimate business purpose should be limited according to job responsibilities.

Additionally, the key return process in Facilities Management should be improved by adding a consistent tracking mechanism to identify when a key is not returned or is lost. Also, an annual review of all master key assignments should be implemented. Lastly, the checkout process should be improved, as recommended by Internal Audit in May 2014.

Management's Response:

- *Facilities Management Key Shop has since deployed a new key system database tied to HR. All social security numbers have been scrubbed and are no longer a part of this system.*
- *Since this audit, Key Shop has deployed a new database with stricter security controls.*
- *Working with Information Security, FM is preparing to deploy a new tracking system that will allow for multiple follow-ups when keys are not returned in a timely manner. FM is also working on a key audit to be performed twice per year to confirm that the keys issued are still in the possession of the person they were issue to.*

- *We will implement a consistent method for tracking key returns in the new key system.*

Estimated Date of Implementation: *September 1, 2016*

Person Responsible for Implementation:
Key Management System: Kelly Kinnard, Director of Physical Plant Services
Checkout Process Improvement: Cris Aquino, Director, Office of Administration

(6) Consolidate Applications
Risk Rating: **Low**

During the audit the following observations were made:

- Premisys (PSYS) application - is utilized for the design and printing of the Comet Cards. The application is managed by the Comet Card department and costs $1,700.
- C-Cure application - also offers the functionality to design and print identification cards.

Through the audit process the Office of Internal Audit attempted to bring key stakeholders together to determine if the functionality that was utilized within the PremiSys could be provided by the C-Cure. However, Internal Audit was unsuccessful in holding a meeting to formally validate the functionality that was available within C-Cure as some stakeholders expressed concerns at the need for a meeting. Based on Internal Audit's limited review of the documentation that was provided by the C-Cure vendor the application would offer all the functionality that is utilized within Premisys. Consolidations of the applications would offer the following benefits:

- Reduced software licensing costs.
- Reduced hardware costs as separate hardware for the different applications would not have to be maintained.
- Reduced maintenance costs as support personnel would not have to maintain two separate applications.
- Reduce need to maintain the integrity of data feeds from Premisys and C-Cure

Efficient use of limited state resources is necessitated to effectively meet external stakeholder expectations.

Recommendation: Determine if C-Cure application can offer functionality that is currently being utilized within PremiSys. Subsequently, transition from PremiSys to the C-Cure application depending on results of the research.

Management's Response: *As a result of the analysis and evaluation of vendor documentation of Ccure features performed by IR and Card Office and based on this review, it seems highly unlikely that moving to a different system at this time would benefit the campus financially or procedurally. Extensive research and analysis was performed which considered multiple products including CCure prior to the selection and purchase of Premisys. The Premisys application provides necessary amount of flexibility and features resulting in highly efficient way for our office to service the campus needs.*

Estimated Date of Implementation: Will Not Implement

Person Responsible for Implementation: *Paulina Schleppenbach, Director Comet Card Office*

Auditor Comment: *An objective assessment of the functionality that is offered by the application now would make it clear that it is a much different application than what it was when we initially implemented PremiSys. It remains clear that the institution continues to maintain two separate applications (Premisys and C-Cure) which are designed to offer the same functionality i.e. identity card printing and managing electronic door access.*

(7) ***Develop Standard for Minimum Physical Access Controls in New Construction***

Risk Rating: **Low**★

The Facilities Management team has standards[3] that must be followed when new buildings are being constructed on campus. After review of the standards, it was noted that chapter 28, which related to electronic safety and security, did not specify any requirements related to minimum physical controls for new construction that takes place. As a result, during construction of new buildings when the project runs into budgetary constraints, physical access controls are at times minimized to keep the project within the budget. Additionally, the Police Department is not provided the mandate to enforce implementation of physical controls at the time new construction projects are planned.

Recommendation: Develop electronic safety and security standards and incorporate within UT Dallas Design Guidelines and Construction Standards. Ensure the Police Department has authority to enforce implementation of physical control standards that are developed.

Management's Response: *UT Dallas currently has a contract with Siemen's Building Access to provide card access systems and controls along with video security. They have been engaged to provide a campus specific specification for all future installations. This specification will be provided to design teams and strictly enforced by Facilities Management.*

[3] https://www.utdallas.edu/facilities/ut-dallas-design-guidelines-construction-standards/

Estimated Date of Implementation: *September 1, 2016*

Person Responsible for Implementation: *Kelly Kinnard, Director Physical Plant Services*

Conclusion

Based on the audit work performed, we conclude that controls within C-Cure, Salient, and the Key Shop database can be strengthened. Implementation of the recommendations outlined in this report will help enhance access controls and the efficiency of existing processes.

We appreciate the courtesy and cooperation received from the management and staff in the Police department and the Key Shop as part of this audit.

Appendix: Definition of Risks

Risk Level	Definition
Priority	High probability of occurrence that would significantly impact UT System and/or UT Dallas. Reported to UT System Audit, Compliance, and Management Review Committee (ACMRC). Priority findings reported to the ACMRC are defined as "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*"
High	Risks are considered to be substantially undesirable and pose a moderate to significant level of exposure to UT Dallas operations. Without appropriate controls, the risk will happen on a consistent basis.
Medium	The risks are considered to be undesirable and could moderately expose UT Dallas. Without appropriate controls, the risk will occur some of the time.
Low	Low probability of various risk factors occurring. Even with no controls, the exposure to UT Dallas will be minimal.