



Fairfax County Internal Audit Office

Fairfax County Public Library
SIRSI Application Audit
Final Report

July 2013

"promoting efficient & effective local government"

Executive Summary

The Fairfax County Public Library (FCPL) uses SIRSI Symphony Workflow, a commercial off-the-shelf library management application, to support its day-to-day operations. The FCPL uses the SIRSI application to check in/out customer books, bill customers for fees and late penalties, accept payments and keep track of library materials.

Our audit found that adequate controls were in place to ensure that the library materials' purchase orders and received library materials were input into SIRSI completely and timely. Additionally, exception reports were generated to monitor the system processing, and errors were corrected timely. We also determined that fees and late penalties were calculated correctly and payment reconciliations were performed on a daily basis. However, compliance with the county's Information Technology Security Policy 70-05.01 v4 related to account management, password, and administrative access needed to be strengthened. The primary issues noted were:

- Of the five regional libraries we sampled, only half of the authorized library staff signed the required fee waiver disclosure form. In addition, we noted that the supervisor was not required to review and sign on the "forgive" receipt (the receipt explaining items waived and the reason for the waiver) to ensure oversight and monitoring of the process.
- Controls over discarding library materials could be strengthened. Each library branch could discard the outdated or damaged library items on site with a unique library card for discarding library items. We noted that any circulation staff in the library branch could use this card to discard the library items in the SIRSI application without the supervisor's approval.
- Library staff shared generic user IDs to log into SIRSI based on their job functions, eliminating individual accountability for transactions performed on the system.
- The SIRSI application did not require users to create strong passwords. In addition, the passwords did not have expiration dates. The circulation staff shared the user ID and password to log in to the SIRSI application. The passwords were not changed for the past ten years.
- The SIRSI application system administrator had access rights to all the system functions. Some of the functions such as cataloging, circulation and acquisitions, were beyond his job responsibilities. The segregation of duties control is compromised if the system administrator can also perform end user job functions.

Scope and Objectives

This audit was performed as part of our fiscal year 2012 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit covered the period of June through November 2012, and our audit objectives were to determine that:

- Controls were in place over data input.
- Customer billing for fees and late penalties were calculated correctly and collected timely.
- Controls were in place over the purchasing library materials and inventory records.
- Access controls and separation of duties were established to ensure data was adequately protected from unauthorized amendment or loss.

Methodology

Our audit approach included a review and analysis of internal controls over the SIRSI application purchase order and received library items input, late fees billing and collection process. We interviewed appropriate employees to understand the system functions, data input, fee waiver procedures, fee payment collection and reconciliation process. We observed employees' work functions; determined if controls were in place to prevent data from unauthorized modification; and tested data input, the fee waiver process, late fee generation, late fee payment collection and payment reconciliation on a sample basis.

Findings, Recommendations, and Management Response

1. Fee Reductions and Waivers

The Fairfax County Public Library had a policy for reducing or waiving overdue fees under certain circumstances. Authorized library staff were required to fill out a fee waiver disclosure form. By signing this form, the authorized library staff agreed to forgive fines in accordance with the Fairfax County Public Library's fee waiver policy. We asked five regional libraries to provide a list of staff that had rights to reduce or waive the overdue fees to verify their signed forms in the file. There were a total of fifty library staff that had the rights to reduce or waive overdue fees, but only half of them signed the fee waiver disclosure form. In addition, authorized library staff were required to create a "forgive" receipt from SIRSI which would be marked with the appropriate circumstance (adjustment or hardship) and initialed by the staff. We

noted that a supervisor was not required to review and sign the “forgive” receipt to ensure oversight and monitoring of the process.

Failure to sign the fee waiver disclosure form increases the risk that library staff may not review the FCPL fee waiver policy and inappropriately waive the overdue fees. In addition, the lack of independent supervisory approval for reduced or waived fees decreases accountability for these transactions and increases the risk of reduced revenue by the elimination of legitimate charges through fraud or error.

Recommendation: FCPL should ensure that library staff authorized to reduce or waive overdue fees have reviewed the agency policy on forgiving fines, and signed and dated the fee waiver disclosure form. Supervisors should sign and date the “forgive” receipt to document their approval of each waived transaction. The approval should be verified during the payment reconciliation process.

Management Response: FCPL will implement a companion product that will work in concert with SIRIS to limit the ability to reduce or forgive fines. This product, Comprise, will have a PC that will integrate with SIRSI that will be dedicated to this process. With the implementation of the Comprise product staff will input the forgive transaction into the Comprise terminal which will interface with SIRSI versus staff updating the SIRSI system directly. Additionally, Comprise will require individual user ID staff sign-on and require a higher-level approval to complete the waive transaction. FCPL will limit the staff to a smaller number of employees who will still be required to sign the fee waiver disclosure form. FCPL’s Financial Services Division will check the authorized personnel against the forms during their annual audit of revenue collection. Additionally, each branch location will be provided a custom stamp to stamp the forgive forms to ensure the consistency of required data across branches. The anticipated completion date for the Comprise system implementation is November 5, 2014.

2. Discarded Library Items

We noted that each branch library had the ability to discard library items on site. Any circulation staff in each library branch could discard library items in the SIRSI application without their supervisor’s approval.

Technical Operations and each branch library had a unique library card for discarding library items, i.e. TEDISCARD for technical operations and CEDISCARD for Centreville Regional Library. Library items were discarded when they were in poor condition or outdated. Library branch staff usually put the library items that needed to be discarded in a bin and sent the bin to technical operations. In the SIRSI application, all the items to be discarded were checked out with the “discard” library card. These items’ status was charged to “discard” and they would automatically be purged from SIRSI on a weekly basis.

FCPL didn’t develop procedures to require supervisory/independent approval for discarding library items in the SIRSI application. The lack of independent supervisory approval for discarding library items in the SIRSI application may

increase the risk of theft through fraudulently deleting library items from the system.

Recommendation: FCPL should require the branch libraries to send the library items that need to be discarded to Technical Operations. If library items must be discarded on-site, the branch library supervisor should review and approve the library items to ensure the discarded item is legitimate.

Management Response: FCPL will develop a process that will require the sign-off/approval of a manager for all discarded items. Further, going forward, actual discards will be sent to Technical Operations. FCPL will develop a report that is generated on a regular basis to compare with discards as they are transferred. The anticipated completion date is October 1, 2013.

3. SIRSI Application Generic User ID

We reviewed the SIRIS user list and noted that each library staff user was not assigned a unique user ID. Library staff shared generic user IDs to log into the SIRSI based on their job functions. The generic user IDs' access rights were determined by user profiles. For example, each branch assigned one generic user ID for its circulation staff and several workstations to log into the SIRSI application. The library circulation desk staff logged into SIRSI by using the generic user ID. The generic user ID allowed the staff user to perform transactions such as create new library customer accounts in the SIRSI application, check in/out books, post fee payments, and forgive charges. Each functional job, such as the branch management team, cataloging staff, cataloging manager, process staff, etc., was assigned a specific generic user ID to share.

Fairfax County Information Technology Security Policy 70-05.01 v4 states that, "Users shall be assigned a unique account and user ID. Credentials shall not be shared or written down."

Shared user IDs decrease accountability for transactions posted on the system, increasing the risk of fraud or error in posting payments, waiving fees, or recording book inventory in the system.

Recommendation: For optimal controls, we recommend that FCPL assign each library staff their own SIRSI user ID and password to comply with Fairfax County Information Technology Security Policy 70-05.01 v4.

According to FCPL, eliminating these SIRSI generic user IDs would have severe implications for the library operations and could cause major disruptions and operational hardships. They believe that these costs outweigh the risk associated with generic user IDs and passwords. When a user logs into SIRSI Symphony Workflows, their user ID sets the "branch" location for all transactions that take place within Symphony during that login session. This affects printing, receipt settings, check-in locations, discharge locations, cash receipts, and a host of other settings. It is also our understanding that FCPL plans to implement Comprise Library Management Products to collect fee payments including cash, check and

credit card. The final goal is to have no library staff involved in the cash/payments collection process. The financial risk for using generic user IDs will be substantially minimized after this new payment collection system is implemented. If FCPL decides to continue using generic SIRSI user IDs, the IT security policy requires FCPL to get an approved exemption from the Chief Information Security Officer (CISO).

During this audit, FCPL received an approved exemption from the CISO. IAO obtained a copy of the signed exemption. Within the approved ISO exemption, the Information Security Office recommended that FCPL fix the application to allow more secure account and user management. No management response is needed. However, we do recommend that FCPL move forward with the implementation of the Comprise Library Management Products fee collection system to mitigate the financial risks.

Management Response: No management response is needed.

4. SIRSI Application Passwords

The SIRSI application did not require users to create strong passwords. In addition, the passwords did not have expiration dates. The circulation staff shared a generic user Id and password to log in to the SIRSI application. The passwords were not changed for the past ten years.

Fairfax County Information Technology Security Policy 70-05.01 v4 requires that, "Fairfax County information systems enforce complexity requirements for all user, administrative, and system account passwords. Users shall ensure to use a minimum of 6 characters when creating passwords, to include uppercase letters, lowercase letters, numbers, and special characters when technically feasible for the system. Passwords shall not be shared with anyone internal or external to the County. Passwords for all general user and administrative accounts shall be changed every 90 days and password reuse minimized according to system specifications. System and service accounts shall comply with the same requirements unless specifically approved through the formal exception process."

Password identification and authentication is critical to every computer system. Weak passwords cannot adequately protect library customer accounts from unauthorized modification, disclosure, or impairment. The SIRSI application is a commercial-off-the-shelf product. This application does not have the built-in functions to automatically enforce strong passwords and periodic password changes.

Recommendation: Although the controls cannot be automated, we still recommend that FCPL manually require users to change passwords every 90 days or whenever a staff using a generic user ID resigns or transfers to other department. Additionally, FCPL should still manually require passwords to be no less than six alpha/numeric characters in compliance with the strong password requirements based on the County's Information Technology Security Policy 70-05.01 v4.

In the meantime, FCPL should coordinate with the vendor to develop strong password automation features in the SIRSI application that comply with the IT Security Policy.

Management Response: FCPL will reach out to SIRSI to continue conversations regarding this request. If custom programming would be available from SIRSI eliminating the manual effort and significant staff time to administer this change, FCPL would try to fund the cost of the programming. Also, FCPL agrees to enact a manual, 90-day strong password policy for all users. The anticipated completion date is October 1, 2013.

5. System Administrator Access Rights

The SIRSI application system administrator had access rights to all the system functions. Many of the functions such as cataloging, circulation and acquisitions were beyond his job responsibilities.

Fairfax County Information Technology Security Policy 70-05.01 v4 requires that, "system accounts should be configured to follow the concept of least privilege and not maintain open excessive privileges for the sake of convenience. System accounts that require administrative privileges must also be formally documented and approved by the ISO. Administrative users shall also be provided a separate general user account in accordance with this policy to perform normal business functions."

If one individual controls all critical stages of a process, it increases the risk that erroneous or fraudulent transactions could be processed. The segregation of duties control is compromised if the system administrator can also perform end-user job functions.

Recommendation: We recommend that FCPL evaluate the system administrator's responsibilities and only assign the access rights necessary to perform his job functions, i.e., configuration. He should be restricted from performing end user job functions.

Management Response: FCPL will evaluate the system administrator's responsibilities and only assign the access rights necessary to perform his job functions. Administrative users will be assigned a separate general user account in accordance with the DIT Security Policy to perform normal business functions. If FCPL chooses to continue to grant the general user rights to the system administrator, FCPL will implement a database script that involves the daily execution and monitoring of the database audit script that identifies the changes/actions, workstation ID, and login time of the system administrator user ID. The script results will be sent to the FCPL technical director for review. The SIRSI system administrator will provide the appropriate documentation that supports the administrator's activities to the technical director. The anticipated completion date is October 1, 2013.