Vendor Management Follow-Up Performance Audit

Report #: 2024-21

Executive Summary

2 CFR 200.318(h) mandates Sound Transit (a non-Federal[1] and public entity) to award contracts only to responsible contractors who demonstrate the ability to perform successfully under the terms and conditions of a proposed procurement. This includes evaluating records of past performance, as well as financial and technical resources. Further guidance is provided by 48 CFR 42.15, which requires the assessment of vendor performance to make informed procurement decisions, monitor high-risk vendors and ensure compliance with applicable regulations.

Accordingly, best practices define vendor management as a strategic process focused on optimizing vendor relationships to maximize value and minimize enterprise risk.

Audit Objective

We performed a follow-up performance audit of the agency's vendor management process to review compliance, implementation, and existing controls where risks were assumed without corrective action. This involved examining procurement and contract documents, checking records for compliance, and conducting interviews and process walkthroughs.

The audit period covers calendar years (CY) 2023 through 2024.

Conclusion

From our audit, we identified two (2) findings and one (1) observation; listed below and discussed in more detail beginning on page 4 of this report.

Summary of results:

Ref #	Title of Issue	Risk Rating
F.1	Vendor performance assessments for public works and A&E contracts are not formalized.	*4C - Medium*
F.2	IT vendor performance is not well documented, and past performance is not considered in procurement decisions.	*4C - Medium*
O.1	Some IT Contracts did not undergo the Vendor Risk Assessment Process	*n/a*

[1] 2 CFR 2900.2 defines a non-Federal entity as a state, local government, [...] that carries out a federal award as a recipient or subrecipient.

Background

Methods of evaluation and verification

To assess compliance during the audit, the auditors completed the following steps:

- Interviewed Procurement, Contracts, and Agreements (PCA) and Information Security (InfoSec) staff to verify their understanding of the current vendor management practices, such as vendor risk and contract management.
- Assessed records for evidence of implementation and adherence to compliance standards.
- Compared agency PCA program-related policies and procedures against state and federal requirements.
- Sampled and reviewed records in public works, architectural & engineering (A&E), and IT contracts to assess compliance.

Audit Standards

We conducted our performance audit in accordance with our charter and Generally Accepted Government Auditing Standards (GAGAS or “Yellow Book”) issued by the United States Government Accountability Office (GAO) and with the Global Internal Audit 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 objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Also, the Audit Division is committed to following safety oversight standards set forth by the Federal Transit Administration (FTA), Federal Railroad Administration (FRA), and all other relevant auditing requirements or standards.

Audit topic overview

The agency uses a decentralized vendor management approach, with contract project managers (PMs), primarily senior management or mid-level managers, responsible for contract oversight, documenting vendor performance and contacting Contract Specialist (CS) when needed. This approach has led to inconsistencies in vendor performance assessments, documentation of issues, and limited monitoring across project teams and divisions.

Information Security (InfoSec), amongst other agency risk stakeholders, has already implemented a Vendor Risk Management (VRM) program; however, it's just one part of a larger framework to manage vendors.

Summary of prior audit

In 2022, we performed an audit over the agency's vendor management process to assess management controls during pre-procurement, continuous monitoring of performance management and vendor risk.

That audit resulted in two (2) findings shared between Procurement (PCA) and IT (InfoSec), consisting of the following:

1. The need to enhance visibility for all in-scope procurements.
2. The need to improve contract management oversight.

PCA management disagreed with the audit findings, indicating that visibility is already provided through various methods, including CREI, Concurrence Review Application (CoRA), Risk Management Division. This is also alongside reporting tools and comprehensive policies, procedures, and training that are already in place.

As part of our review, we found that the 2022 audit follow-up showed progress in several areas:

Division	Action Items	Status
IT / InfoSec	Implement feedback loop for contract language inclusion	Implemented
	Expand vendor risk management program	Implemented
	Information Security contractual oversight for tier 2 & 3	Implemented
PCA / D&C	Contractor/consultant performance evaluation tool and process	In Progress

Table 1. Summary of Remediation Progress. **Note:** Despite broader disagreements, D&C has taken strides towards enhancing their consultant and contractor tools and process, which have been in place since the last audit. Thus, follow-up audit procedures were applied to ensure adequate coverage of this key activity as part of the engagement.

Our follow-up audit showed that the agency is generally in compliance and making progress on the items mentioned. However, we found that the agency needs to improve controls by formalizing and standardizing its processes for assessing and monitoring vendor performance.

Overview of Vendor Management

Best practices define vendor management as a strategic process focused on optimizing vendor relationships to maximize value and minimize enterprise risk.[2] A key component to this process is **vendor performance assessments**, which supports those initiatives and provides a comprehensive view of vendor capabilities that enhance the agency's overall value.

In alignment with this framework, 48 CFR 42.1502 requires that performance evaluations be conducted at least annually and upon the completion of work under a

[2] Best practice frameworks may include (not limited to) COBIT 2019, COBIT 5, etc.

contract or task order. This is particularly important for construction contracts at $750,000 or more and A&E services at $35,000 or more. Evaluations must also be prepared for each contract and order surpassing the simplified acquisition threshold (SAT) of $250 thousand (K). This threshold subjects all purchases above SAT to a more rigorous competitive bidding process to foster economic competition.

From 2023 to 2024, we identified 81 contracts worth $624 million (M). Of that number, we sampled 20 (approximately 27%); including 15 design and construction contracts valued at $338M and 6 IT contracts totaling $68M. These contracts were selected because they are eligible for federal awards and align with our audit focus on assessing the agency's compliance with vendor performance criteria set by federal law. See **Audit Results** in the following section and **Appendix 1** for more details.

Project Managers (PM)s who manage design and construction contracts, are supposed to ensure that contractual terms are being met and performance is satisfactory. PMs are required to conduct annual performance evaluations through the Contractor/Consultant Performance Evaluation process using an online tool; however, this does not include Job Order Contracts (JOCs) or On-Call Contracts.

For other contracts, like IT and services, evaluations aren't formally required and are left to PMs, typically division heads or designated staff, who are encouraged to follow the agency's guidelines and contract management (eLearning course). PMs should also report and document any vendor performance issues with help from the Contract Specialist (CS).

Audit Results

The following table summarizes the analysis performed during fieldwork and the associated exceptions (if any):

Criteria	Tests Performed	Results	Finding or Observation
48 CFR 42.1502 Contractor Performance Information **PCAM Section S Responsibility Contractor and Section III Contract Administration**	Reviewed 15 selected contracts eligible for federal awards (9 public works contracts and 6 A&E). Compared contracts and records against the performance database with relevant regulations and policies.	Only 82 performance assessments of approximately 208 contracts were submitted since 2021, indicative of a lack of a enforceable system and insufficient monitoring. Additionally, many contracts are missing from the database or are still awaiting approval.	Finding

Criteria	Tests Performed	Results	Finding or Observation
	Evaluated current controls for select IT Contracts eligible for federal awards, with a focus on: (1) Level of coordination between PMs and Contract Specialists; and (2) documentation of vendor performance issues.	While we found the level of coordination between PM & Contract Specialist to be compliant, we found no formal performance assessments exist for IT contracts, leading to insufficient documentation and vendor performance issues.	Finding
Vendor Risk Management Standard	Limited review on 25 IT contracts to assess the existence of tier assessments. Gained sufficient understanding through process walkthroughs and interviews with staff.	7 (or 28%) of IT contracts missed the Vendor Risk Assessment process for existing and previously contracted vendors.	Observation

Table 2. Summary Table of Audit Results.

Positive Practices

During the audit, we observed additional positive practices and continuous improvements including:

- Design & Construction (D&C) introduced an online tool for evaluating A&E and Public Works contracts, enhancing the collection of data for future procurement decisions.
- InfoSec lowered its vendor risk management threshold to $100K, expanding contract assessment and monitoring of high-risk vendors.

Moreover, strategic efforts between Executive Leadership and D&C are on-going to improve contract language, specifically targeting vendor performance evaluations and developing policies and procedures alongside associated training.

Recommendations:

Sound Transit should continue enhancing its system of controls for evaluating vendor performance. This process is crucial for tracking how well contractors and consultants are doing, addressing any problems during projects, and using past performance to make better future decisions.

To ensure that the agency achieves its strategic objectives, we recommend the following:

1. Develop formal policies and procedures for assessing vendor performance assessments, including training for ST staff involved in contract and vendor performance management.
2. Enhance contract language to set clear expectations for both ST staff and consultants/contractors.
3. Leverage the upcoming Procurement Automation Tool to monitor vendor performance. Explore features that allow users to perform vendor assessments and perform periodic reviews on high-risk vendors.
4. Improve procurement evaluation forms and instructions to ensure they reference relevant performance assessments for easy audit tracking.

   Responsibility:
   - ✓ **PCA (D&C and MTS)**
   - ✓ **Capital Delivery Program Team**

5. Define validation reporting needs and process requirements for regularly reviewing existing and previous IT contracts that need vendor risk assessment. This involves expanding VRM Standard Section 2 by defining informational requirements and designing a process to ensure a complete risk assessment for relevant IT vendors.

   Responsibility:
   - ✓ **PCA – MTS / Business owner**
   - ✓ **InfoSec**

Appendices

Sound Transit's Title VI notice of rights

Sound Transit conducts Title VI equity analyses for service and fare decisions to ensure they are made as equitably as possible.

More information on Sound Transit's Title VI notice of rights and the procedures to file a complaint may be obtained by:

- Phone: 888-889-6368; TTY Relay 711;
- Email: **stdiscriminationcomplaint@soundtransit.org**;
- Mailing to Sound Transit, Attn: Customer Service, 401 S. Jackson St. Seattle, Washington 98104-2826; or
- Visiting our offices located at 401 S. Jackson St. Seattle, Washington 98104.

A complaint may be filed directly with the Federal Transit Administration Office of Civil Rights, Attention: Complaint Team, East Building, 5th Floor – TCR, 1200 New Jersey Avenue, SE, Washington, DC 20590 or call 888-446-4511.

Report Prepared by:

Travis Ratuita Carbon Digitally signed by Travis Ratuita Carbon Date: 2024.11.04 13:38:18 -08'00'

Travis Ratuita Carbon, Sr. Performance Auditor (Lead Auditor)

Reviewed (QA/QC) by:

Heather F. Wright Digitally signed by Heather F. Wright Date: 2024.11.04 11:37:56 -08'00'

Heather Wright, Deputy Director, Audit Division

Approved for release by:

Patrick Johnson Digitally signed by Patrick Johnson Date: 2024.11.04 11:44:04 -08'00'

Patrick Johnson, Director, Audit Division

Appendix 1: Findings & Observations

Finding #1 Vendor performance assessments for public works and A&E contracts are not formalized. (Rating: 4C - Medium)

Before awarding any contract, regardless of its value, PCA must consider several factors, including past performance on similar projects, as stated in PCAM Section (S)(a)(iv) and RCW 39.04.350. Additionally, FAR Section 42.1502(e)-(f) outlines the documentation requirements for past performance evaluations, particularly for construction contracts at $750,000 or more and A&E services at $35,000 or more.

Aligned with these requirements, D&C has enhanced the Contractor/Consultant Performance Evaluation process by using an online tool for all A&E and construction contracts, excluding Job Order Contracts (JOC)s and On-Call Contracts. This aims to ensure vendor performance data is captured and used for informed procurement decisions.

We reviewed 15 selected contracts eligible for federal awards (9 public works contracts and 6 A&E) to test how well the new process manages and captures such performance data in compliance with legal requirements. We compared selected contracts and records against the performance database with relevant regulations and policies.

We found the following:

1. **There is no enforceable system to ensure that project managers and teams submit vendor performance assessments on time.**
2. **The process for assessing and monitoring vendor performance is not formalized and is currently ineffective.**

Specific testing and issues include:

- The vendor performance database has only 82 performance assessment submissions since 2021. However, ~71% of the submissions were made in June 2024, driven by new leadership in the Capital Delivery Program.
- Many reviewed contracts were not found in the performance assessment database or were still awaiting approval from Project Directors.
- Procurement evaluation forms did not reflect the use of performance evaluation tool data.

D&C senior management, alongside the Capital Delivery Program Team, is working to formalize internal controls around vendor performance assessments. However, these issues may have risen from an insufficient administrative operational structure to ensure process compliance across multiple project teams. Additionally, there aren't enough resources to effectively monitor the new performance assessment process. Currently, this initiative relies heavily on one (1) D&C Business Analyst for technical support and training, and one (1) D&C senior management member for evaluation questions.

As a result, there is 'limited assurance' that the agency is capturing vendor performance data for future procurement decisions and regulatory compliance. This increases the risk of awarding contracts to underperforming vendors.

Finding #2: IT vendor performance is not well documented, and past performance is not considered in procurement decisions. (Rating: 4C - Medium)

According to 48 CFR 42.1502(b), agencies must evaluate contractor performance for each contract and order exceeding the simplified acquisition threshold (SAT). The PCAM outlines a process for procuring goods and services above the SAT of $250K when competitive bidding is not appropriate. This process includes evaluating technical and price factors such as past performance and management during solicitation.

Sound Transit's procurement process requires that all contracts undergo a 'responsibility determination' based on objective evaluations of past performance among other factors, ensuring compliance with state and federal laws. This involves maintaining adequate records of project performance and contract administration, including reasons for contractor selection and post award activities.

Contract Management Guidelines encourages PMs to promptly notify the contract specialist of any vendor performance issue and documenting them as they arise.

During initial interviews, **MTS management indicated that vendor performance assessments do not apply to MTS-type contracts.** In the absence of a formal vendor performance assessment process for these contracts, further due diligence was conducted to assess existing controls, focusing on (1) coordination between PMs and Contract Specialists and (2) documentation of vendor management issues.

In reviewing six (6) IT contracts eligible for federal awards, we found documentation controls over vendor performance issues were lacking for five (5) contracts. Neither the Contract Specialist nor the Project Managers could provide access to records upon request, conflicting with contract documentation requirements. However, one team demonstrated strong communication protocols and tracking tools detailing issues, contractor remediation efforts, and coordination.

During interview, senior management explained that MTS uses a 'Follow-Up by Exceptions Approach,' which requires a risk-based approach[3] to determine the extent of the of the Contract Manager's role and level of administration, monitoring, and relationship management. This model supports management's decision to deploy resources needed to handle the high volume of MTS contracts during planning and pre-award phases.

[3] WA-State Contract Management Manual (dated, January 2019) states that the nature of the goods and services delivered to the Agency will determine the extent of the Contract Manager's role and level of administration, monitoring, and relationship management.

Observation: Some IT Contracts did not undergo the Vendor Risk Assessment Process

Since our last audit, InfoSec expanded its vendor risk management program in June 2023. Currently, contracts valued at $100K and above are subject to review, instead of those over $250K. This enhancement allows for more contracts to be assessed before signing. The program also includes monitoring risks associated with high-risk vendors as their contracts near expiration.

Additionally, the process is guided by the VRM Standard, which provides the scope and applicability of Vendor Risk Assessment process (VRA) over all new contracts, as well as existing and previously contracted vendors.

During our review, **we found that out of 25 IT contracts, seven (7) (or 28%) missed the VRA process for existing and previously contracted vendors.** Specifically:

- Three (3) contracts missed the Information Security's intake process and were not assigned a risk-rating level.[4] According to InfoSec management, two of these contracts were impacted by Finance's delegation of authority feature in the accounting system, which inadvertently allowed an approver to miss the Information Security verification and approval steps.
- Three (3) contracts were approved prior to the process update that took effect in June 2023. This update included lowering the threshold for Information Security E1 approval down to $100K and adding piggyback procurements to the VRM scope. However, these contracts – one software subscription renewal and two piggybacks – were not reassessed and did not have risk ratings when requested.
- For one (1) contract, Information Security could not identify a matching contract in the PCA's Contracts Visibility Tool, which hindered the assignment of a risk-rating level.

Furthermore, 5 out of 6 contracts eligible for federal awards also missed the VRA process, with one particular contract still missing internal controls despite its execution date in 2023.[4] These contracts were previously mentioned in the prior finding.

InfoSec aims to complete the identification of all in-scope vendors by 2026. However, the current conditions are primarily due to workarounds in the validation reporting process. Specifically, InfoSec manually links contracts back to requisitions and checks

[4] **Risk-Rating Level:** Sound Transit developed a scope of work (SOW)/vendor tier classification consistent with a risk-based approach that requires more stringent controls for a tier-3 SOW with greater —in number or severity— information security risk factors than a tier-2 or tier-1 SOW.

For the purposes of this audit, we renamed ‘tier classification’ to risk-rating level for ease of understanding.

results with the PCA visibility tool, but this is not sufficient due to procurement complexities.

Furthermore, the current VRM standard, Section 2, includes coordination with PCA before solicitation. Responsibilities should be expanded to support periodic reporting for validation.

While compensating controls and validation reports have been developed by Finance and InfoSec, much of the contract information is not easily accessible. Without the involvement of key process owners from MTS who know the details, effectively identifying IT contracts that have missed the process will remain a challenge.

Appendix 2: Management Response

Finding #1: Vendor performance assessments for public works and A&E contracts are not formalized. (Rating: 4C - Medium)

<table>
<tr><th colspan="4">Blocks 1 thru 11 to be completed by Auditors</th></tr>
<tr><td>1. Audit Type:
Performance Audit</td><td>2. Business Unit/Function: PCA – D&C</td><td>3. Audit Title/Project Code:
Vendor Management Follow-Up Audit (Report #: 2024-21)</td><td>4. Classification:
FINDING</td></tr>
<tr><td colspan="2">5. Auditor, Email & Phone:
Travis Carbon, Sr. Performance Auditor (206) 398-5452 travis.carbon@soundtransit.org</td><td colspan="2">6. Issued Date:
November 1, 2024</td></tr>
<tr><td colspan="4">7. Issue Description: Vendor performance assessments for public works and A&E contracts are not formalized.

8a. Recommendation: (For Findings Only)
1. Develop formal policies and procedures for assessing vendor performance assessments, including training for ST staff involved in contract and vendor performance management.
2. Enhance contract language to set clear expectations for both ST staff and consultants/contractors.
3. Leverage the upcoming Procurement Automation Tool to monitor vendor performance. Explore features that allow users to perform vendor assessments and perform periodic reviews on high-risk vendors.
4. Improve procurement evaluation forms and instructions to ensure they reference relevant performance assessments for easy audit tracking.

8b. Reference:
• 48 CFR 42.1502 Contractor Performance Information
• RCW 39.04.350 Bidder Responsibility Criteria
• PCAM Section S Responsibility Contractor, pg. 37</td></tr>
<tr><td>9. Risk Rating
4C</td><td colspan="2">10. Assigned Responsible Dept/Division:
PCA – D&C</td><td>11. Response Due Date:
October 24, 2024</td></tr>
<tr><th colspan="4">Blocks 12 thru 16 will be completed by the individual responding to the Finding/Observation</th></tr>
</table>

12. Management Agreement: Management agrees with audit issue raised.

13. Action Plan:

Develop formal policies and procedures

Design & Construction Contracts has provided comprehensive vendor performance evaluations, guidance, & trainings on the HUB at Contractor/Consultant Performance Evaluation - HUB. Additionally, past performance is an important evaluation criterion in our negotiated procurements. We value opportunities to improve.

Departments have the responsibility to administer contracts at Sound Transit. Page 1 of the Evaluation Guidelines states, "Owner Departments are responsible for performing evaluations in compliance with this guidance document. Departments shall ensure that the appropriate individual is responsible for completing contract performance reviews in a timely manner, while maintaining oversight and visibility of each review."

These policies and procedures will be updated and improved in collaboration with the DCEO, Capital Delivery. PCA will review its PCAM for any enhancements needed.

Enhance contract language

The following or similar contract language is under review for inclusion in contract documents:

1.0.22 Performance Evaluations

The CONSULTANT's performance shall be reviewed and evaluated periodically during the term of this Agreement using SOUND TRANSIT's Performance Evaluation Guide, a sample of which will be provided in Exhibit. CONSULTANT shall fully cooperate in all such evaluations as part of its fee for Basic Services.

Leverage the upcoming Procurement Automation Tool

PCA is in the process of selecting and implementing a Procurement Automation Tool. In Phase II of implementation, PCA will fully explore implementation of the vendor performance evaluation feature including evaluation forms/surveys. The Project Management Information System (PMIS) currently under consideration by the Capital Delivery Department may also be evaluated for this purpose.

Improve procurement evaluation forms and instructions

D&C, in collaboration with Capital Delivery, is currently reviewing and updating performance evaluation forms and guides.

14. Risk acceptance for disagreement (If management does not disagree, please mark N/A).

N/A

15a. Date Submitted to Audit:	**15b. Targeted Completion Date of correction:**
October 30, 2024	**October 31, 2025**

***For TeamMate Use Only, not to be published in final report*.**

16a. Management Response Form Completed By:

16b. Responsible Executive:

16c. Business Contact (Person responsible for completing Action Plan):

Blocks 17-19 to be completed by Auditors

17. Finding/Observation Implementation Plan Review	**18. Auditor Name / Signature:** **Date:**
☑ Accept ☐ Reject	Travis Ratuita Carbon Digitally signed by Travis Ratuita Carbon Date: 2024.11.05 20:47:36 -08'00'

19. Reasons for Implementation Plan Rejection by Auditors:

Finding #2: IT vendor performance is not well documented, and past performance is not considered in procurement decisions. (Rating: 4C - Medium)

Blocks 1 thru 11 to be completed by Auditors			
1. Audit Type: Performance Audit	**2. Business Unit/Function:** PCA – MTS	**3. Audit Title/Project Code:** Vendor Management Follow-Up Audit (Report #: 2024-21)	**4. Classification:** FINDING
5. Auditor, Email & Phone: Travis Carbon, Sr. Performance Auditor (206) 398-5452 travis.carbon@soundtransit.org		**6. Issued Date:** November 1, 2024	

7. Issue Description: IT vendor performance issues are not well documented, and procurement decisions do not consider past performance.

8a. Recommendation: (For Findings Only)

1. Develop formal policies and procedures for assessing vendor performance assessments, including training for ST staff involved in contract and vendor performance management.
2. Enhance contract language to set clear expectations for both ST staff and consultants/contractors.
3. Leverage the upcoming Procurement Automation Tool to monitor vendor performance. Explore features that allow users to perform vendor assessments and perform periodic reviews on high-risk vendors.
4. Improve procurement evaluation forms and instructions to ensure they reference relevant performance assessments for easy audit tracking.

8b. Reference:

- 48 CFR 42.1502 Contractor Performance Information
- RCW 39.04.350 Bidder Responsibility Criteria
- PCAM Section S Responsibility Contractor, pg. 37
- Contract Management Guidelines

9. Risk Rating	**10. Assigned Responsible Dept/Division:**	**11. Response Due Date:**
4C	PCA – MTS	October 24, 2024

Blocks 12 thru 16 will be completed by the individual responding to the Finding/Observation
12. Management Agreement: Management partially agrees with audit issue raised.
13. Action Plan: **Developing Formal Policies and Procedures:** The current contract management training program effectively addresses the need for vendor performance management. We will review and enhance the existing program with a focus on reinforcing the importance of documenting performance.

Enhancing Contract Language:

Solicitations include language that past performance will be evaluated. When we evaluate the Procurement Automation Tool for use in a vendor performance evaluation program, we will review our contract language for any needed edits.

Leveraging the Procurement Automation Tool:

We agree that the Procurement Automation tool could be a useful tool for vendor management and will evaluate implementing features that will accomplish this recommendation in Phase II of implementation.

Improving Procurement Evaluation Forms:

PCA is in the process of selecting and implementing a Procurement Automation Tool. In Phase II of implementation, MTS will fully explore implementation of the vendor performance evaluation feature including evaluation forms/surveys. MTS will also continue its current model of contract management including proactively working with PM's on vendor performance issues and utilizing past performance criteria in its evaluation criteria based on our own experience or vendor experience identified in reference checks, etc. of similar projects with other agencies.

14. Risk acceptance for disagreement (If management does not disagree, please mark N/A). N/A

15a. Date Submitted to Audit:	**15b. Targeted Completion Date of correction:**
October 30, 2024	**October 31, 2025**

***For TeamMate Use Only, not to be published in final report*.**

16a. Management Response Form Completed By:

16b. Responsible Executive:

16c. Business Contact (Person responsible for completing Action Plan):

Blocks 17-19 to be completed by Auditors

17. Finding/Observation Implementation Plan Review	**18. Auditor Name / Signature: Date:**
☑ Accept ☐ Reject	Travis Ratuita Carbon Digitally signed by Travis Ratuita Carbon Date: 2024.11.05 20:47:10 -08'00'

19. Reasons for Implementation Plan Rejection by Auditors:

Observation: Some IT Contracts did not undergo the Vendor Risk Assessment Process

Blocks 1 thru 11 to be completed by Auditors

1. Audit Type:	**2. Business Unit/Function:**	**3. Audit Title/Project Code:**	**4. Classification:**
Performance Audit	IT/InfoSec	Vendor Management Follow-Up Audit (Report #: 2024-21)	OBSERVATION

5. Auditor, Email & Phone:	**6. Issued Date:**
Travis Carbon, Sr. Performance Auditor (206) 398-5452 travis.carbon@soundtransit.org	November 1, 2024

7. Issue Description: Some IT Contracts did not undergo the Vendor Risk Assessment Process

8a. Recommendation: (For Findings Only)

8b. Reference:

- Vendor Risk Management Standard

9. Risk Rating	**10. Assigned Responsible Dept/Division:**	**11. Response Due Date:**
Choose an item.	IT InfoSec	October 24, 2024

Blocks 12 thru 16 will be completed by the individual responding to the Finding/Observation

12. Management Agreement: Management agrees with audit issue raised.

13. Action Plan: Management agrees with the core issue outlined in the observation, however, we raise concerns with the interpretation of the data used to arrive at the observation, as it inaccurately inflates the magnitude and frequency of occurrence of the observed issue. With that in mind, management agrees to the following remediation steps:

1. Continue on-going effort to conduct tier assessments of all vendors for identification of tier 2 and 3 vendors to include in the Vendor Risk Monitoring Program. **[In progress; target completion date: June 30, 2026]**
2. Continue on-going collaboration with Finance to monitor for procurements that may bypass the SOW tiering process as a result of the E1 delegation of authority settings.
3. Implement a process for PCA to periodically provide reports of new contracts and agreements to InfoSec allowing better identification of procurements that bypassed the SOW Tier Assessment process. **[Not started; target completion date: March 28, 2025 (contingent on PCA)]**

Any contracts determined through the process controls listed above to have bypassed the tier assessment process, will be recorded and included into the monitored vendor inventory, and a report will be provided to PCA so that remediation of any missing contractual clauses required by the agency's current vendor risk management process can be remediated at the earliest available opportunity (typically, contract renewals or renegotiations).

14. Risk acceptance for disagreement (If management does not disagree, please mark N/A).

N/A

15a. Date Submitted to Audit:	**15b. Targeted Completion Date of correction:**
October 24, 2024	**March 28, 2025**

***For TeamMate Use Only, not to be published in final report*.**

16a. Management Response Form Completed By: (Name, Title, Department)

16b. Responsible Executive:

16c. Business Contact (Person responsible for completing Action Plan):

Blocks 17-19 to be completed by Auditors

17. Finding/Observation Implementation Plan Review	**18. Auditor Name / Signature: Date:**
☑ Accept ☐ Reject	Travis Ratuita Carbon Digitally signed by Travis Ratuita Carbon Date: 2024.11.05 20:46:47 -08'00'

19. Reasons for Implementation Plan Rejection by Auditors: