Cobb County...Expect the Best!

INTERNAL AUDIT DEPARTMENT

Report Number: 2019-006

FINAL REPORT – Review of System Override Activities within the CGI Advantage Financial System

July 24, 2019

Latona Thomas, CPA, Director
Michelle Swaby CPA (inactive), PT Senior Internal Auditor
David Murray, Internal Auditor II
Misi Joseph, CFE, Internal Auditor II

Table of Contents

COBB COUNTY INTERNAL AUDIT

Latona Thomas, CPA
Director

100 Cherokee Street, Suite 250
Marietta, Georgia 30090
phone: (770) 528-2559 • fax: (770) 528-2642
latona.thomas@cobbcounty.org

July 24, 2019

MEMORANDUM

TO: Rob Hosack, County Manager

FROM: Latona Thomas, CPA, Director

SUBJECT: **FINAL REPORT** – Review of System Override Activities within the CGI Advantage Financial System

Attached for your review and comments is the subject final audit report. The overall objective of this review was to ensure that adequate corrective actions were taken to eliminate or mitigate the risk of user access associated to override errors[1] within the CGI Advantage Financial system (the financial system).

Impact on the Governance of Cobb County

The recommendations, when implemented, will ensure that certain system access granted to individuals/groups are appropriate and correlates with their current roles, responsibilities and functions within Cobb County (the County), and that system reported issues are resolved in a timely manner.

Executive Summary

We found that adequate corrective action was taken to mitigate the risks over unauthorized overrides of errors through the 'Override' user access[2], which was granted to several employees. The 'Override' user accesses were updated to remove several employee accesses that were not warranted. However, we have determined that, further review is needed to ensure access for the remaining individuals is appropriate based on their roles and responsibilities, and in accordance with established financial system controls. In addition to the 'Override' user access, we noted other unwarranted access within two other user accesses, that were identified and resolved during our review. We also noted that the timeliness of the resolution of system reported issues need to be improved.

[1] Error is the severity level of a system control message that appears to prevent incomplete and our inaccurate documents from being submitted and paid.

[2] The 'Override' user access allows users to override specific error messages that are set to an override severity level.

Recommendations

We made a total of four recommendations to address the weaknesses in the user accesses of the financial system. Recommendations will address weaknesses in the monitoring of system user accesses, and the timely resolution of system reported issues. For specific recommendations, see the 'Results of Consulting Services' section of this report being on Page 3.

Responses

The Information Services Director provided a response to our draft report and concurred with each of our recommendations. The complete responses to the draft report are included in Appendix VI. We will perform a follow-up on corrective actions in six months. A copy of this report will be distributed to those affected by the report recommendations. Please contact me at (770) 528-2559 if you have questions or Michelle Swaby, Auditor-in-Charge, at (770)528-2642.

Background

Cobb County (the County) utilizes the CGI Advantage Financial[3] (the financial system) to record, process, and monitor all purchasing, financial and personnel transactions. The applications within the financial system are not only vital to the County's day-to-day operations, but also includes confidential and sensitive information for employees, vendors, and County citizens. The financial system is configured to fit the County's business needs and is also used to settle vendor payments and the reporting of both internal and external financial information.

CGI Advantage Financial includes built-in and County-configured system controls containing a variety of programmed features which help the County control access to specific data or functions within the financial system. Individual employee login identifications (IDs) and access to the various functionalities within the financial system is provided upon approval/authorization by the respective County agencies/departments and/or elected officials offices. Employee access for the financial system was formerly managed by a Financial Management Analyst position within the Finance Department, but during FY2018, the position and corresponding responsibilities was transferred to the Information Services (IS) Department. The Controls Analyst II position, under the direction of the IS Department now manages these responsibilities and all requests for login and access within the financial system.

Purpose of Consulting Project

During the preliminary survey of a separate engagement, we noted email correspondence that referenced Payment Request-Matching (PRMs) and/or vendor invoices[4] were being paid for more than the receiver[5] amounts. A PRM is a computer-generated matching document that is created when a three-way match[6] occurs between a purchase document[7], receiver, and vendor invoice. We obtained clarification through discussions from both IS and Finance Department staff, that there were several employees with a system override functionality that were not warranted. The override functionality allows the user to finalize PRMs without having a three-way match, a built-in internal control within the financial system which prevents the payment of incorrect and possible fraudulent invoices. In addition, we obtained potential evidence that several employees had administrative-level system access that may not be consistent with their position and related job duties. We analyzed the information, and assessed the level of risk, in connection with the status of other Internal Audit priorities. Based on our analysis and assessment, we deemed the risk to be significant and thus judgmentally elected to initiate a separate engagement to understand the full context of the issue and to determine what corrective actions were taken to eliminate or reduce the risk to an acceptable level.

---

[3] CGI Advantage Financial is the accounting software or financial management solution built exclusively for the business of government. [Source: www.cgi.com]

[4] Vendor invoices are payment request from a vendor for goods/services that were delivered to the County.

[5] A receiver, per CGI Advantage Financial user guide, is a document "used by departments to show that goods/supplies have been received or services rendered are completed. May be partial or final".

[6] A three-way match, per CGI Advantage Financial user guide, "occurs when a purchasing document, an invoice and a receiver are all finalized and reference each other in CGI Advantage Financial".

[7] Purchase documents, per CGI Advantage Financial user guide, includes Departmental Purchase Orders (PD), Purchase Orders (PO), and Delivery Orders (DO).

Our limited consulting services included interviews, analyses, and other procedures related to the control activities of the stated user accesses within the County's financial system. Major contributors to this report are listed in Appendix III.

Results of Consulting Services

Our objective was to ensure that adequate corrective actions were taken to eliminate or mitigate the risk of user access associated with overriding errors[1] within the CGI Advantage Financial system (the financial system). We conducted additional follow-up interviews with key personnel from the Information Services (IS) and Finance Departments; reviewed various related documents, including email communications; reviewed the system user access identifications (IDs); and compared the transactions to the CGI Advantage Financial user guide for conflicts with the County's three-way match system control.

We noted that adequate corrective actions were taken to mitigate the 'Override' user access risk. The user access was updated to remove the overriding errors functionality for individuals whose access were not justified. However, additional review is needed to ensure that access for the remaining individuals is appropriate based on their roles and responsibilities and in accordance with established financial system controls. During our procedures, we also noted another significant weakness in other user accesses that were identified and resolved during our review. We found that several individuals had administrative-level system access that was not consistent with their position, job duties, and/or best practices. In addition, we found an opportunity for improvement to address the untimely resolution of system reported issues. In the accompanying pages are recommendations to strengthen or improve the control activities over user accesses and the timely resolution of system reported issues.

Control Activities over User Accesses Need to be Strengthened and Improved

We noted that three significant employee user accesses (i.e. 'Override', 'Admin', and 'All Update') were not updated based on business needs and job responsibilities. These accesses were inconsistent and/or in conflict with individual employee assigned roles, responsibilities and current employment status with the County. Below is a description of each user access, the control weaknesses noted, corrective action taken, and additional recommendations, where applicable.

'Override' User Access

We found that an 'Override' user access control weakness had been previously identified, where employees possessed the ability to finalize vendor invoices for payment, bypassing the County's three-way matching system control. Employees were using their 'Override' user access to finalize a PRM for payment without meeting the three-way matching system requirement, with no justification or subsequent reconciliation, validation, or approval by a separate individual. We noted discussion of one override where a vendor was paid $10,000 more than the services reflected in the receiver in the financial system. Specifically, two vendor invoices were received that totaled $21,753, but a receiver in the amount of $11,753 was entered into the financial system. Because the vendor invoice total and receiver did not match, the financial system did not automatically create a PRM document, no check could be generated for payment to the vendor, and a system control 'error' message appeared. A system control 'error' message prevents the PRM from being submitted and vendor payment made, until the matching issue identified is corrected and resolved. 'Error' messages require system permission by a person with the appropriate level of authority or access to override the 'error' but should only be used when properly justified and subsequently validated by a separate person.

In the instance described on Page 3, an employee with the 'Override' user access changed the severity of the system control message from an 'error' to a 'warning'[8], with no justification or other documentation noted or maintained. This change in the severity level of the system control message to a 'warning' allowed the required PRM to be finalized and vendor invoice paid for more than what was inputted on the receiver. Changing the severity level of system control messages and overriding an 'error' increases the risk of overpaying vendor invoice amounts, paying duplicate vendor invoices, and paying for goods and/or services that have not been received. Granting user access to employees whose roles and responsibilities conflict with the rights allowed by the user access resulted in a break-down of the County's financial system internal controls.

Based on documents reviewed and discussions with both IS and Finance Department staff, we noted that this control weakness was identified as far back as November 2016 and initially attributed to a system issue; however, in February 2018, the weakness was determined to be the result of unwarranted access to the system override functionality. After the issue could not be resolved by the financial system support professionals, Finance Department staff ran a system generated report and found that changes to the severity level of the system control message caused the overpayment of the vendor invoice. After further research, Finance Department staff identified 1,252 user IDs that possessed the 'Override' user access functionality within the financial system. During February 2018, IS and Finance Department staff worked together and implemented the corrective action of nullifying[9] all user access to the override functionality, except for 13[10] user IDs. We believe that additional review is needed to ensure the 'Override' user access for the remaining 13 individuals/groups is appropriate based on their position, roles, responsibilities, and in accordance with established financial system controls. See Table 1 to the left for a breakdown of the remaining employees with 'Override' user access.

Employees with Override User Access Functionality

Department	User Access	Current Title
Parks	1	Business Manager
Water	1	Technician III
Finance	1	Not Identified
Finance	1	Accountant II
Finance	2	Accountant III
Finance	4	Division Manager
Purchasing	1	Senior Buyer
Purchasing	1	Procurement Svc. Supervisor
IS	1	Solution Analyst II and Application Support Analyst II *(shared)*
Total	**13**	

Table 1 – Source: Information Services Department

In addition, transactions processed using the 'Override' user access functionality are not tracked, periodically monitored, or reviewed for validity and appropriateness. As such, we were unable to quantify the number of vendor payments made during the timeframe of November 2016 and February 2018, that did not meet the County's three-way match built-in system control and the 'Override' user access functionality was used. We also were unable to determine the overall financial impact due to the complexity of the audit trail functionality and because the information was not readily available. The system control messages are designed to restrict financial system users from usurping established County controls and to ensure adequate segregation of duties exist.

[8] Warning messages is the severity level of a system control error message, that appears to indicate a review of a three-way matching document is needed, however a 'warning' message does not prevent the submission of a document, unlike a severity level of 'error'.

[9] Nullifying a user access is done by eliminating all access to a specific functionality with the system.

[10] As of the date of our fieldwork, 03/05/2019, the number of employees with 'Override' user access remained at 13.

User access and profiles should be reviewed on a periodic basis and with changes in personnel and restricted to functions relevant to individual job duties and based on business needs, to minimize the potential risk of unauthorized or fraudulent transactions. Also, user access profiles should maintain proper segregation of duties to ensure a user does not have conflicting processing capabilities (i.e. the ability to initiate, modify, approve, and/or override vendor payments or other financial transactions without an adequate monitoring function). The continued use of this user access functionality without authorized security protocols, the appropriate level of authorization, and other County guidance or direction significantly increases the risk that unauthorized use, system modification, and/or other misappropriation of assets could go undetected.

'Admin' and 'All Update' User Accesses

We noted instances where current, previous, and transferred employees and third-party vendors had administrative-level ('Admin' and 'All Update') system access that was inconsistent with their current position, roles, responsibilities, and/or contractual agreements. With a coordinated effort between IS and Finance Department staff, the system access was updated during our review, but future corrective action is needed.

'Admin' User Access

During our review, we found 26 user identifications (IDs) with 'Admin' user access. The 'Admin' role is the highest level of user access within the financial system and is intended for system administrators only. It allows full unrestricted access functionality to include but not limited to, the ability to modify all information and documents; access to all agency/department or elected official information; the ability to run system applications; modify current financial system configurations; and modify other user accesses. We discussed the risks of the user accesses with IS staff and asked them to research the original list for current applicability based on job roles and responsibilities. Based on subsequent discussions and validation by the Finance Department staff, 24 user accesses were deemed not applicable or valid and the corresponding accesses removed. After the corrective action, only two system administrator accesses remain: one for the IS Department, and the other for a Finance Division Manager. Table 2 to the right includes a list of the 26 IDs, the corrective action taken, and the current user access status of each. We did note that the County has additional user authentication controls where former employees' network access is removed upon separation from service with the County. This control activity prevents former employees from logging on to the County's network and systems, including the financial system.

List of Employees with 'Admin' User Access and Current Status

User ID	Original User Access	Department	Corrective Action	Current User Access
Current Employees	3	IS	Removed-2; Active-1	1
Current Employees	3	Finance	Removed-2; Active-1	1
Duplicate Access	1	Finance	Removed-1	N/A
General Access	2	Finance	Removed-2	N/A
Former Employees	7	N/A	Removed-7	N/A
Unidentified Access	2	Unknown	Removed	N/A
CGI Employees	8	N/A	Removed-8	N/A
Total	**26**			**2**

Table 2 – Source: Information Services Department

'All Update' User Access

We also found six user IDs with 'All Update' user access. The 'All Update' role enables users to create, modify, and submit all system documents, including purchase orders, budgets, vendors, receivers, invoices, checks, etc. In addition, the 'All Update' role allows a user to update all system tables including the chart of account elements and the MESG table[11]. Like the 'Admin' role, the 'All Update' role gives users access to make updates to system tables across all County agencies, departments, and elected official offices within the financial system. As indicated above, we coordinated with IS and Finance Department staff and determined that the user accesses were not applicable. These user access were subsequently removed. See Table 3 to the right for a list of the six IDs, the corrective action taken, and the current user access status of each.

List of Employees with 'All Update' User Access and Current Status

User ID	Original User Access	Department	Corrective Action	Current User Access
Current Employees	3	Finance	Removed-3	N/A
Former Employees	2	Finance	Removed-2	N/A
Duplicate Access	1	Finance	Removed-1	N/A
Total	**6**			**0**

Table 3 – Source: Information Services Department

Best practices suggest that all user access should be consistent with the roles and responsibilities of the user; include adequate segregation of duties; and ensure the appropriate safeguards over the security of information exists. Written approvals of specific security rights should be required by the appropriate level of authority, prior to granting changes to user access privileges to the financial system. Giving employees unlimited access may increase the risk of theft or fraud. Effective control activities provide assurance that the County's financial system's detection and prevention mechanisms are designed adequately and operating effectively. In addition, proper segregation of duties via access management involves separating activities and system access among different persons to enhance accountability and reduce risk of errors, fraud, and inappropriate activities.

Recommendations

The Information Services Director should:

Recommendation 1: Delegate the Technology Services Manager or designee to coordinate with the Finance Department and perform the following:

- Develop a list of allowable transactions and scenarios of when the 'Override' user access functionality is appropriate for use and the justification that should be included in the financial system;
- Review the current list of user identifications who have retained the 'Override' user access functionality and coordinate with the respective departments to determine if the 'Override' user access is consistent with the employee's current job responsibilities and does not create a segregation of duties weakness;
- Establish a process to periodically monitor and evaluate user compliance and investigate instances of non-compliance; and
- Document the above referenced process and communicate to users that retain the 'Override' user access functionality.

[11] MESG table – is a system control message table that allows users to setup and modify message codes, texts, severity and override levels and/or the corresponding explanation of message in the financial system. System control messages can be error messages, warnings or just informational messages.

Auditee Response: **Concur** – *The response below is an abridged version of the auditee's complete response included in Appendix VI, beginning on Page 15.*

Prior to August 2018, the administration of the CGI Advantage Financial System was done by the Finance Department. Information Services has since hired a team member to fill that role. IS is actively updating and creating Information Services Technology processes, forms and standards that will be presented to the BOC for adoption. Application administration and security is part of these standards. Information Services will review all error messages in Advantage Financial to ensure that they may be overridden only at the appropriate levels. The Finance department will review and approve the security roles/profile recommended by IS based on the minimum level of access needed to complete assigned tasks in the Advantage Financial system.

Information Services will coordinate with the Finance Department and will perform the following:

- Document the various Security Roles with the appropriate rights and override privileges. Have Finance review and approve these Security Roles. Ensure all users are only assigned Security Roles from this established list. Once established, these Security Roles should not be changed unless documented and approved by both Finance and IS.
- Review the list of messages in the Advantage Financial System (numbering 6,000) to determine which should have overrides and what level the override should be set.
- Recommend that the all employees having an override role be instructed to include notes in a field of the Advantage document detailing why override was used. We will identify which field should be used and document instructions.
- Investigate the cost of customizing the justification field into the application for documentation purposes. However, we believe new functionality in our next release will allow us to create a User Defined Field for this use. As there will be a cost associated with this customization, it might be less costly to address this in the next upgrade.

Timeline: The IS Solution Analyst, IS Client Services Manager, or Finance Director will individually and/or collectively implement the corrective actions as described in the auditee's complete response in Appendix VI, between August 2019 and April 2020.

Recommendation 2: Delegate the Technology Services Manager or designee to coordinate with the Finance Department and create a tracking tool to document and track requests for the modification of user accesses, to include the appropriate levels of approvals required based on an agency, department, or elected official office assessment of business need.

Auditee Response: **Concur.** Information Services will work with the Finance Department to develop a process to document details of any changes needed to existing Security Roles after the review presented in Recommendation 1. It is recommended that once all Security Roles have been reviewed by Finance, that they only be changed on a limited basis. However, the creation of a new user with the assignment of an existing Security Roles will go through a standard IS process.

Timeline: The IS Client Services Manager and the IS Solution Analyst assigned to finance will work together to create a form to make adjustments to approved Security Roles within 30 days of completion of Recommendation 1.

The IS Client Services Manager and The IS Solution Analyst assigned to finance will work with IS to establish general guidelines for creating new users in the various applications in the County. The specific document used for Advantage Financial will allow for the selection of established Security Roles for users and require the appropriate Department Head or Elected Official approval. This process and specific document will be completed in January 2020.

Recommendation 3: Delegate the Technology Services Manager or designee to coordinate with the Finance Department to periodically review the user identifications that have access to the 'Override', 'Admin', and 'All Update' functionality and remove those individual or group access that are inconsistent and in conflict with the user's current function, role, responsibility and employment status with the County.

Auditee Response: **Concur.** We will create a report with all users that possess these highest levels of security and review them quarterly. Any of these users that have changed jobs that are inconsistent with this access will have access immediately revoked.

Timeline: The IS Solution Analyst assigned to finance will create this list to review with the IS Client Services Manager and on a quarterly basis commencing in August 2019. They will seek recommendations from Finance as necessary.

Timely Resolution of System Reported Issues Needed

The previously discussed 'Override' user access weakness was not resolved in a timely manner. See 'Override User Access' on Page 3 for additional discussion. We found that the timeframe between when the issue was first reported and subsequently resolved was more than one year. We noted that the 'Override' user access weakness was originally believed to be a system issue and thus, was forwarded to the financial system support professionals in November 2016. We noted that two patches[12] were provided by the financial system provider to resolve the issue but IS and Finance Department staff determined that the patches created other system-related issues when applied, so the implementation had to be discontinued. As such, no changes were made to the 'Override' user access functionality and capabilities until February 2018, when user 'Override' user access was updated based on an internal assessment of justification.

We found no established internal process to include the researching, logging, tracking and monitoring of the financial system reported issues, independent of the system provider. IS and Finance Department staff currently rely on the financial system provider's log to record and track reported issues. We also noted that financial system issues are added to the vendor log without any documented research to appropriately classify and explain the system issue, to include whether the issue could be resolved internally, or the level of vendor involvement needed to be resolved.

The lack of research combined with the sole reliance on the financial system service provider to track and monitor issues resulted in a significant control weakness, 'Override' user access, remaining unresolved for an inadequate length of time. An integral component of any software system to achieve continuous and consistent optimal performance is the timely resolution of system reported issues.

[12] Patches are updates or additions to a computer program or its design to resolve issues or improve performance.

This untimely resolution increased the risk of non-compliance with County system controls, fraud, and errors during the processing of vendor payment transactions. Having an internal monitoring process that enables the County to directly manage system reported issues will facilitate coherence in and accountability of, the timely resolution of system issues. We discussed these risks with both IS and Finance staff and they collectively agreed to implement an internal tracking process. See Recommendation 4 below for specific details.

Recommendation

The Information Services Director or designee should:

Recommendation 4: Develop an internal tracking process and aging log for system reported issues. The tracking process and aging log should include, but not be limited to the following:

- A determination of whether the incident can be resolved in the first 24 hours, and if not, the reported issue should be logged on the tracking log and monitored;
- A determination of whether the issue should be reported to the financial system service provided or whether it can be resolved internally by a coordinated effort between IS and Finance Department staff;
- A determination of the minimum data fields to be included on the log;
- Read only access in a user-friendly format for individuals who initially report the issue;
- A periodic review of aging status and distribution to the appropriate level of management; and
- Written standard operating procedures to support the newly established process, which should be periodically updated to reflect current activities.

Auditee Response: **Concur**. Information Services will develop a tracking process that includes aging for system reported issues. It will be made available for all parties to access. The process of reporting and tracking will be documented and made available to Advantage Finance users.

Timeline: The IS Client Services Manager and will work the IS department to create a tracking program utilized by all applications in the County. The IS Client Services Manager and will work with the IS Solution Analyst assigned to finance to establish specific guidelines for use by Advantage Financial users within 6 months (February 2020).

Appendix I

Detailed Objectives, Scope, and Methodology

We conducted this review in conformance with The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

During the preliminary survey of a separate engagement, we identified a significant system control weakness[1] within the processing of vendor payments within the County's financial system. We analyzed the information, and assessed the level of risk, in connection with the status of other Internal Audit priorities. Based on our analysis and assessment, we deemed the risk to be significant and thus judgmentally elected to initiate a separate engagement to understand the full context of the issue and to determine what corrective actions were taken to eliminate or reduce the risk to an acceptable level. The overall objective of this review was to ensure that adequate corrective actions were taken to eliminate or mitigate the risk of user access associated to override errors within the CGI Advantage Financial system (the financial system).

To accomplish our objective, we performed the following steps:

- Interviewed key personnel in the IS and Finance Departments;
- Reviewed and analyzed various related documents, including email correspondence between IS and Finance Departments and the financial system vendor support professionals;
- Reviewed and analyzed the system user access individual employee login identifications (IDs) related to the 'Override' user access weakness;
- Reviewed the financial system user guide for information on three-way matching system internal control process and functionality;
- Coordinated with IS and Finance Departments to deploy immediate corrective action to eliminate and/or minimize the risks associated with the identified user access weaknesses; and
- Validated the collectively agreed upon changes to the invalid or unwarranted user accesses within the County's financial system.

[1] See 'Purpose of Consulting Project' discussion on Page 3.

Appendix II

Abbreviations and Glossary

‘Admin’ User Access	Access to the entire Advantage Financial system, it gives the user the ability to modify all information within the system, and throughout all departments.
‘All Update’ User Access	Access to create, modify and submit all system documents, including purchase orders, budgets, vendors, receivers, invoices, checks etc., throughout all departments.
‘Override’ User Access	The ‘Override’ user access gives the user the ability to finalize a PRM without have a three-way match.
PRM	Payment Request-Matching

Appendix III

Major Contributors to This Report

Latona Thomas, CPA, Internal Audit Director
Michelle Swaby, CPA *(inactive)*, PT Senior Auditor

Appendix IV

Final Report Distribution List

Sharon Stanley, Information Services Director
Bill Volckmann, Finance Director/Comptroller
Eddie Canon, Support Services Agency Director
Tara Crisp, Technology Services Manager, Information Services
Cobb County Audit Committee
Internal Audit Department File

Appendix V

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on County governance. These benefits will be incorporated into our annual report to the Board of Commissioners, Audit Committee, and County Manager.

Type and Value of Outcome Measure:

- Protection of County Funds – Actual; Recommendations, when implemented, will provide increase controls over County funds used to pay vendors. (See Pages 3 – 9)

Methodology Used to Measure the Reported Benefit:

We noted the increased risks of the misappropriation of County assets, unauthorized use of resources, and unauthorized system modifications due to having users having access to override system controls and modify financial system functionality controls.

Type and Value of Outcome Measure:

- Efficient Use of Resources – Actual; Recommendations, when implemented, will increase the efficiency of Information Services and Finance Departments process involving the resolution of system reported issues. (See Pages 8 – 9)

Methodology Used to Measure the Reported Benefit:

We identified that having an internal tracking mechanism for system reported issues, will result in a streamlined methodology to resolve issues in an accurate and timely manner, thus reducing the number of staff hours required to revisit issues that have been outstanding for an extended period of time.

Appendix VI

Auditee's Response to the Draft Report

100 Cherokee Street, Suite 520
Marietta, Georgia 30090-7000
Phone: 770.528.8700

Sharon Stanley
Director, Information Service

DATE: July 17, 2019

TO: Latona Thomas, CPA, Director, Internal Audit

FROM: Sharon Stanley, Director, Information Services

SUBJECT: DRAFT REPORT – Review of System Override Activities within the CGI Advantage Financial System

Several recommendations were made from Internal Audit during a review of the Advantage Financial System. Responses to those recommendations are included below.

Recommendations

The ***Information Services Director*** should:

Recommendation 1: Delegate the Technology Services Manager or designee to coordinate with the Finance Department and perform the following:

- Develop a list of allowable transactions and scenarios of when the 'Override' user access functionality is appropriate for use and the justification that should be included in the financial system;
- Review the current list of user identifications who have retained the 'Override' user access functionality and coordinate with the respective departments to determine if the 'Override' user access is consistent with the employee's current job responsibilities and does not create a segregation of duties weakness;
- Establish a process to periodically monitor and evaluate user compliance and investigate instances of non-compliance; and
- Document the above referenced process and communicate to users that retain the 'Override' user access functionality.

***Response*: Concur**

Prior to August 2018, the administration of the CGI Advantage Financial System was done by the Finance Department. Information Services has since hired a team member to fill that role.

IS is actively updating and creating Information Services Technology processes, forms and standards that will be presented to the BOC for adoption. Application administration and security is part of these standards.

Overrides are a standard part of the CGI Advantage Financial system. Some override options are for confirmation of a specific entry that is unusual but sometimes necessary. These error messages cause the user to make a specific decision to override while preventing the accidental processing of a document in error. Information Services will review all error messages in Advantage Financial to ensure that they may be overridden only at the appropriate levels. Additionally, override capability will only be assigned to specific Security Roles and those roles only assigned to specific users.

The Finance department will review and approve the security roles/profile recommended by IS based on the minimum level of access needed to complete assigned tasks in the Advantage Financial system. Employees will be assigned various Security Roles as directed and as the segregation of duties dictates in each department. Each Department Head or Elected Official will direct which Security Roles should be assigned to a user in their department. Some specialty Security Roles such as those for A/P and Purchasing cannot be assigned outside of those departments.

Existing Advantage Financial users will be reviewed on a regular basis. An annual review of users and their assigned security roles will take place to address changes in roles, responsibilities and staffing. This annual review will entail a list of Advantage Financial users and their Security Roles being sent to all County Department Heads and Elected Officials to review and modify as needed. Additionally, active users will be compared to the list of employee terminations on a biweekly basis and deactivated as needed.

Information Services will coordinate with the Finance Department and will perform the following:

- Document the various Security Roles with the appropriate rights and override privileges. Have Finance review and approve these Security Roles. Ensure all users are only assigned Security Roles from this established list. Once established, these Security Roles should not be changed unless documented and approved by both Finance and IS.
- Review the list of messages in the Advantage Financial System (numbering 6,000) to determine which should have overrides and what level the override should be set.
- Recommend that the all employees having an override role be instructed to include notes in a field of the Advantage document detailing why override was used. We will identify which field should be used and document instructions.
- Investigate the cost of customizing the justification field into the application for documentation purposes. However, we believe new functionality in our next release will allow us to create a User Defined Field for this use. As there will be a cost associated with this customization, it might be less costly to address this in the next upgrade.

  Note: IS Standards and guidelines are established and will be presented to the Department Heads for review in July, 2019. IS Standard forms are being developed for all Cobb application systems for consistency in application security.

Timeline: The Annual Review of active users will commence annually no later than October 1st 2019 and give Department Heads and Elected Officials until the end of the month to respond with any changes. The IS Solution Analyst assigned to finance will create the list of users and distribute.

The review/comparison of Terminated list to active users will commence beginning August 12th 2019 and occur every pay week. The IS Solution Analyst assigned to finance will be responsible for reviewing regularly.

The documentation of Security Roles in the Advantage Financial System will be documented for review by The IS Solution Analyst assigned to finance within 6 months (January 2020. The documentation will be created and stored by The IS Solution Analyst assigned to finance with the Finance Director reviewing on behalf of Finance. The IS Solution Analyst assigned to finance will then review all users to ensure their security within Advantage follows the established Security Roles.

The review of the error messages will be time consuming given the number of messages in the system. Additionally, we want to be sure that the review is thorough given the implications if an error message isn't set at the appropriate level. We estimate that review will take 9 months (April 2020). The IS Solution Analyst assigned to finance will review these messages.

We will document the Over Ride process to include notes on why it was performed. The documentation of this process will be distributed to contacts in Finance and Purchasing within 60 days (September 2019). The IS Client Services Manager and The IS Solution Analyst assigned to finance will establish the process and distribute as needed. The IS Client Services Manager will look at cost of customizing a message.

Recommendation 2: Delegate the Technology Services Manager or designee to coordinate with the Finance Department and create a tracking tool to document and track requests for the modification of user accesses, to include the appropriate levels of approvals required based on an agency, department, or elected official office assessment of business need.

***Response*: Concur**

Information Services will work with the Finance Department to develop a process to document details of any changes needed to existing Security Roles after the review presented in Recommendation 1. It is recommended that once all Security Roles have been reviewed by Finance, that they only be changed on a limited basis. However, the creation of a new user with the assignment of an existing Security Roles will go through a standard IS process.

Timeline: The IS Client Services Manager and the IS Solution Analyst assigned to finance will work together to create a form to make adjustments to approved Security Roles within 30 days of completion of Recommendation 1.

The IS Client Services Manager and The IS Solution Analyst assigned to finance will work with IS to establish general guidelines for creating new users in the various applications in the County. The specific document used for Advantage Financial will allow for the selection of established Security Roles for users and require the appropriate Department Head or Elected Official approval. This process and specific document will be completed in January 2020.

Recommendation 3: Delegate the Technology Services Manager or designee to coordinate with the Finance Department to periodically review the user identifications that have access to the 'Override', 'Admin', and 'All Update' functionality and remove those individual or group access that are inconsistent and in conflict with the user's current function, role, responsibility and employment status with the County.

Response: Concur

We will create a report with all users that possess these highest levels of security and review them quarterly. Any of these users that have changed jobs that are inconsistent with this access will have access immediately revoked.

Timeline: The IS Solution Analyst assigned to finance will create this list to review with the IS Client Services Manager and on a quarterly basis commencing in August 2019. They will seek recommendations from Finance as necessary.

Recommendation 4: Develop an internal tracking process and aging log for system reported issues. The tracking process and aging log should include, but not be limited to the following:

- A determination of whether the incident can be resolved in the first 24 hours, and if not, the reported issue should be logged on the tracking log and monitored;
- A determination of whether the issue should be reported to the financial system service provided or whether it can be resolved internally by a coordinated effort between IS and Finance Department staff;
- A determination of the minimum data fields to be included on the log;
- Read only access in a user-friendly format for individuals who initially report the issue;
- A periodic review of aging status and distribution to the appropriate level of management; and
- Written standard operating procedures to support the newly established process, which should be periodically updated to reflect current activities.

Response: Concur

Information Services will develop a tracking process that includes aging for system reported issues. It will be made available for all parties to access. The process of reporting and tracking will be documented and made available to Advantage Finance users.

Timeline: The IS Client Services Manager and will work the IS department to create a tracking program utilized by all applications in the County. The IS Client Services Manager and will work with the IS Solution Analyst assigned to finance to establish specific guidelines for use by Advantage Financial users within 6 months (February 2020).