Agenda Item #: 3CC-2

PALM BEACH COUNTY

BOARD of COUNTY COMMISSIONERS

AGENDA ITEM SUMMARY

Meeting Date: **5/1/18**

[X] Consent [ ] Regular
[ ] Public Hearing

Department:
Submitted By: County Internal Auditor's Office

I. EXECUTIVE BRIEF

Motion and Title: Staff recommends motion to receive and file:

A. Audit report reviewed by the Audit Committee at its March 21, 2018 meeting as follows:
1. 18-03 Library Department – Information Technology Management

Summary: Ordinance 2012-011 requires the Internal Audit Committee (the Committee) to review audit reports prior to issuance. Ordinance 2012-012 requires the County Internal Auditor to send those reports to the Board of County Commissioners. At its meeting on March 21, 2018, the Committee reviewed and authorized distribution of the attached audit. We are submitting this report to the Board of County Commissioners as required by the Ordinance. Countywide (DB)

Background and Justification: The Committee reviewed and authorized distribution of audit report 18-03 at its March 21, 2018 meeting.

Attachments:

18-03 Library Department – Information Technology Management

Recommended by: J Bergeron 3.29.18
County Internal Auditor Date

Recommended by: N/A
County Administrator Date

II. FISCAL IMPACT ANALYSIS

A. Five Year Summary of Fiscal Impact:

Fiscal Years	2018	2019	2020	2021	2022
Capital Expenditures					
Operating Costs					
External Revenues					
Program Income (County)					
In-Kind Match (County)					
NET FISCAL IMPACT	None				
# ADDITIONAL FTE					
POSITIONS (Cumulative)					

Does this item include the use of federal funds Yes ___ No X

Is Item Included In Current Budget? Yes ___ No

Budget Account No.: Fund ____ Agency ____ Org. ______ Object ____
Program Number __________ Revenue Source __________

B. Recommended Sources of Funds/Summary of Fiscal Impact:

No fiscal impact

A. Department Fiscal Review:

____

III. REVIEW COMMENTS:

A. OFMB Fiscal and/or Contract Administration Comments:

3/30/18
3/29/18 Budget/OFMB 3/29 3/29

4/4/18 Contract Administration 4/4/18

B. Legal Sufficiency:

4/5/18
Assistant County Attorney

C. Other Department Review:

____
Department Director

This summary is not to be used as a basis for payment.

Office of the County Internal Auditor
Audit Report #2018-03

Library Department

Information Technology Management

Reviewed by Audit Committee
March 21, 2018

DATED January 23, 2018

Stewardship – Accountability – Transparency

WHY WE CONDUCTED THIS AUDIT

We conducted this audit to address the following:

Did the Library Information Technology (IT) Division Director manage the information technology function in accordance with Department and Countywide PPMs, Control Objective for Information and Related Technology (COBIT) Guidelines, and vendor maintenance guidelines to ensure:

- Applications were maintained and supported as prescribed,
- Information Technology assets and data were physically and logically secured, and
- Disaster Recovery/ Business Continuity plans provided for maximum operational availability and recovery.

WHAT WE FOUND

We found that the Library IT Division Director generally implemented effective management controls over the information technology function.

The report includes four findings. The findings address:

- Physical access to computer rooms is not appropriately restricted;
- Departmental policies and procedure need to be documented and updated;
- Logical access to the Integrated Library System (ILS) needs improvement; and
- Vendor recommended routine monthly and quarterly backup tasks are not being performed.

During the course of our engagement, we noted issues related to maintenance verification, user training attendance, MDF room environmental monitoring, and desktop terminal privacy protection, which did not rise to the level of a finding. However, we felt these matters should be brought to management's attention. A management letter was issued to the Library Department Director to identify the conditions with suggestions for informational purposes only.

WHAT WE RECOMMEND

The audit report makes 11 recommendations for improvement in the information technology management process relating to the issues we described above in the "What We Found" section. Library management implemented recommendation #11, we reviewed their actions and consider that recommendation cleared with issuance of this audit report.

DETAILED FINDING AND RECOMMENDATIONS

Finding 1. Physical Access to the Main Distribution Frame (MDF) Rooms is Not Restricted on a Least-Needed Basis

Countywide PPM CW-O-059 entitled "*Information Technology Security Policies*," Attachment A entitled "*Palm Beach County IT Security Policies, 2014, Part 1-- General IT Security Policies,*" under Section, 16. Physical Security indicates the following:

Policy Overview
Only authorized personnel performing their specific job functions are allowed physical access to the facilities, which house computing resources, core network resources and associated information assets.

Roles/Responsibilities Information Systems Services include

- Verification of approved access to computer center facilities are given only to those needing entry to fulfill job responsibilities, and
- Performance of a semi-annual audit of badge access rights to secure facilities.

The "*Control Objectives for Information and Related Technology (COBIT) Guidelines*" indicate that controls over the IT process of managing facilities to provide a suitable physical surrounding to protect IT equipment is enabled by physical controls, which are regularly reviewed for their proper function, taking into consideration physical security. Also, considering whether "key" and "card reader" management procedures and practices are adequate, including ongoing updates and review on a least-access-needed basis.

The Library System has five locations that house data file servers and PBC Information Systems Security (ISS) equipment, which are a Main Computer room located at the Main Branch, and four MDF rooms at other locations. While the Library's Information Technology (IT) Division was able to confirm which individuals had access to the Main Computer Room, they were unable to confirm which individuals had access to the four MDF rooms.

According to the branch manager at the Palm Beach Gardens Branch, the MDF room at their location, which houses the North County Disaster Recovery server and one of three Regional back-up servers, is not restricted as follows:

- The same key for the rest of the building opens the keyed door to the MDF room.
- Cleaning staff have a key to the building; and thus, have access to MDF room.

According to the branch manager at the Boca Raton Glades Branch, the MDF room at their location, which houses the South County Disaster Recovery server and one of three Regional back-up servers, is not restricted as follows:

- Meeting room keys, which are kept hanging at all four service desks, can also open the keyed door to the MDF room.
- Unsure of who has a key that will access the MDF room.

According to the branch manager at the Belle Glades Branch, the MDF room at their location, which houses one of three Regional back-up servers, has both keyed and badge access, and she is unsure of who has a key that will access the room.

The PBC Facilities Development and Operations Department's Electronic Services & Security (ESS) Division processes access badges with privileges for all county locations. Access reports provided by ESS for the two MDF locations with badge reader security showed staff from the Library, PBC Facilities (including ESS), PBC ISS, as well as Stockton Contractors (cleaning staff) had access to these rooms. More specifically:

- For the Belle Glades Branch MDF location, there are 304 individuals with access to the room, with 91 percent (276/304) of those having security clearance at all times, as opposed to only certain hours of the day. Twenty-seven individuals have two clearance codes assigned to them. For the period July 1, 2017, through August 31, 2017, six individuals had accessed the room on multiple dates and times. The IT Division Director was unable to conclude if three of the individuals, who were from Facilities, (3 of 6 individuals or 50 percent) were appropriate.

- For the Annex MDF location, there are 311 individuals with access to the room, with 85 percent (263/311) of those having security clearance at all times, as opposed to only certain hours of the day. For the period July 1, 2017, through August 31, 2017, seven individuals accessed the room on multiple dates and times. The IT Division Director was unable to conclude if these individuals, who were from both the Library and Facilities departments, (7 of 7 individuals or 100 percent) were appropriate.

For example, the ISS Director and Deputy Director are on the access list for the Library Annex MDF room. The ESS Director and the FDO Facilities Management Division Director are also on that list. In addition, the authorized access list for the Library Annex MDF room includes a total of 125 individuals from the Facilities Management Division, 95 individuals from ISS, and 33 individuals from ESS. Furthermore, in our review of access records for the Library Annex MDF room for July and August 2017, we noted only 7 of the 311 authorized individuals accessed the MDF room. Two of the seven were Library staff, four were Facilities Management Division staff, and one was ESS staff.

In our view, these listings contain individuals who do not need access to the MDF rooms.

The IT Division Director confirmed access at the four MDF locations is not reviewed periodically, and there is no policy for authorizing and limiting access to these rooms. In addition, a list of personnel authorized to access these rooms is not maintained.

Not restricting individual access to locations that maintain critical computer equipment can lead to access abuse, unintentional damage, or loss which could impact the integrity of data stored in servers.

We believe that access to the MDF rooms should be at the discretion of the Library IT Division Director, and that personnel from other County departments should not have uncontrolled entry to these rooms. The County's Information System Services and Facilities Development and Operations departments provide services at these locations, which support the Library Department's information technology activities, and thus, discretion should be with the Department.

Recommendations:

The Department Director and the IT Division Director should ensure:

1. Access at each MDF room location is restricted to those individuals with a job responsibility [not rank and title] that requires access to the room. More specifically, access should be controlled with a separate key to the MDF room, badge access restrictions, key distribution records, and periodic re-keying.

2. Access to MDF room locations (i.e. badge, key) is reviewed semi-annually for appropriateness and those identified without a need for entry discontinued. This would include an evaluation of badge access records from ESS and a review of current key distribution records.

Management Comments and Our Evaluation

In responding to a draft of this audit report, the Department Director and the IT Division Director agreed with the finding and both recommendations. The response stated that a project would be undertaken to equip the Glades Road and Gardens branches with electronic badge access. The response also stated that access would be granted based on job responsibility relative to the specific MDF rooms and that the access lists would be reviewed semiannually for accuracy.

We believe the Department and IT Division Directors responses are fully consistent with our recommendations.

Finding 2. Departmental PPMs Are in Need of Documentation and Updating

Countywide PPM CW-O-001 entitled "*Policies and Procedures Memoranda (PPMs)*," indicates all division directors, and all heads of separate offices shall issue and maintain Policies and Procedures (PPMs) to promulgate standard policies and procedures for all areas of operation under the control of the issuing office. Further, it indicates directors are expected to ensure that their staff are aware of and comply with established policies and procedures.

The Executive Summary to the Committee of Sponsoring Organizations of the

Treadway Commission (COSO) report entitled "*Internal Control over Financial Reporting – Guidance for Smaller Public Companies*" contains a very succinct summary and explanation of the usefulness of control documentation to an organization. It indicates that documentation of business processes and procedures and other elements of internal control systems is developed and maintained by companies for a number of reasons:

- One is to promote consistency in adhering to desired practices in running the business.
- Effective documentation assists in communicating what is to be done, and how, and creates expectations of performance.
- Another purpose of documentation is to assist in training new personnel and as a refresher or reference tool for other employees.

Documentation also provides evidence to support reporting on internal control effectiveness.

The Department's PPM CLR-003 entitled "*Computer Systems Backup Procedures*" does not include all aspects of the current backup process such as the daily backup of the complete system [Disaster Recovery] at two locations, and daily sync of the primary file server to a secondary server [Business Continuity] at each of the three regional branch locations.

The Library IT Division's written protocols, adopting the vendor prescribed Routine Administrative Tasks for maintenance of the Integrated Library System (ILS) application, indicates that report retention is 30 days; however, the actual report retention practice is 60 days; thus, this documentation is in need of updating.

Moreover, there are no written policies and procedures to address the following areas:

- Problem Notification System (PNR) helpdesk function, which includes, but is not limited to, a 4-hour unwritten standard for responding to submitted non-critical issues, documentation of complete PNR case notes, prompt population of PNR "status" field, periodic review by supervisors of cases remaining open, and definition of PNR classifications for users.
- Periodic testing of the recovery backup plan.
- Quality Assurance protocols for installing desktop application patches/upgrades.
- Practices for scheduling updates/ conducting maintenance of library applications to mitigate negative impacts to the system and users.
- Business interruption standards for the MDF rooms such as the existence of a backup power supply and surge protection.

Without clear expectations and direction, staff may be uncertain of expectations such as requirements for handling and responding to PNR issues, which may lead to inconsistency in adhering to expectations. In addition, critical protocols may not be consistently and appropriately followed, and critical tasks not performed as required.

Recommendations:

The Department Director and the IT Division Director should ensure:

3. Policies and procedures (PPMs) for key areas of the operations are in writing and clearly communicated to staff, and are reviewed periodically and updated when necessary. Written PPMs should include,

but not limited to, such areas as the PNR function, recovery plan testing, business interruption maintenance, desktop application and update installation protocols, and practices for scheduling and conducting application maintenance.

4. IT staff performance is periodically monitored against key expectations outlined and communicated in written PPMs.

Management Comments and Our Evaluation

In responding to a draft of this audit report, the Department Director and the IT Division Director agreed with the finding and both recommendations. The response stated that a new SOP portal would be established on the Library's intranet site containing policies and procedures relative to IT operations. Specific policies and procedures were identified in the response. The response also stated that a performance tracking system would be developed and that weekly IT staff meetings would include performance metrics as a standard agenda item.

We believe the Department and IT Division Directors responses are fully consistent with our recommendations.

Finding 3. Logical Access to the Integrated Library System (ILS) Needs Improvement

Countywide PPM CW-O-059 entitled "*Information Technology Security Policies*," Attachment A entitled "*Palm Beach County IT Security Policies, 2014, Part 1—General IT Security Policies*," under Section, 22. System Access indicates established policies and procedures for system access control shall be consistent with County Security Policy, which include the following:

- All applications and systems will apply role-based security to ensure individuals are only able to access the functions required to perform their job assignments.
- No user will be provided with system access, which exceeds the needs of the position and job description.
- Processes will be established for all new system accesses to specify which systems and data will be required by new system users, and requests must be authorized by departmental management.
- Departments must ensure all user IDs belong to currently authorized users, and identification data kept current by adding new users, and disabling and/or deleting former users.
- Technical staff and Administrators shall promptly disable and delete system access for terminated and transferred employees for systems under departmental control.
- User IDs and passwords will:
  - Assist in resolving problems and performing forensics.
  - Be protected and not shared or managed in such a way they could be used by an unauthorized person.
  - Have associated controls and standards for developing processes/ schedules for adding, changing, disabling and removing user credentials.
- Passwords must be changed on a periodic basis, and will expire within a maximum of 180 calendar days.
- On an annual basis, application access rights will be reviewed for both business and technical users to ensure they are appropriate and consistent with job functions.

Logical access to the ILS is managed under the IT Division's Library Application Support Section. Access is provided to users with an assigned individual and/or shared user ID and password. Established protocols for adding, changing, disabling, and removing user access are an ad hoc reaction to specific instances for new, transferred, and terminated users. Although Library management has provided direction as to what data and systems that individual should be granted access to, there is no formal documented request with management approval for new user access. According to the IT Training and Technical Assistant Supervisor, a report is generated annually to identify user records for staff no longer employed; however, no additional review of user records is conducted to ensure all current user access (both library and IT) is consistent with job functions. In addition, there is no established schedule to periodically change user passwords; although, shared user IDs and passwords are changed about every six months or when a branch manager terminates, it does not include periodic changing of individual passwords. The system does not allow for users to change their own passwords, which have to be performed by the IT staff.

According to the Customer Care Center Senior Manager for the County's Information Systems Services (ISS) Department, user IDs and passwords should be identity-based to provide for an audit trail and allow for disabling system access of terminated and/or transferred employees. However, 361 of the 401 users (or 90 percent), as of June 26, 2017, were assigned at least one (and in many cases two or three) shared user IDs and passwords, as opposed to an individual user ID and password, to access the ILS. As of this date, 66 shared user IDs and passwords were established to access certain modules and functionality within the ILS system. Moreover, 17 of the 40 users (or 43 percent) with assigned individual access were also assigned at least one shared user ID and password to access additional areas of the system.

Due to the nature of the workflow in certain areas of the Library, which necessitates desktop sharing to access the system, the associated staff are adverse to the use of individual user IDs and passwords, as they believe this would impede task efficiency. In addition, there has not been support from management to do otherwise. While only viewing information in the system does not warrant accountability provided with individual user IDs and passwords, user modification and/or updating of data in the system should be identifiable.

IT Admin Users

Administrative access in the ILS permits a user to set up user IDs and passwords in the system. According to the IT Training and Technical Assistant Supervisor, all IT Division staff have administrative privileges in the system. In addition, access to the system is provided for 9 of the 13 staff persons via the shared user ID, "ADMIN," and a common password. The other four staff person have individual user IDs. However, the IT Division Director indicated only staff persons in the Library Application Support Section should have Administrative privilege in the ILS. Moreover, a review of the user profile for an IT staff person outside the Library Application Support Section confirmed they had Admin access to the system. *Note: The IT Division had taken steps prior to the completion of our fieldwork to assign individual IDs to the IT staff.*

According to the Customer Care Center Senior Manager for the County's Information Systems Services (ISS)

Department, ISS's practice is to establish both a regular and administrative account for users with Administrative rights. This provides for accountability and limits Administrative access use.

In addition, inadequate oversight and control for system access may result in users with access that exceeds their job functions, and a lack of accountability needed to promptly resolve system/ data issues that may arise.

Discussions with other Library Systems that utilize the SirsiDynix Integrated Library System revealed the general practice is to assign both individual and shared IDs and passwords. The reasons given for the use of shared IDs was due to direction from upper management, as well as convenience and ease.

Recommendations:

The Department Director and the IT Division Director should:

5. Assign individual user IDs and passwords where appropriate to senior staff and Library IT staff, and implement a requirement for Library customer service staff working in public service areas to use the Windows lock feature whenever an active computer terminal is left unattended.

6. Develop a formal process that specifies the system and data access required for a new user, and provides for management authorization.

7. Implement a process to promptly identify and disable and/or delete terminated and transferred employee access from the system.

8. Establish a schedule to change passwords periodically, at a maximum of 180 calendar days.

9. Conduct an annual review of current user access rights (both business and technical) to verify access is appropriate and consistent with present job functions and authorized access. Inappropriate access should be identified and disabled promptly.

10. Document user access roles and associated functionality for the ILS to promote role-based security and to ensure users are granted access that is consistent and appropriate with their job functions.

Management Comments and Our Evaluation

In responding to a draft of this audit report, the Department Director and the IT Division Director agreed with the finding and recommendations 6 through 10. The Director did not agree with recommendation 5 as originally proposed. After extensive discussion as to the operational needs of Library customer service staff and the limitations inherent in the ILS as to user IDs and passwords, we revised recommendation 5 to that shown above We believe this revised recommendation along with the Library's practice of limiting the functionality to specific groups in a branch provides a reasonable level of controls to mitigate the risk of accidental access to system records by a member of the public.

As to the other recommendations, the Library IT Director indicated that processes were being developed to implement the recommended changes identified in recommendations 6 through 10.

We believe the Department and IT Division Directors responses are fully consistent with our recommendations, including the revision to recommendation 5.

Finding 4. Vendor Recommended Routine Backup Tasks for Monthly and Quarterly Periods, Adopted and Expanded by the IT Division, Are Not Being Performed.

SirsiDynix Support Center 2.0 "*Routine Administrative Tasks (RATS) for Unix/ Linux SirsiDynix Symphony Systems,*" under

- Monthly Administrative Tasks, recommends "Set aside the daily backup tape created on the first day of the month. Keep a separate rotation of four to six tapes solely for the use on the first day of each month."
- Quarterly Administrative Tasks, recommends "Make a bootable backup of your operating system."

The Library Department's Information Technology Division's adopted the vendor's "*Routine Administrative Tasks for Unix/Linux SirsiDynix Symphony Systems,*" and expanded them under Monthly Administrative Tasks to indicate that the monthly backup tape be set aside for off-site storage.

Daily and Weekly Administrative Tasks for the ILS are performed as recommended by the vendor and adopted by the IT Division. However, the Monthly and Quarterly Administrative Tasks for backups were not being performed, which included:

- a daily backup tape on the first day of the month to be set aside for off-site storage, rotated 4 to 6 months; and
- a quarterly bootable backup of the operating system.

A visit to offsite storage showed a quarterly backup tape was present that was labeled Friday -1 4/14; however, the label on the tape did not match the time period (Sept 2017). Also, the tape had not been included in the tracking log maintained by the IT Division.

Although ILS backup requirements are outlined in writing, they were not followed and clearly understood by the System Administrator who is responsible for system and data backup.

Failure to backup the ILS system as recommended by the vendor, and adopted by the IT Division, could preclude the complete and timely recovery of critical data when needed.

Recommendation:

11. The Department Director and the IT Division Director should ensure backup protocols for the ILS system are implemented and followed as recommended by the vendor and as adopted and expanded by the Information Technology Division; which should also include the accurate labeling and tracking of backup tapes.

Management Comments and Our Evaluation

In responding to a draft of this audit report, the Department Director and the IT Division Director agreed with the finding and recommendation. The Library IT Division Director stated that this recommendation had been implemented. We reviewed the actions taken by management to implement this recommendation and confirmed full implementation. Accordingly, we consider this recommendation closed with issuance of this audit report.

BACKGROUND

The Palm Beach County (PBC) Library's (Library or Department) mission is to connect communities, inspire thought, and enrich lives by providing the public with free access to library materials in a variety of formats; helping people of all ages find information, which meets their personal, educational, and professional needs. It consist of the unincorporated area of Palm Beach County and 24 municipalities that do not provide their residents with library facilities. The Library provides service through the Main Library, 16 branches, and a logistical support center. The Library provides outreach services that include a Bookmobile, Talking Books for the Blind, Books-by-Mail, the Adult Literacy Project, and Outreach to Children's Day Care programs. The Library provides access to holdings of 1.9 million items and offers expanding access to electronic information, as well as internet access at all library locations.

The Library is comprised of the following seven divisions: System Services, Branch Public Service, Finance and Facilities, Information Technology, Collection Development, Technical Services, and Community Relations.

The Library's Information Technology Division (IT Division) provides and maintains the Department's own applications and related IT capabilities (i.e. computers, servers); while the County's Information Systems Services Department (ISS) provides and supports its network capabilities, which include network security and wireless services, as well as acts as their internet service provider. The IT Division has 13 positions in 2 sections: Library Application Support and Systems/Computer Platforms (Desktop Support).

The Department uses the SirsiDynix Symphony Integrated Library System (ILS) as its main information system tool, which serves the functions of cataloging, processing, circulation, acquisition, and other library type functions. It is a workflow system, comprised of multiple business modules with various databases. In addition, the Department subscribes to other vendor applications for specific library services and functions. The vendor supports and maintains the applications either fully or partially.

The Department has a Main Computer room, located at its Main Branch, and Main Distribution Frame (MDF) rooms, located at four other sites throughout the County. The MDF rooms house servers and IT equipment.

In FY 2017, the Library Department reported 424 positions and an annual adopted operating budget of $57 M. Since 2012, our office conducted two audits of the Library Department as follows:

- Audit Report 2015-02, dated January 8, 2015, Procurement to Payroll
- Audit Report 2017-06, dated April 25, 2017, Customer Service

The former resulted in three recommendations that our office confirmed to be resolved, and the latter resulted in no findings. There have been no prior audits conducted by our office to review the management of information technology at the Department. There have not been any other external audits/reviews.

AUDIT SCOPE AND METHODOLOGY

This audit was included in the approved annual audit work plan for FY 2017. For our initial planning, we met with the IT Division Director and other IT staff to discuss the management of the IT function at the Department, as well as the related objectives and associated risks.

We identified three areas of the IT function for further review whose associated risk was determined after obtaining feedback from management to have a higher impact and likelihood of occurrence. These areas were: (1) application maintenance and support, (2) data and asset security, and (3) data recovery and business continuity planning.

The audit scope included a review of these areas during the 12-month period from August 1, 2016, through July 31, 2017, which included an evaluation of the related IT processes and controls in place for managing these IT functions. Audit fieldwork was conducted at the Main Library Offices from August through October 2017. In addition, we conducted site visits at the Library's Annex and Palm Beach Gardens branch locations, and at its off-site storage facility.

To become familiar with the Division's process for managing these specific functions, we conducted interviews with the IT Division Director and staff involved. We discussed the processes and controls used to maintain the Library system and applications, to secure its computer resources, both physical and logical, and to plan for data recovery and business continuity of its operations. We obtained system-access to the Library's portal with the ILS vendor to view and access data related to support and maintenance of the application. In addition, we reviewed applicable Departmental and Countywide policies and procedures memorandums (PPMs), industry guidelines, vendor prescribed maintenance and service agreements, and Florida State statutes.

Our methodology included:

<u>Application Maintenance and Support</u>
An evaluation of vendor service agreement use, installation of vendor application updates/patches for quality assurance, training resources available for users, randomly selected test dates to confirm routine task completion, as well as an analysis of helpdesk data to ascertain response times and identify incident trends.

<u>Information Technology Security (Physical, Logical)</u>
A review of badge access reports provided by the PBC Facilities Department's Electronic Services & Security (ESS) Division, and visits to the main computer room and MDF locations to ascertain environmental and physical controls. In addition, we evaluated practices and reviewed records for providing, restricting,

and terminating user access to the ILS system and granting Administrative rights.

Disaster Recovery and Business Continuity
An evaluation of data recovery plans and practices, and vendor recommended backup protocols for the ILS, as well as verification of the backup media stored off-site and related tracking records.

Further, we conducted interviews with IT Division management and staff, branch managers, ILS users, as well as with management and staff from the County's Facilities and Information Services System departments.

We also referred to the Committee of Sponsoring Organizations of the Treadway Commission (COSO) for information on internal control documentation.

Management and Audit Responsibilities

Management is responsible for establishing and maintaining effective internal controls to help ensure that appropriate goals and objectives are met; resources are used effectively, efficiently, and economically, and are safeguarded; laws and regulations are followed; and management and financial information is reliable and properly reported and retained. We are responsible for using professional judgment in establishing the scope and methodology of our work, determining the tests and procedures to be performed, conducting the work, and reporting the results.

We conducted this performance audit in accordance with generally accepted government auditing standards. These 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.

Joseph F Bergeron

Joseph F. Bergeron, CPA, CIA, CGAP
County Internal Auditor
January 26, 2018
W/P # 2017-05

ADMINISTRATIVE RESPONSE

DATE: February 23, 2018

TO: **Joe Bergeron, Palm Beach County Internal Auditor**

THROUGH: Douglas Crane, Library Director

FROM: Peter Brandt, Director, Information Technology

RE: RESOPNSE TO AUDIT REPORT

Below you will find my response for the internal audit conducted by Caroline Bliss and presented by Joseph F. Bergeron on February 9, 2018.

The audit report contained 4 findings and 11 recommendations that will require further action as outlined below. Note that Finding 4, Recommendation 11 concerning ILS backup implementation was considered closed when the report was issued, so there is no further action required there.

The conclusion presented by the audit was that except for the findings and recommendations below, the IT Division Director managed the information technology function in accordance with Department and Countywide PPMs, Control Objective for Information and Related Technology (COBIT) Guidelines, and vendor maintenance guidelines to ensure:

1. Applications were maintained and supported as prescribed,
2. Information Technology assets and data were physically and logically secured, and
3. Disaster Recovery/ Business Continuity plans provided for maximum operational availability and recovery.

Finding 1. Physical Access to the Main Distribution Frame (MDF) Rooms is Not Restricted on a Least-Needed Basis

Finding 1; Recommendation 1. Access at each MDF room location is restricted to those individuals with a job responsibility [not rank and title] that requires access to the room. More specifically, access should be controlled with a separate key to the MDF room, badge access restrictions, key distribution records, and periodic re-keying.

Response to Finding 1; Recommendation 1: I agree with this recommendation. A construction project will be undertaken to equip the MDFs at the Glades Road and the Gardens Branch with electronic badge access. MDFs at the Annex and Belle Glade Branch are currently equipped with electronic badge access. As part of this process a roster of individuals that require access to MDFs will be created. Access will be granted to individuals based on job responsibility. Badge access will be specific to MDFs.

SOP-003 titled Physical Access to MDFs is being crafted to document this procedure.

Timeline: It is expected that this procedure will be in place by January 1, 2019.

Finding 1; Recommendation 2. Accĕss to MDF room locations (i.e. badge, key) is reviewed semi-annually for appropriateness and those identified without a need for entry discontinued. This would include an evaluation of badge access records from ESS and a review of current key distribution records.

Response to Finding 1; Recommendation 2: I agree with this recommendation. The roster stated in my response to Finding 1, Recommendation 1 will be reviewed semiannually for accuracy.

SOP-003 titled Physical Access to MDFs will also address the semiannual review process.

Timeline: It is expected that this procedure will be in place by January 1, 2019.

Finding 2. Departmental PPMs Are in Need of Documentation and Updating.

Finding 2; Recommendation 3. Policies and procedures (PPMs) for key areas of the operations are in writing and clearly communicated to staff and are reviewed periodically and updated when necessary. Written PPMs should include, but not limited to, such areas as the (A) PNR function, (B) recovery plan testing, (C) business interruption maintenance, (D) desktop application and update installation protocols, and (E) practices for scheduling and conducting application maintenance.

Response to Finding 2; Recommendation 3: I agree with this recommendation. A new SOP portal is being constructed on the Library's Intranet site. This portal will contain IT specific policies and procedures for the (A) PNR system, (B) recovery plan testing, (C) business interruption maintenance, (D) desktop application and update installation protocols and (E) practices for scheduling and conducting application maintenance. Documents on the SOP portal will contain policies related to, but not limited to:

(A) SOP-002 PNR Standard Operating Procedures will be crafted that will document the use and expectations of the PNR system.
(B) PPM CLR-003 Computer Backup will be revised to include monthly media QA.
(C) SOP-004 Business Interruption Maintenance will be crafted to address this concern as well as the presence of UPS devises on library servers in MDFs.
(D) SOP-007 Desktop Application Updates and Maintenance will be crafted. This SOP will address maintenance of the content filters and SIRSI WorkFlows application updates.
(E) The procedures for scheduling and conducting application maintenance will be included in SOP-007 response (D).

Timeline: It is expected that these written procedures will be in place by October 1, 2018.

Finding 2; Recommendation 4. IT staff performance is periodically monitored against key expectations outlined and communicated in written PPMs.

Response to Finding 2; Recommendation 4: I agree with this recommendation. An activity tracking system is being developed to monitor staff performance against key expectations. This procedure will be incorporated into existing weekly IT Staff meetings as a reoccurring agenda item. IT PPMs and SOPs will be reviewed by all IT staff on an annual basis or more frequently as needed.

SOP-006 titled Activity Tracking is being crafted to document this procedure.

Timeline: It is expected that these written procedures will be in place by October 1, 2018.

Finding 3. Logical Access to the Integrated Library System (ILS) Needs Improvement

Finding 3; Recommendation 5. (A) Assign individual user IDs and passwords where appropriate to senior staff and Library IT staff, and (B) implement a requirement for Library customer service staff working in public service areas to use the Windows lock feature whenever an active computer terminal is left unattended.

Response to Finding 3; Recommendation 5: I agree with this recommendation. (A) Individual ILS user accounts will be assigned to public service staff as needed to perform their job functions. Account IDs and ILS access will be documented. (B) All public service staff computers will be configured with a password protected inactivity timer.

(A) SOP-003 titled ILS Account Assignment being crafted to document this procedure.

Timeline: It is expected that this will be completed by October 1, 2018.

(B) SOP -005 titled Desktop Privacy is being crafted to address this process.

Timeline: It is expected that this will be completed by June 1, 2018.

Finding 3; Recommendation 6. Develop a formal process that specifies the system and data access required for a new user and provides for management authorization.

Response to Finding 3; Recommendation 6. I agree with this recommendation. A new component will be developed for the existing PNR Help Desk portal that will be used for managers to formally request the creation of new ILS accounts or modifications to existing based on job classification. This procedure will ensure management authorization. PNRs provide an audit trail of actions taken.

SOP-002 titled PNR Portal is being crafted to document this procedure. Specifically, a section titled ILS Account Requests will be included in this SOP.

Timeline: It is expected that this will be completed by June 1, 2018.

Finding 3; Recommendation 7. Implement a process to promptly identify and disable and/or delete terminated and transferred employee access from the system.

Response to Finding 3; Recommendation 7: I agree with this recommendation. A procedure will be developed which will require Library Staff Development/Personnel to notify IT of any new hires, transfers, promotions, demotions, or terminations. This will occur on a weekly basis. The procedure will be based on the processing of Personal Action (PA) forms. The PA forms will be used to modify or delete ILS accounts as required. Activity will be logged.

An SOP will be crafted to document this procedure.

Timeline: It is expected that these written procedures will be in place by October 1, 2018.

Finding 3; Recommendation 8. Establish a schedule to change passwords periodically, at a maximum of 180 calendar days.

Response to Finding 3; Recommendation 8: I agree with this recommendation. The ILS does not allow staff to change their own password. A portal on the Library Intranet will be constructed that will allow staff to change their password. A procedure will be developed to enforce password changes at 180 days for all staff ILS accounts. Activity will be logged. Note: this procedure will not apply to internal system accounts that are used for ILS maintenance.

An SOP will be crafted to document this procedure.

Timeline: It is expected that these written procedures will be in place by October 1, 2018.

Finding 3; Recommendation 9. Conduct an annual review of current user access rights (both business and technical) to verify access is appropriate and consistent with present job functions and authorized access. Inappropriate access should be identified and disabled promptly.

Response to Finding 3; Recommendation 9: I agree with this recommendation. A review of the current ILS staff accounts and access rights will be conducted. From this review a procedure will be developed that will document ILS user access rights as compared to current job function and access. This document will be reviewed semi-annually. Inconsistencies will be identified and rectified.

An SOP will be crafted to document this procedure.

Timeline: It is expected that these written procedures will be in place by October 1, 2018.

Finding 3; Recommendation 10. Document user access roles and associated functionality for the ILS to promote role-based security and to ensure users are granted access that is consistent and appropriate with their job functions.

Response to Finding 3; Recommendation 10: I agree with this recommendation. Based on the document created in Finding 3, Recommendation 9 a procedure will be developed to ensure users are granted access that is consistent with their job functions.

An SOP will be crafted to document this procedure.

Timeline: It is expected that these written procedures will be in place by October 1, 2018.

Peter Brandt
Director, Information Technology
Palm Beach County Library System