Audit of MassDOT IT PROJECT MANAGEMENT OFFICE

MassDOT Audit Operations (IT)
September 9, 2026

To: Finance and Audit Committee

From: James Logan, Director of Audit Operations
Date: September 9, 2026
RE: **MassDOT IT Project Management Office (PMO) 2025**

Executive Summary

MassDOT's IT Project Management Office (PMO) supports IT projects by guiding project development and resources allocation. The IT PMO also tracks and reports project progress to stakeholders. Additionally, IT PMO identifies, assesses, and mitigates applicable IT risk.

The audit was conducted from January 30, 2025, through August 2025. The period covered by the audit was January 1, 2024, through December 31, 2024.

The objective of this audit was to assess the IT PMO's technology project management program processes, controls, policies, and procedures including their alignment with project goals and objectives. Further, Audit Operations' objectives were to assess, verify, and validate the IT PMO's control environment to ensure that it is well designed and effective to provide sufficient mitigation of risk.

Audit Operations concluded that the IT Project Management Office internal control environment is generally well designed and operating effectively to support successful IT project delivery and mitigate project management risks. Two minor control deficiencies were identified, presenting opportunities to further enhance the design and effectiveness of internal

controls. Detailed audit findings are provided below. Detailed audit findings follow on pages 7-13.

Audit would like to thank the Project Management Office personnel for their assistance during the course of this audit. Attached is the audit report, which details the findings, recommendations, division management responses, and plans for corrective actions (Management Action Plans – MAPS).

Please contact Jim Logan if you have any questions or concerns at 857.368.9777 or James.Logan@dot.state.ma.us.

CC:

Phillip Eng, Secretary and CEO, MassDOT
Jonathan Gulliver, Undersecretary, MassDOT
Meghan Haggerty, Chief Operating Officer, MassDOT
Anu Goutham, Chief Information Officer, MassDOT
Bill Catania, Deputy Chief Information Officer, MassDOT
Annemarie Carter, IT Project Management Office Lead, MassDOT
Christopher Treanor, Senior IT Consultant, MassDOT
Emily Pedersen, Director of Special Audit Unit, OIG
Ashley Amado, Deputy Director, OIG

TABLE OF CONTENTS

I. BACKGROUND.....5

II. AUDIT OBJECTIVE AND SCOPE.....5

III. OVERALL ASSESSMENT.....5

IV. AUDIT FINDINGS.....7-14

V. APPENDIX.....14-15

I. BACKGROUND:

The IT Project Management Office (PMO) is responsible for supporting the implementation of new IT-related MassDOT projects. The IT PMO determines the appropriate project management processes based on the project funding source(s). Assigned Project Managers oversee required system development, coordinate the allocation of resources (e.g., funding, staffing), track project milestones, and communicate progress to stakeholders. Additionally, the IT PMO is responsible for ensuring that projects comply with applicable laws, regulations, industry project management standards, and internal policies from initiation through implementation. Lastly, the IT PMO also identifies, assesses, mitigates, and manages risks throughout the project lifecycle.

II. AUDIT OBJECTIVE AND SCOPE:

Audit Operations conducted this audit to determine whether technology projects follow IT industry best practices and comply with applicable laws, regulations, and MassDOT policies and standards.

Audit Operations evaluated the design, implementation, and effectiveness of the IT PMO's project management internal control environment, including its policies, procedures, and processes. The primary objective of this audit was to determine whether applicable internal controls operate as intended to sufficiently mitigate risks and align with project goals and objectives.

III. OVERALL ASSESSMENT:

Based on the audit work performed, Audit Operations determined that the IT Project Management Office's internal controls are generally well designed and operating effectively to support project delivery and mitigate related risks.

Two minor control deficiencies were identified as opportunities to further strengthen the control environment. Detailed audit findings are provided below.

IV. AUDIT FINDINGS

Finding Title	Ranking	Page
Lack of Proper Recording of Segregation of Duties	Minor	8
Policies and Procedures Are Not Reviewed Regularly	Minor	12

Finding: Lack of Proper Recording of Segregation of Duties

Rating: Minor *(See Appendix A for risk rating details.)*

Segregation of Duties (SOD) reduces the risk of misuse of authorized privileges by ensuring that no single individual controls multiple stages of a critical process.

Per National Institute of Standards and Technology (NIST) guidelines,

> *Separation [segregation] of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example, dividing mission functions (development) and system support functions (among different individuals and/or roles; conducting system support functions with different individuals; and ensuring security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation [segregation] of duties.*

Further, per GUI-12 MassDOT SDLC (Software Development Life Cycle) Guidelines FY25, Pg 14.,

> *…to enforce segregation of duties for production deployments, the resource (person) performing the deployment (i.e., the Release Engineer) must not be the same resource who developed or tested the changes.*

Additionally, per the guidance provided in PRO-003 IT Change Management,

> *…To enforce best practices, the person deploying the changes to production should not be the same person who developed (or approved) the changes.*

The IT Project Management Office (PMO) did not consistently track or record evidence of segregation of duties (SOD) within project documentation or within ServiceNow change (CHG) tickets. Audit Operations reviewed the CRASH VU project materials maintained in SharePoint and found no evidence that the PMO identified, monitored, or documented evidence of compliance with SOD requirements. In addition, Audit Operations' review of 203 Service Now CHG tickets—including a random sample of 40, and a subsequent review of the full population found no Service Now tickets that clearly documented production changes with corresponding SOD controls. Audit Operations' walkthrough with PMO and ServiceNow leadership further showed inconsistent and unclear notation of SOD within ServiceNow, making evidence of compliance with SOD controls not readily identifiable either by the IT PMO or other groups that utilize the Service Now module.

Audit Operations did not perform a comprehensive review of the segregation of duties controls within the Change Management process, as this area fell outside the scope of the current audit. Moving forward, Audit Operations will evaluate this component during the risk-based audit planning process to assess the necessity for a targeted audit in the future.

Risk:

Without consistent tracking, documentation, and monitoring of segregation of duties, the PMO cannot demonstrate that critical SDLC controls are implemented for projects involving changes to the production environment. This increases the risk that unauthorized, unreviewed, or inappropriately approved changes may be migrated to production, potentially compromising system integrity, security, and operational reliability. The lack of transparent SOD evidence also limits management's ability to ensure accountability.

Recommendation: The IT PMO should develop, formalize, and implement standardized procedures requiring consideration of, and consistent documentation and monitoring of segregation of duties across all projects and ServiceNow change activities. These procedures should include:

1. Clear documentation requirements for SOD within project artifacts and ServiceNow CHG tickets, including how SOD must be identified, documented, approved, and retained.
2. A uniform method for documenting SOD in ServiceNow, ensuring that SOD notation is clearly visible, consistently applied, and traceable.
3. Periodic oversight or quality reviews to confirm that PMO staff and project managers follow established SOD documentation and approval processes.
4. Training for PMO and technical staff to ensure consistent understanding and implementation of SOD requirements across all SDLC (Software Development Lifecycle) - related activities.

Implementing these recommendations will strengthen PMO governance, improve control consistency, and reduce the risk of unauthorized or improperly documented changes moving into the production environment.

Management Response:

We acknowledge the audit finding regarding **Proper Recording of Segregation of Duties** and the need for formalized procedures to ensure consistent documentation, monitoring, and oversight of segregation of duties (SOD) across all projects and ServiceNow change activities. We agree and are committed to implementing processes to address the findings.

We aim to complete process improvement within the next **3 months**. Training for staff and oversight activities will commence immediately upon finalization of the procedures, with periodic reviews to evaluate compliance and effectiveness.

We appreciate the recommendation, as it aligns with our commitment to strengthening IT governance and ensuring proper controls exist within our project and change management processes. Should you require further details on our action plan or timeline, please feel free to reach out.

Responsible Parties: Chief Information Officer (CIO), IT Project Management Office Practice Lead

Management Implementation Date: March 30, 2026

Finding: Policies and Procedures Are Not Reviewed Regularly

Rating: Minor *(See Appendix A for risk rating details.)*

IT best practices state that policies and procedures should be reviewed regularly. Additionally, MassDOT's IT policy indicates that governance documents should be reviewed annually.

Specifically, MassDOT Information Security *STA-001 Governance Documentation Standard ver. 1.3, page 8, section 4.3 states*:

> *Document owners are responsible for reviewing their governance documents at the frequency shown in the table of information on the title page, which must be at least annually. Forms and Registers that do not specify this frequency must be reviewed annually. For reviews that do not include changes to the document, the owner.*

MassDOT Information Security STA-001 Governance Documentation Standard ver. 1.3, page 4, section 1, "governance documents" as follows:

> *…governance documents include charters, forms, information system security plans, manuals, policies, processes, standard operating procedures, and standards.*

Audit Operations concludes that the IT PMO does not review its documents consistently, in accordance with IT best practices, and applicable MassDOT policy.

Risk:

Without regular periodic reviews, documentation may not provide employees with the latest guidance in the absence of Management. A lack of up-to-date guidance may result in reputational and/or financial damage to MassDOT.

Recommendation: The IT PMO Management should establish a plan to review its policies and procedures on a regular, periodic basis and when there is a change in key personnel, processes, or state guidance.

Management Response:

We acknowledge the audit finding concerning the need for regular, periodic reviews of IT PMO policies and procedures to ensure alignment with current processes, personnel, and state guidance. We agree with the recommendation and recognize the importance of maintaining up-to-date documentation to mitigate potential risks.

Responsible Parties:

CIO
IT PMO Practice Lead

We are committed to implementing this plan effective January 2026.

Management Implementation Date: January 30, 2026-Closed

VI. *APPENDIX A: DEFINITION OF AUDIT FINDING RATINGS*

Finding Level	Definition	Action Required
Critical	Critical issues occur where required controls and safeguards are deficient or non-existent to mitigate the highest risks and/or to ensure statutory compliance. It is very likely that the issue will pose a significant imminent threat to employee and public safety and/or lead to significant financial loss, legal penalties, and major operational disruptions.	Immediate corrective action is necessary. Management should prioritize addressing these findings to mitigate risks and prevent further issues.
Major	Major issues occur when there are controls in place but may require some improvement or better execution to ensure full coverage of statutory requirements and/or to better mitigate significant risks. While not imminent or critical, the issue could affect safety, compliance, financial accuracy, or operational efficiency. These could become critical if not addressed promptly.	Management should develop and implement action plans promptly to address these findings and improve processes and controls.

Finding Level	Definition	Action Required
Minor	A minor issue that must be addressed in a timely manner. These findings do not pose immediate threats but may lead to minor risks, inefficiencies or process gaps where improvements can enhance efficiency and effectiveness.	Management should address these findings as part of ongoing improvements efforts.
Observation	An observation that does not pose an immediate risk but represents opportunities for improvement. These may include best practices, process optimizations, or areas for increased efficiency.	Management may consider these observations for continuous improvement, but they do not require immediate action.