INTERNAL AUDIT

Utility Billing System & Parks RecTrac System Access Control Audit

Original Prepared by

Craig Hametner, CPA, CIA, CISA, CMA, CFE
City Auditor

And

Follow-Up Done by

Michelle Tressler, CIA
City Auditor

September 26, 2016
Report 201503

Table of Contents

Authorization

The City Auditor has conducted an Access Control audit on the Utility Billing System and Parks RecTrac Systems. This audit was conducted under the authority of Resolution #2013-51 and in accordance with the Annual Audit Plan approved by the League City, City Council in Resolution #2014-27.

Objective

The objective of this audit according to the Annual Audit Plan was to determine if appropriate access controls are in place.

Scope and Methodology

The City Auditor conducted this audit in accordance with Generally Accepted Government Auditing Standards except this audit function has not had an external peer review. Those standards require planning and performing the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. The City Auditor believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

The scope of this audit is FY15.

The sampling methodology is discussed in Exhibit A and the reliability and integrity of information is discussed in Exhibit B.

To adequately address the audit objectives and to describe the scope of work on internal controls, the City Auditor has:

- Reviewed periodicals, contracts, articles and authoritative pronouncements about access controls
- Inquired with Vermont systems (Parks RecTrac), Sungard H.T.E. (Utility Billing) and staff members
- Examined access control lists from both the Parks RecTrac System and the Utility Billing System
- Examined Termination Lists from Human Resources
- Examined Audit Logs

The deficiencies in internal control that are significant within the context of the audit objective and based upon the audit work performed are stated in the Opportunities for Improvement (OFI) section starting on page 4.

Background

Controlled Access Based on the Need to Know is one of the 20 Critical Security Controls according to the Council on Cybersecurity.[1]

According to the National Institute of Science and Technology,[2] access control is the means by which access ability is explicitly enabled or restricted in some way.

Access Control attempts to address three important questions:

- Who has access to what information?
- Is the access appropriate for the job being performed? and,
- Is the access and activity monitored, logged, and reported appropriately?[3]

Why is this important ---- "Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users can intentionally or unintentionally read, add, delete, modify, or exfiltrate data or execute changes that are outside their span of authority."[4]

The City Auditor chose two systems of the city that have impact in providing the citizens with a public service. They were the Utility Billing system and the Parks RecTrac system.

The Utility Billing System provides a vital function to the city. Water, sewer, connection fees, reconnection fees, late fees, meter sales all are processed through this system. It is estimated that over $31,000,000 will be processed through the utility billing system in FY15. Approximately 54 employees have access to this system.

The Parks RecTrac system processes city pool rental fees, pool concessions, swimming lessons, facility rental fees, Rec Program Fees, summer camp fees, pool fees, and pool season pass fees. For FY14, approximately $560,000 was processed through this system. Approximately 28 employees have access to this system.

Typically, access rights are role-based; meaning, certain groups of employees or departments are provided access rights based on how they use the system. For

[1] Reference http://www.counciloncybersecurity.org/critical-controls/
[2] Reference NIST Special Publication 800-12 (An Introduction to Computer Security: The NIST Handbook)
[3] Reference General Technology Audit Guide – Identity and Access Management – Institute of Internal Auditors
[4] Reference GAO's Federal Information System Controls Audit Manual

example, the customer service group has their certain accesses and the Utility Billing Reps have theirs all based on the roles they perform.

Overall Conclusion

There are numerous basic access right principles lacking. They are as follows:

- Policies and Procedures Not in Place
- Logs Not Enabled
- Data Owner Approvals Lacking
- Annual Reviews Not Performed
- No Non-Disclosure Agreement Found for the Parks RecTrac system
- Deactivation Procedures

Opportunities for Improvement

During our audit we identified certain areas for improvement. Our audit was not designed or intended to be a detailed study of every relevant system, procedure, and transaction. Accordingly, the Opportunities for Improvement section presented in this report may not be all-inclusive of areas where improvement might be needed.

Management is in a unique position to best understand their operations and may be able to identify more efficient and effective approaches to the following recommendations:

Opportunity for Improvement #1 – Policies and Procedures

Condition (The way it is)

No Policies and Procedures are in place for the granting of Access Rights.

Criteria (The way it should be)

Policies and Procedures are the foundation of any organization.

The granting of access rights is called user provisioning. This process should be governed by a specific and universally applied policy statement that is written and maintained by the IT Department with input from other departments.

According to the Governmental Accountability Office's Federal Information System Controls Audit Manual, "Access control policies and procedures should be formally developed, documented, disseminated, and periodically updated. Policies should address purpose, scope, roles, responsibility, and compliance issues; procedures should facilitate the implementation of the policy and associated access controls."

Ultimately, access authorization should be formal, well-defined, documented and an auditable process.

Effect (So what?)

Without Policies and Procedures inappropriate access could be attained by not abiding by the "need to know principle" or by a lack of segregation of duties (no one person should have complete control of a transaction from beginning to end).

Cause (Difference between condition & criteria)

Management has not put in place guidelines to perform essential functions of user provisioning.

Recommendation

Put guidelines in place to describe the process of User Provisioning. Examples of items to include are as follows:

- How the request is to be made?
- Where the requests need to be routed?

➢ Timeframes to complete the request? ➢ How deactivated, disabled, and deleted identities will be stored and describes HR's role in this process? ➢ What reports need to be generated and viewed by whom? ➢ How are privileged users determined and monitored? ➢ Who is responsible for monitoring logs?
Management Response
IT met with the HR and Finance Directors along with the Police Chief to discuss ways to improve so that it will make the process easier and more streamlined.
Action Plan
IT will be working with HR to develop a policy/procedure for new & terminated employees along with a termination check list. ALL new hires and terminated employees must be submitted via the help desk software.
Implementation Date
01-01-2016

Follow-Up

An Activation Deactivation procedure has been created and is stored on the IT shared drive, Reference Number ITCJIS. HR is now submitting all new hires and terminations through the help desk software.

Opportunity for Improvement #2 – Logs Not Enabled and Not Monitored

Condition (The way it is)

The Utility Billing logs (audit trails) were not enabled for both regular users and privileged users and not being monitored. The Parks RecTrac logs were not being monitored.

Criteria (The way it should be)

According to the National Institute of Standards and Technology (NIST) Special Publication 800-12 (An Introduction to Computer Security: The NIST Handbook), Page 211, "Audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem solving."

"By advising users that they are personally accountable for their actions, which are tracked by an audit trail that logs user activities, managers can help promote proper user behavior."

Telling employees about the audit logs and that what they do is being tracked is in itself a deterrent against fraud.

Effect (So what?)

Without logs turned on and reviewed, the city has no way of knowing if the system has been compromised or abused by an insider.

Cause (Difference between condition & criteria)

Management believed the Utility Billing logs were turned on. No monitoring was taking place and therefore they did not know the logs were turned off.

Management of the Parks RecTrac was unaware that the system produced audit logs.

Recommendation

During the audit Utility Billing Logs were turned on.

Audit Logs for both systems need to be monitored by IT and the Data Owner over the application and database. Evidence of this monitoring must be present and audit ready.

Management Response

Parks - Agree. The Recreation Superintendent contacted RecTrac to learn how to run Audit Logs and get training on how to review them.

IT - Logs are now enabled. SunGard's response was that they do not enable the logs because they take up to much space. IT staff worked with SunGard to enable the logs. IT staff worked with the Parks department and Vermont Systems to train

staff on how to review their logs.
Action Plan
Parks - Effective June 2015, the Recreation Superintendent at the end of each month will run RecTrac Audit Logs for 4 random days in the month. Those reports and the findings are documented on a spreadsheet and kept on file. If any red flags or discrepancies exist, the Superintendent will address them immediately with IT and determine a course of action from that point. The Recreation Supervisor will also meet with the Recreation staff and inform them of the monthly audits. That meeting and the minutes of the meeting will be documented and kept on file. **IT** - Logging is now enabled
Implementation Date
Parks - June, 2015 **IT - 05-01-2015**

Follow-Up

Logs are now enabled for both Utility Billing (SunGard) and Parks RecTrac system. Parks runs the audit logs monthly and documents any findings.

While the audit log was enabled for SunGard, it is very cumbersome and not very user-friendly to access or interpret. The logs were turned on, but they were not routinely monitored. If an issue had arisen, SunGard would have had to aid in reviewing the log. The SunGard system is in the process of being replaced with Tyler Systems. IT has made sure that the new system has the audit logs turned on and knows how to access and review them. Sample copies of audit logs from Tyler Systems were provided.

Opportunity for Improvement #3 – Data Owner Approvals Lacking

Condition (The way it is)

1) It was discovered during the audit that IT makes some changes to access rights for applications without data owner approval. This lacks the necessary segregation of duties required between IT and the data owner.

2) In one case involving the Utility Billing System an Accounting employee was included in access rights for the Utility Billing Reps. That employee should have been in the User Group for Accounting.

   In the case of the Parks RecTrac system all individuals had the same access. According to Vermont Systems the vendor for the Parks RecTrac system, "In this environment, there are essentially no restrictions on access, or conversely, everyone has full access to everything in the system. While this is by far the easiest and fastest solution to enact, it is also, potentially, the most dangerous, since employees will not be limited by permissions or password restrictions."

3) The Data Owner is the person that owns the data to the application being used and they have the best knowledge as to who should have access and what type of access. Additionally, it was observed on the Utility Billing System that functions and sub functions may not be needed therefore authorization should be disabled. There was no evidence to indicate a review is completed on what is granted to each user group.

Criteria (The way it should be)

Data Owners must be allowed to make the call as to who gains access to their applications and what type of access is granted.

From the Governmental Accountability Office's Federal Information System Controls Audit Manual, "Implementing adequate access controls involves first determining what level a type of protection is appropriate for individual resources based on a risk assessment and on who needs access to these resources. These tasks should be performed by the resource owners."

From CobiT (Control Objectives for IT) DSS05.04, Manage user identity and logical access. "Ensure that all users have information access rights in accordance with their business requirements and co-ordinate with business units that manage their own access rights within business processes."

Effect (So what?)

Improper accesses may take place without the necessary segregation of duties and review of role-based functions and sub functions.

Cause (Difference between condition & criteria)

Management is not applying the proper segregation of duties and monitoring over access rights.

Recommendation

Document that Data Owners are involved in any add, changes or deletions to user provisioning and an annual review of user group functions and sub functions.

Management Response

Parks - Agree, this was addressed in April and has been corrected.

IT - Most changes are approved by the different department systems owners. IT will make every effort to inform the data owners of the changes that are made to their software applications during a software related issue. IT informs users when there are system upgrades and sends an email out with the release notes.

Action Plan

Parks - In April 2015, the Parks recreation Supervisor, Superintendent, and IT Administrator met with RecTrac on-site to discuss security levels and make the necessary changes to provide better institutional controls through the RecTrac system. As a result, 4 different levels of security were created and assigned to staff based on their job responsibilities. They are listed as follows:

Recreation: This is the most basic security level for part-time staff that works the front desk and takes program registrations and reservations.

MOD (Manager on Duty): This security level allows the onsite Manager to override any age requirements, capacity limits, and program discounts. It also allows the Managers to develop programs and fees in RecTrac. This level is assigned to the full-time programming staff;

Finance: This level is assigned to the Finance staff and allows them to run their import / export reports, refund management, plug and play reports, reconciliation, and view and run GL reports.

Supervisor: This level is limited to the Recreation Supervisor, Recreation Superintendent, and IT. This security level includes all levels of MOD, as well as the ability to run Audit Logs, Security Maintenance, User Menu Maintenance, and create and delete user accounts.

IT - IT will meet once a year with the department system data owners to review their staff's access. IT will also require that all new hires and position changes be sent through the help desk software so that there is a paper trail. Note: IT did

make a similar change to anyone requesting access to accounts. All access to accounts or changes must come from the Finance office via email to the help desk so that there is a paper trail.
Implementation Date
Parks – April 2015 **IT - 07-01-15**

Follow-Up

Four different levels of security have been created in the RecTrac system and all employees have been assigned a security level. IT meets with the department system data owners annually to review their staff's access. IT met with Parks and Rec on 8/26/16 and Utility Billing will be skipped this year due to the implementation of Tyler Systems and their impending move to the new system. Parks and Rec routinely reviews their staff's access and removes employees as they leave and/or no longer need access.

Opportunity for Improvement #4 – User Entitlement Reviews Not Performed

Condition (The way it is)
No User Entitlement Reviews have been performed on an annual basis.
Criteria (The way it should be)
User Entitlement Reviews should be performed at least on an annual basis. According to the Global Technology Audit Guide, Practice Guide, Identity and Access Management, "Managers can review the access granted to their direct reports, while application owners can review the access granted to all individuals who use the application to identify and revoke potentially inappropriate access. This review process should be performed at least annually or more frequently for critical applications or high-risk individuals."
Effect (So what?)
Accesses to applications and databases may be out-of-date and inappropriate.
Cause (Difference between condition & criteria)
No documentation exists to substantiate the performance of User Entitlement Reviews.
Recommendation
Perform and document User Entitlement Reviews on an annual basis.
Management Response
IT does perform these audits; they were not logged via our help desk software which is now required so that there is a paper trail.
Action Plan
IT is creating an automated schedule in our help desk software that will auto create a work ticket to perform these audits. The including anything for Windows users access, building security, and software that the city utilizes.
Implementation Date
08-01-2015

Follow-Up

The automated schedule has been created and these User Entitlement Reviews/audits are scheduled to be performed every 6 months. Utility Billing's audit is scheduled January and July and RecTrac's audit is scheduled February and August.

Opportunity for Improvement #5 – Non-Disclosure Agreement
Condition (The way it is)
The City does not have a nondisclosure agreement (NDA) for the Parks RecTrac vendor who supports the Parks RecTrac applications and database.
Criteria (The way it should be)
An NDA should be in place to protect the City's Parks RecTrac data from unauthorized access, disclosure, publication or dissemination.
Effect (So what?)
Without a Non-Disclosure Agreement with the vendor, the City may not have any legal recourse over the misuse or exposure of sensitive data in the Parks RecTrac system.
Cause (Difference between condition & criteria)
No guidelines exist to inform IT or the Data Owner that an NDA is required.
Recommendation
IT should obtain a signed NDA from the vendor pertaining to vendor support access for the Parks RecTrac application and database.
Management Response
IT was not aware that we did not have this agreement with this vendor.
Action Plan
IT contacted the vendor and received a NDA from them. The City Attorney's office reviewed the document. The City now has a signed NDA with this vendor.
Implementation Date
07-16-2015

Follow-Up

An NDA has been received from Vermont Systems and the signed agreement is in Laserfiche.

Opportunity for Improvement #6 – Deactivation Procedures

Condition (The way it is)

No procedures exist for deactivation processes.

For the Parks RecTrac System 2 out of 28 users (Employee A terminated 12/17/14 and still active on 1/16/15 and Employee B terminated 11/19/14 and still active on 1/16/15) were found to be terminated but still active on the system.

Criteria (The way it should be)

Deactivation of terminated employees should be made as soon as possible.

Periodic reviews should be performed to ensure that accounts are deactivated when no longer needed.

Effect (So what?)

Active accounts that are no longer needed may be potentially misused for unauthorized use.

Cause (Difference between condition & criteria)

There are no procedures in place to memorialize this process.

A monitoring mechanism is lacking to double check if the deactivation has actually been completed.

Recommendation

IT should create deactivation procedures.

The administrative users need to review their access control lists on a monthly basis and document that review.

Management Response

Parks - Agreed, action taken immediately.

IT - IT met with Kenny and Chien to verify that they will also now be checking terminated employees. NOTE: When IT receives a help desk request from HR to terminate an employee, they are terminated on that date in Windows, which prohibits them from accessing the parks and recreation software.

Action Plan

Parks - Effective June 2015, the Recreation Superintendent began reviewing the Security File Maintenance Log at the beginning of each month and documented that review. The Superintendent reviews that log to verify all users that have access to RecTrac are active employees with the City of League City. If any discrepancy is noted, the Superintendent will get with IT to make the necessary adjustments and inactivate staff that have left or no longer need RecTrac access.

IT - This coincides with #1, “IT will be working with HR to develop a policy/procedure for new & terminated employees along with a termination check list. ALL new hires and terminated employees must be submitted via the help desk software.”
Implementation Date
Parks - June 1, 2015. **IT - 01-01-2016**

Follow-Up

See Opportunity for Improvement #1 – Deactivation Policy, Reference Number ITCJIS, has been created and is available from IT.

EXHIBIT A

Sampling Methodology

Used the RecTrac Access Control List for 10/11/14 and 1/16/15.

Used the Utility Billing System Access Control List for 11/5/14.

Used the logs for 3/25/15 for both Parks RecTrac and Utility Billing System.

Used the Human Resources Terminations Listing from 1/16/15.

EXHIBIT B

Reliability and Integrity of Information

OFIs 1, 2, 3, 4, and 5 are inquiry based. The particular items were nonexistent or there was no other source to compare the information with.

OFI 6 used computer-generated data. For example, the employee listing was compared with the access control lists. That comparison ensured the reliability and integrity of the access control lists.