Montgomery County Data Center Colocation

AUDIT REPORT

Audit #: MC-001-2019

The Maryland-National Capital Park and Planning Commission

Office of the Inspector General

June 27, 2019

Maryland-National Capital Park and Planning Commission
Office of the Inspector General
7833 Walker Drive, Suite 425
Greenbelt, MD 20770

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

June 27, 2019

To: Mazen Chilet
Henry Mobayeni
Mike Riley
Carol Rubin
Tanya Stern
Gwen Wright

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

Renee M Kenney

Re: Montgomery County Data Center Colocation (MC-001-2019)

Enclosed is our final report summarizing the results of our audit of Montgomery County's Data Center Colocation initiative.

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 Ms. Renee Kenney at 301-446-3334 or by e-mail at Renee.Kenney@mncppc.com.

CC:

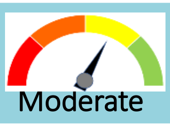
Executive Committee
Elizabeth Hewlett
Casey Anderson
Anju Bennett

Audit Committee
Dorothy Bailey
Norman Dreyfuss
Ben Williams
Lori Depies

Maryland-National Capital Park and Planning Commission
Adrian Garner
Joseph Zimmerman

Executive Summary – Montgomery County Data Center Colocation

Conclusion	The result of document review and interviews with IT management to determine the process followed to ensure risks associated with the project were reasonably considered and controls implemented indicated an inadequate risk management approach with regards to formally identifying and documenting possible risks associated with the data center colocation initiative and corresponding mitigating controls prior to project execution. Also, there was a level of reluctance on the part of IT Management in requesting for information and documentation from the College, which rendered some management assertions unverifiable.

Overall Audit Rating	Issue Classification			Significance
 Moderate	Recommendations			The colocation data center at Montgomery College which the departments are seeking to leverage, will be housing the full data center infrastructure of Montgomery County's Dept. of Parks and Dept. of Planning, namely but not limited to GIS data, file servers, Active Directory, etc. Hence, protection of these assets with appropriate controls is necessary to ensure continuous operation of the business.
	Critical	Strategic	Important	
Audit Fieldwork	1	-	3	
February 2019				

Audit Risk Ratings by Functional Area*

High	Elevated	Moderate	Low
▪ Disaster Recovery	▪ None	▪ Power Supply & Redundancy ▪ Data Center Operations	▪ Contract Management

Top Initiatives Prioritized with Management	Issue Classification	Functional Area
Establish and implement a disaster recovery strategy for Commission assets at the colocation data center to ensure successful restoration of systems and data in the event of a disaster. *Expected Implementation Date – December 2019*	*Critical*	Disaster Recovery
Perform formal risk assessment and retain all necessary supporting materials as part of project documentation. *Expected Implementation Date – December 2019*	*Important*	Power Supply & Redundancy
Implement a solution to remotely monitor IT equipment for uptime and system health at the colocation data center. *Expected Implementation Date – Completed*	*Important*	Data Center Operations

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

Business Overview

Data center collocation (“colo”) is a process through which an organization can rent a shared, secure space for enterprise businesses to store and operate hardware related to data storage and other equipment. It enables sharing the existing pool of data center resources to be used for deploying and hosting data center services for external or retail customers/organizations. The customer usually supplies the equipment (e.g. servers and other hardware) necessary for daily operations while the colocation entity stores it securely in a cool, monitored environment ideal for servers, while ensuring bandwidth needs are met.

Colocation facilities provide space, power, cooling, and physical security for the server, storage, and networking equipment of facility tenants/customers and connects them to a variety of telecommunications and network service providers with minimal cost and complexity. Data center colocation primarily enables organizations to deploy a data center facility without the need to buy or manage it.

Colocation provides a high-performance environment for critical IT infrastructure. Customers can benefit from improved uptime and focus on core business rather than managing the operations of a data center, an opportunity to reduce operational costs, scalability of resources due to business growth, among others. Additionally, colocation provides dedicated, private connection options to hundreds of network, cloud and IT service providers to help streamline your architecture.

Montgomery County Department of Parks and Montgomery County Planning Department have executed a project to move their data center from the Montgomery County Regional Office (MRO) building to a colocation data center facility operated by Montgomery College. While data center outsourcing offers many benefits, there are still risks associated, such as:

- control over data, as you run the risk of accidental data loss when you charge another entity with critical data processing assets;
- contractual constraints, as tenants may realize that the limitations of the contracts are not to their benefit in the areas of contract termination and renewal, data and equipment ownership;
- power capacity and redundancy not meeting the tenant’s needs; and
- disaster recovery capabilities of the colocation facility in the event of a disaster.

Fundamental to “outsourcing” the hosting of the physical servers to an external facility is accepting that, while service delivery and some data center operations are transferred, accountability remains firmly with the management of the Commission — which must ensure that risks are properly managed and there is continued delivery of value from the colocation partner.

Audit Objective, Scope & Methodology

Objective: The objective of Montgomery County Data Center Colocation audit was to provide management with reasonable assurance that risks have been assessed and adequate controls conceived and implemented to ensure that legal, operational and information security gaps associated with the departments' data center move to the colocation site have been appropriately considered and treated.

Scope: The scope of the audit included but was not limited to review the areas of: Contract Management; Environmental and Physical Security; Power Supply and Redundancy; Data Center Operations; Audit and Compliance; and Disaster Recovery, as it pertains to the colocation engagement. The review included, but was not limited to, the following audit procedures:

- Verification and review of contract/agreement/MOU in place between the Commission and Montgomery College, with all necessary legal clauses and Service Level Agreement/Operation Level Agreement defined;
- Assessment of the environmental and physical security provisions and controls in place at the colocation facility to ensure that Commission IT assets are properly safeguarded;
- Evaluation of the power distribution systems at the colocation facility and the amount of built-in redundancy to ensure Commission operations are not frequently disrupted due to outages;
- Review of the controls to ensure uptime of IT equipment, and SOPs in place around data and equipment storage and overall asset management at the colocation facility;
- Evaluation of the independent 3rd party assurance assessment that the colocation facility undergoes to validate the operating effectiveness of its internal controls in safeguarding Commission data and equipment within the facility; and
- Review of the disaster recovery strategy and capabilities of the colocation facility and the Commission's responsibilities in the event of a disaster to ensure systems and network connectivity can be timely restored to enable continuous business operations.

Scope Limitation

Decision-making process leading up to the business case and ROI determination for the data center colocation initiative and alignment with Commission's long-term strategic goals weren't considered as part of the review. Rather, engagement focused on risk management processes followed during the execution of the project.

The audit to be conducted in accordance with the U.S. Generally Accepted Government Auditing Standards. Those standards require that the audit be planned, and fieldwork performed to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the established audit objectives.

Summary of Recommendations

Rec. #	Title*	Expected Imp. Date	Accountable	Functional Area
Important Recommendations				
1	Establish and implement a disaster recovery strategy for Commission assets at the colocation data center to ensure successful restoration of systems and data in the event of a disaster.	December 2019	ITI	Disaster Recovery
2	Perform formal risk assessment and retain all necessary supporting materials as part of project documentation.	December 2019	ITI	Power Supply & Redundancy
3	Implement a solution to remotely monitor IT equipment for uptime and system health at the colocation data center.	Completed	ITI	Data Center Operations
4	Define acceptable service levels and metrics to be used for monitoring data center performance, ensuring quality of service.	December 2019	ITI	Contract Management

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

Recommendations & Action Plans

Recommendation 1

Establish and implement a disaster recovery strategy for Commission assets at the colocation data center to ensure restoration of systems and data in the event of a disaster.

Overall Accountable	Risk Type	Risk Rating	Regulatory Impact
	IT Governance	High	No

Issue	During discussions with the Montgomery County Park and Planning IT team (ITI), it was noted that a formal and documented disaster recovery strategy/plan has not yet been formulated to ensure the successful restoration of Commission IT assets at the secondary data center at Saddlebrook (disaster recovery site) in the event systems at the colocation data center are not accessible. According to IT Management, the Saddlebrook location currently being used by Park Police will serve as a secondary data center for Montgomery County's Department of Park and Department of Planning. For the purpose of disaster recovery, critical data and systems will be replicated at the Saddlebrook data center and leveraged in the event of a disaster. IT management however stated that a formal disaster recovery plan and procedures haven't been formulated to enable the recovery of said data and systems from the secondary data center.
Criteria	The existence of a disaster strategy and plan ensures that IT resources (systems, data) are successfully restored to ensure continuation of business operations in the event the primary data center experiences a natural disaster or an unexpected prolonged outage.
Impact	In the absence of a formal and effective IT disaster recovery plan, the Commission will be unable to recover critical IT assets in the event the colocation data center experiences an outage which renders the accessibility of IT resources at the facility impossible.

Action Item(s)	Executor(s)	Target Date
1) Identify and document all systems and data at the colocation data center which are imperative to the continuous operations of the Commission. 2) Establish and implement formal disaster recovery procedures aimed at restoring critical business data and systems in the event the colocation data center is no longer operational due to an outage or unforeseen circumstances. Additionally, put measures in place to, at least, annually test the disaster recovery plan for effectiveness.	ITI	December 2019

Management Response	A document recovery operating procedure is now in place. Formal documentation is being prepared. At the time of audit, the colocation was in its initial stages with no production systems in place; therefore, a formal and effective disaster recover plan was premature.
Action Plan	Prior to installing any equipment or moving any production servers or applications into the colocation facility, we identified the need for a backup and recovery plan for the collocated servers. We met with several industry standard disaster recovery companies such as Zerto, HPE and an independent contractor (Infosys) to discuss disaster recovery strategies, options and software. After reviewing several options and determining a strategy, we proceeded with moving several test servers into the data center to test backing up and restoring critical systems and data. 1. For VMWare virtual servers (which constitutes 85% of our production environment), we utilize Veeam Backup and Replication for backing up our virtual servers. Further, we have tested replicating the virtual servers to our disaster recovery site (Park Police). This procedure replicates an exact snapshot of the virtual server to the location. In the event of a failed server or other event, the replicated server can be failed over to and brought into production in a matter of minutes; with a few adjustments such as IP changes. 2. For physical servers we are utilizing the Veeam Microsoft Agent to backup the physical server to the Veeam repository. The backed up data is then replicated to Park Police but utilizing the Remote Copy feature built into the HPE 3PAR 7400 system. This utilizes the HPE 3PAR virtual volumes and we can replicate (copy) entire volumes to the destination. This method initially takes a 24 – 48 hours to synch and then continually updates the replicated data when changes are made. In case of failure at the collocated facility, these volumes can be mounted and presented to other servers to retrieve the data or attach the virtual volume to a different server. 3. Our plan is to move the current HP 3PAR HPE 6400 at MRO to the Park Police facility and utilize backup to tape as a secondary archiving solution for both the virtual servers and physicals servers (#1 & #2 above).
Follow-Up Date	January 2020

Recommendation 2

Perform formal risk assessment and retain all necessary supporting materials as part of project documentation.

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

Issue	During discussions with the Montgomery County Park and Planning IT team, it was noted that documentation of a formal risk assessment being performed prior to project execution—identifying all possible risk areas of the initiative and proposed mitigating controls—couldn't be obtained upon request. IT management stated that a risk assessment was performed but evidence couldn't be obtained for verification. Specifically, a request was made to obtain formal documentation describing the power distribution systems and redundancy controls built into the design of the colocation data center but only a verbal description of said design and controls could be obtained from Commission IT personnel and so could not be verified.
Criteria	Every business decision has its own set of risks involved. Performing a risk assessment before an IT initiative ensure that possible risks that could undermine the normal operation of a system or a business process are proactively accounted for and treatment prepared prior to execution. Also, it is more cost-effective to treat risks during the planning stage when after a system/process becomes fully functional.
Impact	Non-performance of a comprehensive risk assessment of a project/system/process prior to full go-live could lead to inadequate controls in place to mitigate critical risks resulting in financial loses.

Action Item(s)	Executor(s)	Target Date
Implement procedures requiring a formal risk assessment (identification of possible process or system risks and mitigating controls) to be performed for data center projects and other Commission IT engagements prior to project execution and formally document and retain all project due diligence materials in a secured location as part of overall project documentation for future IT initiatives.	ITI	December 2019

Management Response	Planning for the data center colocation began more than one year in advance of the installation of the first test equipment at the data center. Risk assessment was in the forefront of the planning process, addressed in the MOU with Montgomery College, and risks were identified and mitigated throughout the planning phase. All remaining risks have been identified and accounted for in our standard operating procedures.
Action Plan	ITI will provide documentation of standard operation procedures as recommended. Background: Prior to the final decision to move equipment to the colocation facility, we met with several consultants and the data center manager to discuss the risks associated with having our servers hosted at an off site location. All meeting attendees had on-hands experience with data center moves and co-locations. These discussions included many areas such as disaster recovery, remote monitoring, power requirements, security, accessibility and responsibilities. The auditor was given a very indepth tour of the facility and he spoke with the on-duty technicians regarding the power distribution systems and how the redundant power system works; fire suppression systems, water detection systems and security camera monitoring inside the data center.
Follow-Up Date	January 2020

Recommendation 3

Implement a solution to remotely monitor IT equipment for uptime and system health at the colocation data center.			
Overall Accountable	Risk Type	Risk Rating	Regulatory Impact
	Safeguarding of Assets	Moderate	No

Issue	A review of the colocation agreement revealed that the College is only responsible for monitoring the status and health of their infrastructure at the data center but not equipment belonging to the Commission. During discussions with the Montgomery County Park and Planning IT team, the OIG inquired about a solution in place to ensure that Commission equipment installed at the data center could be continuously monitored for uptime and status. It was however stated by IT Management that there currently isn't a solution available for that purpose but there is an ongoing discussion to procure a tool that will give IT personnel the capability to perform such remote system monitoring.
Criteria	Monitoring of data center IT equipment ensures that IT resources are readily available for end-users and also leads to quicker detection and subsequent resolution of issues that arise with the data center infrastructure.
Impact	Not having a means of monitoring the status and health of IT equipment at the data center could result in late detection and resolution of issues, leading to prolonged downtime and lost productive.

Action Item(s)	Executor(s)	Target Date
Implement a solution to enable Commission IT personnel to be able to remotely monitor equipment uptime and health at the colocation data center in real time basis to ensure issues are immediately detected and timely resolved.	ITI	Completed

Management Response	The audit process took place during the initial stage of data center collation with no production servers in place. Since the audit, the ITI Division has installed sophisticated monitoring software for remote monitoring and diagnostics of all production servers in place at the data center on a 24/7/365 basis.
Action Plan	Background: During the active audit, we were in the process of implementing What's Up Gold which monitors the connectivity and health of the equipment and servers at the co-location facility. We are also utilizing a Harbornet application which also monitors the uptime and network connectivity of the equipment and to some extent hardware issues. In addition, the data center has built-in environmental controls that alert the on-duty techs if any heat issues are in the racks. The techs also do several walk arounds per day, physically looking at the equipment in the racks to see if any flashing red or amber lights are present. We currently have remote access to all of our equipment and have the capability to reboot anything remotely.
Follow-Up Date	January 2020

Recommendation 4

Define acceptable service levels and metrics to be used for monitoring data center performance, ensuring quality of service.

Overall Accountable	Risk Type	Risk Rating	Regulatory Impact
	IT Governance	Low	No

Issue	During discussions with the Montgomery County Park and Planning IT team, it was noted that no operational metrics have been defined and established to monitor service delivery performance to ensure quality of service (uptime, bandwidth).
Criteria	Defining acceptable service standards in a partnership ensures that IT and the business are aware of the service delivery expectations and obligations, and avoids confusion.
Impact	Not having an agreed-upon Service Level Agreement (SLA) with acceptable service level standards defined in place could result in disagreements with regards to service expectation amongst the parties.

Action Item(s)	Executor(s)	Target Date
Define acceptable service level standards for critical data center infrastructure (power, connectivity, etc.) and implement key operational metrics for measuring their performance.	ITI	December 2019

Management Response	Bandwidth and uptime of M-NCPPC equipment, located at the data center, is a function of the network infrastructure, not the data center. We do rely on the data center power; however, the power infrastructure at Montgomery College is redundant and is superior to MRO and rated tier 3 in the industry. The move to the data center does not jeopardize bandwidth or uptime but increases its reliability due to power improvements.
Action Plan	We are currently connected to the College data center utilizing the Montgomery County Fibernet. Fibernet is also utilized at many Park and Planning locations throughout the County. Currently, there is an SLA from the Montgomery County Government Department of Technology Services, Network Services Group dated May 25, 2016 for agencies using the Fibernet connections. This document is available for review upon request. Bandwidth and quality of service is handled by the DTS division and Fibernet is being monitored by a NOC 24/7. Any outages or issues are reported by the NOC to all agencies. Fibernet is continually improving and evolving as the need for higher bandwidth is required for applications such as Office 365 (off premise email service); SharePoint, Microsoft Teams, and cloud hosted applications and servers in Azure and Google. ITI will maintain SLA on file for reference.
Follow-Up Date	January 2020

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.