SOUNDTRANSIT

Audit Report

IT Access Management

Report Number: 2021 - 13 | Report Date: December 14, 2021

Executive Summary

Audit Report No.: 2021 – 13 **December 14, 2021**

WE AUDITED the current IT Access Management processes to ensure controls to mitigate access risks are effectively and efficiently mitigated.

Our **AUDIT OBJECTIVES** were to determine whether Sound Transit (ST or Agency) has effective controls in place over IT Access Management to ensure:

- Agency Information is adequately safeguarded and appropriately granted.
- Access is consistently managed and removed in a timely manner.

The audit examined documents, processes and controls in place as of October 15, 2021.

Patrick Johnson

Patrick Johnson
Director, Audit Division

WHAT WE FOUND

Overview:

Sound Transit manages access to systems, applications, datasets and other resources through its Access Management program, overseen by the Information Technology (IT) Information Security (InfoSec) division. Access Management processes are performed collaboratively by resource owners and InfoSec. The guiding criteria is the Sound Transit Access Control Standard (version 3.1).

Consistent with industry best-practice, the Agency's approach to Access Management is a 'need to know' or 'least privilege' and requires appropriate management of risk through active commitment and participation from resource owners.

Observations:

Audit evaluated current processes, applicable standards and compared them to determine how well current outcomes meet the identified standards. Based on potential risk impacts (both likelihood and severity), access management for three crucial systems were evaluated:

- Enterprise Asset Management System (EAMS)
- EnterpriseOne (E1)
- Office 365

Overall, exceptions (deviances from the standards) were found across all three systems related to the granting of access and removal of access.

Conclusion:

While the IT Access Management program has made recent improvements, the audit found that the program overall is still developing and implementing controls to manage risk at the level necessary. We identified **one finding related to the strengthening of program controls**. The audit noted several areas where current controls are not effective in managing risk.

Key Recommendations:

Audit recommends clarifying roles and responsibilities for access management, creating cross-departmental collaboration and commitment to consistent risk management and allocation of resources to adequately mitigate risks to the acceptable level.

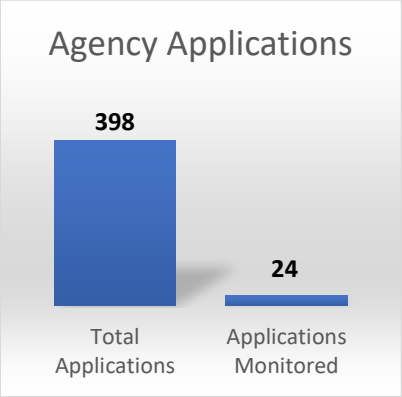
Table of Contents

Background

Sound Transit (ST or Agency) utilizes a variety of applications and platforms to enable staff to carry out work. Applications include systems that manage assets, financial information, communications and more. Together, systems, applications, datasets and other resources for which access is managed make up informational resources or "assets" that are managed by individual asset owners (also known as 'system owners' or 'application owners') with oversight provided by the Information Security (InfoSec) Division of the Information Technology (IT) department. InfoSec has established the Sound Transit Access Control Standard[1] as the minimum criteria for access management in order to facilitate accurate compliance reporting.

As necessary to perform work, staff and contractors are granted access to assets and access is subsequently removed when it is no longer needed (e.g. when work is complete related to the specified resource). This method of access management is often referred to as 'need to know' or 'least privilege' and "helps Sound Transit implement security best practices with regard to logical security, account management, and remote access."

The agency currently owns approximately 400 applications and systems either directly or through contractual agreements ('software as a service'). Some applications are managed through a 'single sign-on' (SSO) platform and access can be granted or revoked for multiple resources at a time. Other applications are 'stand-alone' and access is managed manually by the asset owner. Traditionally, the Agency has managed access in a de-centralized manner with processes differing across resources, depending on the group managing the asset. Currently, some of the highest risk existing programs and all new programs are supported by InfoSec.



InfoSec provides support for the access management function over time in the form of oversight for 24 of these assets through quarterly user access reviews with asset owners. These reviews are performed under the umbrella of an existing InfoSec service, Compliance Support, and aid in compliance reporting. It is InfoSec's intent to continue expanding the coverage of assets determined to be of significant importance, and eventually implement an "Identity and Access Management" service when resources are allocated to do so.

InfoSec has led the collaborative process to update and implement revised processes and standards over the past 1-2 years to better reflect the Agency's current state and ensure risk is appropriately managed. This includes the revision of the Access Control Standard, development of the Operations Technology (OT) Information Security manuals and the addition of automated controls administered through the ServiceNow platform.

[1] Sound Transit Access Control Standard, Version 3.1 was released September 28, 2021 and is the most recent revision.

Audit notes that although InfoSec provides support for the Access Management program, the appropriate management of risk relies on active commitment and participation from asset owners to be successful.

Audit Objectives & Scope

To determine whether Sound Transit (ST or Agency) has effective controls in place over IT Access Management to ensure:

- Agency Information is adequately safeguarded and appropriately granted.
- Access is consistently managed and removed in a timely manner

Audit reviewed policies, processes, procedures and reports as of October 15, 2021. For the purposes of this audit, we determined to observe the controls over Operations Technology (OT) during this audit's follow-up due to the current state of the revised security manual implementation.

Approach & Methodology

Over the course of the audit, we gained an understanding of the Access Management processes at the agency, department and division levels through data analysis, observation, documentation reviews, and personnel interviews.

We identified risks in the processes and assessed management controls in place to mitigate those risks. Based on our assessment of management control effectiveness, we focused on controls over the agency's process related to: (1) safeguarding of information, including appropriate granting of access, and (2) consistent management and timely removal of access.

To determine whether the identified controls are effective, we performed the following procedures:

Objective 1:

1. Reviewed the roles and responsibilities for Service Portfolio Owners, Service Owners and System Owners to determine whether roles and responsibilities for Access Management are clearly defined.
2. Observed physical controls over systems to ensure adequate safeguarding of assets such as systems and hardware.
3. Compared a listing of 6,187 Active Directory (AD)[2] accounts to listings of current users in stand-alone applications to determine whether all users with access to a resource have an associated Active Directory account. Stand-alone applications included:
    a. EnterpriseOne (E1) - 1,019 users
    b. Enterprise Asset Management System (EAMS) – 1,350 users
    c. Office 365 (Administrative Access) – 36 users

[2] Sound Transit utilizes the Microsoft program "Active Directory" to manage access to a suite of programs including email, Teams, MS Office products, etc. Current standards dictate that all system users should have an associated AD account.

4. Performed a walkthrough of the Security Information and Event Management System (SIEM) to determine whether unauthorized access attempts are recorded, in what cases staff are alerted to these events and what action is taken (if any).
5. Reviewed current controls and systematic structure to determine whether Multi-Factor Authentication (MFA) is applied to assets classified as “sensitive” or “restricted”.

Objective 2:

1. Evaluated the current process for attesting to review of currently granted access for designated applications as performed by the application owner on a quarterly basis.
2. Compared a listing of 6,187 Active Directory accounts to listings of current users in stand-alone applications to determine whether users who are ‘disabled’ in Active Directory have had standalone application access removed. Stand-alone applications included:
    a. EnterpriseOne (E1) - 1,019 users
    b. Enterprise Asset Management System (EAMS) – 1,350 users
    c. Office 365 (Administrative Access) – 36 users
3. Walked through the processes for access reviews and attestations to determine whether a formal review process is conducted on a quarterly basis by Information Security (as oversight).

Conclusion

While the IT Access Management program has made recent improvements, the audit found that the program overall is still developing and implementing controls to manage risk at the level necessary. The audit noted several areas where current controls are not effective in managing risk.

Please review **Finding #1** below.

Findings and Recommendations

Finding One: Access Management controls need to be strengthened.

The audit found that the current controls over appropriate granting and timely removal of access are not effective in managing the risk to ensure users have the 'least privileged' access to resources, specifically:

- Not all users were granted access through an Active Directory (AD) account
- User access was not consistently removed for users who had left the agency or no longer needed access to a resource.

Access granted through Active Directory (AD)

Sound Transit's Access Control Standard section 2.3.1 *Access Control Authorization* requires that "Access to Sound Transit resources will be provided through the provision of a unique Active Directory account".

For the population of the systems observed the following exceptions to this requirement were found:

System/Application	No AD Account
EnterpriseOne (E1)	5
Enterprise Asset Management System (EAMS)	20
Office 365 (Administrative Permissions)	0
Total	**25**

Access not removed timely

Sound Transit's Access Control Standard section 2.3 *Implementation* requires that "Authorized users shall be given access only at the appropriate level required to perform their job function, this includes: […] timely removal of access rights (de-provisioning)."

For the population of the systems observed the following exceptions to this requirement were found:

System/Application	Access remaining after user has exited the agency	Significantly different name, spelling or transposition error
EnterpriseOne (E1)	6	10
Enterprise Asset Management System (EAMS)	35	24
Office 365 (Administrative Permissions)	3	3
Total	**44**	**37**

Audit notes that although associated accounts were found, users who have significantly different names (e.g. last name change), spellings and transposition errors between systems present a higher risk that stand-alone application access may not be disabled if a request for access in other applications is made. It was also noted that some of these

differences exist due to system requirements such as Enterprise One which requires an "Address Book Name"[3] versus Active Directory which can use a nickname or preferred name. Currently, the systems do not communicate with each other to associate a user's address book name with any nicknames, preferred names or name changes that may have occurred across all systems.

At the time of this report issuance, some of the above exceptions have been corrected to ensure appropriate access.

Causes & Impact

Through discussion with Information Security the primary causes of these issues include (but are not limited to):

- Clarity of roles and responsibilities for access management.
- Commitment and participation in consistent resource management by resource owners.
- Lack of resources to formally support identity and access management at the required level.

Without clear roles and accountability, it is difficult to allocate access management tasks and designate individuals to grant or remove access for each resource. This leads to cases in which access may be granted or removed by several and/or no individuals at a given time which inhibits effective resource management (e.g. payment for an appropriate number of software licenses) and increases risk of inappropriate access (e.g. a user who has left the agency accesses systems and makes accidental or intentional changes to critical information). Assigning accountability is necessary to ensure that all assets are being managed and are not exposed to unnecessary risk that goes unnoticed.

A lack of commitment and participation in consistent resource management negates the purpose of an access management function. The purpose of the function, "managing risks from end user access", cannot be achieved without dedicated resource owners providing the management of said risks on a consistent basis to ensure the 'least privilege' approach is maintained to protect the Agency's information. Although InfoSec provides oversight, the division is not the appropriate knowledge expert for each system and its users at the level of detail needed to grant and remove permissions at the appropriate level at the appropriate time.

Further, the agency needs to strengthen its risk management culture and allocate the appropriate resources (e.g. systems, budgeted funds, staffing, time, etc.) to mitigate risk at the level necessary to protect the agency. Industry best-practices for access management include using a 'single source of identity' or a single system/resource from which all access is granted to a user, ensuring that when a user enters the agency or leaves the agency, all resources to which they have access can be identified and all aliases (e.g. nicknames, last name changes, etc.) can be captured. These types of access management solutions reduce

[3] The E1 Address Book Name is managed by HR as a source record for the persons legal name. This is only accessible by HR and they have to manually update this if the person requests a legal name change with Sound Transit.

the need for multiple accounts, decrease duplication in tracking efforts and automate portions of the processes for granting and removing of resources. Assuming that a system solution such as this is implemented and covers all agency systems, a staff member dedicated to access control could reasonably monitor the function to ensure compliance and risk mitigation at an appropriate level.

Audit noted that InfoSec had two approved staffing requests for 2020 to develop and implement an identity and access management service offering. One position was intended to be administrative while the other was intended for technical management and implementation of IT's identity and access management solution. These positions were subsequently eliminated due to the financial constraints of the COVID-19 pandemic, effectively preventing InfoSec from implementing the program as outlined in the "Sound Transit Information Security Strategy 2020-2025" document.

Recommendations:

To enhance controls over the IT Access Management Program, we recommend management implement the following:

1. Clarify roles and responsibilities for Access Management and Access Control including (but not limited to) the roles of:
    - Information Security
    - Service Portfolio Owners
    - Service Owners
    - System Owners
    - Staff authorized to grant and remove access

2. In collaboration with Executive Leadership and key stakeholders, determine the Agency's acceptable level of risk associated with the potential likelihood and severity of access management-related risks such as:
    - Compromise, theft, destruction and/or misappropriation of agency information including financial, safety and asset-related information.
    - Overpayment for software licensing, duplicated programs, etc.
    - Adverse effects of potentially missing an abnormal event, unauthorized user accessing the system or other signal that would indicate a compromise of information has occurred.

    Based on the acceptable risk level, allocate the appropriate resources to achieve the desired level of mitigation which may include additional budgeted funds, staffing, software solutions and additional controls.

3. Create or renew cross-departmental collaboration to clarify and fully implement consistent resource access monitoring at the level that achieves the desired level of risk mitigation for the agency.

Management Response:

Prepared by: Jason Weiss
Date: 12/14/21
Audit: 2021 IT Access Management

Management Response:

Management agrees with the audit report results and recommendations.

Action Plan:

Thank you for giving the IT Department the opportunity to participate and respond to the Internal Audit on Access Management. We agree with the results and recommendations from this audit and have activities underway to improve Sound Transit's Identity and Access Management practices (See Remediation Actions below), however, we would like to clarify that Sound Transit IT does not currently operate an "Identity Access Management Program" as stated in the finding, but it conducts Identity and Access Management activities as part of its routine operations.

It should be noted that Information Security had two approved staffing requests for 2020 to develop and implement an identity and access management service offering, which aimed at addressing some of the observations included in the audit finding. One position was intended to be administrative while the other was intended for technical management and implementation of IT's identity and access management solution. These positions were subsequently eliminated due to the financial constraints of the COVID-19 pandemic, effectively preventing InfoSec from implementing the new function and associated controls, as outlined in the "Sound Transit Information Security Strategy 2020-2025" document. Information Security hopes to resurface this effort as part of the response to this audit.

Remediation Actions

1. Working with IT Leadership and Service Owners, InfoSec will facilitate the effort to update and clarify the roles and responsibilities relating to identity and access management within Sound Transit.
2. We seek Executive Leadership and key stakeholders support to collaborate on an effort to present risk scenarios around identity and access management. Based on these conversations, we hope to achieve the following:
    a. A comprehensive understanding of acceptable risk levels associated with identity and access management, as established by Executive Leadership
    b. Develop a strategic plan to address Identity and Access Management holistically to ensure residual risks are within acceptable levels established by Executive Leadership

3. Supported by the strategic plan, we will facilitate a cross-departmental collaboration effort to implement the remediation plan to ensure identity and access management practices across the agency are consistent and incorporate the necessary controls to manage identified risks.

Timeline for corrective action:

We are committed to our remediation efforts laid out above, and have set the following timelines for their implementation:

Action Item	Due Date
Review and Update Roles and Responsibilities related to identity and access management	Q2 2022
Facilitate risk management discussions and the development of strategic remediation plan for identity and access management risk scenarios	Q3 2022
Facilitate cross-departmental collaboration effort to ensure identity and access management practices across the agency are consistent	Q4 2022

Auditing Standards

We conducted this audit in accordance with the International Standards for the Professional Practice of Internal Auditing and Generally Accepted Government Auditing Standards (GAGAS). 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 and reported upon below provides a reasonable basis for our findings and conclusions based on our audit objectives.