Internal Audit Report

PARKS DIRECT Post Implementation Review

Audit #: PGC-010-2018

The Maryland-National Capital Park and Planning Commission
Office of the Inspector General

June 29, 2018

THE MARYLAND-NATIONAL CAPITAL PARK AND PLANNING COMMISSION
Office of the Inspector General • 7833 Walker Drive, Suite 425 • Greenbelt, Maryland 20770

June 29, 2018

To: Mazen Chilet, Chief Information Officer

Darin Conforti, Acting Director, Prince George's County Department of Parks and Recreation

From: Renee Kenney, CPA, CIG, CIA, CISA
Inspector General

Sadat Osuman, CISA, CRISC
IT Audit Manager

Re: PARKS DIRECT Post Implementation Review (PGC-010-2018)

Enclosed is our final audit report summarizing the results of our audit of the PARKS DIRECT application.

We wish to express our appreciation to you and your staff for the cooperation and courtesies extended during the course of the review. If you have any questions or comments, please contact Mr. Sadat Osuman at 301-446-3337 or by e-mail at Sadat.Osuman@mncppc.com.

CC:

Executive Committee	Audit Committee	Maryland-National Capital Park and Planning Commission
Casey Anderson	Dorothy Bailey	Reggie Dixon
Elizabeth Hewlett	Norman Dreyfuss	Adrian Gardner
Patricia Barney	Karen Tobat	Duane Prophet
	Benjamin Williams	Lissette Smith
		Joseph Zimmerman

Executive Summary – PARKS DIRECT Post Implementation Review

Conclusion	Overall, the post implementation review of the PARKS DIRECT software indicated satisfactory controls around logical security and business continuity, and a reduction of scope for PCI Data Security Standards. However, significant deficiencies were noted in project management practices and system testing which have to be addressed in future projects to ensure risks are effectively managed.

Overall Audit Rating	Issue Classification			Significance
 Moderate	Recommendations			PARKS DIRECT is Prince George's Department of Parks and Recreation's primary user and event/activity registration software utilized by all facilities. Aside supporting facility operations, the software also maintains financial data which is transmitted to the Lawson ERP system.
	Critical	Strategic	Important	
Audit Fieldwork	-	1	4	
February 2018				

Audit Risk Ratings by Functional Area*			
High	Elevated	Moderate	Low
▪ None	▪ None	▪ Training, Operational Support & Testing ▪ Project Management	▪ Data Migration & Security ▪ Patch & Change Management ▪ Logical Security

Top Initiatives Prioritized with Management	Issue Classification	Functional Area
Adopt and implement a Commission-wide system development methodology and ensure that industry best practices are followed in the execution of future IT projects. *Expected Implementation Date – 03/01/2019*	*Strategic*	Project Management
Establish detailed test plans and complete testing of all system components prior to go-live for future projects. *Expected Implementation Date – N/A***	*Important*	Training, Operational Support & Testing
Establish quality control procedures around data migration as part of project planning to ensure completeness and accuracy of operational data. *Expected Implementation Date – N/A***	*Important*	Data Migration & Security

*See Appendix for Criteria Leveraged to Assign Risk Ratings by Functional Area.

**This recommendation is to be implemented in future IT projects by DPR since the deficiency was identified within project initiation and cannot be revisited.

Business Overview

Prince George's County Department of Parks and Recreation's retired its legacy user registration software, Class (internally referred to as "SMARTlink"), after it reached its end-of-life in November 2017. The legacy software had to be replaced with a newer solution or risk using a software no longer supported by the vendor, hence, increasing the likelihood of the system not being able to continuously support business operations and a possible system compromise. The Parks and Recreation department chose to implement Vermont Systems' PARKS DIRECT software (internally referred to as "PARKS DIRECT") as its replacement. PARKS DIRECT has been operational since November 2017.

The PARKS DIRECT software manages all the administrative and financial functions previously managed in SMARTlink. A significant benefit of PARKS DIRECT is that the application complies with Payment Card Industry Data Security Standards (PCI-DSS). PARKS DIRECT will also introduce new capabilities that expand on existing functionality and meet the objectives of the 2040 master plan.

The functional deliverables of the new PARKS DIRECT system have been identified as follows by project stakeholders:

- PCI compliant, cloud-hosted, web-based software and hosted payment processing
- Online customer portal with web-based course and league registration and account management
- Program management including attendance tracking
- Membership pass sales; pass printing and scanning
- Facility/equipment reservations and rental/facility schedule management
- Real-time data access and robust reporting capabilities
- Point of Sale environment with inventory management, custom prompts, ticketing, barcode scanning, coupons, gift cards, web sales, etc.
- Multi-lingual (Spanish) and mobile access capabilities
- Subsidy management for fee assistance/scholarships

Audit Objective, Scope & Methodology

Objective: The objective of the PARKS DIRECT Post-Implementation Review was to provide management with an independent evaluation of the project outcomes, security design, solution support post go-live and the recovery strategy in the event of service disruption or disaster.

Scope: This review included, but was not limited to the following audit procedures:

- Ensured a business case justifying the IT investment was prepared and approved by the appropriate level of management, and adherence of project to baseline cost and schedule.
- Evaluated the PARKS DIRECT project plan to ensure functional requirements, test plans, responsibilities, data conversion and implementation planning have been defined.
- Evaluated the PARKS DIRECT project plan to ensure PCI security requirements are mapped to controls implemented within the PARKS DIRECT solution – logical security, data privacy, change and patch management are in place.
- Evaluated the strategy in place to ensure a smooth transition to PARKS DIRECT through the provision of adequate training and the availability of support staff to help resolve issues that arise in the early stages of go-live.
- Ensured that all issues encountered during the project were recorded and issues learned noted to ensure they are incorporated into future projects.

The audit covered the period from February 1, 2017 through February 28, 2018.

Scope Limitation

The audit did not include an assessment of cash handling practices and procedures and review of patching practices (by vendor) before they are released to customer instances. The patching practices couldn't be independently verified by the OIG because vendor couldn't provide a 3rd party independent assurance of their practices

The audit was performed 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.

Summary of Recommendations

#	Title*	Expected Imp. Date	Accountable	Functional Area
Important Recommendations				
1	Adopt and implement a Commission-wide system development methodology and ensure that industry best practices are followed in the execution of future IT projects.	03/1/2019	Reggie Dixon	Project Management
2	Establish detailed test plans and complete testing of all system components prior to go-live for future projects.	N/A	Lissette Smith	Training, Operational Support & Testing
3	Establish quality control procedures around data migration as part of project planning to ensure completeness and accuracy of operational data.	N/A	Lissette Smith	Data Migration & Security
4	Formally document procedures for requesting and granting user access to PARKS DIRECT.	06/28/218	Lissette Smith	Logical Security
5	Formally document procedures for requesting, reviewing and approving changes to PARKS DIRECT.	06/28/2018	Lissette Smith	Patch & Change Management

*Refer to Recommendations & Action Plans Section for additional details surrounding each recommendation.

Recommendations & Action Plans

Recommendation 1

Adopt and implement a Commission-wide systems development methodology and ensure that industry best practices are followed in the execution of future IT projects.			
Overall Accountable	Risk Type	Risk Rating	Regulatory Impact
Reggie Dixon	IT Governance	Moderate	No

Issue	A. Through discussion with the project team and confirmation from the newly formed Project Management Office (PMO), it was noted that there isn't a Commission-wide system development methodology that has to be followed in the execution of Commission projects to ensure consistency and general leverage of best practices. B. Through discussion with the project team, it was noted that governance around change management as it relates to project scope, deliverables and baselines were informally communicated and not documented within the project plan. Also, a comprehensive project cost baseline could not be obtained to determine if the project schedule was in line with the actuals. Cost estimates, as indicated in the contract, only showed the estimated cost of utilizing the software and not other costs such as labor costs associated with the project.
Criteria	An adopted methodology ensures that projects are executed in an organized and consistent manner. According to the *Global Technology Audit Guide, Practice Guide, Auditing IT Projects*, "A good methodology explains the relationships among all the relevant project management and organizational processes. It is a comprehensive structure of repeatable processes that provides a road map on when, how, and what events should occur in what order."
Impact	Lack of a system development methodology would result in projects not following best practices and key risks and controls being left unaddressed.

Action Item(s)	Executor(s)	Target Date
1.) Adopt a Commission-wide system development methodology and effectively communicate to all departments within the Commission to ensure a consistent development process is followed in the execution of IT projects.	Reggie Dixon	03/01/2019
2.) Management should perform a comprehensive analysis of future project cost estimates/baselines as part of project planning and document within the project plan to be tracked and monitored as the project progresses. **3.)** Management should collaborate with the Commission's Project Management Office, where necessary, in obtaining tools and support in the form of an advisory in effectively executing future IT projects.	**To be implemented during future IT projects.	

**This recommendation is to be implemented in future IT projects by the Dept. of Parks and Recreation since the deficiency was identified within project initiation and cannot be revisited.

Management Response	A consistent project management methodology from the Project Management Office (PMO) has not been adopted by the IT Council as a Commission wide standard. The Office of the Chief Information Officer (OCIO), which oversees the PMO, continues to work through enterprise level governance issues with the Commission's Executive Committee. Once that governance is clearly established and championed by the Executive Committee, the PMO can begin to developing a plan to communicate the methodology and best practices to be used across the Commission.
Action Plan	• Work with the IT Council to adopt the project management methodology standards put forth by the PMO • Establish a well-defined project and program management methodology/framework that is aligned with the Commission goals and that is based on industry best practices • Drive the adoption of the PM/PgM framework into the various Commission initiatives • Make available to the Commission through central repositories the latest trends and industry best practices in project management tools, processes and methodologies • Serve as the Commission's Quality stewards for project and program management processes
Follow-Up Date	April 30, 2019

Recommendation 2

Establish detailed test plans and complete testing of all system components prior to go-live for future projects.

Overall Accountable	Risk Type	Risk Rating	Regulatory Impact
Lissette Smith	IT Governance	Moderate	No

Issue	Through discussions with the project team regarding the testing strategy for PARKS DIRECT, it was noted that a formal test plan wasn't formulated in the earlier stages of the project. The Department of Parks and Recreation currently utilizes 11 out the 12 RecTrac modules but testing documentation could only be obtained for the Activity Registration and Trip Reservation modules. Per the team, informal testing was performed for the remaining by virtue of an initiative undertaken to manually transfer reservations/registrations from SMARTlink to PARKS DIRECT prior to go-live, but documentation wasn't retained.
Criteria	Detailed testing ensures that system functionality is operating as required. According to the *FFIEC IT Handbook-Development and Acquisition*, "The testing phase requires organizations to complete various tests to ensure the accuracy of programmed code, the inclusion of expected functionality, and the interoperability of applications and other network components. Thorough testing is critical to ensuring systems meet organizational and end-user requirements…If organizations use effective project management techniques, they will complete test plans while developing applications, prior to entering the testing phase. Weak project management techniques or demands to complete projects quickly may pressure organizations to develop test plans at the start of the testing phase."
Impact	Inadequate testing may result in system deficiencies not being identified and timely resolved prior to go-live.

Action Item(s)	Executor(s)	Target Date
1.) Formulate detailed test plans that cover all critical system components, as identified during the requirements gathering phase, for future IT projects increasing the likelihood of testers identifying weakness or defects prior to implementation. 2.) Maintain documentation of test scripts and test results as part of project documentation.	**To be implemented during future IT projects.	

**This recommendation is to be implemented in future IT projects by the Dept. of Parks and Recreation since the deficiency was identified within project initiation and cannot be revisited.

Management Response	The Parks Direct project team of the Helpdesk Unit within the Department of Parks and Recreation – Management Services Division did create testing documentation for modules currently in use in the system. The modules that contained testing documentation directly targeted for public use. The test plans for the modules that were used for internal purposes were not formally documented. However, in agreement with the audit recommendations, the Help Desk Project Team will develop a department directive for software testing to ensure that all future projects, test plans will be formally developed, followed, and kept for management review.
Action Plan	N/A
Follow-Up Date	N/A

Recommendation 3

Establish quality control procedures around data migration as part of project planning to ensure completeness and accuracy of operational data.			
Overall Accountable	Risk Type	Risk Rating	Regulatory Impact
Lissette Smith	IT Governance	Low	No

Issue	Through discussion with the project team, it was determined that household data from the legacy system, "SMARTlink", was migrated to PARKS DIRECT prior to go-live. However, no formal quality control check was performed to ensure the completeness and accuracy of the data upon arrival in PARKS DIRECT. According to project team, random spot checking was performed for some accounts but no the whole data but this activity wasn't documented.
Criteria	Quality control procedures should be performed after data migration to ensure accuracy and completeness of transported data. To ensure this, according to the *Global Technology Audit Guide, Practice Guide, Auditing IT Projects*, it is important to confirm that "Data converted reconciles with data in legacy systems."
Impact	Failure to perform data reconciliation between legacy and new systems may result in missing data required for normal business operations.

Action Item(s)	Executor(s)	Target Date
Document and incorporate quality control processes/procedures aimed at reconciling data within the project plan for future projects to ensure the accuracy and completeness of operational data. This will mitigate the risk of data loss and service disruption as a result of missing household information.	**To be implemented during future IT projects.	

**This recommendation is to be implemented in future IT projects by the Dept. of Parks and Recreation since the deficiency was identified within project initiation and cannot be revisited.

Management Response	The Department of Parks and Recreation will ensure that future Helpdesk projects identify and document an appropriate percentage of records for quality control testing during data migrations to reduce the risk of compromising data integrity.
Action Plan	N/A
Follow-Up Date	N/A

Recommendation 4

Formally document procedures for requesting and granting user access to PARKS DIRECT.			
Overall Accountable	Risk Type	Risk Rating	Regulatory Impact
Lissette Smith	Safeguarding of Assets	Low	No

Issue	A. Through discussion with the project team, it was noted that there is currently no documented policy or procedures for requesting and granting user access rights to the PARKS DIRECT software. The current process requires facility managers to send an email request to the mailbox customerservice@pgparks.com for a new user to be provisioned system access. B. Also, there is no formal and documented process to periodically review and re-certify privileged/administrative user accounts.
Criteria	Formal procedures regarding the provisioning and deprovisioning of user accounts should be established and privileged accounts reviewed, at least, annually. According to the *Global Technology Audit Guide, Practice Guide, Identity and Access Management*, "This review, while facilitated by the IT Department, should be conducted primarily by the organization with approvals received from each responsible business owner. In addition, privileged and IT account identities should be reviewed by an appropriate manager or system owner." Formal procedures provides governance around user access to the PARKS DIRECT software.
Impact	User access provisioning responsibilities not being clearly defined, coupled with non-performance of privileged account reviews may result in unauthorized access to the software.

Action Item(s)	Executor(s)	Target Date
1.) Establish and implement formal procedures and guidelines for the provisioning of user access for PARKS DIRECT. Guidelines/procedures should address: a. How access requests are made; b. Authorization to request and approve user access request; c. Where the requests need to be routed; and d. How to deprovision user access upon termination. **2.)** Periodically review access of all accounts with super user/privileged access to PARKS DIRECT to ensure that privileged access is and remains legitimate.	Duane Prophet	06/28/2018

Management Response	Due to the audit recommendations, the Department of Parks and Recreation has established a formal procedure for granting and removing user accounts in Parks Direct. The Helpdesk Operations Team have documented this process by way of the User Access Procedure. This procedure can be accessed through the Helpdesk online resource "screen steps": http://pgparks.screenstepslive.com/s/18299/m/78239/l/904308-user-access-procedure
Action Plan	N/A
Follow-Up Date	05/30/2019

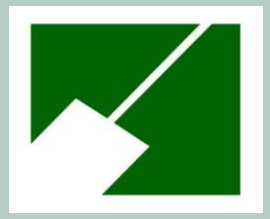
Recommendation 5

Formally document procedures for requesting, reviewing and approving changes to PARKS DIRECT.			
Overall Accountable	Risk Type	Risk Rating	Regulatory Impact
Lissette Smith	IT Governance	Low	No

Issue	Through inquiry, it was noted that there aren't formally documented procedures for requesting, reviewing and approving changes associated with the PARKS DIRECT software. It was explained that change requests are either submitted by an approved team lead or senior leadership, depending on the nature of the change request, to VSI for consideration and subsequent resolution.
Criteria	Change management procedures should be established and formally documented to provide guidance on how changes are to be management throughout its lifecycle. According to the *Global Technology Audit Guide, Practice Guide, Change and Patch Management Controls: Critical for Organization Success*, "The goal of the change management process is to sustain and improve organizational operations. This is accomplished by ensuring that standardized methods and procedures are used for effective and efficient handling of all changes and minimizing the impact of change-related incidents on service quality and availability."
Impact	Without formal change management procedures, unauthorized changes could be made to a system resulting in a service disruption and unplanned downtime.

Action Item(s)	Executor(s)	Target Date
Establish and document formal procedures for requesting, evaluating and approving changes to the PARKS DIRECT software. Procedures should, at least, address the following: a. who's authorized to request for changes b. the review process for requested change c. who has authority to approve change requests before routed to VSI d. procedures to ensure that changes do not introduce risks to the production environment.	Duane Prophet	06/28/2018

Management Response	Due to the audit recommendations, the Department of Parks and Recreation has established a formal procedure for requesting, reviewing, and approving changes in Parks Direct. The Helpdesk Operations Team have documented this process by way of the Software Change Control Procedure. This procedure can be accessed through the Helpdesk online resource "screen steps": http://pgparks.screenstepslive.com/s/18299/m/78239/l/904300-software-change-control-procedure
Action Plan	N/A
Follow-Up Date	05/30/2019



Appendix

Criteria for Assigning Risk Ratings to Functional Areas

Risk Ratings*	Attributes of Audit Findings & Recommendations
High	▪ Multiple "Critical" Recommendations ▪ Significant gaps in the design and/or operating effectiveness of multiple key controls ▪ Audit findings render overall system of controls for functional area unreliable
Elevated	▪ One "Critical" Recommendation and/or multiple "Important" Recommendations ▪ Significant gaps in the design and/or operating effectiveness of one or more key controls ▪ Audit findings render select key controls within functional area unreliable
Moderate	▪ One or more "Important" Recommendations ▪ Moderate gaps in the design and/or operating effectiveness of key and/or secondary controls ▪ Audit findings highlight opportunities to improve the design or effectiveness of select controls within functional area; however, no key controls are deemed unreliable
Low	▪ Audit findings limited to "Observations" ▪ Minor gaps in the design and/or operating effectiveness of secondary controls ▪ Effective and reliable system of internal controls within functional area

*Risk Ratings are reflective of the estimated Probability and Impact of financial reporting errors/irregularities; misappropriation of assets; vulnerabilities of systems/sensitive data; noncompliance with policies or regulations; and adverse reputational consequences which could occur as a result of the internal control gaps identified within a given functional area.