Internal Audit Report

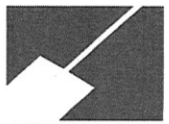
Enterprise IT Change Management Audit

Audit #: CW-011-2018

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

June 30, 2018

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



CW-011-2018

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

June 30, 2018

To: Mazen Chilet, Chief Information Officer

Joe Bistany, Enterprise IT Division Chief

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

Sadat Osuman, CISA, CRISC
IT Audit Manager

Re: Enterprise IT Change Management Audit (CW-011-2018)

Enclosed is our final audit report summarizing the results of our audit of Commission-wide systems' change management processes.

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
Casey Anderson
Elizabeth Hewlett
Patricia Barney

Audit Committee
Dorothy Bailey
Norman Dreyfuss
Karen Tobat
Benjamin Williams

M-NCPPC
Chip Bennett
Adrian Gardner
Barbara Walsh
Joseph Zimmerman

IT Council
Jim Cannistra
Darin Conforti
Tina Patterson
Mitra Pedoeem
Carol Rubin
Bill Spencer

Executive Summary – Enterprise IT Change Management

Conclusion	Overall, the result of interviews and testing performed to assess the effectiveness of IT change management controls for the in-scope systems and applications indicated highly inconsistent practices across the Commission. There is no formal guidance on how changes are to be managed throughout the life cycle and as a result, different procedures are followed for each of the systems. Additionally, supporting documentation at each stage of the current change management processes are not retained.

Overall Audit Rating	Issue Classification			Significance
 Moderate	Recommendations			Change management is a process designed to understand and minimize risks while making IT changes. Businesses have an expectation of the services provided by IT to be: stable, reliable, and predictable **and** able to change rapidly to meet evolving business requirements. The in-scope applications are heavily relied upon across the Commission and so requires a controlled process to implement changes to ensure system availability.
	Critical	Strategic	Important	
Audit Fieldwork	-	1	2	
May 2018				

Audit Risk Ratings by Functional Area*

High	Elevated	Moderate	Low
▪ None	▪ None	▪ Change Management Process ▪ Segregation of Duties	▪ Emergency Changes ▪ Monitoring & Reporting

Top Initiatives Prioritized with Management	Issue Classification	Functional Area
Establish and implement a Commission-wide IT change management policy to serve as the governance framework for managing changes within the Commission's IT landscape. *Expected Implementation Date – 06/30/2019*	*Strategic*	Change Management Process
Appropriately establish business ownership of Commission systems and applications. *Expected Implementation Date – 12/31/2018*	*Important*	Change Management Process
Establish, implement and formalize a medium through which IT-related changes are submitted for review and subsequent approval. *Expected Implementation Date – 01/31/2019*	*Important*	Change Management Process

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

Business Overview

IT change management is a process designed to understand, evaluate, and minimize risks associated with making changes to the IT infrastructure. The IT infrastructure typically contains various systems and applications as well as the network topology. The Maryland-National Capital Park and Planning Commission's (Commission) Enterprise IT team (EIT) provides support for systems and applications classified as enterprise (i.e. – used by several Commission departments and units). The in-scope applications and systems included:

- Lawson V9 ERP
- Kronos
- EnergyCAP
- Accounting Online System (AOS)
- Firewall which controls inbound and outbound traffic on the Commission's network.

IT landscapes change over time to keep pace with evolving technology (e.g. system upgrades) and business needs. Failure to effectively manage changes made to systems and applications could result in service disruption. A change not properly assessed could result in system downtime, and inefficiencies in business processes. The goal of most IT change management processes is to implement changes in the most efficient manner, while minimizing the negative impact on customers. A properly implemented change management process can enable a greater volume of useful changes by:

- Assuring all proposed changes are evaluated for their benefits and risks, and that all impacts are considered;
- Prioritizing changes to ensure limited resources are allocated to changes that produce the greatest benefits;
- Requiring all changes to be thoroughly tested;
- Identifying a back-out plan to restore to the state of the environment in the event that the deployment fails; and
- Ensuring a configuration management system is available and updated to reflect the effect of all changes on dependent systems.

Audit Objective, Scope & Methodology

Objective: The objective of the Enterprise IT Change Management audit was to perform a review of the current IT change management process and practices to provide management with assurance that they are controlled, monitored and follows best practices.

Scope: The audit assessed the operating effectiveness of the change management process and supporting activities from other processes necessary to manage the entire life cycle of an IT change request (from initiation to implementation). The review included, but was not limited to the following systems/applications – Lawson ERP, Kronos, EnergyCAP, AOS and EIT Firewalls, and audit procedures:

- Evaluated documented IT change management procedures and practices for appropriateness and ensured they are consistently adhered to commission-wide;
- Evaluated different change management roles and ensured there is segregation of incompatible duties in the process;
- Reviewed the impact analysis methodology utilized as part of the IT change management process and ensured that implemented changes did not introduce any unplanned or adverse effects into the IT landscape;
- Reviewed a sample implemented system and application changes to ensure that the proper procedures of change request, change planning, change review and approval by the appropriate personnel, change implementation and change closure were followed;
- Evaluated documented process in place to initiate, review, approve, implement and close out emergency changes; and
- Determined whether metrics have been established to track the performance of the IT change management process and are being reported on to senior management.

The audit period was from April 1, 2017 through April 30, 2018.

Scope Limitation

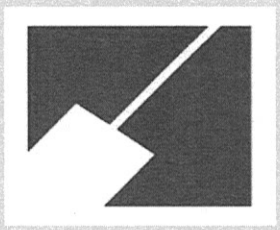
Processes affecting functions prior to the request or incident/problem ticket entering the change management process are out of scope for this review.

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

Rec. #	Title*	Expected Imp. Date	Accountable	Functional Area
	Important Recommendations			
1	Establish and implement a Commission-wide IT change management policy to serve as the governance framework for managing changes within the Commission's IT landscape.	06/30/2019	[redacted]	Change Management Process
2	Appropriately establish business ownership of Commission systems and applications.	12/31/2018	[redacted]	Change Management Process
3	Establish, implement and formalize a medium through which IT-related changes are submitted for review and subsequent approval.	01/31/2019	[redacted]	Change Management Process

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



Recommendations & Action Plans

Recommendation 1

Establish and implement a Commission-wide IT change management policy to serve as the governance framework for managing changes within the Commission's IT landscape.			
Overall Accountable	Risk Type	Risk Rating	Regulatory Impact
[redacted]	IT Governance	High	No

Issue	A. Through discussion with various stakeholders of the in-scope applications and systems, it was noted that the Commission currently doesn't have an IT change management policy to provide guidance on how changes to information systems are to be managed and controlled. B. Through discussion with various stakeholders of the in-scope applications and systems, it was noted that there isn't a formal requirement for maintaining segregation of duties within the change management process. C. Through discussion with the EIT team, it was noted that there's currently no provision or guidance on how emergency changes that require bypassing the normal change process are to be handled and controlled to ensure that operations are not severely impacted. D. Through discussion with EIT, it was noted that the performance of the change management process is not being monitored and reported on, using metrics and indicators, to provide management information on the process effectiveness and reveal areas of improvement.
Criteria	Policies serves as the foundation and governance framework for any organization as it provides guidance on what is acceptable behavior and vice versa. According to *GTAG: Auditing IT Governance*, "IT governance supports the organization's regulatory, legal, environmental, and operational requirements to enable the achievement of strategic plans and aspirations".
Impact	In the absence of formalized policies and procedures, changes could be made to information systems without proper authorization and in an uncontrolled manner.

Action Item(s)	Executor(s)	Target Date
1.) Establish and implement a Commission-wide change management policy to serve as the governance framework for managing IT-related changes to information systems. Policy should be appropriately communicated to all stakeholders and address, at a minimum, the following: a. guidelines for when a post implementation review is required after a change has been implemented. b. a requirement for all changes to have a formal and documented back out plan prior to deployment. c. a requirement for assessing, at least, the business and security impact of all changes as part of the evaluation process. d. a requirement for maintaining segregation of incompatible duties within the change management process. e. guidelines for managing and controlling IT-related emergency changes within the Commission's system landscape. f. a requirement to assess and document all possible impacts a change could potentially have on other dependent systems prior to implementation. **2.)** Identify and implement key operational metrics for measuring the performance of the change management process so as to drive continuous improvement.	[redacted]	06/30/2019

Management Response	Management agrees with the recommendation and notes the significance of the implications outlined. The CIO will actively work on developing and implementing a Commission-wide change management policy to serve as the governance framework for managing IT-related changes to information systems. The policy will be applied the Commission's IT landscape with the objective of mitigating the identified risks.
Action Plan	• Gain IT Council support to develop and implement a Commission-wide change management policy to serve as the governance framework for managing IT-related changes to information systems. • Revisit existing Change Management control process documentation and updating it to reflect current environment. • Enforce the use of the Change Management Policy to ensure that all changes are appropriately authorized, tested, approved, monitored and documented. • Optimize the use of existing change management tools to ensure that all changes are effectively identified and recorded. • Develop a complete IT Change Management Process to accomplish IT changes in the most efficient manner while minimizing the business impact, costs, and risks. • The change management process will be developed to include the following key steps: ➢ Formal Change Request ➢ Categorize the change ➢ Prioritize the Change ➢ Analyze the change ➢ Approve/Deny the change ➢ Schedule the change ➢ Plan and Complete the Implementation of the Change. ➢ Post-Implementation Review • Consider using version management technology platform to ensure that adequate monitoring and controls are in place to capture and document all IT changes in the Commission's selected technology platform. • Policy should be appropriately communicated to IT Council and other stakeholders.
Follow-Up Date	July 31, 2019

Recommendation 2

Appropriately establish business ownership of Commission systems and applications.			
Overall Accountable	**Risk Type**	**Risk Rating**	**Regulatory Impact**
[redacted]	IT Governance	Low	No

Issue	During the performance of field work, OIG couldn't identify the appropriate business system owners for the Accounting Online System (AOS) and EnergyCAP applications. For both AOS and EnergyCAP, Accounts Payable noted that IT was the business owner which IT denied. IT's role, however, is to provide technical support for the systems/applications based on needs dictated by the business and should not be assigned overall business ownership of Commission financial applications.
Criteria	Systems and applications are assigned a business owner. By assigning a business owner, it can be ensured that IT changes made to the system are in alignment with business goals and priorities and not cause any adverse effects on business operations.
Impact	In the absence of a business owner, IT cannot maintain an effective alignment with the business in ensuring that system capabilities and enhancements that could benefit users are being communicated and realized in full potential.

Action Item(s)	Executor(s)	Target Date
Establish ownership of Commission-wide information systems by assigning business owners to ensure that business needs and potential system enhancement opportunities are being communicated to and executed by IT.	[redacted]	12/31/2018

Management Response	Management agrees with the recommendation and notes the significance of the implications outlined. The CIO will work Finance and DHRM and the IT Council as appropriate to establish distinct ownership of Commission-wide information systems where EIT implements business requirements for enhancement of existing and the development of new systems with the objective of mitigating the identified risks.
Action Plan	Management agrees with the recommendation and notes the significance of the implications outlined. The CIO will work Finance and DHRM and the IT Council as appropriate to establish distinct ownership of Commission-wide information systems where EIT implements business requirements for enhancement of existing and the development of new systems with the objective of mitigating the identified risks.
Follow-Up Date	January 31, 2019

Recommendation 3

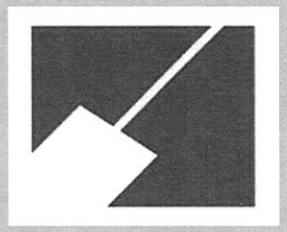
Establish, implement and formalize a medium through which IT-related changes are submitted for review and subsequent approval.

Overall Accountable	Risk Type	Risk Rating	Regulatory Impact
[redacted]	IT Governance	Low	No

Issue	Through discussion with system and application stakeholders, it was noted that while firewall changes mostly required a request for change (RFC) form to be filled out and sent for necessary reviews and approvals, the other systems did not. Lawson changes are requested by opening a Jira ticket with Lawson AMS; AOS and Kronos changes are requested through email; and EnergyCAP changes (mostly in the form of software upgrade or database changes) do not go through a formal review and approval process prior to implementation. Moreover, change requests and other supporting documentation are stored in disparate forms and location across the Commission.
Criteria	All IT change requests should be reviewed and approved with supporting documentation centrally stored. This provides a single source of truth for Commission-wide IT change requests.
Impact	An informal and disparate process could result in the inability to produce supporting documentation to support implemented IT changes in the context of regulatory and legal compliance.

Action Item(s)	Executor(s)	Target Date
Adopt a single system/mechanism to be used in the request, evaluation and approval of all IT changes for all in-house systems and applications, as dictated by IT Change Management Policy, and ensure that all associated supporting documentation are centrally stored.	[redacted] & Project Management Office	01/31/2019

Management Response	Management agrees with the recommendation and notes the significance of the implications outlined. The CIO is actively working on the practical implementation of sound change management processes for EIT and across the organization with the objective of mitigating the identified risks.
Action Plan	• Gain IT Council Support to develop standard process utilizing a specific Change Management tool (Track-It!) and rollout to EIT and Departmental IT Divisions. • IT Council to review and approve the Change Management Plan • Implement the approved standard for EIT and Commission-Wide • Regular Change Control Meetings, to be reported back to the Joe Bistany, Enterprise IT
Follow-Up Date	February 28, 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.